Міністерство освіти і науки України

ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ РАДІОЕЛЕКТРОНІКИ

ISMA UNIVERSITY

НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ

ІНСТИТУТ ПРОБЛЕМ РЕЄСТРАЦІЇ ІНФОРМАЦІЇ

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ЛЬВІВСЬКА ПОЛІТЕХНІКА»

ВІЙСЬКОВА АКАДЕМІЯ ЗБРОЙНИХ СИЛ АЗЕРБАЙДЖАНСЬКОЇ РЕСПУБЛІКИ

Третя міжнародна
науково-технічна конференція

«КОМП'ЮТЕРНІ ТА ІНФОРМАЦІЙНІ СИСТЕМИ І ТЕХНОЛОГІЇ»

23 – 24 квітня 2019 року

«COMPUTER AND INFORMATIONAL SYSTEMS AND TECHNOLOGIES»

April 23 – 24, 2019

Харків 2019

Третя міжнародна науково-технічна конференція «Комп’ютерні та інформаційні системи і технології». Збірник наукових праць. Харків: ХНУРЕ. 2019. – 146 с.

Видання підготовлено
кафедрою електронних обчислювальних машин
Харківського національного університету радіоелектроніки (ХНУРЕ)

61166, Україна,
м. Харків, просп. Науки, 14.
тел: +38 (057) 702-13-54
E-mail: info@csitic.com

СПІВГОЛОВИ ПРОГРАМНОГО КОМІТЕТУ

ДОДОНОВ Олександр Георгійович	д.т.н., проф., Інститут проблем реєстрації інформації НАН України, *(м. Київ, Україна)*
ФЕДАСЮК Дмитро Сергійович	д.т.н., проф., Національний університет "Львівська політехніка" *(м. Львів, Україна)*
КОРЧЕНКО Олександр Григорович	д.т.н., проф., Національний авіаційний університет *(м. Київ, Україна)*
МАШТАЛІР Володимир Петрович	д.т.н., проф., Харківський національний університет радіоелектроніки *(м. Харків, Україна)*
РУБАН Ігор Вікторович	д.т.н., проф., Харківський національний університет радіоелектроніки *(м. Харків, Україна)*
БАЙРАМОВ Азад Агалар огли	д.ф.-м.н., проф., Військова академія Збройних сил Азербайджанської республіки *(м. Баку, Азербайджан)*
DJAKONS Deniss	Dr.oec, Associate professor, Rector, ISMA University (Riga, Latvia)
KARPINSKI Mikolaj	Dr.Sc., Professor, Chairman of Department of Computer Science and Automatics, University of Bielsko-Biala *(Bielsko-Biala, Poland)*
LEVASHENKO Vitaliy	prof. Ing., PhD, University of Zilina *(Zilina, Slovakia)*

ЧЛЕНИ ПРОГРАМНОГО КОМІТЕТУ

АХМЕТОВ Бахиджан Сражатдінович	д.т.н., проф., Інститут інформаційних та телекомунікаційних технологій Казахського національного технічного університету ім. К.І. Сатпаєва *(м. Алмати, Казахстан)*
БАРАБАШ Олег Володимирович	д.т.н., проф., Державний університет телекоммунікацій *(м. Київ, Україна)*
ГАШИМОВ Ельшан Гіяс огли	к.т.н., Військова академія Збройних сил Азербайджанської республіки *(м. Баку, Азербайджан)*
КОЧУРКО Павло Анатолійович	к.т.н., доц., Брестський державний технічний університет *(м. Брест, Білорусь)*
КОСЕНКО Віктор Васильович	д.т.н., доц., ДП «Харківський науково-дослідний інститут технології машинобудування» *(м. Харків, Україна)*
КУЧУК Георгій Анатолійович	д.т.н., проф., Національний технічний університет «Харківський політехнічний інститут» *(м. Харків, Україна)*
ЛЕВЧУК Віктор Дмитрович	к.т.н., доц., Гомельський державний університет імені Франциска Скорини *(м. Гомель, Білорусь)*
ЛЕВИКІН Віктор Макарович	д.т.н., проф., Харківський національний університет радіоелектроніки *(м. Харків, Україна)*
ЛЕМЕШКО Олександр Віталійович	д.т.н., проф., Харківський національний університет радіоелектроніки *(м. Харків, Україна)*
МАШТАЛІР Сергій Володимирович	д.т.н., проф., Харківський національний університет радіоелектроніки *(м. Харків, Україна)*
МІХАЛЬ Олег Пилипович	д.т.н., доц., Харківський національний університет радіоелектроніки *(м. Харків, Україна)*
ПРИХОДЬКО Сергій Іванович	д.т.н., проф., Український державний університет залізничного транспорту *(м. Харків, Україна)*
СЕМЕНОВ Сергій Геннадійович	д.т.н., проф., Національний технічний університет «Харківський політехнічний інститут» *(м. Харків, Україна)*
СМЕЛЯКОВ Кирило Сергійович	д.т.н., проф., Харківський національний університет радіоелектроніки *(м. Харків, Україна)*
ФЕДОРОВИЧ Олег Євгенович	д.т.н., проф., Національний аерокосмічний університет ім. М.Є. Жуковського «Харківський авіаційний інститут» *(м. Харків, Україна)*
ФІЛАТОВ Валентин Олександрович	д.т.н., проф., Харківський національний університет радіоелектроніки *(м. Харків, Україна)*
ХАРЧЕНКО В'ячеслав Сергійович	д.т.н., проф., Національний аерокосмічний університет ім. М.Є. Жуковського «Харківський авіаційний інститут» *(м. Харків, Україна)*

ЧУМАЧЕНКО Ігор Володимирович	д.т.н., проф., Харківський національний університет міського господарства імені О. М. Бекетова *(м. Харків, Україна)*
ЦИМБАЛ Олександр Михайлович	д.т.н., проф., Харківський національний університет радіоелектроніки *(м. Харків, Україна)*
ШМАТКОВ Сергій Іванович	д.т.н., проф., Харківський національний університет імені В.Н. Каразіна *(м. Харків, Україна)*
GOPEJENKO Viktors	Dr.sc.ing., Professor, Vice Rector for Research, ISMA University *(Riga, Latvia)*
ZAITSEVA Elena	*prof. Ing., PhD, University of Zilina* *(Zilina, Slovakia)*

ГОЛОВА ОРГАНІЗАЦІЙНОГО КОМІТЕТУ

КОВАЛЕНКО Андрій Анатолійович	д.т.н, доц., Харківський національний університет радіоелектроніки *(м. Харків, Україна)*

ЧЛЕНИ ОРГАНІЗАЦІЙНОГО КОМІТЕТУ

ЄРЕМЕНКО Олександра Сергіївна	д.т.н, доц., Харківський національний університет радіоелектроніки *(м. Харків, Україна)*
ЄРЬОМІНА Наталія Сергіївна	к.т.н, Харківський національний університет радіоелектроніки *(м. Харків, Україна)*
КУДРЯВЦЕВА Марина Сергіївна	к.т.н, доц., Харківський національний університет радіоелектроніки *(м. Харків, Україна)*
ЛЯШЕНКО Олексій Сергійович	к.т.н, Харківський національний університет радіоелектроніки *(м. Харків, Україна)*
МОВСЕСЯН Яна Самвелівна	к.т.н, Харківський національний університет радіоелектроніки *(м. Харків, Україна)*
МАРТОВИЦЬКИЙ Віталій Олександрович	Харківський національний університет радіоелектроніки *(м. Харків, Україна)*
РОСІНСЬКИЙ Дмитро Миколайович	Харківський національний університет радіоелектроніки *(м. Харків, Україна)*
ТКАЧОВ Віталій Миколайович	к.т.н, Харківський національний університет радіоелектроніки *(м. Харків, Україна)*
ФЕДЮШИН Олександр Іванович	к.т.н, доц., Харківський національний університет радіоелектроніки *(м. Харків, Україна)*

РОЗРОБКА І ФУНКЦІОНУВАННЯ КОМП'ЮТЕРНИХ ТА ІНТЕЛЕКТУАЛЬНИХ ІНФОРМАЦІЙНИХ СИСТЕМ

Розподілена інтелектуальна обробка великих даних у комп'ютерних системах призначення

Аксак Наталія Георгіївна[1]
[1]Харківський національний університет радіоелектроніки, пр. Науки 14, м. Харків, UA-61166, Україна, nataliia.axak@nure.ua

Росінський Дмитро Миколайович[2]
[2] Харківський національний університет радіоелектроніки, пр. Науки 14, м. Харків, UA-61166, Україна, dmytro.rosinskyi@nure.ua

Лебедєв Валентин Олегович[3]
[3] Харківський національний університет радіоелектроніки, пр. Науки 14, м. Харків, UA-61166, Україна, lebedevvalen@gmail.com

Кіян Світлана Олександрівна[4]
[4] Харківський національний університет радіоелектроніки, пр. Науки 14, м. Харків, UA-61166, Україна, svetulyakiyan@gmail.com

Анотація. *Показано напрямок розвитку сервіс-орієнтованих комп'ютерних систем. Надано формалізацію процесу розподіленої інтелектуальної обробки великих даних у комп'ютерних системах спеціального призначення.*

Ключові слова: *сервіс-орієнтована система; обробка великих даних.*

I. Вступ

На сьогодні сервіс-орієнтована технологія (Service Oriented Apllication, SOA) активно розвивається і тим самим дозволяє розширити самі можливості IT сфери. Свідченням тому є оцінки аналітичних компаній і зусилля крупних постачальників програмного забезпечення щодо просування цього підходу. Швидкий розвиток вбудованих інтелектуальних пристроїв і комп'ютерних мереж породив багато різноманітних мережевих додатків і послуг, таких як, Інтернет речей IoT (Internet of Things), Інтернет транспортних засобів IoV (Internet of Vehicles), всеохопний Інтернет IoE (Internet of Everything), розумну планету, розумне місто, розумну мережу та мережу послуг. Зросла популярність доповненої реальності AR (Augmented reality), транспортних засобів безпілотних літальних апаратів UAVs (Unmanned aerial vehicle) та інших нових мережевих додатків та послуг.

У [1] запропонована концепція планування у сервісно-орієнтованих архітектурах (SOA) та агентських середовищах за допомогою їх об`єднання, що сприяє розробці автономних та розподілених об'єктів, які спроможні стандартно підключатися до широкого спектру доступних функціональних можливостей реального світу (або послуг). Наведені проблеми використання агентських технологій під час вирішення задач реального світу в теорії (комунікаційні витрати, виразність мов описання, подання знань, вирівнювання онтології) і на практиці (засоби розробки, наприклад, для налагодження, моніторингу виконання, планування в безперервних просторах параметрів, евристики для управління переходом від домена до планування загального призначення).

Сервіс визначається як семантично описана дія агента, а також як базовий будівельний блок конструкцій, що називається «планом». Сучасним аналітичним методам, що базуються на великих даних, присвячено достатньо багато робіт. Найбільше цитування визначення великих даних включає п'ять характеристик: об'єм, різноманітність, швидкість, достовірність и цінність. Проблеми обробки великих даних, що пов'язані з їх різноманіттям, з труднощами збору, зберігання, управління та аналізу, об'ємом пам'яті та швидкістю обчислень приведені в [2,3], описані методики та алгоритми, що використовуються для управління великими наборами даних

Нейронні мережі стали багато дисциплінарним науковим контекстом. Практичні додатки, що використовують нейромережеве програмне забезпечення, забезпечують найкращий результат в багатьох прикладних областях.

У зв'язку зі стрімким накопиченням інформації про системи або процесах і методів її аналізу, все більш актуальним стає питання про пошук закономірностей, укладених у великій кількості параметрів даних. Для аналізу багатовимірних даних шляхом наочного уявлення їх структури або результатів дослідження, необхідно вирішити задачу візуалізації багатовимірних даних [4].

Таким чином, проведений аналіз показав, що існує множина проблем, які пов'язані з неможливістю обробки великих обсягів даних традиційними методами, з організацією розподілених та паралельних обчислень у сервіс-орієнтованих середовищах. Принциповою проблемою є інтеграція вже існуючих і розроблених програмних модулів в єдиний комплекс. Результатом інтеграції повинно бути не тільки забезпечення функціональних характеристик (рішення задачі), а й досягнення максимальної продуктивності. Це обумовлює актуальність питання - як задовольнити всі вимоги, що пов'язані з швидким зростанням нових мережевих додатків і послуг, використовуючи централізовану парадигму обчислень.

II. Вирішення проблеми

Вхідними даними є $H_D(i)$ - зображення досліджуваного об'єкту, в якого значення яскравості в крапці з координатами (k, j) визначені як $h_{k,j} = \overline{0, 255}$ ($h_{kj} = \overline{0, 255}$, $k = \overline{1, m}$, $j = \overline{1, n}$,), показники датчиків, вимірювальних та мобільних пристроїв і т.і.;

$H_P(i)$ - інформація про користувача веб-сервісів $U(i)$ ($i=\overline{1,M}$), які подаються у матричному вигляді $H(i)=\{H_D(i),H_P(i)\}$, $(i=\overline{1,M})$.

Розподілена інтелектуальна обробка великих даних у спеціалізованих комп'ютерних системах являє собою процес надання спеціалізованих послуг $Service(\ell)$, який передбачає наявність постійної підтримки експертів у даній проблемній області та консультативний супровід їхніх дій у діагностично складних випадках (рис.1).

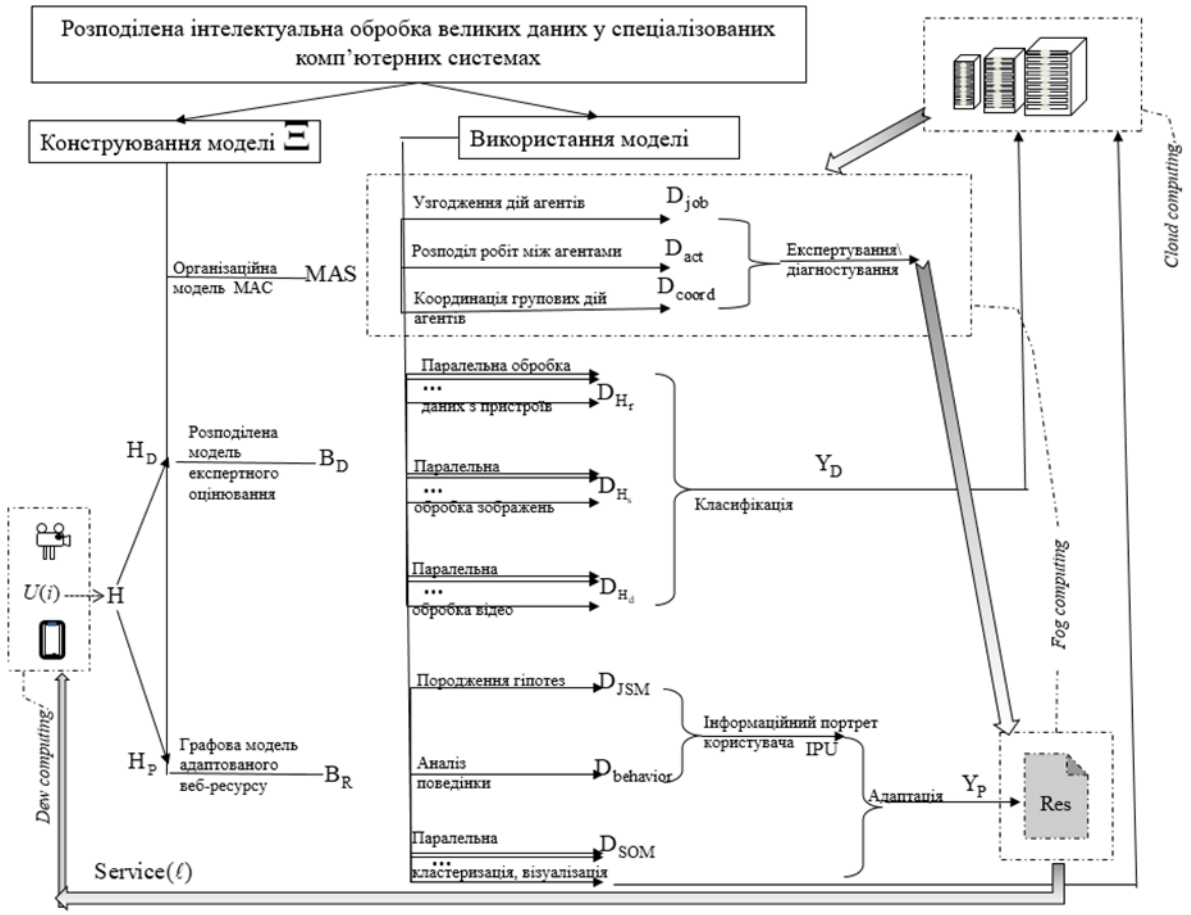


Рисунок 1. Процес розподіленої інтелектуальної обробки великих даних у спеціалізованих комп'ютерних системах

У загальному вигляді шуканий процес може бути представлений як розробка:

– загальної моделі інформаційного супроводу процесу надання спеціалізованих послуг Ξ, її складових компонентів та їх взаємодії;

– методологічної основи побудови та функціонування спеціалізованої комп'ютерної системи, яка забезпечує кожному користувачу $U(i)$ ефективний доступ до адаптованого під $R(n)$ -у категорію користувачів сервіс-орієнтованого середовища Res для надання спеціалізованих послуг $Service(\ell)$ та дозволяє оперативно реагувати на критичне змінення стану досліджуваного об'єкту.

III. Висновки

В роботі запропоновано єдиний підхід, який забезпечує ефективний доступ до сервіс-орієнтованого середовища, передбачає постійну підтримку експертів і консультативний супровід у складних випадках, та дозволяє оперативно реагувати на критичне змінення стану досліджуваного об'єкту

Перелік Літератури

[1] Lützenberger M. et al. Multi-Agent System in Practice: When Research Meets Reality //Proceedings of the 2016 International Conference on Autonomous Agents & Multiagent Systems. – International Foundation for Autonomous Agents and Multiagent Systems, 2016. – С. 796-805.

[2] Zerhari B. 'Big data clustering: Algorithms and challenge'/ B. Zerhari, A. A. Lahcen, S. Mouline //Proc. of Int. Conf. on Big Data, Cloud and Applications (BDCA'15). – 2015.

[3] Kurasova O. Strategies for big data clustering/ O. Kurasova et al. //2014 IEEE 26th International Conference on Tools with Artificial Intelligence. – IEEE, 2014. – С. 740-747. DOI: 10.1109/ICTAI.2014.115.

[4] Shklovets A. V. Visualization of High Dimensional Data Using Two Dimensional Self Organizing Piecewise Smooth Kohonen Maps/ A. V. Shklovets and N. G. Axak// ISSN 1060 992X, Optical Memory and Neural Networks (Information Optics), 2012, Vol. 21, No. 4, pp. 227–232. © Allerton Press, Inc., 2012.

Оптимальное проектирование размещения микроблоков на печатной плате

Косолап Анатолий Иванович[1],

[1]Украинский государственный химико-технологический университет, 8 проспект Гагарина, Днепр, 49005, Ukraine, anivkos@ua.fm

Аннотация. *Задача оптимального размещения микроэлементов на печатных платах давно привлекает исследователей, проектировщиков и производителей печатных схем. Разработаны многие пакеты программ для проектирования печатных схем, однако эти программы не позволяют находить оптимальные решения. Вычислительная сложность этой задачи значительна, поэтому поиск эффективных методов ее решения продолжается. В данной работе предложена новая математическая модель этой задачи и используется эффективный метод, позволяющий находить ее численное решение.*

Ключевые слова: *печатная схема, оптимизационная модель, глобальная оптимизация, метод EQR, численное решение задачи.*

I. Введение и постановка задачи

Имеется прямоугольная пластина со сторонами a и b, на которой необходимо расположить заданное число микроэлементов. Часть микроэлементов соединены между собой проводниками. Чем короче суммарная длина проводников, тем выше быстродействие данной печатной схемы. Эта длина зависит от расположения микроэлементов на пластине. При построении математической модели этой задачи основная сложность заключается в условиях непересечения микроэлементов. Обычно микроэлементы являются прямоугольниками, которые, как правило, располагаются по горизонтали или вертикали пластины. Условия непересечения легко выписать для кругов. Так, два круга не пересекаются, если расстояние между их центрами не меньше суммы их радиусов. Это равносильно неравенству

$$(x_i - x_j)^2 + (y_i - y_j)^2 \geq (r_i + r_j)^2, \qquad (1)$$

где (x_i, y_i) – центр i-го круга, а r_i – его радиус. Тогда каждый прямоугольный микроэлемент представим заданной последовательностью вписанных кругов.

Например, пусть микроэлемент представлен 8 кругами (по 4 круга в каждом ряду), тогда необходимо учитывать, что центры верхнего ряда кругов расположены на одной прямой

$$x_1 + x_3 = 2x_2, y_1 + y_3 = 2y_2,$$
$$x_2 + x_4 = 2x_3, y_2 + y_4 = 2y_3. \qquad (2)$$

Аналогичные равенства выписываем для нижнего ряда. Расстояние между первым и вторым рядом кругов равно сумме двух радиусов

$$(x_1 - x_5)^2 + (y_1 - y_5)^2 = 4r^2, (x_4 - x_8)^2 + (y_4 - y_8)^2 = 4r^2. \qquad (3)$$

Для других кругов должны выполняться условия (1).

Теперь необходимо вычислить суммарную длину соединений между микроэлементами. Эти соединения можно представить графом $G(N, V)$, где N – множество его вершин (микроэлементов), а V – множество дуг (соединений). Тогда целевой функцией данной задачи будет следующая

$$\min\{\sum_{i,j \in V}[(x_i - x_j)^2 + (y_i - y_j)^2]\}. \qquad (4)$$

Мы получили квадратичную задачу оптимизации (1)-(5) с квадратичными и линейными ограничениями. В этой задаче искомыми являются координаты центров кругов. Целевая функция (4) задачи выпуклая. Сложность задачи связана с ограничениями (1), которые порождают ее многоэкстремальность. Для ее решения будем использовать метод точной квадратичной регуляризации [1]. Используем квадратичную регуляризацию для преобразования задачи (1)-(4) к виду

$$\max\{\| z \|^2 | \sum_{i,j \in V}[(x_i - x_j)^2 + (y_i - y_j)^2] + (r-1)\| z \|^2 \leq d,$$
$$(r_i + r_j)^2 - (x_i - x_j)^2 + (y_i - y_j)^2 + r \| z \|^2 \leq d, \forall i \neq j,$$
$$r_i \leq x_i \leq a - r_i, r_i \leq y_i \leq b - r_i, (x_i, y_i) \in S, i = 1,...,n\}, \qquad (5)$$

где множество S определяет условия принадлежности кругов микроэлементам, которые аппроксимируются последовательностью кругов. Параметр $r > 0$ выбираем таким, чтобы допустимое множество задачи (5) было выпуклым. Для данной задачи достаточно взять $r \geq 4$. В задаче (5) необходимо найти минимальное значение d^*, при котором решение задачи z^* удовлетворяет условию $r\|z^*\|^2 = d^*$. Задачу (5) при фиксированном значении d решаем прямо-двойственным методом внутренней точки [2], а значение d^* находим методом дихотомии.

Для численного решения задачи (5) использовалась программа OpenSolver, а значение d^* выбиралось интерактивно. Численные эксперименты подтверждают эффективность рассмотренного метода решения задач оптимального размещения микроэлементов на печатных схемах.

II. Заключение

Проведенные численные эксперименты по оптимальному проектированию расположения микроэлементов на печатных схемах показали, что предложенная технология может быть рекомендована для использования в промышленности, после разработки соответствующего программного обеспечения.

Литература

[1] А. И. Косолап, Глобальная оптимизация. Метод точной квадратичной регуляризации. Днепропетровск: ПГАСА, 2015.
[2] J. Nocedal and S.J. Wright, Numerical optimization: Springer, 200

Integration Version Control System into the teaching workflow

Nosyk Andrii Mihajlovych[1],
Nosyk Kateryna Andriivna[2]

[1]*National Technical University "Kharkiv Polytechnic Institut", 22 Kyrpychova str, Kharkiv UA-61002, Ukraine, nampbch@i.ua*
[2]*Kharkiv National University of Radio Electronics, 14 Nauky Ave, Kharkiv UA-61166, kateryna.nosyk@nure.ua*

Abstract*. In the article discussed most popular Version Control Systems, their differences, advantages and disadvantages. Shown ability and improvements that integration of the version control system bring into the teaching workflow. Choosen version control system and tools that best match specified requirements.*

Keywords: *Version Control System, Git, Subversion, teaching workflow, software development.*

I. Introduction and Problem statement

Problem solving during the educational process should be carried out by the same methods and means, as in the production process of the professional sphere. It means people should use professional development tools and teamwork.

One of the key tools for developing modern software is the Version Control System. The Version Control System (VCS or Revision Control System) is a software for facilitating work with changeable information. The VCS allows to save several versions of the same document, and if necessary, to return to earlier versions, to determine who and when did a particular change, and much more [1].

II. Problem solution and Results

The study and use of version control tools organically fit into the disciplines, the subject of which is the study of programming languages or of software development.

The most common version control systems are Git, Subversion (SVN), Microsoft Team Foundation Server (TFS) [2-4]. Git represents a distributed system, whereas SVN and TFS represent a centralized one. [5].

The principle of centralized system's operation is considered on the example of SVN. SVN users check out files and commit changes back to the server. SVN Data Flow shown on the Figure 1. [6].

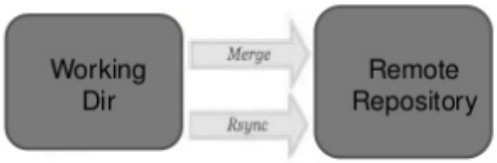


Figure. 1. SVN Data Flow

Git changes happen locally. The advantage is that the developer doesn't have to be connected all the time. Once all the files are downloaded to the developer's workstation, local operations are faster. Git Data Flow shown on the Figure 2 [6].

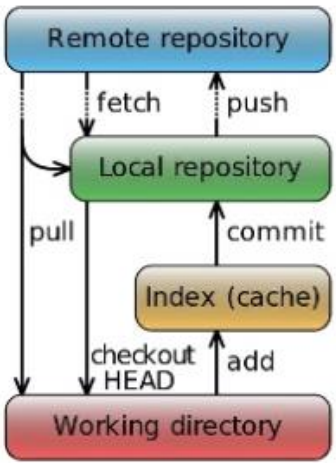


Figure. 2. Git Data Flow

This factor and a number of others make it more expedient to use Git in the learning process compared to other version control systems.

III. Conclusions

Git allows you to simplify the work of the teacher and students. Besides, it can keep track of the history of changes in the program code of laboratory and course works. Git determines the contribution of each student to the development of the code, obtains statistics on the regularity of the implementation of course and laboratory work by a particular student, if you create an account for each students' group.

Using the version control system in the learning process allows students to develop the following skills and abilities:

- reading and understanding of someone else's program code;
- expansion of knowledge of design patterns and idioms of languages in the source code;
- self-control and self-discipline;
- teamwork.

On the other hand, using of the version control system in the learning process allows students to work more transparently, reduce the risk of losing the results of the performed work. It helps to evaluate the student more equitably for his work.

There are two possible options for server location: in a local network of educational institutions or on a hosting software server. The server deployment in a local network requires additional technical, organizational and financial resources, and the use of a cloud server is limited only by the packages of provided services. The most popular services are code.google.com, bitbucket.org, sourceforge.net and github.com. All of these services focused exclusively on the professional use of small groups of developers to enterprise

solutions. But still they allow to be used to some extent in the organization of the educational process. Github.com provides a set of utilities for teachers and students named GitHub Education [7]. GitHub Education helps students, teachers, and schools access the tools and events they need to shape the next generation of software development.

With GitHub Classroom [8] you can set up the industry-standard workflow and free up your time to focus on teaching. Classroom will automatically create student repositories, track assignments in your dashboard and integrate with third-party tools like automated testing.

Using of the version control system involves performing of the organizational tasks' set for the teacher to get the effect of using of this system in the learning process. In addition to training projects, the Version Control System can be used in the development of teaching aids, in the performance of scientific work, in personal projects of students and teachers. It is easy to determine the extent of the contribution of each project participant. It should be noted that this approach can be applied not only in technical but also in humanitarian disciplines.

The most valuable aspect of this approach is that the skill of working with the version control system develops because of practical activity. An obligatory condition for employment of an IT specialist is the knowledge and practical skills of working with one of the control system versions.

REFERENCES

[1] https://uk.wikipedia.org/wiki/http://git-scm.com/Система_керування_версіями

[2] https://git-scm.com/

[3] http://subversion.apache, org/packages. html

[4] http://www.microsoft.com/visualstudio/eng/products /team-foundation-service

[5] http://www.ibm.com/developerworks/ru/library/l-vercon/index. html?S_TA CT=105A GX99&SJZMP-GROl

[6] https://slideshare.net/VinothKumarKannan/svn-vs-mercurial-vs-github

[7] https://education.github.com

[8] https://classroom.github.com

Розробка системи реагування на запити громадян

Яцюк Сергій Вікторович[1],

[1]*Херсонський національний технічний університет, 24 Бериславське шосе, Херсон 73008, Україна, sergey.shambal@gmail.com*

Кірюшатова Тетяна Григорівна[2],

[2]*Херсонський національний технічний університет, 24 Бериславське шосе, Херсон 73008, Україна, tanyakir1963@gmail.com*

Анотація. *Проведено аналіз стану використання інформаційних технологій у процесах діяльності державних органів. Розглянуто питання актуальності створення системи реагування на запити громадян. Визначені вимоги, яким повинна відповідати розроблювана система. Описані загальний принцип роботи системи і структура бази даних. Досліджено питання вибору програмно-технічних засобів для розробки описуваної системи.*

Ключові слова: *державне управління; система реагування на запити громадян; навантаження системи; база даних; ідентифікація користувача.*

I. Вступ і постановка задачі

В останні десятиліття інформаційні технології набули стрімкого розвитку. У провідних країнах вони поступово інтегруються в процеси діяльності держави. Особливо цікавий приклад подає Естонія [1]. В Україні цей процес сильно гальмується; більшість функцій держава вирішує тими ж засобами, що були доступні ще в УРСР, а громадяни мають лише декілька цифрових сервісів для взаємодії із державою, таких як ProZorro [2], Єдиний державний портал адміністративних послуг [3] й інші. Сьогодні Україна має потребу у створенні і впровадженні цифрових ресурсів для роботи державних органів [4].

Ціль роботи – визначити вимоги і критерії до системи реагування на запити громадян, розробити алгоритм роботи системи і описати загальний принцип її роботи.

II. Вирішення проблеми і результати

Головне питання – це безпека, тобто доступ до системи. Скористатися системою повинні мати право лише люди, що проживають на території України; необхідно виключили можливість подавати запити під виглядом іншої людини; кожен повинен нести відповідальність за свої дії в системі. Для цього необхідно зв'язати реєстрацію і авторизацію на державному рівні із документом, що ідентифікує користувача, як реальну людину [5].

Зареєстрований користувач має можливість створювати різні запити, які будуть оброблені відповідальними органами, а також можуть бути переглянуті іншими користувачами. Для прискорення обробки, запит може бути прив'язаний до певної області, району чи міста, тим самим уникаючи витрат часу на розглядання інстанціями верхнього рівня і розподілу на нижчі рівні. Для виявлення більш актуальних запитів доцільно втілити підсистему популярності. Також має бути окремий розділ із описом виконуваних або запланованих дій.

Для зберігання даних основної частини програмного продукту база даних повинна містити опис таких сутностей: Users (Користувачі), Cities (Міста), Comments (Коментарі), Districts (Райони), Fields (Сфери діяльності), Proposals (Пропозиції), Regions (Області), Votes (Голосування).

Рисунок 1. Схема модулів системи

Ще одна проблема – швидкість оброблення запитів. Передбачувана аудиторія програмного продукту – декілька десятків мільйонів громадян країни, у процесі створення архітектури програмного продукту і вибору інструментів розробки необхідно в першу чергу надавати перевагу не швидкості і легкості написання коду, а оптимізації під роботу на високих навантаженнях, можливості паралельного виконання коду, підтримки горизонтального масштабування [6].

III. Висновки

Запропонована система реагування на запити громадян дозволить повністю змінити форми і методі взаємодії громадян із державою, значно скоротити час на донесення запиту до державних установ, прискорити реагування на запити. Окрім цього це збільшить рівень структурованості роботи, відкритість і прозорість, значно зменшить рівень бюрократії і шляхів для розповсюдження корупції.

Список літератури

[1] BBC. Could Estonia be the first "digital" country? http://www.bbc.com/future/story/20171019-could-estonia-be-the-first-digital-country

[2] ProZorro. https://prozorro.gov.ua/

[3] Єдиний державний портал адміністративних послуг. https://my.gov.ua/

[4] Глушков, В.М. Основы безбумажной информатики / В.М. Глушков. – М.: Наука, 1982.– 552 с.

[5] Електронний цифровий підпис. https://uk.wikipedia.org/wiki/Електронний_цифровий_підпис

[6] Benchmarking the request time of Laravel, ASP.NET Core and Django. https://medium.com/@jamesjudd_21057/benchmarking-the-request-time-of-laravel-asp-net-core-and-django-7c1c3e9663d

Метод оцінювання тестів у дистанційних системах навчання на основі когнітивних карт

Даниленко Дарина Олексіївна
Харківський Національний Університет Радіоелектроніки, пр. Науки, 14, Харків UA-61166, Україна, daryna.danylenko@nure.ua
Мартовицький Віталій Олександрович
Харківський Національний Університет Радіоелектроніки, пр. Науки, 14, Харків UA-61166, Україна, vitalii.martovytskyi@nure.ua

Анотація. *У доповіді розглянуті найпопулярніші системи навчання, якими користувалося людство впродовж своєї історії. Особлива увага приділяється дистанційним системам навчання, які є на сьогоднішній день найбільш затребуваними, їх перевагам та недолікам, порівнянню існуючих аналогів. Також розглянуті найпоширеніші методи перевірки знань учнів в умовах дистанційного навчання. Проведений аналіз показав, що основною проблемою цих методів є складність об'єктивної оцінки знань студента. Після аналізу можливих рішень пропонується вирішувати це питання за допомогою системи когнітивних карт, яка є більш гнучкою у порівнянні з іншими методами.*

Ключові слова: *система навчання; оперантне обумовлення; система дистанційного навчання; scorm; оцінювання; когнітивні карти.*

I. Вступ

Серед усіх існуючих систем навчання перспективними для подальшого розвитку є дистанційні системи, як вид навчання. Їх перевагами є наявність цілодобово доступу до матеріалів дисципліни, наявність чіткої структури вивчення дисципліни, можливість віддаленого доступу до матеріалів, наявність методів тестування та оцінки знань[1]. Тестування - це засіб, який дозволяє виявити рівень і якість засвоєння учнями матеріалу, допомагає контролювати та організовувати управління навчальним процесом[2]. Серед основних недоліків методу тестування є відсутність об'єктивного оцінювання рівня засвоєння матеріалу.

II. Вирішення проблеми та результати

Найпоширенішим способом вирішення проблеми оцінювання є використання дихотомічної системи оцінки тестових завдань, в якій за кожне завдання можна отримати 0 або 1 бал. Дана система зручна при оцінюванні завдань з вибором однієї правильної відповіді, тобто завдань закритого типу. Однак існує багато інших типів тестових завдань і так як учень може дати неповну або частково правильну відповідь, в запропонованій системі це буде недостатньо точно оцінюватися.

Для ефективного вирішення даної проблеми можна використовувати політомічну систему оцінювання, в якій допускається декілька категорій відповіді на завдання. Наприклад, за повністю вірну відповідь призначається 2 бали, за частково вірну - 1 і за невірну - 0 балів. Недоліком цієї системи є складність обчислення загального результату на основі балів, отриманих за завдання. Крім того, в цьому випадку не враховуються неправильно обрані варіанти відповіді.

Для вирішення даної проблеми пропонують введення безперервної системи оцінювання знань на інтервалі від 0 до 1 і спеціалізовані технології визначення оцінок за виконання кожного з типів тестових завдань[3]. Попередні дослідження в області побудови системи контролю знань показали необхідність поділу завдань на рівні складності, однак якщо сильному студенту трапляються тільки складні завдання, а слабкому - лише легкі, то в результаті оцінювання у обох студентів буде однаковий рівень знань, що не відповідатиме дійсності[4].

Вирішенню всіх цих проблем може допомогти, на мою думку, система когнітивних карт[5]. Це сукупність параметрів процесу навчання і методів їх обробки, що дозволяє в автоматизованому режимі виявляти прогалини знань, відображати динаміку навчання і сприяти виробленню рекомендацій щодо підвищення ефективності роботи користувача з системою в рамках одного програмного сервісу.

III. Висновки

Головною метою сучасних систем навчання є максимізація ефекту навчання. Особливістю навчального тестування[6], є його безпосередній вплив на якість навчання. Ось чому так важливо розвивати апарат оцінювання досягнень. Когнітивні карти – це відносно новий та гнучкий перспективний засіб вирішення даної проблеми. В даний час методологія когнітивного моделювання розвивається в напрямку вдосконалення апарату аналізу та моделювання ситуації.

Список літератури

[1] Раззаков Ш. И., Нарзиев У. З., Рахимов Р. Б. Контроль знаний в системе дистанционного обучения // Молодой ученый. — 2014. — №7. — С. 70-73.

[2] Гаврилова Л. А. Дистанционное образование. Электронные курсы: Учебно-методическое пособие для преподавателей. — Екатеринбург: УГГУ, 2006. — 74 с.

[3] [Belous N., 2004] Belous N., Voytovich I. Lifelong education conception using computer testing // Материалы VIII Международной конференции Украинской ассоциации дистанционного образования "Образование и виртуальность", 2004. – с. 307-313.

[4] Бондаренко, М. Ф., Семенець, В. В., Белоус, Н. В., Борисенко, В., Куцевич, И. В., Белоус, И. А., & Мележик, О. (2009). Технология оценивания тестов в зависимости от типа и уровня сложности тестовых заданий на основе интегрированной модели.

[5] Углев В. А. Потенциал применения когнитивных карт диагностики знаний для задач автоматизированного обучения / В. А. Углев // Нейроинформатика, ее приложения и анализ данных: XVIII Всероссийский семинар. Красноярск, 2010. с. 107–112.

[6] [Аванесов В.С., 1999] Аванесов В.С. Трудность теста и тестовых заданий // "Управление школой" № 40, октябрь, 1999г

Алгоритм идентификации горящего вещества по акустическому излучению реакции горения

Левтеров Александр Антонович

Национальный университет гражданской защиты Украины, ул.Чернышевская, 94, Харьков 61023, Украина, alionterra@gmail.com

Анотация. *Предложен алгоритм идентификации горючего вещества в зоне очага возгорания на основе анализа акустической эмиссии процесса горения по спектру и фрактальной размерности.*

Ключевые слова: *процесс горения, акустическая эмиссия процесса горения, обнаружение реакции горения, фрактальная размерность*

I. Введение и постановка проблемы

Эффективность обеспечения пожарной безопасности зависит от вероятности раннего обнаружения очага возгорания[1]. Вследствие этого, проблема заключается в повышении эффективности и достоверности обнаружения возгорания и идентификации горящего вещества, особенно на объектах со сложной пожарной нагрузкой, требующей разных огнетушащих составов в системах автоматического пожаротушения.

Для решения данной проблемы, в качестве факторов, характеризующих процесс загорания, необходимо использовать не применявшиеся ранее физические явления, сопровождающие процесс загорания.

К таким новым факторам можно отнести эффект акустической эмиссии (АЭ) процесса горения. Для исследования этого фактора необходимо разработать методику и алгоритм идентификации процесса горения материалов по акустическому излучению.

II. Решение проблемы и результаты

Целью данной статьи является развитие научно-технических основ и программных средств для достоверной идентификации АЭ процесса раннего загорания. Суть АЭ при горении заключается в том, что в процессе горения возникает спектр колебаний, связанных с возникновением и разрушением на молекулярном уровне напряжений в кристаллической решетке материала [2]. В жидкостях происходит перемещение масс реагентов и продуктов и образование пузырьков газа, приводящих к колебаниям окружающей среды объекта загорания. Чем больше молекул вещества задействовано в процессе протекания реакции, тем интенсивнее горение и мощнее звуковое излучение. В связи с этим, идентификация и регистрация данного явления, связанна с решением задачи измерений волновых процессов и их последующей обработки.

Эффект АЭ имеет место на всех стадиях горения. При появлении открытого пламени интенсивность звуковых колебаний резко возрастает. Это обусловлено тем, что при горении твердых тел усиливается эффект деструкции и деформации материала. Увеличение интенсивности звуковых колебаний при горении жидкофазных материалов связано с переходом в стадию кипения поверхностного слоя на границе пламени. При этом необходимо отметить, что и само пламя вызывает значительные колебания воздуха за счет неравномерности течения реакции горения [3].

Для оценки идентификационных признаков случайного стохастического процесса сгорания материалов, по результатам экспериментально обнаруженного эффекта излучения спектров АЭ, сформированы временные ряды, характерные для каждого из рассматриваемых материалов, и проведен их спектральный и фрактальный R/S анализ [4]. Подробно об этом описано в статье автора [5].

Поскольку АЧХ в каждый момент времени (временной отсчет – n) представляет собой функцию $A_n(f)$, где A – амплитуда, а f – частота, то путем известных математических преобразований [6] можно найти ее экстремумы и соответствующие им частоты, которые характеризуют спектр АЭ горения вещества. Также акустический сигнал реакции горения имеет фрактальные характеристики, что можно использовать для идентификации вещества по дробной фрактальной размерности [4].

При обработке и записи звукового излучения и мгновенных срезов спектра использовалось программное обеспечение Adobe Audition CC v9.2; обработка, спектральный и фрактальный анализ акустического излучения реакции горения реализован в среде MatLab R2016b.

На рис.1 приведены амплитудно-частотные характеристики акустического излучения реакции горения, полученные от 5-ти опытов горения ацетона, где видно, что они имеют схожий характер по характерным частотам спектра.

Для идентификации горящего вещества разработан алгоритм (см. рис.2), реализующий способ [7], включающий блок: 1 – калибровки по эталонному сигналу для проверки работоспособности системы обнаружения очага возгорания; 2 – записи фонового сигнала. Продолжительность записи зависит от особенностей частотных и амплитудных характеристик фона в помещении или при анализе территорий, где производится детектирование. В блоке 3 –сравнение акустического спектра фона на характерные частоты и амплитуды (число экстремумов) и значения фрактальной размерности [4] для каждого вещества, полученных экспериментально и хранящиеся в базе данных для исключения ложного обнаружения, поскольку в момент записи фона (блок 2) возможно наличие сигнала от источника загорания.

При совпадении или близком значении частот (разница не более 400-600Гц), исследуемого спектра и спектра из базы данных, осуществляется запись (число регистраций сигнала и время (блок 4, 5) зависят от параметров фона) и анализ сигнала на число характерных частот на заданных частотных диапазонах. Если число таких частот 4 и более, процесс акустического излучения идентифицируется как «Горение».

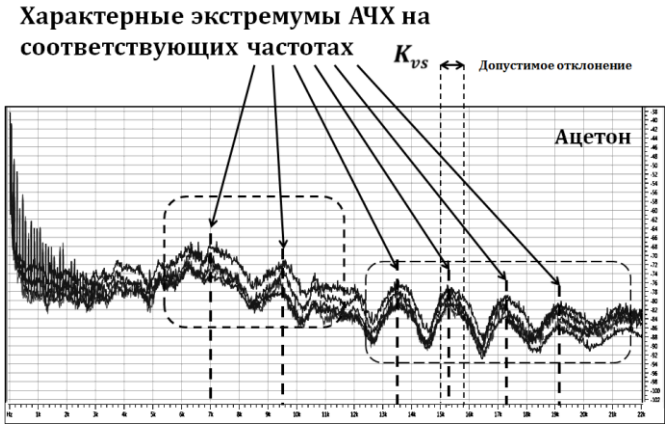


Рисунок 1. Сравнение спектров горения жидкости (n опытов)

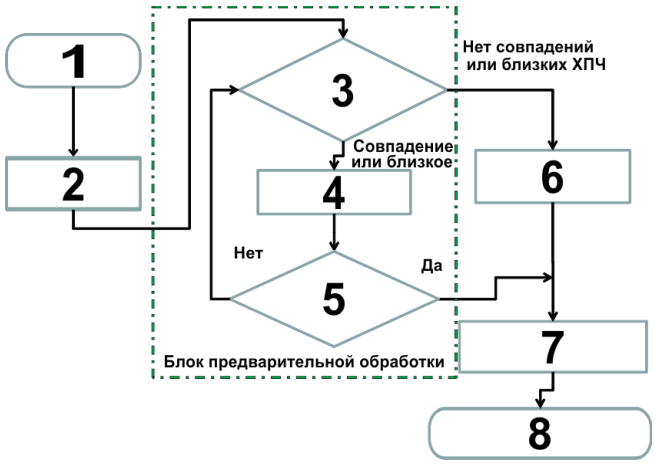


Рисунок 2. Алгоритм обработки спектров акустической эмиссии источника загорания

Таким образом, при детектировании и для исключения попадания в фоновый сигнал сигналов АЭ от источников горения блоки 3,4 и 5 формируют модуль предварительной обработки сигнала. В 6 – при отсутствии в принимаемом сигнале характерных параметров спектра в записанном фоне производится запись фона, как параметра для фильтрации; 7 – обработка полезного сигнала, которая включает: преобразование Фурье, фильтрацию сигнала от фона и посторонних шумов, анализ сигнала с помощью эволюционных алгоритмов и систем искусственного интеллекта, расчет дробной фрактальной размерности акустического излучения реакции горения. В блоке 8 – наличие информации о результатах обработки полезного сигнала в форме команды «обнаружено /не обнаружено» и передача ее на исполнение.

III. ВЫВОДЫ

Явление акустической эмиссии при горении различных веществ, позволяет идентифицировать процесс горения и вещество при помощи анализа спектра и фрактальных свойств акустического излучения реакции горения, что указывает на высокую эффективность возможного обнаружения и установления фактов возгорания.

Предложен алгоритм, позволяющий идентифицировать горящее вещество в условиях сложной пожарной нагрузки, где требуется несколько видов огнетушащих веществ, дает возможность технической реализации системы пожаротушения с несколькими огнетушащими веществами.

Описан алгоритм обработки фоновых сигналов, позволяющий повысить степень достоверности обнаружения АЭ очага загорания.

Результаты проведенных экспериментов подтверждают, что процесс АЭ может быть использован как новый фактор для обнаружения раннего возгорания.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

[1] World Fire Statistics. [Электронный ресурс]. – Режим доступа: http://www.ctif.org/sites/default/files/ctif_report22_world_fire_statistics_2017.pdf.

[2] Фадеев Г.Н. Акустическая резонансная частота химических реакций / Г.Н. Фадеев, В.С. Болдырев, Н.Н. Кузнецов // Инженерный журнал: наука и инновации. – 2013. – Вып. 6. [Электронный ресурс]. – Режим доступа: http://engjournal.ru/catalog/fundamentals/chem/787.html

[3] Беликов В.Т. Использование результатов наблюдений акустической эмиссии для изучения структурных характеристик твердого тела / В.Т. Беликов, Д.Г. Рывкин // Акустический журнал. – 2015. – т. 61. – № 5. – С. 622 – 630.

[4] Федер Е. Фракталы / М.: Мир, 1991. — 258 с.

[5] Левтеров А.А. Методы идентификации процесса горения целлюлозосодержащих материалов на основе эффекта акустической эмиссии. / В.Д. Калугин, В.В. Тютюник // Проблемы пожарной безопасности. – Харків: НУЦЗУ, 2017. Вип. 42. С. 72 – 84

[6] Ильин В.А. Основы математического анализа (в двух частях) / В. А. Ильин, Позняк Э. Г//.— М.: Физматлит, 2005. — 648 с.

[7] Пат. SU 1683782 A1 Україна, МПК A62C 3/00, G 01R 29/26, G08C 19/00, G08B 31/00. Спосіб раннього виявлення осередку займань / Калугін В. Д., Лєвтєров О. А., Тютюник В. В. заявник і патентовласник «Національний університет цивільного захисту України». – № 01387; заяв. 12.02.2018; опубл. 25.07.2018, Бюл. №14, 2018.

Моніторинг придатності продуктів харчування

Міщенко Анастасія Тарасівна[1]

[1]*Національний університет «Львівська політехніка», вул. С.Бандери 12, Львів 79013, Україна, mishenko971110@gmail.com*

Басюк Тарас Михайлович[2]

[2]*Національний університет «Львівська політехніка», вул. С. Бандери 12, Львів 79013, Україна, Taras.M.Basyuk@lpnu.ua*

Анотація: *Дана стаття присвячена дослідженню питань моніторингу придатності продуктів харчування в цифровому домі. Виділено основні причини виникнення даної ситуації, проаналізовано відомі способи її вирішення та показані недоліки в процесі їх застосування. Спроектована модель варіантів використання, яка відображає загальні вимоги до функціональної поведінки проектованої системи. Описано архітектуру інформаційної системи, яку розроблено з використанням модульного принципу, що надає засоби із побудови системи із функціонально-завершених частин.*

Ключові слова: *продукти харчування; моніторинг; якість; модуль; розпізнавання..*

I. Вступ та постановка задачі

На сьогоднішній день, цифрові технології стрімко увійшли у всі галузі життєдіяльності людини: від роботизованих хірургічних втручань до керування віддаленими сателітами. Проте, на фоні такого прогресу залишаються невирішеними множина проблем, однією з яких є проблема сміття, що викликана в першу чергу купівлею як непотрібних так і надлишкових товарів та продуктів харчування [1,2].

II. Вирішення проблем та результати

Проведене дослідження показало, що основними причинами виникнення такої ситуації є: відсутність моніторингу якості продуктів харчування в холодильних камерах та недотримання умов зберігання [3]. Існуючі підходи до вирішення даної проблеми, які пропонуються фірмами-гігантами (Samsung, LG, Bosch) націлені в першу чергу на використання вартісного обладнання моніторингу, яке є недоступним широкому загалу [4-6]. З огляду на те, актуальною задачею є створення системи яка надасть засоби моніторингу як придатності так і наявності продуктів харчування в цифровому домі, що сприятиме обґрунтованості покупок та зменшить кількість зіпсованих продуктів харчування. Діаграма варіантів використання проектованої системи відображена на рис.1.

Архітектура системи складається з таких модулів:

1) Ядро – основний програмний модуль, який координує роботу решти частин системи і безпосередньо застосовується в процесі комунікації з користувачем.

2) База даних – містить вичерпну інформацію щодо продуктів харчування, термінів та умов їх зберігання. Необхідною умовою є наявність відомостей щодо базових термінів придатності, що застосовується для поштучних продуктів та товарів без відповідного маркування.

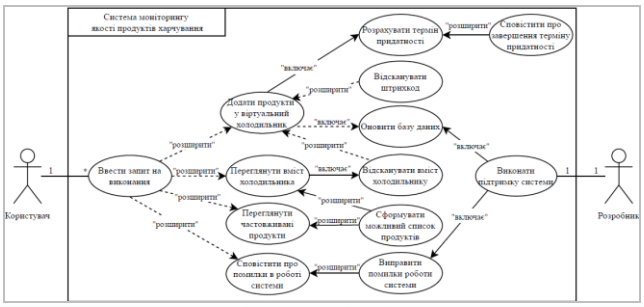


Рисунок 1. Діаграма варіантів використання

3) Модуль розпізнавання продуктів харчування містить нейронну мережу, що використовується для виділення типу продукту харчування.

4) Модуль сканування штрих коду використовується для ідентифікації маркованого товару, що зменшує час опрацювання та сприяє можливості використання простішого апаратного забезпечення.

5) Модуль моніторингу – включає процедури із визначення терміну придатності товару та систему сповіщення про його завершення. Користувач має змогу налаштувати параметри сповіщення в залежності від особистих міркувань.

III. Висновки

У статті проаналізований сучасний стан області дослідження та наведені підходи до вирішення поставлених проблем. Запропонований підхід може використовуватись не лише в індивідуальних цілях, але й для потреб бізнесу, що створить передумови із зменшення кількості харчових відходів. Подальші дослідження будуть спрямовані на реалізацію відповідної інформаційної системи та верифікацію її роботи.

Список літературних джерел

[1] Бурко Р. А., Терёшина Т. В. Экологические проблемы современного общества и их пути решения // Молодой ученый, №11, 2013. – С. 237-238.

[2] Вісім екологічних проблем України [Електронний ресурс]. Режим доступу: https://comments.ua/life/247396-vosem-ekologicheskih-problem.html (дата звернення: 6.03.2019);

[3] А.А. Мельников “Проблемы окружающей среды и стратегия её сохранения”, Академический Проект, 2009. – 724с.

[4] #GADGETSTYLE: лучшее мобильное приложение для холодильника [Електронний ресурс]. Режим доступу: https://www.gadgetstyle.com.ua/best-mobile-apps-for-fridge/ (дата звернення: 9.03.2019);

[5] Е. В. Сысоева, Г. Кутырев “Контроль качества продуктов питания”, Казань: КНИТУ. – 112с.

[6] Обзор программ для учета срока годности продуктов питания [Електронний ресурс]. Режим доступу: https://yablyk.com/obzor-programm-na-iphone-kotorye-pomogut-otsledit-sroki-godnosti-produktov/ (дата звернення: 2.02.2019).

Problem of self-organization of s-bot group movement in unorganized physical environment

Churymov Gennadiy[1]

[1]*Kharkiv National University of Radio Electronics, Nauka ave. 14, Kharkiv, UA-61166, Ukraine, g.churyumov@ieee.org*

Tokariev Volodymyr[2]

[2]*Kharkiv National University of Radio Electronics, Nauka ave. 14, Kharkiv, UA-61166, Ukraine, tokarev@ieee.org*

Tkachov Vitalii[3]

[3]*Kharkiv National University of Radio Electronics, Nauka ave. 14, Kharkiv, UA-61166, Ukraine, tkachov@ieee.org*

Abstract. *The modern development of distributed and robotic systems, hereinafter called «Swarm-bot» systems, rapidly covers applied areas related to work in undetermined and extreme conditions from space and deep-sea research, maintenance of nuclear power plants, recovery from the aftermath of man-made accidents and disasters, fighting against terrorism and use for the benefit of the armed forces, police and other special forces, performing the most complicated medical surgeries, automation of the public utility sector, organization of life and leisure.*

Keywords: *s-bot, reconfiguration, unorganized physical environment, planning, reconfiguration methods, information technology.*

I. Overview of the subject area

Currently, there are four main tasks arising in the management of a group consisting of intelligent mobile objects, hereinafter called «s-bots» with various functional purposes [1-6]:

- choice of a group management strategy;
- global planning;
- local planning;
- processing of information received by the «s-bot» group during their functioning.

Fig. 1 shows a diagram of the tasks interaction in management of the «s-bot» group with various functional purposes [1-6].

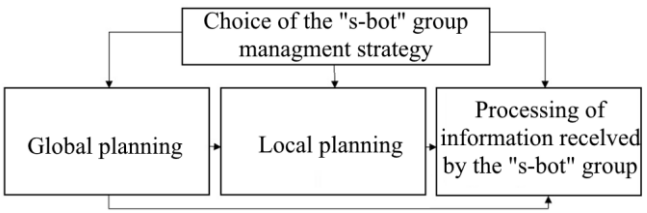


Fig. 1. The diagram of tasks interaction in management of the «s-bot» group with different functional purposes

The strategy of group management means the general principle of organizing management of an «s-bot» group. The strategy determines who and at what level of management solves the tasks of global and local planning, performs the processing of the information received. The group management strategy is selected depending on the number of «s-bot» group members and based on the rate of parameters change in the unorganized physical environment.

Global planning is the decomposition of a complex global task into simpler tasks as well as the distribution of tasks among the «s-bot» group obtained as a result of decomposition. Moreover, this distribution must satisfy some given optimality criterion.

Local planning includes solving a set of problems associated with the implementation of the «s-bot» tasks, which were formed and distributed at the global planning stage, for example, planning the trajectory of the mobile «s-bots» when they move to the specified target points.

In the process of performing tasks, «s-bots» receive useful information that needs to be processed. On the basis of the received data, a new task can be formed for the mobile «s-bot» group.

When building a «Swarm-bot» system, the most important and challenging task is to develop a management system capable of solving global and local planning tasks in accordance with the selected group management strategy and information obtained by the «s-bot» [1-6].

II. Setting a research problem

This paper addresses the problem of local planning. One of the main tasks in solving the problem of local planning is the self-organization of the movement of the «s-bot» group in the unorganized physical environment (PE). The most famous approach to solving this problem is the Reynolds model [13]. The Reynolds model describes the behavior of birds in a flock and includes three principles of self-organization of movement of a separate «s-bot» in the group, hereinafter referred to as a flock, namely [13]:

- adhere to the average speed of movement of neighbors in the flock;
- strive to occupy a position in physical environment (PE) close to the center of the local neighborhood, i.e. stay together;
- keep a safe distance in the flock.

Each «s-bot» in the flock has its own local neighborhood. It has a spheroid form (Fig. 2), the radius of which depends on the V-speed of movement and is determined by the sensory capabilities of the «s-bot». Each «s-bot» of the flock, alien agent or obstacle inside the neighborhood is determined by the distance and the position of the end of the radius vector on the spheroid in the coordinate system associated with «s-bot». An «s-bot» can have restrictions on the maximum number of other «s-bots» of the flock that it can observe in its neighborhood.

Other objects outside of the spheroid local neighborhood do not exist for the «s-bot» at the given time. Movement of the flock involves formation of the trajectory of each «s-bot» movement depending on the movement of the «s-bots» remaining in the flocks and the location of various obstacles within the operating area. There are many algorithms and methods for planning the trajectories of the mobile «s-bot». Among them, the most famous are:

- wave algorithm;
- Dijkstra's algorithm;
- A algorithm;
- fuzzy logic;
- potential method.

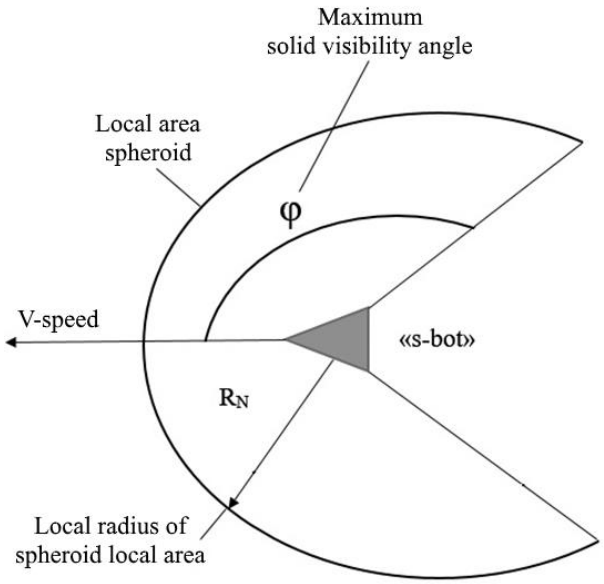


Fig. 2. Local neighborhood of the «s-bot»

Planning the trajectories of the mobile «s-bot» using the wave algorithm, Dijkstra's algorithm, and A algorithm involves structuring the physical environment, building a mobile «s-bot» area map and requires significant power of the «s-bot» on-board computers. The disadvantage of fuzzy methods of planning the trajectories of the mobile «s-bots» is the impossibility of a preliminary mathematical analysis of the expected results. That is, it is impossible to determine in advance how a fuzzy system will behave in a given situation.

The advantage of the potential method is its simplicity. Algorithms based on this method have low computational complexity. A distinctive feature of the potential method lies in the fact that there is no need to structure the operating space and build a mobile «s-bot» area map, which significantly reduces the requirements for on-board equipment.

Thus, the formation of the trajectories of mobile «s-bots» operating in a team is advisable to carry out using the potential method.

III. Conclusions

1. A diagram of the interaction of tasks in management of the «s-bot» group with various functional purposes is presented. Definitions of the following notions are given:

- choice of a group management strategy;
- global planning;
- local planning;
- processing of information received by the «s-bot» group during their functioning.

2. The local neighborhood of a separate «s-bot» is described based on the Reynolds model.

The studies were conducted in the educational and scientific laboratory «Reconfigurable and mobile systems» at the Department of Electronic Computers of Kharkiv National University of Radio Electronics.

References

[1] Ткачов В.М. Проблема передачі даних типу Big Data у мобільній системі «мультикоптер-сенсорна мережа» / В.М. Ткачов, В.В. Токарєв, В.О. Радченко, В.О. Лебедєв // Системи управління, навігації та зв'язку. – 2017. – №2 (42). – С. 154-157.

[2] Радченко В.О. Мобильная подсистема «Мультикоптер-сенсорная сеть» в компьютерной системе хранения Big Data / В.О. Радченко, Д.А. Руденко, В.Н. Ткачев, В.В. Токарев // Системи управління, навігації та зв'язку. – 2017. – №4 (44). – С. 102-105.

[3] Ruban I.V. Provision of Survivability of Reconfigurable Mobile System on Exposure to High-Power Electromagnetic Radiation / I.V. Ruban, G.I. Churyumov, V.V. Tokarev, V.M. Tkachov // Selected Papers of the XVII International Scientific and Practical Conference on Information Technologies and Security (ITS 2017). – CEUR Workshop Processing. – Kyiv, Ukraine, November 30, 2017. – Pp. 105-111.

[4] Churyumov G. Scenario of Interaction of the Mobile Technical Objects in the Process of Transmission of Data Streams in Conditions of Impacting the Powerful Electromagnetic Field / G. Churyumov; V. Tokarev; V. Tkachov; S. Partyka // 2018 IEEE Second International Conference on Data Stream Mining & Processing (DSMP). – 21-25 Aug. 2018. – Pp. 183-186.

[5] Tkachov V. Method of Data Collection in Wireless Sensor Networks Using Flying Ad Hoc Network / V. Tkachov, V. Tokariev, Y. Dukh, V. Volotka // 5th International Scientific-Practical Conference Problems of Infocommunications. Science and Technology, October 9-12, 2018 Kharkiv, Ukraine. – Pp. 197 – 201.

[6] Додонов О.Г. Задачі управління і забезпечення живучості системи мобільних технічних об'єктів / О.Г. Додонов, О.С. Горбачик, М.Г. Кузнєцова // Друга міжнародна науково-практична конференція «Комп'ютерні та інформаційні системи і технології». – Збірка наук. праць. – Харків, ХНУРЕ. –2018. – С.57-59.

Анализ свёрточных и капсульных нейронных сетей

Береснев Дмитрий Владимирович

Белорусский государственный университет информатики и радиоэлектроники, ул. П. Бровки 6, Минск 220039, Беларусь,
beresnev.dima8@gmail.com,

Анотация. *Рассмотрены основные и наиболее популярные модели для распознавания изображений. Приведено описание и дана характеристика сверточных нейронных сетей. Приведено описание и дана характеристика капсульных нейронных сетей. Проведен анализ преимуществ и недостатков каждой из архитектур моделей. Выделены перспективы использования данных моделей.*

Ключевые слова: *анализ данных, обработка больших данных, глубокое обучение, свертка, max-polling, аугментация, сверточные нейронные сети, капсульные нейронные сети, капсулы, динамический роутинг.*

I. Введение и Постановка Проблемы

Сегодня существует широкий круг задач, в которых изображения рассматриваются как источник информации, на основе которой необходимо принять некоторое решение.

Следует дать несколько определений и объяснить основные термины. *Иску́сственная нейро́нная се́ть* (ИНС) — математическая модель, а также её программная и/или аппаратная реализация, построенная по принципу организации и функционирования биологических нейронных сетей — сетей нервных клеток живого организма по модели Маккалока-Питтса. На данный момент отсутствует однозначное разделение ИНС на классические и глубокие НС. *Глубокая нейронная сеть* (ГНС) – это математическая модель, а также её программная и/или аппаратная реализация, построенная по правилам создания ИНС и имеющая в составе своей архитектуры большое количество скрытых слоев. *Глубокое обучение* (*глубинное обучение*; англ. *Deep learning*) — совокупность методов машинного обучения (с учителем, с частичным привлечением учителя, без учителя, с подкреплением), основанных на обучении представлениям (англ. *feature/representation learning*), с помощью алгоритмов машинного обучения, которые пытаются моделировать высокоуровневые абстракции в данных, используя архитектуры, состоящие из *множества нелинейных преобразований* (преобразования, при которых изменяется форма сигнала и происходит обогащение его спектра новыми частотными компонентами). Таким образом, граф, описывающий сложную иерархию высокоуровневых абстракций, будет глубоким – содержащим много уровней. Поэтому такой подход в ИИ называется глубоким обучением.

Основой для решения задач распознавания изображений является теория распознавания образов, которая особенно активно развивается в связи с созданием систем искусственного интеллекта. В рассматриваемом нами случае, носящем с точки зрения теории распознавания образов прикладной характер, является изображение. Задача распознавания образов заключается в классификации изображений на основе определенных требований, причем изображения, относящиеся к одному классу образов, обладают относительно высокой степенью близости.

Принятый подход к распознаванию образов заключается в классификации на множестве признаков, вычисляемых по наблюдаемому изображению. Можно также сказать, что классификация образов заключается в отображении пространства признаков в пространство решений. При таком подходе распознавание образов включает две задачи:

- отбор и упорядочивание признаков;
- собственно классификация.

II. Характеристика Моделей

Сверточные нейронные сети (*convolutional neural network, CNN*) [1] — специализированная архитектура ИНС, предложенная Яном Лекуном в 1988 году и нацеленная на эффективное распознавание образов, входит в состав технологий глубокого обучения. идея свёрточных нейронных сетей заключается в чередовании свёрточных слоёв (*convolution layers*) и субдискретизирующих слоёв (*subsampling layers* или *pooling layers*, слоёв подвыборки). Структура сети — однонаправленная (без обратных связей), многослойная архитектура. Для обучения используются стандартные методы, чаще всего метод обратного распространения ошибки. Функция активации нейронов — передаточная функция, которая выборается исследователем. Архитектура сети [2] получила свое название ввиду наличия операции свёртки, которая каждый фрагмент изображения умножается на матрицу (ядро) свёртки поэлементно, а результат суммируется и записывается в аналогичную позицию выходного изображения. Данный тип архитектуры имеет следующие особенности: операция свертки, регулиризация, специализированная инициализация, батч-нормализация, аугментация, раняя остановка.

Чтобы размер нейронной сети не был большим и не зависел от размера обучаемых данных, следует использовать специальную структуру нейронной сети, называемую свёрточной нейронной сетью. При обучении для каждого образца на вход свёрточной нейронной сети попадает не вся картинка, а только ее часть.

При использовании свёрточной нейронной сети возникает проблема – большое количество выделенных признаков [3]. Использование огромного количества признаков для решения задач распознавания изображений оказалось неэффективно. Для уменьшения размера пространства признаков проводим субдискретизацию (англ. pooling), разделив карту признаков, полученных от

свёрточной нейронной сети, на фиксированное количество частей (см. рис. 1.4) на каждой части вычисляется ее максимальное значение (англ. max pooling) или среднее значение (англ. mean pooling).

Таким образом, следует выделить следующие преимущества сверточной нейронной сети :

- Уменьшение количества обучаемых параметров и повышение скорости обучения по сравнению с полносвязной нейронной сетью.
- Возможность распараллеливания вычислений и реализации алгоритмов обучения сети на графических процессорах (GPU).
- Устойчивость к сдвигу позиции объекта во входных данных. При обучении свёрточная нейронная сеть сдвигается по частям объекта. Поэтому обучаемые признаки не зависят от позиции «важных частей», т.е. свёрточная нейронная сеть выделает одинаковые признаки для двух картинок, хотя позиции на изображениях могут быть разные. Таким образом, это свойство свёрточной нейронной сети помогает повышать качество при решении разнообразных задач распознавания изображений.

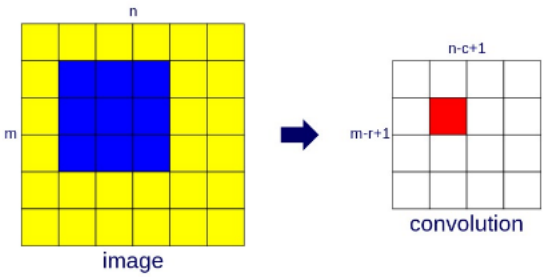


Рисунок 1. Пример свертки

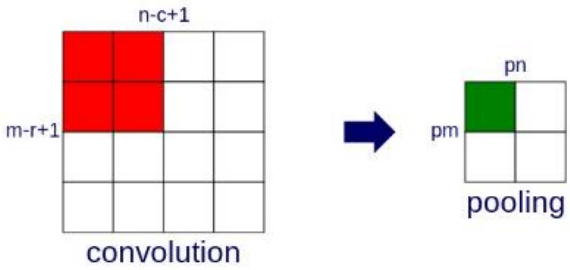


Рисунок 2. Пример пулинга

Свёрточную нейронную сеть можно применять для решения различных типов задач. При использовании свёрточной нейронной сети можно существенно уменьшать количество обучаемых параметров и получать высокое качество распознавания.

Капсульные нейронные сети — новая архитектура нейронных сетей, которая является серьезной доработкой сверточных нейронных сетей [4]. Важная часть CapsNet — традиционный сверточный слой. Цель данного слоя состоит в извлечении из входного изображения самых базовых признаков. Еще одной особенностью капсульных нейросетей является ReLU (формально известный как линейный выпрямитель). Это активационная функция, аргументом которой является значение. Если это значение отрицательно, ReLU зануляется, если положительное — принимает значение аргумента.

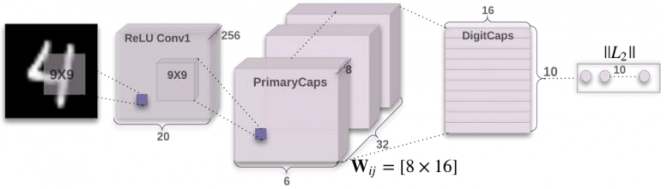


Рисунок 3. Архитектура CapsNet

Слой PrimaryCaps начинается как обычный сверточный слой, но в этот раз проводится свертывание по стеку из 256 выходов из предыдущих сверток. Вместо ядра 9x9 имеем тензор размера 9x9x256. Еще один метод используемый в капсульных нейросетях — направление по соглашению (routing by agreement) [5].

III. Выводы

Таким образом, подводя итог, следует отметить, что технологии машинного обучения и анализа данных, нейронные сети в частности, обладая такими особенностями как: гибкость при построении моделей для нелинейной аппроксимации многомерных функций, реализуемость средств прогнозирования во времени для процессов зависящих от многих переменных, способность решать задачи классификации по многим признакам, способность решать задачи распознавания изображений, реализуемость инструментов для поиска по сложным ассоциациям, возможность реализации моделей для поиска закономерностей и структуры в данных, свобода от некоторых ограничений по сравнению с классическими методами за счет параллельной обработки и особенностей построения интеллектуальных моделей, способность к полной обработке информации, самоорганизованность, способность к кодированию информации, надежность и относительная устойчивость, обучаемость, способность к обобщению, способность к абстрагированию и т.д. В настоящее время неслучайно вызывают повышенный интерес при построении интеллектуальных систем различного масштаба и назначения. Алгоритмы и методы машинного обучения и анализа данных позволяют решить огромнейших пласт интеллектуальных задач, таких как распознавание изображений и видео, распознавание и синтез речи, распознавание и перевод текстов, прогнозирование событий и рядов и т.д. Поэтому интеллектуальное ПО позволяет повысить удобство использования компьютерных систем на новый качественный уровень и делает дисциплину Data Science одним из ключевых направлений в сфере исследований искусственного интеллекта.

Список Источников

[1] Krizhevsky, Alex. "ImageNet Classification with Deep Convolutional Neural Networks". Retrieved 17 November 2013.

[2] Krizhevsky, Alex; Sutskever, Ilya; Hinton, Geoffrey E. (2017-05-24). "ImageNet classification with deep convolutional neural networks". Communications of the ACM. 60 (6): 84–90. doi:10.1145/3065386. ISSN 0001-0782.

[3] LeCun, Yann. "LeNet-5, convolutional neural networks". Retrieved 16 November 2013

[4] S. Sabour, N. Frosst, G. E Hinton, “Dynamic Routing Between Capsules”, arXiv:1710.09829 [cs, cv], Nov. 2017.

[5] S. Sabour, N. Frosst, G. E Hinton, “Capsule Network Performance on Complex Data”, arXiv:1712.03480 [cs, cv], Dec. 2017.

Метод визначення контурів елементів міської інфраструктури на оптико-електронних зображеннях бортових систем

Рубан Ігор Вікторович[1]
Худов Геннадій Володимирович[2]
Маковейчук Олександр Миколайович[1]
Хижняк Ірина Анатоліївна[2]
Соломоненко Юрій Станіславович[2]
Юзова Ірина Юріївна[2]
Худов Ростислав Геннадійович[3]

[1]*Харківський національний університет радіоелектроніки, проспект Науки, 14, Харків, 61166,* Україна, 2345kh_hg@ukr.net
[2]*Харківський національний університет Повітряних Сил ім. Івана Кожедуба, вул. Сумська, 77/79, Харків, 61063,* Україна
[3]*Харківський національний університет ім. В.Н. Каразіна, майдан Свободи, 4, Харків, 61022,* Україна, 2345kh_hg@ukr.net

Анотація. *Запропоновано для виявлення елементів міської інфраструктури на оптико-електронних зображень бортових систем застосовувати двоетапний метод визначення контурів елементів міської забудови. На першому етапі проводиться виділення границь за допомогою детектору границь Канні. На другому етапі – визначення контурів елементів міської інфраструктури за допомогою перетворення Хафа. Візуальна оцінка якості результатів обробки зображення дозволяє визначити об'єкти інтересу.*

Ключові слова: *оптико-електронне зображення, метод визначення контурів, об'єкти інтересу, детектор границь Канні, перетворення Хафа*

I. Вступ та Постановка Проблеми

Відомо [1, 2], що методи отримання інформації про місцевість, об'єкти та процеси з використанням аеро- та космічних засобів значною мірою заповнюють недоліки контактного способу збору інформації, а в деяких випадках повністю його замінюють. Основною метою моніторингу населених пунктів є постійна актуалізація інформації про зміни на земельних ділянках, облік інфраструктури об'єктів, транспортних систем, стан природних й природно-антропогених ландшафтів тощо [1]. Тому актуальним є використання матеріалів аерокосмічного знімання для моніторингу населених пунктів.

Мета роботи: розробка методу визначення контурів елементів міської інфраструктури на оптико-електронних зображеннях бортових систем.

II. Рішення Проблеми і Результати

На оптико-електронних зображеннях елементи міської інфраструктури (мости, дороги, будинки тощо) є досить контрастними і представлені у вигляді простих примітивів (пряма, коло, еліпс тощо). Отже, якщо для кожного каналу кольорового простору представлення кольорового зображення (наприклад RGB) за допомогою деякого детектора знайти границі, то за допомогою перетворення Хафа в кожному каналі можна виділити прості примітиви. Якщо фігура об'єкта знаходяться в усіх трьох каналах RGB одночасно, то це є ознакою штучного походження об'єкту. Якщо тільки в одному каналі – об'єкт має природне походження (наприклад, річка), якщо в двох каналах – класифікація ускладнена (це може бути, наприклад, польова дорога).

Одним з найбільш ефективних методів пошуку аналітично заданих примітивів є група методів, що використовують перетворення Хафа [3]. Існує можливість модифікації перетворення Хафа для роботи з реальними даними на зображеннях, коли потрібно знайти той чи інший геометричний примітив, заданий аналітичним рівнянням, і при цьому на зображенні є не дві і не три, а значна кількість голосуючих контурних або особливих точок.

Отже, визначення контурів елементів міської інфраструктури будемо розглядати як двоетапний метод, а саме, застосування деякого детектора границь та застосування безпосередньо перетворення Хафа. На першому етапі проводиться виділення границь, на другому – виділення простих фігур.

В якості детектора границь будемо застосовувати детектор границь Канні, який має наступні етапи [4, 5]:

1. Згладжування. Проводиться з метою зменшення впливу шумів на визначення границь, для чого використовується фільтр Гауса.

2. Пошук градієнту. Для визначення градієнту на зображенні після фільтру Гауса будемо використовувати оператор Собеля. Основою перетворення Собеля є припущення, що функція розриву яскравості на гранях становиться значно більше. Після використання оператора Собеля інтенсивність кожного пікселя вихідного зображення дорівнює градієнту вектору яскравості.

3. Придушення хибних максимумів. Мета цього етапу – перетворити "розмиті" границі в "чіткі". Це

досягається збереженням локальних максимумів та видаленням всього іншого. Для кожного пікселя виконуються наступні дії:

– напрямок градієнту округляється до найближчого значення, що кратне 45°;

– якщо у поточній точці досягається локальний максимум у напрямку градієнту, то вона є частиною границі;

– у противному випадку точка видаляється.

4. Подвійна порогова фільтрація. Сутність – кожен піксель, що перевищує верхній поріг, відмічається як "сильний", кожен піксель, що попадає між двома порогами, – "слабкий" (яскравість таких пікселів приймає фіксоване середнє значення та буде уточнюватися на наступному етапі), пікселі, що менше нижнього порогу – видаляються.

Використання подвійного порогу дозволяє зменшити вплив шуму (за рахунок верхнього порогу) та не втратити "хвости" (за рахунок нижнього порогу).

5. Трасування області невизначеності. Задача зводиться до виділення груп пікселів, що отримали на попередньому етапі проміжне значення, та віднесенню їх до границі (якщо вони з'єднанні з однією з встановлених границь) або їх придушенню (в противному випадку).

У якості вихідного будемо розглядати зображення, що отримане з бортової системи оптико-електронного спостереження Ikonos (рис. 1) [6].

Рисунок 1. Вихідне зображення [6].

Детектор границь Канні застосовано окремо для кожного каналу кольорового простору RGB вихідного зображення (рис. 1). Результат наведений на рис. 2.

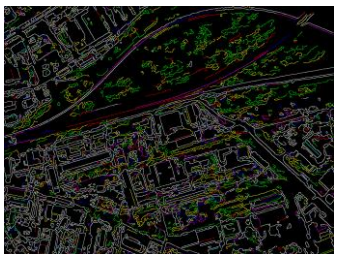


Рисунок 2. Результат застосування до вихідного зображення (рис. 1) детектору границь Канні

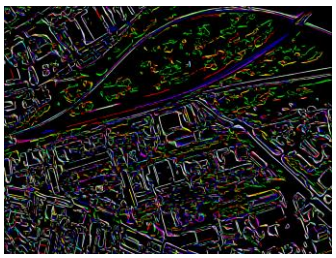


Рисунок 3. Результат застосування перетворення Хафа до зображення після першого етапу (рис. 2)

Після першого етапу можуть з'явитися "втрачені" точки на кривій або невеликі відхилення від ідеальної форми прямої. На другому етапі застосовується перетворення Хафа, призначенням якого є вирішення проблеми угрупування граничних точок шляхом застосування певної процедури голосування до набору параметризованих об'єктів зображення.

На рис. 3 наведено результат застосування перетворення Хафа до зображення після першого етапу (рис. 2). Обробка проводилася окремо для кожного каналу кольорового простору RGB зображення (рис. 2).

На рис. 4 наведено результат накладення рис. 3 на вихідне зображення (рис. 1) з метою визначення контурів елементів об'єктів інфраструктури. Визначені контури елементів міської інфраструктури (доріг, будинків, споруд тощо) наведені на рис. 5.

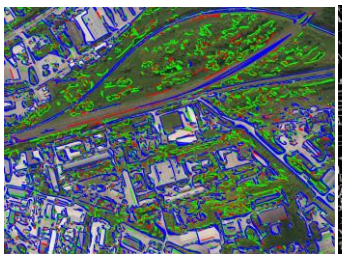


Рисунок 4. Результат накладання зображення після другого етапу (рис. 3) на вихідне зображення

Рисунок 5. Визначені контури елементів міської інфраструктури

III. Висновки

Візуальна оцінка якості дозволяє виявити елементи міської інфраструктури з використанням двоетапного методу обробки оптико-електронного зображення. Отже, отримані результати показують, що даний метод може бути використано для знаходження елементів міської інфраструктури. Для покращення роботи методу необхідно використовувати обробку багатомасштабної послідовності зображень бортових систем.

Список літературних джерел

[1] Chemin, Y. Remote Sensing of Planet Earth / Yann Chemin // Rijeka, 2012. – 250 p.

[2] Барталев С.А. Анализ возможностей применения методов сегментации спутниковых изображений для выявления изменений в лесах / С.А.Барталев, Т.С.Ховратович // Современные проблемы дистанционного зондирования Земли из космоса, 2011. – Т. 8. - № 1. – С. 44-62.

[3] Gonzalez, R. Digital Image Processing / Rafael C. Gonzalez and Richard E. Woods // Second Edition, Prentice Hall, Upper Saddle Rever, 2005.

[4] Canny J. F. A Computational Approach to Edge Detection / J. F. Canny // IEEE Transactions on Pattern Analysis and Machine Intelligence. — 1986. — № 8. — P. 679–698.

[5] Худов Г. В. Оцінка відстані Кульбака-Лейблера при тематичному сегментуванні оптико-електронного зображення методом Канні / Г. В. Худов, В. Г. Худов, І. А. Хижняк, І. В. Новікова // Сучасні інформаційні технології у сфері безпеки та оборони. — 2017. — № 2 (29). — С. 83–90.

[6] Худов Г. В. Метод визначення об'єктів міської забудови на зображеннях бортових систем оптико-електронного спостереження з використанням перетворення Хафа / Г. В. Худов, О. М. Маковейчук, І. А. Хижняк, Ю. С. Соломоненко, І. Ю. Юзова // Системи управління, навігації та зв'язку. — 2018. — № 6(52). — С. 20–24.

Підвищення точності визначення та оперативності прогнозування параметрів руху космічних апаратів

Пічугін Михайло Федорович[1]
[1]Харківський національний університет Повітряних Сил ім. І. Кожедуба, 61023, м. Харків, вул. Сумська 77/79, Україна, michaylo.f.pichugin@gmail.com

Кожушко Ярослав Миколайович[2]
[2]Харківський національний університет Повітряних Сил ім. І. Кожедуба, 61023, м. Харків, вул. Сумська 77/79, Україна, oficer2003@ukr.net

Борцова Марія Вікторівна[3]
[3]Харківський національний університет Повітряних Сил ім. І. Кожедуба, 61023, м. Харків, вул. Сумська 77/79, Україна, masha.v.bortsova@gmail.com

Таран Ігор Андрійович[4]
[4]Харківський національний університет Повітряних Сил ім. І. Кожедуба, 61023, м. Харків, вул. Сумська 77/79, Україна, igortaran2009@gmail.com

Дзеверін Ігор Григорович[5]
[5]Харківський національний університет Повітряних Сил ім. І. Кожедуба, 61023, м. Харків, вул. Сумська 77/79, Україна, DzeverinIgorGryg@gmail.com

Пічугін Ігор Михайлович[6]
[6]Харківський національний університет Повітряних Сил ім. І. Кожедуба, 61023, м. Харків, вул. Сумська 77/79, Україна, igor.m.pichugin @gmail.com

Клімішен Олексій Олексійович[7]
[7]Харківський національний університет Повітряних Сил ім. І. Кожедуба, 61023, м. Харків, вул. Сумська 77/79, Україна, kl_s_kh@ukr.net

Гричанюк Олександр Михайлович[8]
[8]Харківський національний університет Повітряних Сил ім. І. Кожедуба, 61023, м. Харків, вул. Сумська 77/79, Україна, alexander.gricci@gmail.com

Анотація. *У роботі для вирішення задачі підвищення точності визначення параметрів руху космічного апарату запропонований метод, в основі якого є мінімізація з побудовою області початкових наближень. Запропонований метод реалізує нелокальний підхід до мінімізації цільової функції, за рахунок чого забезпечується краща порівняно з традиційними методами збіжність. Для підвищення оперативності прогнозування руху космічного апарата запропоновано використовувати математичний апарат диференціальних перетворень. Це дозволило при збереженні заданої точності у 3-4 рази зменшити обчислювальні витрати порівняно зі штатними балістико-навігаційними алгоритмами.*

Ключові слова: *космічний апарат; балістико-навігаційне забезпечення; оптимізація; параметри руху; оперативність прогнозування руху; диференціальні перетворення.*

I. Вступ

Космічні системи сьогодення широко використовуються для вирішення найрізноманітніших задач – як цивільних (екологічний моніторинг, метеорологічні дослідження, забезпечення зв'язку) [1], так і військових (виявлення та ідентифікація військових об'єктів, спостереження за діяльністю угрупувань військ, уточнення характеристик театру воєнних дій при плануванні бойових операцій; цілевказівка засобам ураження, оперативне визначення результатів нанесення ракетно-бомбових ударів тощо) [2, 3].

На сучасному етапі застосування космічних систем спостерігається чітка тенденція постійного зростання вимог до точності і оперативності використання космічних засобів на всіх етапах їх експлуатації. Ця тенденція безпосередньо поширюється на вимоги до якості балістико-навігаційного забезпечення управління польотом космічних апаратів (КА). При цьому саме показники точності і оперативності істотно впливають на ефективність функціонування та кінцеві результати роботи всієї космічної системи. Такий вплив стає особливо важливим в умовах однопунктної технології управління КА, коли використовується лише один командно-вимірювальний пункт з наземною станцією командно-вимірювальної системи. Саме така технологія реалізована в Україні, що зумовлено об'єктивними особливостями територіальних обмежень на розташування наземного сегмента космічної системи. А отже, актуальним є питання розробки і удосконалення балістико-навігаційного забезпечення управління КА, і одним із перспективних напрямів удосконалення цього забезпечення є реалізація координатних методів управління космічними апаратами.

Координатні методи управління реалізуються за допомогою керуючих впливів, які закладаються на КА і видаються по досягненню потрібних координат [4]. Вони полягають у тому, що керуючі команди формуються як функції вимірюваних поточних координат положення КА, поточного стану підсистем КА і вихідних даних, необхідних для виконання цільових завдань КА. Для здійснення координатного методу управління на КА є джерело навігаційно-балістичної інформації, що дозволяє проводити вимірювання параметрів руху центру мас КА у будь-який момент часу. У залежності від заданих координат цілей і поточних координат КА у бортовій цифровій обчислювальній машині мають вироблятися керуючі команди

на включення (виключення) бортової апаратури. Такий метод забезпечує точність виконання команд, необхідну для досягнення заданих координат.

За формування керуючих команд відповідає балістико-навігаційне забезпечення. Його задача – визначення інформації щодо положення КА та прогнозування параметрів його руху на заданий момент часу. Характеристики оперативності і точності рішення саме цих завдань і визначають оперативність і точність усього балістико-навігаційного забезпечення управління космічними апаратами.

Підвищення ефективності балістико-навігаційного забезпечення управління польотом космічними апаратами за такими показниками як оперативність і точність може забезпечуватися шляхом рішення двох підзадач, а саме шляхом підвищення точності або зменшення похибки визначення параметрів руху космічних апаратів та зменшення обчислювальної складності або підвищення оперативності прогнозування руху космічних апаратів.

Метою даної роботи є розробка підходів щодо підвищення точності визначення параметрів руху космічних апаратів і оперативності їх прогнозування.

II. ПІДВИЩЕННЯ ТОЧНОСТІ ВИЗНАЧЕННЯ ПАРАМЕТРІВ РУХУ КОСМІЧНОГО АПАРАТУ

У загальному випадку на результуючу точність визначення початкових умов руху КА впливають три чинники – випадкова складова, зумовлена наявністю випадкових помилок у траєкторних вимірюваннях (чим більше оброблюється вимірювальної інформації, тим менша результуюча помилка), динамічна складова, зумовлена наявністю динамічних помилок використовуваної моделі руху космічного апарату (чим більший інтервал часу, що розглядається, тим більша результуюча помилка) та помилка, що визначається розміром області збіжності методу мінімізації, який використовується для вирішення багатоточкової крайової задачі. Остання складова є характеристикою математичного методу і полягає в тому, що чим менше розмір області збіжності методу, тим кількість вимірювальної інформації для його нормальної роботи має бути більшою. При цьому часовий інтервал, на якому проводиться траєкторна обробка, не може бути меншим, ніж інтервал, що забезпечує збіжність методу мінімізації.

Вплив перших двох факторів – випадкової і динамічної складових помилки на результуючу похибку визначення параметрів руху КА є протилежним, а третій фактор – це обмеження. Так, для одержання найменшої похибки визначення параметрів руху КА необхідно обробляти деяку оптимальну кількість вимірювальної інформації, яка забезпечує достатню компенсацію випадкових похибок і, водночас, не дає динамічній похибці чинити істотний вплив. При цьому слід враховувати, що кількість вимірювальної інформації не може бути меншою за необхідну для забезпечення збіжності алгоритму визначення цих параметрів руху.

У ході досліджень був розроблений спосіб визначення оптимальної кількості мірних витків для оцінювання параметрів руху космічного апарату за критерієм мінімуму похибки оцінки, зумовленої випадковою та динамічною складовими. В основу такого способу покладено уявлення вихідної задачі як багатокритеріальної з подальшим вирішенням за нелінійною схемою компромісів професора Вороніна А.Н. [5]. У сформованій багатокритеріальній задачі у якості суперечливих функцій якості була обрана залежність динамічної і випадкової похибок від обсягу вимірювальної траєкторної інформації, вираженого в кількості мірних витків.

Суть метода полягає у тому, що спочатку формуються залежності для частинних критеріїв оптимальності для випадкової $\eta\left(N_{PKO}\right)$ та динамічної $\xi\left(N_{PKO}\right)$ складових помилки (N_{PKO} – кількість мірних витків). Потім складається узагальнений критерій, який виступає у ролі цільової функції:

$$N_{PKO}^{*} = \arg\min \sum_{k=1}^{2} \gamma_k \left[1-\varphi_{0k}(N_{PKO})\right]^{-1}, \qquad (1)$$

де γ_k – вагова функція; $\varphi_{0k}(N_{PKO})$ – критеріальні функції.

Рішення оптимізаційної задачі із цільовою функцією (1) дозволяє знайти оптимальне значення кількості мірних витків.

Залежності критеріальних функцій від кількості мірних витків показані на рис. 1.

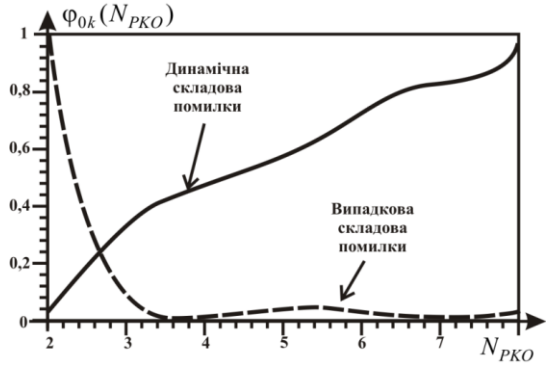


Рисунок 1. Залежність критеріальних функцій від кількості мірних витків

Аналіз балістичних даних з управління космічним апаратами "Січ-1" і "АУОС-СМ-КФ" показав, що оптимальна кількість мірних витків в залежності від ступеня поточної сонячної активності складає від 3 (в період підвищеної сонячної активності) до 6 (при нормальній сонячної активності).

У вітчизняній практиці балістико-навігаційного забезпечення при визначенні параметрів руху космічних апаратів використовуються градієнтні методи мінімізації, які характеризуються невеликою областю збіжності і потребують накопиченні вимірювальної інформації на 5–6 мірних витках. Отже, традиційно, при визначенні параметрів руху космічних апаратів кількість необхідної вимірювальної інформації зумовлюється не вимогами результуючої точності визначення параметрів руху космічних апаратів, а кількістю вимірювань для забезпечення збіжності алгоритму визначення цих початкових умов, тобто характеристикою математичного методу мінімізації.

Досліджено можливості визначення параметрів руху космічного апарату за 3-ма – 4-ма мірними витками за допомогою градієнтних методів мінімізації, які реалізовані в штатних вітчизняних програмних комплексах балістико-навігаційного забезпечення управління космічними апаратами. Результати показані на рис. 2 (для розрахунків використовувався метод Ньютона).

Аналіз рис. 2 показує, що градієнтні методи за рахунок реалізації локального підходу до мінімізації цільової функції не забезпечують збіжність вирішення поставленого завдання, тобто є недієздатними при такій кількості вимірювальної інформації.

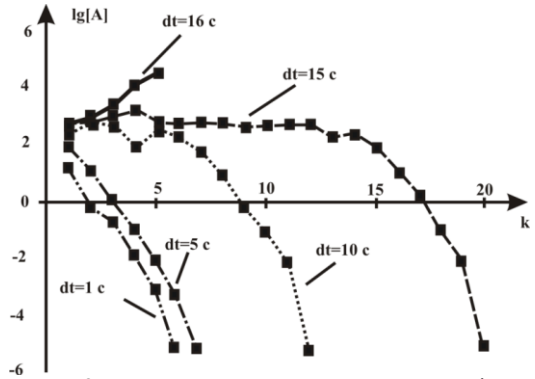


Рисунок 2. Результати визначення параметрів руху за допомогою метода Ньютона

Пропонується при визначенні параметрів руху космічних апаратів замість градієнтних методів використовувати пошуковий метод мінімізації з побудовою області початкових наближень. У якості такого методи був обраний метод оптимізації Нелдера-Міда [6].

Цей метод визначення параметрів руху КА за результатами траєкторних вимірювань реалізує нелокальний підхід до мінімізації цільової функції, що надає йому значно ширшу область збіжності в порівнянні зі штатним алгоритмом, і це дозволяє забезпечити збіжність ітераційного процесу оцінювання параметрів руху космічного апарату при скороченому обсязі траєкторних вимірі. Результати застосування цього методу показані на рис. 3.

Таким чином, впровадження у вітчизняне балістико-навігаційне забезпечення пошукового методу оптимізації з побудовою області початкових наближень забезпечить підвищення точності визначення початкових умов руху космічних апаратів, що необхідно для перспективних вітчизняних космічних систем.

III. ПІДВИЩЕННЯ ОПЕРАТИВНОСТІ ПРОГНОЗУВАННЯ РУХУ КОСМІЧНОГО АПАРАТА

У штатних вітчизняних програмних комплексах балістико-навігаційного забезпечення управління космічними апаратами рішення задачі прогнозування руху космічних апаратів здійснюється шляхом інтегрування відповідних диференціальних рівнянь збуреного руху космічного апарату. Для цього використовуються чисельні методи інтегрування диференціальних рівнянь – метод Адамса [7] 7-го порядку і метод Рунге-Кутта [7] 4-го порядку. Ці традиційні чисельні методи мають істотний недолік, який полягає у підвищеній обчислювальній складності, причому спроби її зменшити призводять до суттєвих втрат в точності розрахунків.

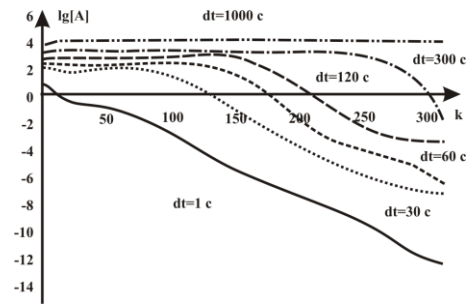


Рисунок 3. Результати визначення параметрів руху за допомогою метода Нелдера-Міда

Слід окремо зазначити, що особливо актуальним є питання зменшення обчислювальних витрат на прогнозування руху космічних апаратів при впровадженні перспективних координатних методів управління, коли всі обчислення або їх значну частину необхідно проводити на борту космічного апарату. Це накладає суттєві обмеження на характеристики бортових обчислювальних засобів на яких проводяться розрахунки.

Вирішити протиріччя "точність-обчислювальна складність" можливо шляхом використання математичного апарату диференціальних перетворень. Застосування формалізованого операційного методу диференціальних перетворень дає можливість розробити алгоритми прогнозування руху космічних апаратів із меншими у 3–4 рази, порівняно зі штатними алгоритмами, обчислювальними витратами при забезпеченні заданої точності за рахунок точного рекурентного визначення відрізка ряду Тейлора рішення диференціального рівняння руху космічного апарату [8]. Такий підхід дозволить істотно знизити вимоги до необхідної швидкодії бортового обчислювального засобу при проведенні прогнозу руху космічних апаратів.

IV. ВИСНОВКИ

Для підвищення точності визначення параметрів руху космічних апаратів слід оптимізувати необхідну кількість мірних витків. Для цього був розроблений алгоритм визначення параметрів руху космічних апаратів із значно ширшою областю збіжності, ніж має штатний алгоритм. Запропонований алгоритм залучає пошуковий метод оптимізації з побудовою області початкових наближень.

При впровадженні перспективних координатних методів управління космічними апаратами для підвищення оперативності прогнозування руху космічних апаратів необхідно істотно зменшити обчислювальні витрати на прогнозування руху космічного апарату. Для цього пропонується використовувати математичний апарат диференціальних перетворень.

СПИСОК ЛІТЕРАТУРНИХ ДЖЕРЕЛ

[1] Пашков Д.П. Аналіз можливостей застосування космічних систем дистанційного зондування землі для вирішення екологічних завдань / Д.П. Пашков // Наука і техніка Повітряних Сил Збройних Сил України. – №2(15), 2014. – С. 184–188.

[2] Пічугін М.Ф. Огляд програм та вимог керівних документів країн НАТО стосовно космічної ситуаційної обізнаності / М.Ф. Пічугін, Д.В. Карлов, О.О. Клімішен, Я.М. Кожушко // Збірник наукових праць Харківського університету Повітряних Сил. - №2 (51), 2017. - С. 59-63.

[3] Пічугін М.Ф. Оцінка можливостей виявлення об’єктів космічними засобами дистанційного зондування землі в інтересах інформаційного забезпечення груп космічної підтримки збройних сил / М.Ф. Пічугін, Д.А. Іщенко, Я.М. Кожушко, О.О. Клімішен // Системи озброєння і військова техніка. – №3 (55), 2018. – С. 28–36.

[4] Варламов І.Д. Перспективні методи управління польотом космічних апаратів оптико-електронного спостереження / І.Д. Варламов, А.М. Воронін, Ю.І. Міхєєв // Вісник ЖДТУ. – № 4(43), 2007. – С. 65–70.

[5] Воронин А.Н. Многокритериальные решения: модели и методы / А.Н. Воронин, Ю.К. Зиатдинов, М.В. Куклинский. – К.: НАУ, 2011. – 348 с.

[6] Пантелеев А.В. Теория оптимизации для инженеров и экономистов / А.В. Пантелеев, Т.А. Летова. – М.: Вузовская книга, 2016. – 568 с.

[7] Демидович Б.П. Численные методы анализа. Приближение функций, дифференциальные и интегральные уравнения / Б.П. Демидович, И.А. Марон, Э.З. Шувалова. – Рипол Классик. – 2013. – 374 с.

[8] Пічугін М.Ф. Балістико-навігаційне забезпечення управління перспективними вітчизняними космічними апаратами / М.Ф. Пічугін, Д.В. Карлов, О.О. Клімішен, О.Ю. Чернявський // Наука і техніка Повітряних Сил Збройних Сил України. – №2(8), 2012. – С. 128–132.

Застосування інформаційно-пошукових систем для забезпечення наукових робіт архівними метеорологічними даними

Новіков Андрій Миколайович

Інститут проблем безпеки АЕС НАН України,
вул. Лисогірська, 12, Київ, 03028, Україна,
e-mail:andreyn@ua.fm

Абстракт. *Розглянуті питання пошуку та аналізу можливих для використання в наукових роботах джерел архівних метеорологічних даних. Надані посилання на інформаційні ресурси метеорологічних даних та наведений приклад застосування on-line сервісу Вольфрам Альфа (Wolfram|Alpha).*

Ключові слова: *archive Weather data, Google, Вольфрам Альфа (Wolfram|Alpha), Чорнобиль.*

I. Вступ і постановка задачі.

Наукові роботи в області екологічної безпеки, розробки, верифікації та використання систем моделювання і прогнозування радіоекологічної обстановки потребують метеорологічного забезпечення та залучення все більшого об'єму інформації [1 - 5].

Зростаючі темпи інформаційних процесів (інформаційних технологій [6]), висока швидкість обробки даних, швидкий пошук інформації, розосередження даних, доступ до джерел інформації незалежно від місця їх розташування призводять до збільшення кількості сервісів та ресурсів щодо задоволення інформаційних потреб. Загально доступні пошукові системи (Google [7], Bing [8] тощо) досить швидко формують посилання на Веб-сторінки, які містять ключові слова запиту. В той же час, оскільки обсяг інформації збільшується та ніщо не гарантує достовірності і відсутності дезінформації, знайдені дані можуть не відповідати в повній мірі поставленим задачам, бути неповними та неоднорідними, потребувати додаткового часу для аналізу, уточнень, обробки та збереження. Все це призводить до збільшення навантаження на користувача [9].

На відміну від звичних пошукових систем, які видають перелік посилань на заданий запит, вартий уваги on-line сервіс Вольфрам Альфа (Wolfram|Alpha) [10], котрий дозволяє розширити перелік метеорологічних даних та в деяких випадках автоматизувати роботу. Зокрема, в рамках оцінки швидкості випадінь радіоактивних аерозолів, дослідження кореляційних залежностей, аналізу та інтерпретації накопичених після Чорнобильської аварії даних проведено попереднє уточнення та розширення наявного переліку метеорологічних даних, залучення до розгляду додаткових метеопараметрів таких, як кількість, інтенсивність та вид опадів, а також даних різної часової дискретності.

Ціллю даного дослідження є попередній опис джерел, що надають можливість інформаційного забезпечення наукових робіт архівними метеорологічними даними.

II. Основна частина

Головним джерелом гідрометеорологічних даних для території України є систематичні спостереження, що проводяться на мережі станцій та постів гідрометеорологічної служби України.

Матеріали спостережень зберігаються в архіві Центральної геофізичної обсерваторії (ЦГО). Користуватися документами Національного архівного фонду або їх копіями має право кожен громадянин України на підставі особистої заяви і документа, що засвідчує особу. Працювати з архівами можна безкоштовно, проте лише безпосередньо в читальному залі Галузевого державного архіву гідрометслужби, який міститься за адресою: м. Київ, проспект Науки, 39, корпус 2. (044 525 03 30) (згідно ст. 15 Закону України від 13 грудня 2001 р. «Про національний фонд і архівні установи»).

Відомо, що ведуться роботи по створенню національного архіву на технічних носіях з використанням сучасних інформаційних технологій [11].

З поточними матеріалами спостережень ЦГО (метеорологічні дані метеостанції Київ з автоматизованих датчиків(з різною дискретністю)) можна ознайомитись на сайті: //www.cgo.kiev.ua, де доступні також певні архівні дані - карти середньомісячної температури повітря та опадів по Україні починаючи з липня 2009 року.

Google

Пошукова система Google, доступна через будь-який веб-браузер, надає список веб-сайтів, з яких в подальшому можна отримати необхідну інформацію. Пошук сайтів система Google проводить досить швидко, а ось основний час витрачається на перегляд та опрацювання самих веб-сторінок.

Нижче наводяться джерела архівних даних метеорологічної інформації та їх короткий аналіз для міста Чорнобиль.

Сайт http://rp5.ua/ [12]. На цьому сайті наявні почасові дані метеостанції (WMO ID)-33231: швидкість та напрямок вітру, температура, вологість, опади й ін.; є можливість автоматично скачати архів з даними за весь проміжок часу, документ в форматі xls (Excel) або CSV (текстовий). Також цей сайт надає можливість отримати архіви метеорологічних даних починаючи з 01.01.2005.

Сайт https://meteo.ua [13]. На цьому сайті наявні погодні дані, надані Українським гідрометеорологічним центром з 01.01.2003 р., а саме: характеристики погоди (ясно, хмарно…), температура, вітер, тиск, вологість. Проте цей сайт має певні обмеження: (1) проміжок відображення становить один день; (2) відсутня інформація про кількість опадів; (3) відсутня, або незрозуміла, процедура

завантажування, що змушує вдаватися до ручного переписування.

Сайт http://pogoda-service.ru/archive_gsod.php [14]. На цьому сайті надаються географічні координати точки вимірів (51.283,30.233), мах., мін., сер. температура, швидкість вітру, опади. Проте цей сайт також має певні обмеження: (1) відсутній напрямок вітру та вид опадів, (2) дані неоднорідні, (3) наявні пропуски (наприклад, відсутній ряд даних по Чорнобилю за 05, 14 та 27.02.1986р., з 04.05.1986р. по 01.05.1988р.) та інш.

Сайт http://eca.knmi.nl/ European Climate Assessment & Dataset [15]. На цьому сайті надаються дані з 01.07.1959р., а саме мінімальна та максимальна температура, опади. Ці дані представлені в текстовому форматі txt.

Сайт pogoda-service.ru [16]. Цей сайт надає добові дані, зокрема мінімальну, максимальну та середню температуру, швидкість вітру, опади. Є можливість копіювання масиву даних.

Вольфрам Альфа (Wolfram|Alpha).

Набір обчислювальних алгоритмів поєднаних з базою знань - Wolfram|Alpha на відміну від Google, поставлені задачі розв'язує шляхом математичного пошуку, самостійно знаходить та обробляє дані, відображаючи їх в досить стислому конструктивному вигляді. Рушій Wolfram|Alpha заснований на обробці природної мови (англійської), великій бібліотеці алгоритмів і NKS-підході для відповідей на запити [17].

Розпочати роботу в Wolfram|Alpha можна двома шляхами.

1. Через веб-браузер, перейшовши на сайт Wolfram|Alpha - http://www.wolframalpha.com, на панелі завдань (пошуку) достатньо ввести запит англійською, наприклад для одержання метеорологічних даних в місті Чорнобилі за 1986 рік - weather Chornobyl 1986, отримаємо систематизовані метеорологічні дані. На жаль, завантаження отриманих результатів доступне лише в передплачених версіях Wolfram|Alpha Pro.

2. Через систему комп'ютерної алгебри Mathematica, яка містить функції Wolfram|Alpha, та робоче місце, підключене до мережі Інтернет, маючи доступ до системи знань, можна отримувати дані, в подальшому опрацьовувати та зберігати, зокрема експортувати в Excel [18].

Наприклад для міста Чорнобиля, щоб отримати добові значення за 1986 рік та експортувати їх до Excel, необхідно в новий відкритий документ Mathematica ввести (скопіювати) наведені нижче запити та натиснути <Shift+Enter> на клавіатурі.

1. для температури -

```
t=WolframAlpha["weather in Chernobyl
1986",{{"WeatherCharts:WeatherData",1},"TimeSeriesData"}]
Export["Temp_1986.xls",t, "xls"]
SystemOpen["Temp_1986.xls"]
```

2. для кількості опадів -

```
Cc=WolframAlpha["weather in chernobyl
1986",{{"WeatherCharts:WeatherData",2},"TimeSeriesData"}
]
Export["Chernobyl_1986.xls",Cc, "xls"]
SystemOpen["Chernobyl_1986.xls"]
```

III. ВИСНОВКИ

Проведений попередній пошук, аналіз та опис можливих для використання в наукових роботах джерел архівних метеорологічних даних.

Напрацювання даної роботи мають практичне застосування, а саме використані для забезпечення метеорологічними параметрами наукової роботи щодо ретроспективного аналізу даних вимірювань швидкості осадження Cs-137 після Чорнобильської аварії.

СПИСОК ЛІТЕРАТУРНИХ ДЖЕРЕЛ

[1] Талерко Н.Н. Восстановление параметров Чернобыльского выброса по измерениям мощности экспозиционной дозы в г. Припять. Ядерная физика и энергетика, 2010, т. 11, № 2, с. 169 - 177 Режим доступа: http://jnpae.kinr.kiev.ua/11.2/Articles_PDF/jnpae-2010-11-0169-Talerko.pdf

[2] Талерко Н.Н., Гаргер Е.К. Оценки первичного выброса из аварийного блока ЧАЭС с помощью моделирования атмосферного переноса (обзор). // Проблеми безпеки атомних електростанцій і Чорнобиля. - 2006. - Вип. 6. - С. 80 - 90. Режим доступу: http://mntc.smn.com.ua/downloads/2006_05/c80.pdf

[3] Закон України «Про оцінку впливу на довкілля», прийнятий Верховною Радою 23.05.17 (№ 2059-VIII). Режим доступу: URL: https://zakon3.rada.gov.ua/laws/show/2059-19

[4] Гаргер Е.К. Скорость сухого осаждения радиоактивных веществ чернобыльского происхождения по данным наблюдений. Проблеми безпеки атомних електростанцій і чорнобиля 2018 вип. 31. С. 85-103. Режим доступа: URL: doi.org/10.31717/1813-3584.18.31.10

[5] Лев Т.Д. Информационно-аналитическое и картографическое обеспечение систем аварийного реагирования АЭС / Т.Д. Лев, О.Г. Тищенко, В.Н. Пискун // Проблеми безпеки атомних електростанцій і Чорнобиля. — 2011. — Вип. 16. — С. 17–26. Режим доступу: http://dspace.nbuv.gov.ua/bitstream/handle/123456789/112903/02-Lev.pdf?sequence=1

[6] Закон України «Про Національну програму інформатизації», (Відомості Верховної Ради України (ВВР), 1998, № 27-28, ст.181). Режим доступу: URL: https://zakon.rada.gov.ua/laws/show/74/98-%D0%B2%D1%80/ed20160801/sp:max15#n17

[7] Офіційний сайт www.google.com – Пошукова система Google.

[8] Офіційний сайт www.bing.com – Пошукова система Bing.

[9] Yang, C.C.; Chen, Hsinchun; Honga, Kay (2003). Visualization of large category map for Internet browsing. Decision Support Systems 35 (1): 89–102. doi:10.1016/S0167-9236(02)00101-X.

[10] Офіційний сайт http://www.wolframalpha.com - on-line сервіс Вольфрам Альфа (Wolfram|Alpha)

[11] Использование современных информационных технологий при создании базы метеорологических данных Украины / В. П. Евстигнеев, М. П. Евстигнеев, Н. И. Кульбида, В. А. Наумова, Н. И. Швень // Наукові праці Українського науково-дослідного гідрометеорологічного інституту. - 2013. - Вип. 264. - С. 81-90. - Режим доступу: http://nbuv.gov.ua/UJRN/Npundgi_2013_264_12.

[12] Электронный ресурс - http://rp5.ua/Архів_погоди_в_Чорнобилі

[13] Электронный ресурс - https://meteo.ua/ua/archive/18/chernobyil/2003-1-1

[14] Электронный ресурс - http://pogoda-service.ru/archive_gsod.php

[15] Электронный ресурс - http://eca.knmi.nl/

[16] Электронный ресурс - http://pogoda-service.ru/archive_gsod.php?

[17] Wolfram S. A New Kind of Science. Wolfram Media, 2002. — 1192 p. Режим доступу: https://www.wolframscience.com/nks/

[18] Зеленица А.М. Інтерактивний україномовний підручник з Wolfram Mathematica. Переклад і оформлення А.М. Зеленица. — 4-е вид. — Україна, Київ, 2012-2016. Режим доступу: http://infrastructure.kiev.ua/ua/133/

Анализ методов понижения размерности пространства

Береснев Дмитрий Владимирович
Шараев Евгений Владимирович

Белорусский государственный университет информатики и радиоэлектроники, ул. П. Бровки 6, Минск 220039, Беларусь,
beresnev.dima8@gmail.com,
eugen.sharayev@gmail.com

Анотация. *Рассмотрены основные методы понижения размерности пространства признаков. Приведено описание существующих нелинейных подходов и методов для понижения размерности пространства признаков. Проведен анализ преимуществ и недостатков каждого из методов. Проведен анализ новых методов.*

Ключевые слова: *многомерное пространство, признаковое пространство, анализ данных, методы понижения размерности, таксономия методов понижения размерности пространства, локальные нелинейные методы понижения размерности.*

I. Введение и постановка проблемы

Ежедневно в различных областях науки возникает необходимость решения разнообразных задач анализа данных, таких как классификация, прогнозирование, кластеризация, а также выявления скрытых зависимостей, распознавания изображений и поддержки принятия оптимальных решений. На практике при решении задач анализа данных и машинного обучения информация об объектах представлена в виде сложного многомерного массива данных. Таким образом, возникает необходимость извлечения из входных многомерных данных набора признаков, которые будут наиболее информативны с точки зрения дальнейшего решения задачи. Любые многомерные данные всегда можно представить в виде вектора чисел. Такие вектора обычно имеют большую длину в виду многомерности пространства, а некоторые признаки, которые содержаться в данном векторе не всегда информативны. Поэтому решается задача понижения размерности пространства признаков, которое описывает входные данные, с целью получения относительно компактного множества информативных признаков. *Понижение размерности пространства признаков* – это процесс сжатия признакового пространства к некоторой заданной размерности с минимальными потерями информации. Большое количество признаков приводит к высоким временным затратам на обработку данных, большим объемам памяти, требуемой для хранения информации, а также к необходимости сбора большого числа прецедентов для уверенного восстановления скрытых зависимостей в существенно многомерном пространстве. Уменьшение размерности пространства признаков может преследовать множество целей:

- Сокращение вычислительных затрат при обработке данных;
- Борьба с переобучением. Чем меньше количество признаков, тем меньше требуется объектов для уверенного восстановления скрытых зависимостей в данных и тем выше качество восстановления подобных зависимостей;
- Сжатие данных для более эффективного хранения информации;
- Визуализация данных. Проектирование выборки на двух-/трехмерное пространство позволяет графически представить выборку;
- Извлечение новых признаков. Новые признаки, полученные в результате преобразования, могут оказывать значимый вклад при последующем решении задач;
- Сохранение принципа топологии (соседние в многомерном пространстве объекты должны оставаться таковыми в пространстве меньшей размерности) и расстояний между объектами (степень подобия).

II. Характеристика подходов и методов

Таксономия методов понижения размерности данных. На рис. 1 изображено общая схема таксономии методов понижения размерности пространства признаков. На рис.1 как и в данной работе рассмотрены не все нелинейные методы, ввиду их большого количества.

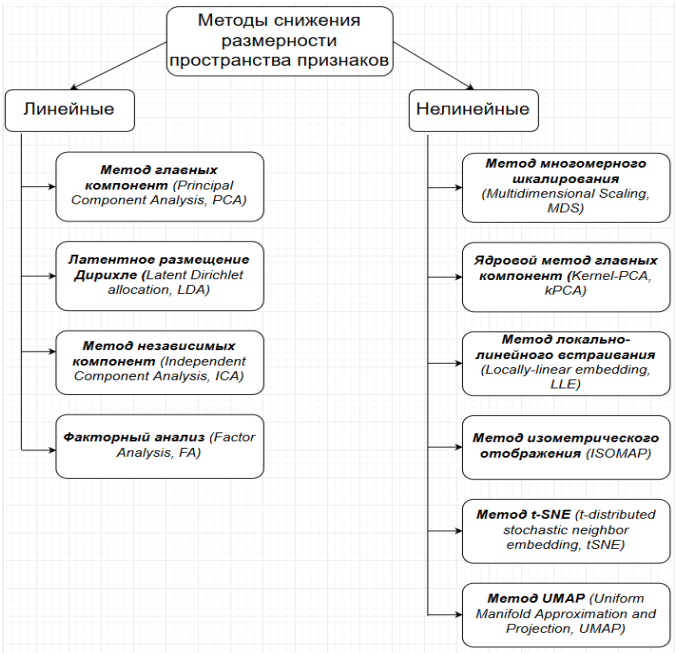


Рисунок 1. Таксономия методов

Метод главных компонент (разложение Карунена-Лоева, principal component analysis, PCA) является простейшим методом уменьшения размерности в задачах анализа данных [1]. Суть метода заключается в поиске в исходном пространстве гиперплоскости заданной размерности с последующим проектированием выборки на данную гиперплоскость. При этом выбирается та гиперплоскость, ошибка проектирования данных на

которую является минимальной в смысле суммы квадратов отклонений.

Данный метод обладает следующим рядом особенностей:

- Неплохо работает на данных с линейной зависимостью;
- Позволяет найти такие пространства меньшей размерности, при ортогональных проекциях на которые среднеквадратическое отклонение (разброс данных) максимально;
- Позволяет найти такие пространства меньшей размерности, при ортогональных проекциях на которые расстояние между точками максимально;
- Позволяет для данной многомерной случайной величины построить такое ортогональное преобразование координат, в результате которого корреляции между отдельными координатами будут нулевыми;
- Плохо работает с очень большими векторами признаков (десятки тысяч и более);
- Неэффективен с точки зрения вычислительной нагрузки, в виду использования сингулярного разложения матриц, которое ограничивает использование данного метода на слишком длинных векторах признаков.

Таким образом, видно, что особенности метода PCA, как и других линейных методов, накладывают ограничения на применение данного класса методов на широком спектре задач анализа данных. Поэтому последние исследования нацелены на класс нелинейных методов.

Многомерное шкалирование [2] – это метод, позволяющий располагать точки, соответствующие изучаем объектам (шкалируемые объекты), в некотором многомерном признаковом пространстве, так, чтобы попарные расстояния между точками в этом пространстве как можно меньше отличались от эмпирически измеренных попарных мер близости этих изучаемых объектов. Основное отличие данного метода от остальных заключается в анализе не самих данных, а матрицы близости объектов между собой. Соответственно, цель многомерного шкалирования заключается в описании матрицы в терминах расстояний между точками в каком-либо подпространстве.

Ядерный метод главных компонент [3] является одним из нелинейных методов уменьшения размерности данных. Данный метод объединяет линейный метод главных компонент и специальный набор преобразований, называемый kerneltrick. Kerneltrick позволяет преобразовать любой алгоритм, который использует скалярное произведение двух векторов. Для применения такого преобразования используется замена всех скалярных произведений на ядерную функциию. Таким образом, можно сказать, что линейный алгоритм преобразуется в нелинейный. Этот нелинейный алгоритм эквивалентен линейному, только в пространстве большой размерности. Основное отличие данного метода от линейного метода главных компонент в том, что ковариационная матрица заменяется на ядерную матрицу.

Метод локально-линейного встраивания – алгоритм, базируется на гипотезе о том, что данные в многомерном пространстве лежат на сглаженном нелинейном многообразии меньшей размерности [4]. Данный метод находит глобальную нелинейную структуру.

Метод изометрического отображения [5] – особенность данного метода заключается в том, что линейность метода присутствует локально, только между ближайшими соседями. Но в глобальном смысле выстраиваемая структура, представляющая расстояние, не линейна. Метод изометрического масштабирования является усовершенствованием метода многомерного масштабирования.

t-SNE [6] — это алгоритм для понижения размерности, разработанный Лоренсом ван дер Маатеном и Джеффри Хинтоном. Метод проецирует каждый объект высокой размерности в заданную размерность таким образом, что похожие объекты проецируются близко расположенными точками, а непохожие точки проецируются расположенными далеко друг от друга.

UMAP (Uniform Manifold Approximation and Projection) — это новый алгоритм уменьшения размерности, библиотека с реализацией которого вышла относительно недавно [7]. По результатам последних исследований, у UMAP нет ограничений на размерность входного пространства признаков, которое необходимо уменьшить, он намного быстрее и более вычислительно эффективен, чем t-SNE, а также лучше справляется с задачей переноса глобальной структуры данных в новое подпространство. UMAP постоянно совершенствуется и дорабатывается, однако уже сейчас можно сказать, что по качеству работы на реальных задачах он не уступает другим алгоритмам и возможно, наконец, решит основную проблему современных методов понижения размерности — невысокая скорость работы.

III. Выводы

В большинстве реальных практических задач анализ данных, не имеющих определенную структуру в исходном пространстве показал, что спрогнозировать какой из методов больше подходит под определенную задачу без эксперимента невозможно. Использование методов, которые базируются на территории графов не всегда эффективны и часто работают крайне медленно. Стоит отметить, что нельзя утверждать что какой-то метод самый лучший или худший: каждый метод имеет свою специфику и область применения, многое зависит от природы и структуры самих данных. Также сегодня важную роль играет скорость работы алгоритма.

Список источников

[1] K. Pearson , “LIII. On lines and planes of closest fit to systems of points in space,” The London, Edinburgh, and Dublin Philosophical Magazine and Journal of Science, vol. 2, no. 11, pp. 559–572, Nov. 1901

[2] I. Borg and P. J. F. Groenen, Modern Multidimensional Scaling: Theory and Applications, 2nd ed. New York: Springer-Verlag, pp. 207–212, 2005.

[3] B. Schölkopf, A. J. Smola, and K.-R. Müller, “Nonlinear Component Analysis as a Kernel Eigenvalue Problem,” Neural Computation, vol. 10, pp. 1299–1319, 1998.

[4] S. T. Roweis and L. K. Saul, “Nonlinear dimensionality reduction by locally linear embedding,” Science, vol. 290, no. 5500, pp. 2323–2326, Dec. 2000

[5] J. B. Tenenbaum, V. de Silva, and J. C. Langford, “A Global Geometric Framework for Nonlinear Dimensionality Reduction,” Science, vol. 290, no. 5500, pp. 2319–2323, Dec. 2000.

[6] L. J. P. van der Maaten and G. E. Hinton, “Visualizing High-Dimensional Data Using t-SNE,” Journal of Machine Learning Research, vol. 9, no. nov, pp. 2579–2605, 2008.

[7] L. McInnes, J. Healy, and J. Melville, “UMAP: Uniform Manifold Approximation and Projection for Dimension Reduction,” arXiv:1802.03426 [cs, stat], Feb. 2

Expansion of Neural-like structures inputs using combined approximation

Oleksandra Mishchuk[1]

[1]Lviv Polytechnic National University, 12 Bandera street, Lviv, 79013, Ukraine, oleksandra.myroniuk@gmail.com

Roman Tkachenko[1]

Abstract. *The article is aimed at the investigation of new algorithms of combined approximation of surface response of neural networks. It is described that on the basis of clustering of the k-means method, new algorithms of combined data approximation for regression assignments were created. The newly developed methods of combined approximation of the surface response are analyzed and with comparing found predicted errors the most effective one is determined. Moreover, in the article is proved that neural-like structures of Geometric Data Transformations with combined approximation of the surface response provide fast and accurate data prediction.*

Keywords: *neural-like structures; Geometric Data Transformations; linear regression; data approximation; clustering; k-means method; prediction error.*

I. INTRODUCTION

Artificial Neural Networks (ANN) are the emulations of the human brains: the best decision-making machines [1]. These are models, which consists of simple processes (neurons) that interact with each other and can do self-learning. They are capable to execute the programmed sequence of actions on predetermined data and to analyze the new input information by themselves [2].

The most commonly used are the following artificial neural networks: single-layer perceptrons, Adaline and Madaline networks that form linear response surfaces; ANN with reverse engineering, forming the stepped surface [3]; multilayer perceptrons, which form non-linear surfaces of sigmoid slopes; and radial basic functions neural networks that form nonlinear surface of the response, built on hyperspheres [4].

All of these neural networks have specific properties in terms of the complexity of the adjustment, the training time, the ratio of the characteristics of accuracy with speed. In terms of reliability and speed of training, the most attractive are single-layer perceptrons, but their use is limited to a class of linearly separate tasks. Neural networks of reverse dissemination are also fast and efficiently trained, but predicting errors in most cases significantly exceeds the permissible values [5]. So, there is a goal to research neural-like structures to provide high accuracy of training and predicting, while simultaneously maintaining the appropriate level of generalization and the speed.

Therefore, there is a need in creating, analyzing and exploring new training and predicting methods to find algorithms that provide not only fast, but also the most accurate expected results that will meet market needs. Because fast and reliable data prediction is the first step in solving a large number of business tasks [6].

This assignment can be achieved with neural networks based on Geometric Data Transformations, using algorithms of combined approximation of the surface of the response. For this purpose, there is a need to create new training methods of neural-like structures with the use of combined data approximation of the surface of the response. Also, there is a need to analyze and research the chosen algorithm, in which training and predicting errors will be the smallest.

II. THEORETICAL BASIS OF TRAINING METHODS

It is known that neural networks are not programmed in the literal sense of the word, but learn. Ability to learn is one of the main advantages of neural networks in the traditional trivial algorithms. Technically, the learning is to find the coefficients of the relationship between neurons. In the learning process, the neural network is capable of detecting complex interdependencies between input and output data, as well as generalization [7]. This means that in the case of successful learning, the network will be able to return the correct result based on data that were missing in the training sample, and also on incomplete, partially distorted data.

Every year new methods of ANN learning are explored, including for predicting data. The tasks of learning artificial neural networks and data prediction are focused on finding the differences between predicted and testing data, using the search of prediction error [8]. If the error is the smallest, then the result is considered more precise, so the method is more efficient, and the artificial neural network is more reliable.

In the research, the real task of predicting of electricity consumption is considered using training and testing data samples, the parts of which can be seen in the Figure 1.

Matrix for training

	x1	x2	x3	x4	x5	x6	x7	x8	x9	x10	x11	y
1	0,992160	0,854419	1	0	10	0	0	0	11,4	84	0,969444	266067,7054
2	0,992923	0,851830	0	0	30	0	0	0	14,8	88	0,858333	399213,7541
3	0,993650	0,849284	0	0	20	0	0	0	13,7	94	1,344444	308883,6862
4	0,994342	0,846781	0	0	10	0	0	0	16,2	98	0,288889	246431,2379
5	0,994997	0,844322	0	0	50	0	1	0	14,4	84	0,352778	455089,7725
	...											
365	0,990535	0,857050	0	0	60	0	0	0	14,10	83,0	0,666667	459405,0804

Matrix for testing

	x1	x2	x3	x4	x5	x6	x7	x8	x9	x10	x11	y
1	0,991364	0,854419	0	0	40	0	0	1	10,8	91	1,313889	464373,0739
2	0,992160	0,851830	0	0	20	0	0	0	11,4	99	0,840000	316854,1401
3	0,992923	0,849284	1	0	10	0	0	0	7,9	87	0,561111	239680,2697
4	0,993650	0,846781	1	0	10	0	0	0	8,5	83	0,519444	242339,7119
5	0,994342	0,844322	0	0	50	0	1	0	10,5	89	0,497222	455924,5373
	...											
214	0,759874	1,243905	0	1	30	1	0	1	-7,1	96	0,011111	363715,8311

Figure 1. Training and testing data samples.

The matrix for training A consists of 365 vectors, which include the obtained data for the same number of days of the previous year. The matrix for testing B consists of 214 vectors describing the appropriate number of days for the next year for which prediction was performed in the testing mode. The vectors of both samples A and B include 11 input signals x_{ij}, which consist of the state of the electrical network, obtained from the telemetry data, and one output y_i , which shows the daily values of the consumed electricity.

The task of prediction is made by using linear type of neural-like structures with geometric data transformations [9], where the combined approximation of the surface response is done in the hyperplane form. Linear neural-like structure with geometric data transformations provides a bit higher accuracy and simultaneously higher learning speed compared with the multi-layer perceptron [10].

The selected task is performed by using regression analysis examining the dependence of one variable Y_x from several independent variables x_1, x_2, ... x_i in a particular place and time. Regression analysis is based on the constructed regression equation (1) and determines the contribution of each independent variable in the variation of the investigated (predicted) dependent variable [11].

The regression equation (1) shows how the output feature (Y_x) changes in average, influenced by changes in factor variables (x_i). In general, the regression equation can be represented as follows:

$$Y_x = f\ (x_1, x_2, \ldots, x_n), \qquad (1)$$

where Y_x – dependent variable;

x_i – independent variables (factors).

The main task of regression analysis is to determine the impact of factors on the output indicator. First of all, for this purpose, the equation of relationship is chosen [12], which corresponds to the nature of the analytical stochastic dependence between investigated features. The simplest equation of a straight line (2), which describes the linear relationship between factor and effective features, has the following form:

$$Y_x = a_0 + a_1 x, \qquad (2)$$

where Y_x – dependent variable, which is predicted (effective characteristic);

a_0 – open member of the equation;

a_1 – coefficient of the regression;

x – independent variable (factor characteristic) used to determine the dependent variable.

There are several approximation methods, such as: numerical, linear, kernel-based, viscosity and other approximation techniques for solving various types of mathematical problems. Linear approximation is an approximation of a general function using a linear function (more precisely, an affine function). This approximation method is widely used in the method of finite differences to produce first order methods for solving or approximating solutions to equations.

In many cases of prediction, the linear approximation methods are used, since most of real processes in business and economics are characterized by linear models. But not always the accuracy of approximation by linear methods is suitable, so, to increase accuracy, combining different methods are used.

III. THE DESCRIPTION OF DEVELOPED METHODS

Previously, several developed methods of combined approximation of the surface response were investigated. Experiments with several clustering variants were performed to achieve better results and more accurate prediction [13]. Obtained prediction errors were compared in several methods:

- the model of auto-regression with a moving average has the prediction error is the highest one and is 10.9%;
- multilayer perceptron has the prediction error is 4.2%;
- the artificial neural network of the model of geometric transformations has an error 4.19%.

It was described that the average results of two methods are 3.69% and 3.44%, and it is proved that one of the developed methods with a certain number of clusters results with an error of 1% less than prediction without using the combined approximation of the surface response.

To achieve even more accurate and at the same time fast result, the task of creating and analyzing new methods of combined approximation of the surface response was determined, therefore some new algorithms of combined data approximation were created and investigated.

Since the selection of algorithms for using in the combined approximation depends on the data peculiarities, experiments with several variants of clustering were performed in the discovering the best combination of methods for better results and more accurate prediction.

Among the large number of existing methods of clustering data, one of the most frequently used methods is the k-means method. This method differs in that the number of clusters is known from the beginning and they are determined by the number *k* [14]. This method is used in the research, because it is easy to implement and modify.

The k-means algorithm divides the input set of values into clusters so that the average values in clusters are maximally different [15]. In the research used the algorithm k-means that divided into the following steps:

a) Determine centers of each cluster using formula (3):

$$c_{(x,y)} = \frac{\sum_i m_i x_i}{\sum_i m_i}, \qquad (3)$$

where c – points of the vector with centers of masses.

b) Determine the affiliation of objects to clusters. Find the Euclidean distance d by the formula (4):

$$d(x,y) = \sqrt{\sum_{i=1}^{n} (x_i - y_i)^2}, \qquad (4)$$

where x_i – point from vector of the training matrix,

y_i – point from the vector with centers of masses.

Each of the points of the set belong to the cluster, the distance to which is minimal [13].

c) If in the previous steps no point has passed to another cluster, or if the maximum number of iterations is made, stop working. Otherwise, looking for new cluster centers.

For example, Figure 2 shows the result of clustering 365 vectors from the training matrix A for 10 clusters. This figure shows how many vectors belongs to a particular cluster after passing a certain number of iterations.

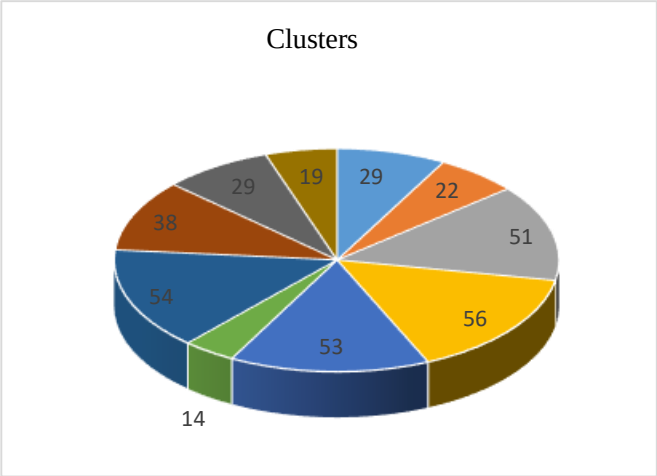


Figure 2. Clustering by k-means method for 10 clusters

The first step that needs to be performed for all methods of combined approximation is the normalizing of input vectors X_j.

Consequently, the result of this phase is the normalized training A and testing B data samples.

The next steps will describe established methods of the combined approximation.

Method 1 consists of the following steps:

1) Form a united C data sample from the normalized training A and testing B data samples, where C=A+B (365 + 214);
2) Cluster a united matrix with k-means method for 11 benchmark inputs for k compact sets of points, where k is the number of clusters;
3) Divide the united sample back to the training and testing matrices with known vectors relations to certain clusters;
4) Expand both matrices with adding to the inputs of each vector of the studied samples:

a) *k* additional inputs, where the extra input in vector assigns 1, if the vector belongs to a defined cluster, and the other inputs assign zeros;

b) *c* additional inputs by the formula (5):

$$c_i = \frac{1}{\left(1+x_i^2\right)}, \qquad (5)$$

where x_i – initial inputs of the matrix.

5) Learn and apply neural network by finding testing and prediction MAPE errors - mean absolute percent errors for learning and prediction.

Next two methods are based on the Method 1, so include previous 1-4a steps.

The investigated Method 2 is composed of the following:

1) After adding *k* inputs using previous method, extend training and testing matrices with adding *l* additional inputs to every vector of the studied samples, using formula (6):

$$l_i = \frac{x_i}{\left(1+x_i^2\right)}, \qquad (6)$$

where x_i – primary inputs of the matrix;

2) Learn ANN with enhanced data samples, which vectors contain $11+k+l$ inputs and 1 output, and apply neural network with finding MAPE errors.

The Method 3 introduces the next steps:

1) After adding *k* inputs in Method 1, replace 11 first-source inputs with 22 new inputs ($c+l$), using formulas (5) and (6) from previous methods
2) Learn ANN with extended data samples, which vectors contain $k+c+l$ inputs and 1 output;
3) Apply neural network with finding MAPE errors.

Described algorithms was performed a certain number of times to find MAPE errors for various specified number of clusters. Also, errors were found to compare the results of the developed methods and to define which method has less error, so is more accurated.

Training and prediction errors found during execution of the developed Method 3 are smaller than errors found in the performance of Methods 1 and 2. Investigated errors are shown in the Table 1.

Table 1. Results of developed Methods 1-3

	Method 1		Method 2		Method 3	
Number of clusters	Training error,%	Prediction error,%	Training error,%	Prediction error,%	Training error,%	Prediction error,%
k=10	2,78	3,17	2,53	2,92	2,91	2,91
k=15	2,69	3,09	2,5	2,94	2,48	2,93
k=20	2,44	3,02	2,23	2,78	2,23	2,77
k=25	2,41	3,1	2,19	2,84	2,19	2,83

Analyze the following two methods of the combined approximation. These methods experimenting with the same steps as in the previous three methods, but in a different order.

So, for the Method 4 perform the following steps:

1) Extend training matrix with adding *c* extra inputs to each vector, using function in formula (5) of the Method 1;
2) Clustering the training matrix by the k-means method by 22 inputs on *k* compact sets of points, where *k* is the number of clusters;
3) Find the centers of masses of each cluster and the Euclidean distance d by formulas (3) and (4) severally, described earlier;
4) Each vector from the testing sample of data relates to that cluster, where the Euclidean distance to the vectors centers of mass is the smallest. Thus, all the vectors of the training matrix are clustered;
5) Add *k* extra inputs to each vector of the training and testing samples, where *k* is the number of selected clusters;
3) Learn ANN using extended training data samples, where vectors have 22 *k* inputs and 1 output, and apply neural network by finding prediction MAPE errors.

The last investigated Method 5 consists of the following steps:

1) Extend training matrix with adding *l* extra inputs to each vector, using function in formula (6) of the Method 2;
2) Do steps from #2 to #6 from the Method 4.

In Table 2, compare the results of implementation of the Method 3, where testing and prediction errors are the smallest among all the previous investigated methods, and Methods 4 and 5.

Table 2. Results of researched Methods 3-5

	Method 3		Method 4		Method 5	
Number of clusters	Training error,%	Prediction error,%	Training error,%	Prediction error,%	Training error,%	Prediction error,%
k=10	2,91	2,91	2,63	3,03	2,43	2,73
k=15	2,48	2,93	2,49	3,15	2,39	2,76
k=20	2,23	2,77	2,48	3,23	2,21	2,74
k=25	2,19	2,83	2,45	3,13	2,21	2,81

Thus, comparing all methods 1-5, testing and prediction errors using 20 clusters are the lowest for all methods on a permanent basis. Summing up, errors received by using the developed Method 5 are the smallest among the errors detected by using all other methods.

III. CONCLUSIONS

Characteristics of methods of combined approximation are analyzed. The results of investigation Neural-like structures with Gradual Geometric Transformations using the combined approximation of the surface response is presented. The effectiveness of the proposed approach for predicting data is confirmed.

It is proved that the investigated algorithms of combined approximation with additional inputs extension using functions complement and improve the methods of combined approximation.

The results of prediction using developed algorithms of combined data approximation are shown. The results of the performed methods are compared and it is stated that least errors of learning and predicting are based on method 5. Specifically, using twenty clusters, the error of learning is 2.21%, and the prediction error is 2.74%.

Consequently, the use of combined approximation provided the creation of neural network models of small structural complexity, with high accuracy of application on data that were not used in the training.

Proposed method for predicting data based on the Neural-like structures with Gradual Geometric Transformations can be used in huge amount of science aspects for different purposes.

Next investigations should be based on deeper researching of developed method with the use of Neural-like structures in different spheres and to find better results.

REFERENCES

[1] K.V. Murphy “Machine Learning: A Probablistic Perspective”, Massachusetts Institute of Technology, Library of Congress Cataloging-in-Publication Information, 2012.

[2] R. Kruse, C. Borgelt, F. Klawonn, C. Moewes, and M. Steinbrecher “Computational Intelligence: A Methodological Introduction”, Springer, London, 2016, doi 10.1007/978-1-4471-7296-3_1

[3] H.B. Nezhad, M. Miri, and M. Ghasemi, “New neural network-based response surface method for reliability analysis of structures”, Neural Computing and Applications, Springer, London, 2017, pp. 1-15. doi: 10.1007/s00521-017-3109-2

[4] J. Stastny, and V. Skorpil, “Analysis of Algorithms for Radial Basis Function Neural Network”, In: Bestak R., Simak B., Kozlowska E. (eds) Personal Wireless Communications, The International Federation for Information Processing (IFIP), vol 245, Springer, Boston, MA, 2007, pp.54-62. doi: 10.1007/978-0-387-74159-8_5

[5] R. Tkachenko, “Neural network means of artificial intelligence: a tutorial”, NU “LP”, 2017.

[6] V. Kolmykov Comparative analysis of the statistical model and the neural network of reverse distribution in the prediction task, Applied Informatics, Litrus, no. 6 (30), 2010, pp. 111-118.

[7] S. Haykin Neural Networks: A Comprehensive Foundation (2nd Edition), Williams, 2006. ISBN 0-13-273350-1

[8] E. Boj, T. Costa, J. Fortiana “Prediction Error in Distance-Based Generalized Linear Models”, In: Palumbo F., Montanari A., Vichi M. (eds) Data Science. Studies in Classification, Data Analysis, and Knowledge Organization, Springer, Cham, 2017, pp. 191-204. doi: 10.1007/978-3-319-55723-6_15

[9] U. Polishchuk, P. Tkachenko, R. Tkachenko, I. Yurchak, Features of the auto-associative neurolike structures of the geometrical transformation machine (GTM), 5th International Conference on Perspective Technologies and Methods in MEMS Design, Zakarpattya, 2009, pp. 66-67.

[10] R. Tkachenko, I. Yurchak, and U. Polishchuk, “Neurolike networks on the basis of Geometrical Transformation Machine”, 2008 International Conference on Perspective Technologies and Methods in MEMS Design, Polyana, 2008, pp. 77-80. doi: 10.1109/MEMSTECH.2008.4558743

[11] N. Matloff, “Statistical Regression and Classification: From Linear Models to Machine Learning”, CRC Press, Davis, 2017.

[12] Y. Li, J. Liu, Q. Bao, W. Xu, R. Sadiq, and Y. Deng, “A new method of mapping relations from data based on artificial neural network”, nternational Journal of System Assurance Engineering and Management, Springer, vol. 5, 2014, pp. 544-553.

[13] O. Mishchuk, P. Vitynskyi, “Artificial neural network with combined aproximation surface reflection”, Naukovi Visti NTUU KPI, Kyiv, 2018, (2), 18— 24. doi: 10.20535/1810-0546.2018.2.129022

[14] U. Volosiuk, “Analysis of clustering algorithms for data analysis tasks”, Collection of scientific works of the Military Institute of Kyiv National Taras Shevchenko University, vol. 47, 2014, pp. 112-119.

[15] J. Wu, “Advances in K-means Clustering”, Springer, Berlin, Heidelberg, 2012. doi: 10.1007/978-3-642-29807-3

[16] R. Tkachenko, A. Doroshenko, I. Izonin, Y. Tsymbal, and B. Havrysh, “Imbalance Data Classification via Neural-like Structures of Geometric Transformations Model: Local and Global Approaches” In: Z.B. Hu, S. Petoukhov (eds) Advances in Computer Science for Engineering and Education (ICCSEEA2018), Advances in Intelligent Systems and Computing, Springer, Cham, 2018.

Аналіз інструментів для розробки мобільних ігор

Філімончук Тетяна Володимирівна,
Ващенко Андрій Сергійович

Харьковский национальный университет радиоэлектроники, пр. Науки 14, Харьков, 61166, Украина,
tetiana.filimonchuk@nure.ua, johnrocket.1996@gmail.com

Анотація. *У доповіді проведено аналіз можливостей, функціоналу, переваг та недоліків сучасного набору програмних компонентів та візуальних інструментів, який дозволяє створювати і запускати інтерактивні додатки з графічним забезпеченням в реальному часі (Unreal Engine та Unity). Також розглянуто середовище розробки та сумісність програмного коду з більшістю сучасних платформ та операційних систем (Android, iOS, Linux, Mac OS, Windows, PlayStation 4, PSP, Xbox One, PS Vita тощо).*

Ключові слова: *Unreal Engine, Epic Games, Blueprints, Unity, Autodesk Maya.*

I. Вступ та постановка задачі

На сьогоднішній день відеоігри посідають одну із невід'ємних частин сучасного життя. Завдяки технологіям, що постійно розвиваються, можливо грати в улюблені відеоігри будь де. Цей процес можливо порівняти з переглядом фільму або серіалу, але над розробкою фільмів працюють сотні людей, а завдяки сучасним технологіям відеогру може створити одна людина. Метою доповіді є аналіз існуючих технологій (Unreal Engine та Unity), які можливо використовувати для розробки мобільних ігор.

II. Рішення проблеми та результати

Можливості Unreal Engine 4 (UE4) дозволяють створювати та редагувати елементи 3D анімації, спецефекти у відеоіграх та кінофільмах, розробляти різноманітні програми для розвитку дітей та підлітків. Програмний код додатку сумісний з більшістю сучасних платформ та операційних систем.

Unity – це один із найкращих ігрових інструментів в галузі розробки 2D та 3D ігор, який має безкоштовну версію та охоплює 24 платформи (мобільні пристрої, VR, ПК), консолі та веб-платформи) [1]. UI-редактори для створення рівнів в обох продуктах мають браузери контенту для ассетів, скриптів та інших файлів проекту [2]. Ігрові об'єкти можна перетягувати в область сцени і таким чином додавати в її ієрархію. Об'єкти в редакторі сцени змінюються за допомогою інструментів переміщення, повороту та масштабування – вони схожі в обох двигунах. Властивості Unity-об'єктів відображаються в Inspector, а UE4 – в частині Details. В обох продуктах є стейт-машини [1,2], які визначають переходи з одного стану ассета в інший (у UE4 – Persona, у Unity – Mecanim).

У UE4 анімацію можливо редагувати, в Unity – практично немає такої можливості, особливо погано справа йде з рухами персонажів, тому для їх реалізації краще обирати програми на кшталт Blender або Autodesk Maya, а результат імпортувати в вигляді додаткових файлів до проекту.

У UE4 вбудований постпроцесінг, тобто до сцени можливо застосовувати bloom-ефект, тонування та антиалиасинг, як глобально, так і до окремих її частин. У Unity є стек постпроцесінгу, який можна завантажити з магазину ассетів.

В разі обрання інструменту розробки мобільних ігор слід враховувати технічні можливості реальних сматфонів та ПК. На рисунку 1 зображено кількість кадрів у секунду (FPS) при порівнянні однакових сцен на Unity та UE4.

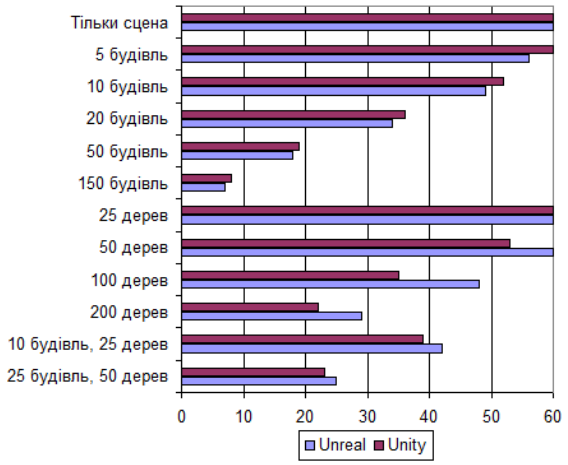


Рис. 1. Порівняння сцен на Unity та UE

Результати, які наведено на рисунку 1, приблизно однакові, але UE4 частіш показує кращій результат, якщо мова йде про більшу кількість однакових об'єктів, тому що він добре вміє їх систематизувати.

Для програмування Unreal Engine 4 використовує мову C++, яка не усім подобається через складність та тривалість процесу компіляції. Але завдяки Blueprints можна досягти приблизно тих самих результатів, що і з C++. У свою чергу Unity використовує C# та UnityScript. API та його концепт схожий з аналогічним у UE4.

III. Висновки

У кожного із розглянутих інструментів є свої сильні та слабкі сторони для різних задач. Unity підійде новачкам в той час як Unreal – це продукт строго для професійних розробників. Набір функцій Unreal Engine краще підходить для тривимірних проектів, в той час як у Unity величезний послужний список на мобільних пристроях. Якщо необхідно розробити мобільну гру або VR-проект має невеликий бюджет – слід обрати Unity. У випадку, коли треба розробити дорогу гру для консолей з досвідченою командою розробників – в якості рішення слід обрати Unreal Engine 4.

Перелік літератури

[1] Michael Dawson, "Beginning C++ Through Game Programming",Cengage Learning PTR, 2010, 352 p.
[2] Jessica Plowman, "3D Game Design with Unreal Engine 4 and Blender",Packt Publishing, 2016, 252 p.

Применение голограмм

Heletto Violetta Maksimovna

Kharkiv National University of Radio Electronics, 14 Nauky Ave, Kharkiv UA-61166, Ukraine, violetta.heletto@nure.ua

Abstract. *A hologram is an image that appears to be three dimensional and which can be seen with the naked eye. Holography is the science and practice of making holograms. Typically, a hologram is a photographic recording of a light field, rather than an image formed by a lens. The holograpic medium, i.e., the object produced by a holographic process (which itself may be referred to as a hologram) is usually unintelligible when viewed under diffuse ambient light. It is an encoding of the light field as an interference pattern of variations in the opacity, density, or surface profile of the photographic medium. That is, the view of the image from different angles represents the subject viewed from similar angles.*

Современного человека уже не удивить 3D принтером, видео-, аудио- связью с любой точкой мира, пультом управления приборов на расстоянии, мобильной связью, камерой Kinect, GPS-навигацией, NFC-технологией и многими другими вещами, которые вошли в нашу повседневную жизнь. Но наука не стоит на месте и постоянно развивается. Показ фильмов в 2D технологии уже мало кому интересен, разговоры по Skype, Viber, WhatsApp и др., не говоря уже про обычную мобильную связь медленно теряют свою актуальность.

Человечеству постепенно становится возможным изобретение голограмм. Благодаря таким свойствам световых электромагнитных волн как интерференции, дифракции, флуоресценции, внешнего фотоэффекта это становится все более и более реализуемым. На данный момент существует несколько теорий и разработок данного приспособления, но к чему-то конкретному и работающему еще не пришли. В основном они все построены на использовании лазеров, а именно использовании вышеперечисленных свойств света. Направляя лазер в место в пространстве можно добиться появления голограммы. По сути, картинка должна появиться при возбуждении электронов с помощью направленных на них фотонов, что возможно благодаря явлению электромагнитных световых волн (внешнего фотоэффекта и флуоресценции). Фотоэффект — это явление испускания электронов веществом под действием света. Энергию фотона при этом можно вычислить по формуле:

$$E = h\nu = h \cdot \frac{c}{\lambda},$$

где $h = 6{,}6 \cdot 10^{-34}$ Дж*с – постоянная Планка, ν – частота света, λ – длина световой волны, $c = 3 \cdot 10^{8}$ м/с –скорость света в вакууме.

Флуоресценция – это физический процесс, при котором происходит выделение излучения, обычно света, из вещества, атомы которого получили избыточное количество энергии при бомбардировке частицами, как правило, ультрафиолетового излучения электронов. Длина волны, необходимая для возбуждения электрона, зависит от типа флуоресцентного материала. Излучаемый свет имеет в N раз меньшую длину волны, когда N фотонов поглощаются одновременно. Этот эффект возникает при использовании лазера относительно низкой интенсивности (достаточно энергии от нДж до мДж).

Также, существует возможность изменять цвет передаваемого изображения. Так как цвет волны на прямую зависит от длины волны. Чем больше длина волны, тем более красным будет цвет картинки и чем короче, тем более синим (фиолетовым). И таким образом с помощью регулировки частоты волны можно и изменять цвет передаваемого изображения. Если подавать волны несколькими лазерами для транслирования одной картинки, то ее и вовсе можно сделать разноцветной.

Изменять расстояние, на котором будет размещено изображение относительно лазера можно про помощи пространственного модулятора света, который используется в проекторах и чаще всего управляемый компьютером. Это устройство представляет из себя некий объект, который накладывает определённую форму пространственной модуляции на луч света. Как правило, пространственный модулятор света изменяет интенсивность светового пучка. Тем не менее, также возможно изготовление и устройств, которые модулируют фазу пучка, или интенсивность и фазу одновременно.

Есть сложность в том, какое изображение будет транслироваться. Для того чтобы показывать объемную фигуру, она должна быть в устройстве или передаваться на него. Можно использовать много камер, которые будут снимать и оцифровывать изображение с множества сторон и таким же объемным его будет транслировать лазер. Таким образом, к примеру, во время разговора, собеседники смогут видеть друг друга как в живую, полностью объемными. Это так же вызывает сложности в нахождении помещения, которое будет оснащена камерами. Но это добавляет дополнительные возможности для голографических лазеров и их применении.

Однако при использовании лазера, существует опасность попадания его лучей на кожу и слизистую оболочку глаз. Это может быть достаточно опасным и порождать раны на коже, доходя до ожогов разных степеней. Не говоря уже, про ухудшение зрения при попадании луча лазера в глаза. Для того чтоб избавится от этого негативного дефекта стоит попробовать увеличить частоту электромагнитной волны. Благодаря тому, что воздействие на ткани будет проходить крайне маленькое количество времени, опасность получения ожогов значительно уменьшится.

Применения данное приспособление может найти в нашей обыденной жизни. Если оно войдет в обиход, то может использоваться буквально повсюду. Это, и телевидение, и видеосвязь, и видеоигры, и даже медицина и другие различные отросли других наук. Любая графическая информация может быть выведена с помощью голограмм, отображая объем и реальный размер фигуры. Это позволит получать максимально качественное изображения и улучшит многие отросли нашей жизни.

Інформаційна технологія управління розподіленим обчислювальним процесом

Волк Максим Олександрович,
Філімончук Тетяна Володимирівна,
Рисухін Максим Володимирович

Харьковский национальный университет радиоэлектроники, пр. Науки 14, Харьков, 61166, Украина,

maksym.volk@nure.ua, tetiana.filimonchuk@nure.ua, risuhin.max@gmail.com

Анотація. *У доповіді обговорюються базові етапи інформаційної технології управління розподіленим обчислювальним процесом. Відмінні особливості технології: використання апріорної та статистичної інформації щодо програмних завдань та обчислювальних ресурсів, врахування гетерогенної природи завдань та ресурсів, наявність етапу імітаційного моделювання, паралельне застосування методів аналізу та вибору плану призначення завдань за обчислювальними ресурсами, підтримка функціональної стійкості обчислювального процесу. Наведено результати впровадження інформаційної технології у систему моделювання розподіленого обчислювального процесу.*

Ключові слова: *інформаційна технологія, система управління розподіленими обчислюваннями, схема розподілу, ефективність розподілу, зв'язність та обчислювальна складність завдання.*

I. Вступ та постановка задачі

Інформаційна технологія застосовується для зниження трудомісткості процесів використання інформаційних обчислювальних ресурсів і об'єднує сукупність методів та програмних засобів, що згруповані в єдиний комплекс. Цей комплекс спрямовано на збір, зберігання, обробку та передачу даних [1].

В системах, які орієнтовані на розподілені обчислення, вхідними даними можуть виступати спеціалізовані файли вхідної інформації, конфігураційні файли, моделі та методи розподілу вхідних завдані на обчислювальні ресурси, що надходять на вхід планувальника (брокеру), який виступає центральним компонентом розподіленої системи. Планувальник здійснює побудову розкладу використання обчислювальних ресурсів розподіленої системи, який в подальшому використовується системою управління розподіленими обчислюваннями для направлення вхідних завдань на обчислювальні ресурси.

Метою даної роботи є розробка інформаційної технології управління розподіленим обчислювальним процесом, яка націлена на формування нової інформації про програмні компоненти, які зберігаються в базі даних. В подальшому зібрана інформація може бути використана модулям системи управління розподіленими обчислюваннями для оцінки схем призначення

II. Рішення проблеми та результати

Розроблена технологія управління розподіленим обчислювальним процесом передбачає наступні етапи.

На першому етапі від користувача надходить вхідне завдання, яке приведено до відповідного виду:

$$n_1 = \left\{ Z_i, \bigcup_{j=1}^{N} \mathrm{Pr}_j^i, D_j^i, W^i \right\}, \quad (1)$$

де Z_i – конфігураційний файл опису завдання [1]; Pr_j^i – програмні компоненти завдання; D_j^i – вхідні файли даних; W^i – вихідні файли результатів виконання завдання.

Наступні два етапи (2 та 3) працюють паралельно. На другому етапі проходить ініціалізація вхідних даних про розподілені програмні компоненти, після чого завдання надходить у чергу очікування для подальшого розподілу. По закінченні даного етапу здійснюється перехід до п'ятого етапу.

На третьому етапі проводиться перевірка наявності в базі даних інформації про попередні розподіли вхідного завдання на обчислювальні ресурси розподіленої системи. Якщо база даних має необхідні дані, то здійснюється їх завантаження до системи та перехід до п'ятого етапу, інакше – перехід до четвертого етапу.

На четвертому етапі здійснюється запуск програмних моделей, які відповідають за моделювання обчислювального процесу, а також проводиться аналіз поведінки програм в завданні за різними методами синхронізації [2,3,4]. Результатом роботи цього етапу є вектор який відображає зміну в часі характеристик обчислювальних ресурсів:

$$O = < I, \overline{T_i}, \overline{TR_i}, \overline{TR_i^n}, \overline{TP_i^n}, \overline{V_i}, \overline{V_i^n} >, i = \overline{1, N}, \quad (2)$$

де I – кількість кроків моделювання; $\overline{T_i}$ – модельний час; $\overline{TR_i}$ – реальний час виконання компонентів завдання; TP_i^n – час простою ресурсу; $\overline{V_i}$ – обсяги пам'яті, яка містить програмні компоненти та завдання, n – індекс, що встановлює належність до відповідного програмного компоненту завдання.

На п'ятому етапі здійснюється формування множини схем призначення обчислювальних ресурсів за допомогою стандартних методів розподілу, тобто розподіл програмних модулів на доступні ресурси розподіленої системи [5]. У якості результату роботи наведеного етапу виступає множина схем призначення. Ефективність розподілу вхідних завдань за обчислювальними ресурсами визначається або мінімізацією часу, який необхідний для імітації, або вартістю використання доступних обчислювальних ресурсів.

На шостому етапі здійснюється аналіз розподілених програмних компонентів за допомогою трьох методів: методу порівняння ефективності розподілення за максимальним просуванням модельного часу, методу оцінки можливості розподілу програмних компонентів на основі динамічної зміни обсягів віртуальної пам'яті та методу отримання простою обчислювальних ресурсів під час використання різних методів синхронізації розподілених програмних компонентів. Результатом роботи цього етапу є схема призначення, яка має найменший час виконання. Отримані результати аналізу застосування методів оцінки схем розподілу заносяться до бази даних для наступного використання. Кожен з експериментів має свої атрибути, що дозволяють здійснити асоціативний пошук даних [6, 7].

На сьомому етапі реалізується фізичний розподіл локальних програмних компонентів на доступні обчислювальні ресурси розподіленої системи по результатам обраної на шостому етапі схеми розподілу.

Восьмий етап відповідає за підтримку розподіленого обчислювального процесу. В ході його виконання здійснюється моніторинг, підтримка функціональної стійкості [8,9], збір динамічних параметрів та внесення їх до бази даних для подальшого аналізу та використанню.

На дев'ятому етапі результати, які були отримано в ході виконання вхідного завдання, передаються користувачеві у вигляді множини результатів (файли виконання завдання, статистичні дані по завданню), які в подальшому допоможуть, у випадку необхідності, провести аналіз виконання цього завдання на доступних обчислювальних ресурсах розподіленої системи.

Для дослідження запропонованої інформаційної технології управління обчислювальним процесом була проведена низка експериментів. Спочатку, враховуючи вимоги (1) сформована множина вхідних завдань, яка враховує зв'язність його окремих частин та складність його виконання. Також сформовані множини програмних модулів, що моделюють обчислювальні ресурси та канали обміну даними, реалізують методи розподілу ресурсів та забезпечення функціональної стійкості.

Реалізовані згідно інформаційної технології програмні модулі, було інтегровано в середовище імітаційного моделювання. В результаті експериментів отримано час виконання кожного пулу завдань, який відображено на рис. 1. Аналіз результатів підтверджує зменшення часу виконання завдань з різними характеристиками при використанні запропонованої технології управління обчислювальним процесом.

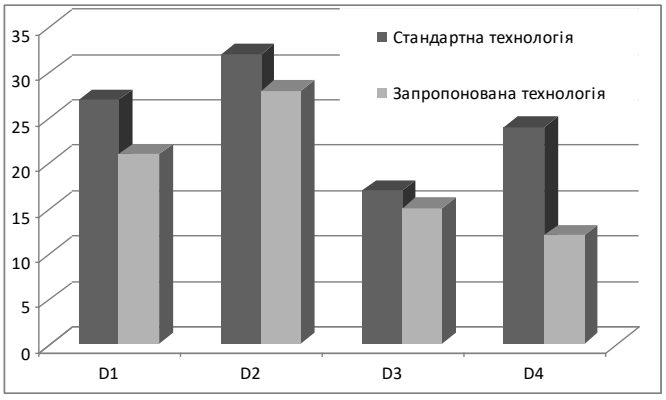


Рисунок 1. Ефективність застосування наведеної технології

III. Висновки

Запропонована інформаційна технологія управління обчислювальним процесом в розподілених комп'ютерних системах реалізована за допомогою дев'яті етапів. Другий та шостий етапи, наведеної технології управління розподіленим обчислювальним процесом, дозволяють формувати інформацію, яка в подальшому буде використовуватися на етапі розподілу програмних модулів за доступними обчислювальними ресурсами розподіленої системи.

Загалом, впровадження інформаційної технології управління розподіленим обчислювальним процесом дозволило скоротити час виконання завдань, які надходять на вхід розподіленої системи, від 7 до 48 процентів (рис. 1). Як можна бачити з рисунку, ефективність застосування наведеної технології залежить від типу завдань [1]. В роботі наведено результати вибору системи управління для чотирьох типів завдань, які відрізняються взаємовідношенням обчислювальної складності та зв'язністю програмних компонентів в завданні (D1 – мала зв'язність, велика обчислювальна складність; D2 – велика зв'язність, велика обчислювальна складність; D3 – мала зв'язність, велика обчислювальна складність; D4 – мала зв'язність, мала обчислювальна складність). Плани розподілу завдань за ресурсами отримані з використанням стандартного та модифікованого методу Backfill [2].

Перелік літератури

[1] T. Filimonchuk, M. Volk, I. Ruban, V. Tkachov, "Development of information technology of tasks distribution for grid-systems using the GRASS simulation environment", Eastern-European Journal of Enterprise Technologies. Information and controlling system. Vol.3/9 (81), 2016, pp. 45–53.

[2] М. А. Волк, М. А. Филимончук, Муаз Ал Шиблак, Р. Н. Гридель, "Анализ распределенных имитационных моделей с консервативными алгоритмами синхронизации", Збірник наукових праць ХУПС, 2012, вип. 1(30), С. 95–98.

[3] М.А. Волк, "Журнализация состояний программных распределенных мооделей и ее использование в оптимистических алгоритмах синхронизации", Збірник наукових праць ХУПС, 2010, вип. 1 (23), С.104–107.

[4] Д. А. Гавриш, С. Н. Саранча, М.А. Волк, "Метод распределения задач с учетом затрат синхронизации при параллельном моделировании сложных цифровых систем в гетерогенной вычислительной среде", Системи обробки інформації, 2015, вип. 5, С. 122–128.

[5] Т. В. Филимончук, М. А. Волк, "Разработка модифицированного метода обратного заполнения Backfill для консервативного резервирования", Системи обробки інформації, Харків: ХУПС, 2017, №1 (147), С. 33–37.

[6] V. Mukhin, Yu. Romanenkov, Ju. Bilokin. "The Method of Variant Synthesis of Information and Communication Network Structures on the Basis of the Graph and Set Theoretical Models", International Journal of Intelligent Systems and Applications (IJISA), vol. 9, №11, 2017, pp. 42–51.

[7] I. Ivanisenko, M.Volk, "Simulation methods for load balancing in distributed computing," in Proceedings of IEEE East-West Design & Test Symposium (EWDTS'2017), Novi Sad, Serbia, September 27 – October 2, 2017, pp. 690–695.

[8] М.О. Волк, "Обеспечение функциональной устойчивости систем распределенного имитационного моделирования. Матеріали першої міжнародної науково-технічної конференції «Комп'ютерні та інформаційні системи і технології». Збірка наукових праць. Харків: ХНУРЕ. 2017. Р. С. 15.

[9] I. Ruban, M. Volk, T. Filimonchuk, I. Ivanisenko, M. Risukhin, Y. Romanenkov, "The Method for Ensuring the Survivability of Distributed Computing in Heterogeneous Computer Systems", 5th International Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S&T), Kharkiv, Ukraine, October 9-12, 2018, P. 233–2

Стратегії управління групою мобільних об’єктів

Додонов Олександр Георгійович[1]
Горбачик Олена Семенівна[2]
Кузнєцова Марина Глібівна[3]

[1]*Інститут проблем реєстрації інформації НАН України, в.Шпака, 2, Київ 03113, Україна, dodonov@ipri.kiev.ua*
[2] *Інститут проблем реєстрації інформації НАН України, в.Шпака, 2, Київ 03113, Україна, ges@ipri.kiev.ua*
[3] *Інститут проблем реєстрації інформації НАН України, в.Шпака, 2, Київ 03113, Україна, margle@ipri.kiev.ua*

Анотація. *Доповідь присвячено оцінюванню стратегій групового управління мобільними технічними об’єктами, що функціонують в середовищі, де наявні непередбачувані вражаючі впливи. Пропонується при прийнятті рішень щодо стратегії управління враховувати показники живучості групи.*

Ключові слова: *стратегія управління, група мобільних технічних об’єктів, показник живучості групи.*

I. Вступ

Завдання управління групою мобільних технічних об’єктів є актуальним для багатьох сфер, зокрема, при виконанні робіт у місцях природних або техногенних катастроф, бойових конфліктів, розвідки територій і акваторій тощо. Застосування групи технічних об’єктів є більш ефективним при виконанні складних завдань в екстремальних умовах функціонування, ніж одного надскладного вартісного об’єкта. До того ж питання функціональної стійкості до екстремальних умов функціонування можуть бути вирішені не за рахунок ускладнення інженерних і технічних рішень, а завдяки простому збільшенню чисельності групи. Мініатюризація електронних пристроїв дозволяє розв’язувати питання взаємодії мобільних технічних об’єктів за рахунок підвищення інтелектуальних можливостей окремого об’єкта.

Завдання управління мобільною групою технічних об’єктів в умовах наявності вражаючих впливів, що протидіють досягненню загальносистемної цілі, потребує, з одного боку, вирішення задачі управління взаємодією окремих об’єктів для досягнення групової цілі, а з іншого боку – забезпечення реалізації самих взаємодій засобами групи у реальному часі і з урахуванням змін, що відбуваються у середовищі їх функціонування. Нажаль немає визнаних достатньо узагальнених підходів і методик розв’язання цих задач, тому алгоритми управління формуються, виходячи з конкретних вимог прикладної сфери. Наявність перманентних змін параметрів середовища функціонування групи технічних об’єктів, непередбачуваність появи вражаючих впливів на них зумовлюють необхідність оцінки якості управління за показником живучості групи. Обрані стратегії, методи, алгоритми управління системою можуть як знижувати, так і підвищувати живучість групи, як системи.

II. Основна частина

У задачах управління рухом групи рух окремого об’єкта групи неважливий, необхідно визначити характеристики руху усієї сукупності об’єктів, що утворюють складну просторово-часову структуру. У разі ж управління рухом об’єкта у складі групи – важливими стають характеристики руху окремого об’єкта і його поведінки та взаємодія з іншими об’єктами групи.

Основною ціллю управління є забезпечення досягнення загальносистемної цілі групою технічних об’єктів, яку можна подати як систему [1]:

$$\Omega = \{O, E, G\},$$

де O – група (множина) технічних об’єктів, що утворюють відповідну просторово-часову структуру при функціонуванні системи, E – система каналів обміну інформацією, G – загальносистемна ціль функціонування.

У найбільш загальному вигляді окремий технічний об’єкт групи може бути поданий:

$$O_i = \langle E_{ij}, G_i, A_i, C_i, B_i \rangle,$$

де E_{ij} – матриця, що описує зв’язки об’єкта з іншими об’єктами групи, G_i – множина цілей об’єкта, до того ж $G = \bigcup_i G_i$, A_i – множина характеристик автономності, самоорганізації об’єкта, C_i – множина стратегій поведінки, B_i – база знань i-го об’єкта.

Показником живучості групи може слугувати середньозважена сума показників якості функціонування окремих об’єктів групи:

$$\Psi = \frac{1}{S}\sum_{i=1}^{S} z_i ,$$

де z_i характеризує функціональність окремого об’єкта групи.

Загальносистемну ціль, у більшості прикладних задач, визначає певний об’єкт (структура) більш високого рівня. Окремий об’єкт групи може пересуватись у просторі, виконувати обмін інформацією з іншими об’єктами групи щодо формування цілі, змін в умовах функціонування і поведінці.

Непередбачуваність середовища функціонування і наявність вражаючих впливів потребує, щоб у окремих об’єктів з групи (в залежності від ступеню інтелектуальності) була можливість самостійно формувати ціль на основі наявної бази знань окремого об’єкта, поточної інформації від інших об’єктів групи і з середовища функціонування.

Приналежність до групи вимагає від окремого об’єкта здатності до узгодження своєї поведінки з поведінкою інших об’єктів групи. Це відбувається завдяки обміну інформацією з іншими об’єктами групи, зокрема, щодо визначення повноважень, оповіщення про можливості дій, стан середовища, поточний стан інших об’єктів з групи, інформування про виконання чи неможливість виконання свого завдання тощо. Якість взаємодії та обміну інформацією в групі характеризується орієнтованістю, селективністю,

інтенсивністю, динамічністю, інформативністю та стійкістю взаємодії об'єктів групи.

Стратегії управління можуть вибудовуватись централізовано чи децентралізовано в середині групи або самостійно кожним об'єктом групи. Централізоване формування стратегії передбачає, що управління покладено на деякий «центр» (стаціонарний чи мобільний), що отримує і опрацьовує всю необхідну інформацію. У разі децентралізованого формування стратегії процес прийняття рішення й управління відбувається всередині групи і покладається на самі об'єкти. Між об'єктами управління відбувається активний обмін поточною інформацією та знаннями з баз даних об'єктів і результатами аналізу ситуації засобами й алгоритмами, що задіяні в окремих об'єктах. Об'єктивні конфліктні ситуації, що повинні виникати і безумовно виникають при колективному прийнятті рішень, значно ускладнюють реалізацію цього підходу. Основою розв'язання об'єктивних конфліктних ситуацій при колективному управлінні може бути єдина платформа знань у всіх об'єктів групи, яка дозволить робити однакові логічні висновки зі схожих передумов.

У разі, якщо об'єкти групи самі визначаються із стратегією, то відповідно кожний об'єкт групи приймає рішення самостійно, обмінюючись інформацією з іншими з групи і спираючись на власний досвід (переваги). Ця стратегія доцільна, коли кожний об'єкт групи виконує власну задачу і тим вносить особистий вклад у досягнення групової цілі. Задача окремого об'єкта є порівняно нескладною, оскільки він вирішує задачу оптимізації лише своїх дій у складі групи, не оптимізуючи дії всієї групи.

Будь-яка стратегія групового управління має забезпечувати мобільність об'єкта групи і узгодженість його дій з іншими об'єктами. Так, у групі безпілотних літальних апаратів (БПЛА) необхідно забезпечити політ по визначеним траєкторіям, виключаючи зіткнення БПЛА між собою. У разі централізованого управління, коли управління, наприклад, виконується оператором, виникає питання психофізичної здатності оператора реалізовувати одночасно управління великою групою БПЛА. Для зменшення розмірності задачі управління групою і зниження навантаження на оператора БПЛА з бортовими системами управління розділяються на підгрупи, у кожній з яких визначається ведучий. Підгрупи можуть включати менші підгрупи зі своїми ведучими. Управління здійснюється за рівнями: ведучий елемент верхньої підгрупи керує ведучим елементом нижньої підгрупи. Закон управління польотом за траєкторією формується тільки для ведучих. Інші учасники руху дотримуються заданих інтервалів і дистанцій відносно ведучого. Застосування такого алгоритму управління дозволяє підвищити живучість, зменшити розмірність задачі управління і відповідно мати обчислювальну простоту її розв'язання.

Алгоритм централізованого управління групою, як правило, використовують при виконанні спільних дій з пілотованими літальними апаратами - ведучими групи БПЛА. Оператор виконує дальнє наведення, а вони, у свою чергу, управляють кожним об'єктом групи. Недоліком такого алгоритму управління є неповна відповідність принципам роботизації БПЛА, адже основні задачі аналізу обстановки, прийняття рішення і управління покладені на людину-оператора [2].

Важливою перевагою децентралізованих стратегій групового управління є підняття в цілому живучості групи. Оскільки усі технічні об'єкти рівнозначні у групі, то втрата чи пошкодження будь-якого з них не призводить до втрати працездатності всієї групи. І підвищення живучості групи досягається без додаткових витрат, а лише за рахунок самої децентралізованої організації групового управління [3].

До децентралізованих стратегій управління групами мобільних технічних об'єктів належать колективні, зграйні та ройові стратегії управління.

Колективна стратегія управління передбачає, що кожний об'єкт групи отримує інформацію від усіх інших об'єктів і передає зібрану ним інформацію про зовнішнє середовище і власний поточний стан у канал зв'язку таким чином, що ця інформація була доступна усім іншим об'єктам групи. Отже, інформаційний обмін у групі при колективному управлінні відбувається за принципом «кожен з усіма», завдяки чому кожний об'єкт групи може самостійно оцінювати ситуацію і приймати рішення про подальші свої дії. Навантаження на канали зв'язку зростає прямо пропорційно зростанню числа об'єктів у групі [4].

При зграйному принципі управління кожний об'єкт збирає інформацію про зовнішнє середовище самостійно і також самостійно приймає рішення щодо своїх дій таким чином, щоб зробити внесок у виконання групового завдання. Зграйне управління забезпечує високу автономність об'єктів групи при розв'язанні задач і економію каналів обміну інформацією, та не гарантує відсутність зіткнень учасників групи у процесі розв'язання спільної задачі і складності взаємодії при напрацюванні управління. Головною перевагою зграйного управління є масштабованість – при зростанні числа об'єктів у групі обчислювальна складність задачі управління не зростає [4].

Алгоритми на принципах рою (їх ще називають мережними) формують сигнали управління окремо на кожному об'єкті з урахуванням цільового призначення групи, поточного положення у просторі самого об'єкта та інших об'єктів групи. Застосування таких алгоритмів потребує досить високу автономність об'єктів, певний рівень інтелектуальності, бо вони самі напрацьовують рішення стосовно своїх дій. Ройові алгоритми управління мають досить широку область застосування [5].

III. Висновки

Стратегії децентралізованого групового управління складно алгоритмізуються і їх застосування не гарантує оптимальність рішення групової задачі, та у разі підвищених вимог до живучості групи технічних об'єктів слід обирати саме децентралізовані стратегії управління групою.

Список літератури

[1] О.Г. Додонов, О.С.Горбачик, М.Г.Кузнєцова Організація управління групою мобільних технічних об'єктів, ITS 2017, Selected Papers of the XVII International Scientific and Practical Conference on Information Technologies and Security. Kyiv, Ukraine, November 30, 2017. CEUR Workshop Proceeding. 2018. Vol.2067. P.1-7. http://ceur-ws.org/Vol-2067/paper1.pdf

[2] Попов С.А., Дрындин К.Р., Старков А.М. Проблемные вопросы реализации групповых действий БПЛА. URL: http://www.mivlgu.ru/conf/zvorykin2016/pdf/sec12/sec12_pap8.pdf.

[3] Додонов О.Г., КузнєцоваМ.Г., Горбачик О.С. Живучість складних систем: аналіз та моделювання: навч.посіб. у 2-х ч. НТУУ «КПІ», Київ, 2009.- 264 с.

[4] Каляев И.А., Гайдук А.Р., Капустин С.Г. Методы и алгоритмы коллективного управления в группах роботов, Москва, 2009.- 280 с.

[5] Рубан И.В., Чурюмов Г.И., Токарев В.В., Ткачев В.Н. Функциональная стойкость универсальной мобильной реконфигурируемой системы при воздействии электромагнитного излучения высокой мощности, ITS 2017, Selected Papers of the XVII International Scientific and Practical Conference on Information Technologies and Security. Kyiv, Ukraine, November 30, 2017. CEUR Workshop Proceeding. 2018. Vol.2067. P.105-111. http://ceur-ws.org/Vol-2067/paper1.pdf

АНАЛІЗ СПОСОБІВ ПОШУКУ ЗОБРАЖЕНЬ У МЕРЕЖІ ІНТЕРНЕТ

Бартновський Артем Дмитрович,

Сумцов Дмитро Вікторович

Харківський національний університет радіоелектроніки, пр.Науки 14,Харків, 61166 , e-mail: artem.bartnovskyi@nure.ua

Анотація: *Метою даної роботи є аналіз існуючих та розробка нових методів аналізу зображень для пошуку у мережі Інтернет. У цій статті розглянуто кілька алгоритмів рішення цієї задачі.*

Ключові слова: *зображення, комп'ютер, пошук, точки, колір, метадані.*

I. Вступ та постановка проблеми

Пошук зображень в Інтернеті давно став звичним: користувач очікує від пошукової системи точної, швидкої та повної відповіді так само, як і під час пошуку текстової інформації. Більшість популярних пошукових систем поряд за пошуком веб-сторінок з текстовою інформацією почали працювати над пошуком зображень.

На початковому етапі свого існування пошук зображень ґрунтувався виключно на отриманні та аналізі метаданих, пов'язаних безпосередньо з зображеннями: атрибутів, заголовків сторінок та текстів посилань на зображення. Поступово для пошуку зображень стали враховувати також і текст, розташований на тій самій веб-сторінці, що й зображення. Таким чином, завдання пошуку зображення певний час обмежувалося знаходженням усієї можливо пов'язаної з ним текстової інформації та визначенням ступеня правдоподібності, з яким ця інформація відноситься до зображення.

II. Рішення проблем та результати

Паралельно з пошуком зображень за метаданими розвивався й інший напрямок – пошук зображень за їх вмістом. Цей вид пошуку ґрунтується на технології комп'ютерного зору. Він покликаний навчити машину дивитися на зображення очима людини, розуміти й аналізувати його вміст: колір та форму об'єктів, їх текстуру та взаємне розташування. Набір метаданих, що характеризують зображення, обмежений, а комп'ютерний зір дозволяє значно розширити кількість атрибутів, які враховуються під час пошуку зображень та ранжирування результатів.

Можна виділити кілька способів пошуку: Метадані. Зазвичай графічні файли в собі, окрім власне зображення, зберігають ще багато інформації, починаючи від місця, де було зроблене фото (досить увімкнути геолокацію в налаштуваннях камери смартфону), закінчуючи назвою альбому, в якому зберігався файл. Власне, цієї інформації може бути багато, тому пошуковий робот, отримуючи максимум з цієї інформації, може знайти зображення й без використання інших способів.

Метадані використовуються для підвищення ефективності пошуку. Пошукові запити, що використовують метадані, можуть позбавити користувача зайвої ручної роботи з фільтрації. Інформуючи комп'ютер про те, як пов'язані елементи даних і як саме враховувати ці зв'язки, стає можливим здійснювати досить складні операції з фільтрації та пошуку. Наприклад, якщо пошукова система «знає» про те, що «Ван Гог» є «голландським художником», то вона може видати у відповідь на запит про голландських художників веб-сторінку про Ван Гога, навіть якщо слова «голландський художник» не зустрічаються на цій сторінці. Такий підхід, званий поданням знань, відноситься до сфер семантичної мережі та штучного інтелекту.

Зокрема, метадані створюються для оптимізації алгоритмів ущільнення із втратою якості. Наприклад, якщо до відео додаються метадані, які дозволяють комп'ютеру розділити зображення на основну частину і фонову, то остання може бути ущільнена сильніше, що дозволить досягти більшого значення коефіцієнта ущільнення.

2. Знаходження опорних точок картинки. Використовуючи спеціальний складний алгоритм можна обрати на зображенні кілька точок (наприклад знайти найконтрастніші різні кольори на зображенні). Далі запам'ятовують розташування точок відносно одна до одної. В результаті кожному зображенню співставляється деяке рівняння, що описує розташування цих точок. Порівнюючи рівняння всіх зображень, наявних у базі даних, можна знайти схожі. Перевага цього способу полягає у можливості виявляти трансформовані або деформовані зображення й знаходити схожі. Але разом з цим можливо пропустити дуже схожі фото одного й того самого об'єкту, зроблені з різних ракурсів.

3. Пошук за кольором. Ідея цього способу дуже проста – на зображенні знаходять найчастіше повторювані кольори та запам'ятовують, після чого порівнюють їх із результатами аналізу інших зображень. Але практична реалізація є набагато складнішою. Вочевидь, може бути знайдено дуже багато подібних за кольором зображень зовсім різного наповнення. До того ж, повторюваних кольорів зазвичай на зображенні виявляється занадто мало, що суттєво ускладнює пошук.

Тому майбутнє пошукових систем представляється розумним сполученням розглянутих підходів.

Перелік використаної літератури:

[1] А. Моржін, А. Ходарев, В. Князь, С. Желтов, Ю. Візільтер. Обробка та аналіз цифрових зображень - М .: ДМК Пресс 2007 - 464 с.

[2] Юрін Д. В., Крилов А. С., Волегов Д. Б., Насонов А. В., Свєшнікова Н. В. Методи і алгоритми суміщення зображень і їх застосування в задачах відновлення тривимірних сцен і панорам, аналізі медичних зображень, Москва, В МиК МГУ

[3] Волегов Д.Б. , Юрін Д.В. Грубе суміщення зображень за знайденими на них прямих лініях // Праці конференції Графікон 2006, осибірськ., С. 463-466

ЗАВДАННЯ СИСТЕМ АВТОМАТИЗОВАНОГО КЕРУВАННЯ РУХОМИМ СКЛАДОМ

Міненко Микола Владиславович,

Сумцов Дмитро Вікторович

Харківський національний університет радіоелектроніки, пр.Науки 14,Харків, 61166 , e-mail: nickminenko1996@gmail.com

Анотація: *Метою даної роботи є аналіз та впровадження сучасних методів автоматизованого керування рухомим складом залізниці. У доповіді розглянуто кілька алгоритмів рішення цієї задачі в межах однієї станції. Розглянуто типову вузлову станцію та вивчено детальний розклад руху пасажирських, вантажних потягів, а також розклад маневрових робіт. Це дозволило визначити періоди максимального та мінімального завантаження станції в різні проміжки доби, внаслідок чого з'явиться можливість рівномірно розподілити навантаження по станції, а також мінімізувати вплив людського фактору на процеси)*

Ключові слова: *залізничний; транспорт; управління; станція; автоматизований.*

I. Вступ та аналіз проблеми

В умовах розвитку транспортного ринку ключовими питаннями для системи залізничних перевезень є: своєчасне забезпечення вагонами відповідного типу усіх відправників вантажу відповідно до їх замовлень; подальше закріплення залізничного транспорту на ринку перевезень шляхом розвитку маркетингу, створення збалансованої тарифної політики; удосконалення організаційних структур управління залізничним транспортом, технології перевізного процесу та організації перевізної роботи на основі широкого впровадження автоматизованих систем управління, автоматизації диспетчерського контролю просування поїздів; перехід до фінансової моделі управління залізницями, заснованої на обраній раціональної формі власності; підвищення ефективності управління інвестиційною діяльністю; подальше стимулювання праці і удосконалення кадрової та соціальної політики.

Аналіз сучасного стану залізничної галузі і перспектив її розвитку диктує необхідність здійснення комплексних заходів, що сприяють розвитку перевезень і удосконаленню обслуговування клієнтури, з орієнтацією на впровадження високих логістичних технологій, обчислювальної техніки, на удосконалені системи телекомунікації на основі складних ієрархічних інфраструктурних системах корпоративного управління.

Формування технології перевезень за критерієм отримання прибутку від цієї діяльності передбачає мінімізацію собівартості шляхом освоєння прогнозованих вантажопотоків і пасажиропотоків із використанням оптимальної кількості вагонів і локомотивів. Це вимагає освоєння нових технологій та нових підходів до організації вагонопотоків, до складання плану формування поїздів і графіка руху поїздів, а також удосконалення технічного нормування, оперативного управління і регулювання вагонних парків операторських компаній, організації тягового обслуговування поїздів. Застосування ефективних технологій цілком відповідає умовам ринкового середовища. Для рішення названих задач необхідні також чіткий пономерний облік та контроль за дислокацією вагонів, регулювання якості використання вагонного парку і впровадження мікропроцесорних систем диспетчерського управління поїздами. Як свідчить досвід, найбільший ефект від реалізації всіх сучасних елементів організації перевізного процесу може бути досягнуто за умови централізованого управління перевезеннями з єдиного центру (ГЦУП).

II. Рішення проблем та Результати

Оскільки впровадження єдиної АСК на потужностях ПАТ «Укрзалізниця» є дуже масштабним проектом і потребує багато часу для узгодження та залучення додаткового фінансування, у даній роботі пропонується розглянути приклад впровадження такої АСК у межах однієї станції в рамках пілотного проекту. У перспективі, за умови зростання показників, планується поступове впровадження Системи по всіх регіональних філіях ПАТ «Укрзалізниця». Створення центру управління перевезеннями дозволить удосконалити перевізний процес в умовах реформування залізничного транспорту України, забезпечити стійке його функціонування на внутрішньому і міжнародному ринках транспортних послуг, дасть можливість збільшити доходи від основної діяльності, створити умови для зменшення собівартості перевезень і скороченню транспортних витрат. Основними напрямками роботи системи управління перевезеннями повинні бути – суворе дотримання графіків руху поїздів, ефективне регулювання наявного вагонного парку, парку локомотивів і локомотивних бригад, раціональний розподіл вагонопотоків. В цих умовах потрібно удосконалити принципи використання пропускної і провізної спроможності дільниць, проміжних станцій та інших інфраструктурних елементів. Це вимагає введення нових визначень пропускної спроможності залізничної інфраструктури. Зокрема, відповідно досвіду залізниць країн ЄС, існує додаткове поняття – практична пропускна спроможність, яка являє собою реальну пропускну спроможність, що може бути реалізована за умов прийнятого рівня завантаження або надійності. Створена за останнє десятиріччя система АСК ВП УЗ-Є дозволяє вирішувати багато нових складних задач щодо управління перевізним процесом. Однак, реалізовані інформаційні технології на існуючих засобах обчислювальної техніки та зв'язку дають лише розрізнену інформацію щодо ходу процесу перевезень. .

Відсутність цілком реалізованих автоматизованих систем планування і моделювання процесів перевезень ускладнює рішення питань подальшої оптимізації експлуатаційної роботи. Крім того, наявність на даний час на залізницях лише окремих моделей перевізного процесу (відправної, заявок і планування перевезення вантажів у

всіх сполученнях, нормативний графік і інші) не дозволяє вирішувати низку не тільки прогнозних та аналітичних задач щодо ефективного використання рухомого складу (регулювання, підведення порожніх і подачу вагонів у місця навантаження відповідно до заявок відправника та обмежень пропускної спроможності залізничної інфраструктури), але і взаємопов'язаних поточних питань управління вагонними парками та контролю технологічних параметрів їх використання.

Найбільш поширеними оптимізаційними задачами, які застосовуються в управлінні залізничними перевезеннями, є транспортна задача й задача пошуку найкоротшого шляху (маршрутизації).

Для вирішення транспортної задачі розроблені спеціальні методи, які дозволяють знайти оптимальне з множини можливих рішень. Одним з таких методів є розподільний метод, який має декілька різновидів, що відрізняються в основному способом визначення оптимального рішення. Найбільш відомі три різновиди: метод Хічкова; метод Креко; модифікований розподільний метод (або метод потенціалів). Первинне допустиме рішення може бути отримано кількома способами. Найбільш простим є спосіб північно-західного кута. Для отримання більш наближеного до оптимального початкового допустимого плану перевезень найчастіше пропонується використовувати метод найменшого елемента в матриці, метод подвійної переваги або метод апроксимації Фогеля.

III. Висновки

Практично на всіх АСК відсутнє прогнозування процесу перевезень, планування й аналіз показників використання вагонів з урахуванням оптимізації втрат як для національного парку, так і суміжних країн, а також вагонів компаній-операторів, роль яких як перевізників останнім часом значно зростає.

Математична постановка задачі маршрутизації залежить від типу маршруту, за яким планується здійснювати перевезення вантажу двонаправленими або односпрямованими маршрутами. У першому випадку розв'язується задача ув'язки поїздок, в другому – задача комівояжера.

Програмна реалізація вказаних задач безумовно знайде своє застосування в системах автоматизованого керування рухомим складом на залізничному транспорті.

Перелік посилань

[1] В.С. Алейник, О.П. Бочаров, Д.В. Ломотько, С.І. Приходько Удосконалення системи диспетчерського керування рухом на залізницях України // Інформаційно-керуючі системи на залізничному транспорті, УкрДАЗТ, 2014– №1. – С. 3-8.

APPROACHES ON BENCHMARKING POSTGRESQL OPTIMIZED WITH MACHINE LEARNING

Sharayeu Yauhen Uladzimiravich

Belarusian State University of Informatics and Radioelectronics, 6 P. Brovki Street, Minsk 220013, Belarus, eugen.sharayev@gmail.com

Abstract. *Here are described principles of benchmarking PostgreSQL database, optimized with machine learning algorithms. The main focus here is to list common practices and possible pitfalls that are specific to the described problem including the definition of types of benchmarking approaches, industry standard benchmarks, experiment setup steps, various performance metrics, testing utilities, PostgreSQL-specific configurations for performance evaluation and machine learning-related benchmarking process nuances.*

Keywords*: postgresql, benchmarking, machine learning.*

I. INTRODUCTION

PostgreSQL is one of the most advanced and feature reach open source RDBMS for today. Despite the number of configurations to tune the performance, it still has several problems with queries speed. One of those problems is proper cardinality value estimation. Cardinality stands for a number of database records, which returns a query on a given step. It's used by the Planner/Optimizer module to find the most effective execution plan. However, Planner/Optimizer module doesn't take into account functional dependencies between table attributes that directly affect the performance of queries, which contain conditions on those attributes. In order to address the problem, it was proposed to implement multi-column statistics which would store all the required data as multidimensional histograms [1] (instead of one-dimensional). It was implemented in PostgreSQL 10 as multivariate statistics feature. However, this feature has several drawbacks. The first problem is the exponential growth of statistics data that have to be stored and maintained, so it may not be feasible to create multivariate statistics on a large number of attributes. Along with that, functional dependencies can be difficult to discover for database admins, which will also lead to performance degradation.

There are several researchers including working prototypes (like aqo) that are aimed to improve queries performance using machine learning algorithms as a complement or even a replacement of the multivariate statistics feature for cardinality estimation. In order to compare them and introduce further enhancements, it's required to define a set of principles on how to do benchmarking and produce relevant performance evaluation results.

II. GENERAL PRINCIPLES

Commonly, there are several principles to perform correct benchmarks [2]. The first principle is "results repeatability" that stands for the ability to receive equal (with some approximation) results using the same setup and parameters as well as the ability for others to reproduce the benchmarks following the same well-defined setup steps. Another principle is "completeness" which means testing all the contribution to the performance of an application including also possible performance decreases. The "Relevancy" principle is denoted as meaningfulness and representativeness of given benchmarks, which is required to provide substantiation of the optimization module implementation and demonstration of its flaws.

III. BENCHMARKING APPROACHES

There are a lot of metrics to estimate model quality like mean squared error, mean absolute, root mean squared error etc. Though they are great for finding a model which is best for performing a task, these metrics don't show the overall picture. The first problem is that these metrics are not linearly dependent on the final query performance. Despite the more precise predictions than with regular statistics, Planner/Optimizer won't necessarily decide to use a better plan. Training and evaluation of the model also require CPU and RAM. Besides, model-related data have to be stored and fetched every occasionally, that also takes some time and leverages database, file system and CPU level caches. Because of this, the usage of benchmarks along with model-level metrics is required.

On a high level of abstraction, benchmarks can be divided into three categories: micro-benchmarks, standard benchmarks, and real-life applications [3].

Micro-benchmarks are used to test small modules of a system. These benchmarks are better in some ways than using just model quality metrics as they interact with the working system, which gives more precise output about the direct effect on queries performance optimization. Comparing to more sophisticated and long-running tests, they allow fitting a wide range of hyperparameters to find the best configuration for machine-learning models setup and obtain relatively quick feedbacks about them. In terms of optimization modules development, micro-benchmarks are also handy for analyzing an implementation since their results are relatively easy to interpret. However, there are a lot of drawbacks. Despite micro-benchmarks involve the entire application run, they are still detached from the real world examples. Their results can be difficult to generalize and extrapolate on real-world applications as far as they are

imitating only small queries. In terms of PostgreSQL machine learning-based optimization testing, the majority of them should be represented as simple SELECT requests. However, it is also required to provide other kinds of requests where performance degradation may occur (more detailed discussion follows below).

Industry standard benchmarks is a set of predefined instructions on how to setup and run experiments to evaluate the performance. The first advantage of this kind of benchmarks is that it imitates real-life application schemas and queries. Another benefit of it is standardization, which allows doing performance tests not only in terms of the given database but also across other databases including non-relational storage systems without extra efforts to implement benchmark scenarios from scratch. Comparing to micro-benchmarks, standard benchmarks can be more complicated to setup and run if corresponding scripts are not provided. Also, these benchmarks can be quite limited in diversity comparing to the real-life applications as they cannot provide a lot of flexibility due to their strict definitions. However, the last drawback can be turned into a trade-off by sacrificing compliance to a standard and modifying the scenarios. One of the most popular examples of standard benchmarks is TPC family.

Real-life applications usage gives an advantage of evaluating performance experiments against real-life setups with all the existing problems and pitfalls. The biggest disadvantage of these benchmarks is bad reproducibility due to public inaccessibility of most of them (including their data).

IV. Tools and metrics

Pgbench is a default program for PostgreSQL benchmarking. It implements TPC-B compliant standard benchmark, that includes SELECT, INSERT and UPDATE queries (with command line options to skip all or some of them), but is also able to run custom test scenarios defined by a user. It reports performance results by calculating average tps rate (transactions per second) after multiple runs within multiple database sessions. Also, it gives the ability to analyze latencies.

Another common option is Sysbench benchmarking tool. It's developed to work with various storage systems using drivers and includes slightly different metrics for performance estimation. It has options for testing file system-level io, CPU, memory, OLTP-like scenarios (OnLine Transaction Processing) and some other options that can be useful for finding developed machine learning module bottlenecks (for example, extra memory consumption or excessive CPU usage, that could affect on overall database server performance).

V. Problem-specific notes

Although machine learning module is aimed to improve SELECT queries performance, it's also important to evaluate other kinds of queries including INSERT and UPDATE in order to follow the completeness principle as far as the module implementation may include extra disk storage consumption for storing models weights, providing extra indexes or triggers for storing extra data (like min-max index to normalize model features) and so on.

It is also necessary to decide whether to benchmark cold or warm system. There are no formal definitions of these terms, but usually, cold state benchmark stands for running a scenario on a system in the state similar to that after the reboot where no database, file system or CPU cache is loaded. The warm state stands for conditions where any queries that are relevant for benchmarking are executed before the experiment. Usually it's suggested to warm-up the system before running benchmarks [4] as it could lead to noise in measured metrics (for example, running a query with cold and warm database shows 3.8 times bigger wall clock difference [2]), but in terms of optimization with machine learning it also makes sense to evaluate model training time separately to be able to make decision on what kind of model to use by balancing between quick learning, overall performance impact, and other features. It also makes sense to run PostgresSQL-specific maintenance activities like VACUUM, ANALYZE (to gather statistics; can be combined with VACUUM), CHECKPOINT and others, that could affect the performance.

Usually, it's suggested to run benchmarks several times (for pgbench it’s from several minutes to several hours [5]) that is aimed to promote reproducibility and mitigate any noises.

Another important thing is to test performance depending on the database scale. TPC family of benchmarks supports sf (scale factor) parameter that configures populated database size. It’s important to know how a system would behave in cases with a small amount of data stored (whether machine learning execution and training overheads result in degradation of overall performance or not), with big data and also investigate the dependency between optimization effectiveness and sf value growth.

VI. Conclusions

The ideas discussed above can be used to conduct benchmark testing of PostgreSQL machine learning-driven performance improvements. However, it’s necessary to remember that each problem is completely individual and therefore it’s also necessary to use approaches and principles tailored to the problem in addition to the general ones.

References

[1] P. Furtado and H. Madeira, “Summary Grids: Building Accurate Multidimensional Histograms,” 1999.

[2] E. van der Kouwe, D. Andriesse, H. Bos, C. Giuffrida, and G. Heiser, “Benchmarking Crimes: An Emerging Threat in Systems Security,” arXiv:1801.02381 [cs], January 2018.

[3] S. Manegold and I. Manolescu, “Performance evaluation in database research: principles and experience,” 2009.

[4] F. Coelho, “PgBench – Work in Progress,” p. 29, November 2017.

[5] “PostgreSQL: Documentation: 11: pgbench.” [Online]. Available: https://www.postgresql.org/docs/current/pgbench.html. [Accessed: 21-Mar-2019].

Анализ подходов к построению умной парковки

Немилостивый Денис Сергеевич
Харьковский Национальный Университет Радиоэлектроники, Пр-т Науки 14, Харьков 61166, Украина, denis11361@gmail.com

Бологова Наталия Николаевна
Харьковский Национальный Университет Радиоэлектроники, Пр-т Науки 14, Харьков 61166, Украина, natalka.bologova@gmail.com

Анотация. *Одной из главных проблем во многих крупных и густонаселенных городах является проблема поиска парковочных мест для транспортных средств. В качесте решения данной проблемы можно предложить систему «умной парковки», которая сможет помочь пользователям найти доступное парковочное место для автомобиля. В этой статье приводятся направления развития системы «умная парковка» и средства с помощью которых они реализуются. Приводятся описания датчиков благодоря которым возможна реализация системы «умная парковка», их принципы работы, пложительные и отрицательные стороны.*

Ключевые слова: *умная парковка; датчик; транспорт; автомобиль; автоматическая парковка.*

I. Введение

Количество транспортных средств на дороге быстро опережает количество доступных парковочных мест. Проблема поиска парковочного места стала широко распространенной проблемой в густонаселенных городах. Эта проблема может быть частично решена внедрением систем по типу «умная парковка». Целью умной парковки является облегчение рутинного процесса поиса водителями свободных парковочных мест, улучшение эффективнести использования парковочных мест, уменьшение цены и уменьшение пробок на дорогах вызванных водителями которые ищут свободную парковку. Это известный факт, что поиск парковочного места в людном районе густонаселенного города может быть очень напряженным. Тратя топливо и время, водители разъезжают по городу в поисках парковки, что в сдедствии вызывает сопутствующие проблемы, такие как пробки. Исследования показывают, что в среднем 30% трафика в густонаселенном городе из-за автомобилей, которые ищут парковочное место[1]. Эта проблема не обязательно связана с недоступностью, а скорее с неэффективным использование доступных парковок. Она возникает из-за отсутствия информации о наличии мест на разных парковках. Согласно исследованию Бостонского университета - у более чем 30% водителей занимает около 7,8 минут, чтобы припарковать свое транспортное средство[2]. Большинство существующих систем умной парковки предоставляют только информацию о местонахождении парковочных мест и количестве свободных мест на этой парковке, но они не могут найти точное местоположение свободного места для парковки.

II. Решение проблемы и результаты

Основным направлением развития системы «умная парковка» являются «умные» датчики парковки. Такие датчики встраиваются в дорожное полотно на места парковок и отслеживают занято или свободно место над ними, передавая данные на сервер. Используя сеть таких датчиков, создается карта парковки, состояние которой передается пользователям на улицах с помощью специальных экранов, веб-сайта или мобильного приложения.

В целом датчики обнаружения делятся на два типа: встраиваемые в дорожное покрытие и поверхностные. Встраиваемые датчики включают в себя:

– активные инфракрасные датчики. В основе их конструкции лежит оптическая система из нескольких лучей, состоящая из передатчика и приемника. Извещатель формирует сигнал что место занято при одновременном прерывании двух и более лучей[3,5]. Активные инфракрасные датчики чувствительны к изменениям окружающей среды такие как дождь или снег. Поэтому это не подходит для открытых парковок. Они должны быть установлены на всех парковочных местах для эфективного распознования машин;

– электромагнитные. Принцип действия основан на изменении амплитуды колебаний генератора при попадании в активную зону датчика металлического объекта определенных размеров, а данном случае автомобиля[5]. Они обычно используется на въезде и выезде, чтобы узнать количество автомобилей, которые находятся на парковке, для определения количества свободных мест. Эти датчики дороги в установке и обслуживании, и они обычно используются на крытых парковках, чтобы получить количество доступных парковочных мест. Тем не менее, состояние отдельно взятого места не может быть определено с помощью электромагнитных датчиков;

– пьезоэлектрические датчики давления. Работа пьезоэлектрического датчика основана на преобразовании механической энергии в электрическую. Таким образом, когда машина наезжает на такой датчик, он посылает сигнал о том что место было занято.

Примерами внешних датчиков служат:

– пассивные инфракрасные датчики. Датчик, чувствительный к инфракрасному излучению, устанавливается над парковочным местом и обнаруживает тепловое излучение от автомобиля при занятии места[3]. Эти датчики чувствительны к окружающей среде, их показания не будут точными, если идет снег или дождь. Пассивные инфракрасные датчики следует размещать под землей или на потолке. Эти датчики подходят для закрытых парковок, которые находятся внутри зданий и не подходят для открытых парковок;

– ультразвуковые датчики расстояния. Датчик регулярно испускает пучки ультразвуковых волн. Затем датчик переключается в режим приёма и ожидает возврата отраженных волн, после чего анализирует их и делает вывод занято ли парковочное место. Они обычно крепятся на потолке и чувствительны к изменениям погоды, таким как дождь и снег[4]. Следовательно, они подходят для крытых парковок, а не для открытых парковок. Для того, чтобы проверить состояние парковочного места, эти датчики должны быть размещены над каждым парковочным местом. Ультразвуковые

датчики датчики относительно недорогие, но установка, обслуживание нескольких датчиков и подключение их к сети будет дорого стоить в долгосрочной перспективе;

– радиолокаторы. Принцип действия похож на ультразвуковой датчик, но в отличии от него излучает радиоволны. Радиолокаторы не чувствительны к окружающей среде и могут быть использованы как на открытых так и на закрытых парковках. Они должны быть размещены на каждом парковочном месте для определения статуса парковочного места. Что делает их достаточно дорогими для устанавки и обслуживания в больших масштабах. Большинство вышеперечисленных датчиков работают от батареек, срок службы которых в среднем составляет до 7 лет;

– видеокамеры. Основным преимуществом видеокамер является отсутствие необхобимости в приобретении дополнительных датчиков для определения состояния парковочного места, можно даже использовать камеры безопасности. Камеры могут быть использованы как для распознавания номерных знаков так и для определения занятости парковочного места. Камера может быть расположена возле въезда на парковку для распознавания номерных знаков. На основании количества распознанных транспортных средств которые въехали и выехали со стоянки можно получить количество свободных парковочных мест. Определение статуса занятости парковочных мест с использованием камер не идеально, так как требует непрерывной передачи большого потока данных на сервер[6]. Камеры отправляют поток видео на сервер, где оно кадрируется и специально разработанное програмное обеспечение распознает автомобиль и определяет состояние парковочного места. Камеры подходят для открытых парковок, так как они могут охватывать большое количество парковочных мест. Тем не менее, камеры подвержены эффектам окклюзии и затенения, искажения изображения и изменения освещения. Поскольку небольшое количество камер может покрывать большие количество парковочных мест, расходы можно считать минимальными.

Еще одним направлением умных парковок является разработка и внедрение автоматизированных парковок (чаще всего многоуровневых), в которых действия водителей сведены к минимуму. Водитель заезжает на специальную площадку/платформу и выходит из машины. Затем платформа сама переносит автомобиль на специально отведенное, зарезервированное или свободное место, и сообщает водителю его номер. Чтобы получить свое транспортное средство, водителю необходимо авторизоваться и ввести данный номер на специальном табло или пульте управления, после чего платформа также самостоятельно спустит автомобиль на площадку.

III. Выводы

В данной статье были расмотрены несколько датчиков для определения состояния парковочного места. Однако большенство рассмотренных датчиков имело смысл использовать только на закрытых парковках. И практически ни одина из технологий не использовалась для повышения эффективности парковки на открытых парковках. Ультразвуковой и инфракрасный датчики чувствительны к условиям окружающей среды что может привести к неточной информации о занятости парковочного места. Радиолокатры не подвержены условиям окружающей среды, но дороги в установке и обслуживании на открытых парковках. Даже если цены на сами датчики снизятся то все равно будут расходы, связанные с установкой и техническим обслуживанием, которые деляют их слишком затратными в использовании на открытых парковках. Таким образом датчики не идеальны для открытых парковок, так как расходы связанные с ними слишком высоки.

Обнаружение занятости парковочного места с использованием камер варьируются между закрытыми и открытыми парковками, так как условия освещения на открытой парковке могут значительно отличаться от освещения на закрытой. Ранее уже упоминались проблемы, с которыми сталкиваются при недостаточном освещении и затенении. Определение состояния парковочного места с использованием камеры является одной из возможных технологий умной парковки для получения информации о месте на открытых парковках в режиме реального времени. Обнаружение машин с помощью камеры может быть реализовано с использованием сверточных нейронных сетей.

Список литературы

[1] Donald C. Shoup, ”Cruising for Parking” Transport Policy, vol. 13, no. 3, 2006.

[2] O. Dokur, S. Katkoori and N. Elmehraz, “Embedded system design of a real-time parking guidance system”, Annual IEEE Systems Conference (SysCon), Orlando, FL, 2016, pp. 1-8.

[3] Г. Виглеб, “Датчики. Устройство и применение” Москва «Мир» 1989

[4] Kianpisheh, A., Mustaffa, N., Limtrairut, P., et al.: ‘Smart parking system (SPS) architecture using ultrasonic detector’, Int. J. Softw. Eng. Appl., 2012, 6, (3), pp. 51–58

[5] Shaheen, S.: ‘Smart parking management field test: a bay area rapid transit (bart) district parking demonstration’ (Institute of Transportation Studies, Davis, CA, USA, 2005)

[6] Enríquez, F., Soria, L.M., Álvarez-García, J.A., et al.: ‘Existing approaches to smart parking: An overview’. Int. Conf. on Smart Cities, Malaga, Spain, 2017

Класифікація методів корекції сигналу для систем автоматичного розпізнавання мовлення

Закаблук Максим Володимирович
Шевченко Олексій Тарасович
Мовсесян Яна Самвелівна

Харківський Національний Університет Радіоелектроніки, Харків, проспект Науки 14, 61166, Україна
e-mail: yana.movsesian@nure.ua

Анотація. *Системи автоматичного розпізнавання мовлення (АРМ) широко використовуються в голосових користувацьких інтерфейсах. Голосовий сигнал до надходження в систему АРМ піддається впливу шумів (фоновий шум, реверберація і т.д.) та апаратним завадам, пов'язаними з неідеальністю каналу передачі (помилки кодування). В роботі проведена класифікація методів корекції голосового сигналу для підвищення завадостійкості систем автоматичного розпізнавання мовлення, виділено найбільш успішні методи для придушення шуму та реверберації та проаналізовані їх особливості.*

Ключові слова: *реверберація; корекція; шум; мовлення; глибинне навчання; нейронні мережі; системи АРМ*

I. Вступ Та Постановка Задачі

На даний момент існує декілька успішних підходів до корекції мовленнєвого сигналу від шуму та реверберації. Якість їх роботи чи можливість використання в певних умовах залежить, наприклад, від параметрів вхідного сигналу, ресурсів, необхідних для обчислення обраного алгоритму, наявності інформації про оточуюче середовище, тощо [1].
Мета даної роботи полягає в класифікації існуючих підходів і методів корекції голосового сигналу, що працюють окремо від системи АРМ, а також виділення їх особливостей.

II. Вирішення Проблеми Та Результати

Корекція голосових сигналів може бути виконана в препроцесорі та/або всередині системи АРМ. Вагомою перевагою обробки в препроцесорі є можливість не змінювати параметри і структуру існуючих систем АРМ. Для придушення адитивного шуму успішно використовують фільтрацію Вінера або відновлення у часовій області [2] та спектральне віднімання [3]. Для роботи вінерівської фільтрації необхідна наявність інформації про відношення сигнал-шум на певних частотах; а для роботи алгоритму спектрального віднімання – наявність входу зі зразком шуму, який необхідно придушити.
Класифікуючи методи придушення реверберації, розрізняють повне і часткове придушення реверберації. Задача повного придушення реверберації відноситься до зворотних задач і повинна вирішуватися методом зворотної фільтрації. До методів повного придушення реверберації належать: деконволюція на основі гармонік [4] та спектральне віднімання [3]. Деконволюція на основі гармонік залежить від присутніх частот у вхідному сигналі та частоти їх зміни.
На результати обробки цими методами сильно впливатимуть будь-які зміни в ІХ (імпульсивна характеристика) приміщення, тому середовище передачі має бути відомим і постійним.
На практиці, інформація про ІХ приміщення відсутня і в такому випадку необхідно провести «сліпу» корекцію спотвореного сигналу. До методів сліпої корекції можна віднести: спектральне віднімання з виділенням пауз між словами [5] та сліпу деконволюцію [6]. В роботі [7] запропонований метод максимальної правдоподібності. Сутність вимірювань часу реверберації, якого полягає в отриманні параметрів імпульсного відгуку в паузах голосового сигналу, де дія реверберації проявляється у вигляді звукових «шлейфів», що тягнуться за останніми звуками слів. Даний метод апроксимує значення часу реверберації з кожним обробленим фреймом. Та по якості корекції дещо перевершує вищезазначені методи придушення реверберації.

III. Висновки

Спираючись на складність існуючих систем автоматичного розпізнавання мовлення, більша частина необхідної обробки сигналу має проводитись в препроцесорі, що дозволяє зберігати незмінною структуру і параметри системи АРМ. Адитивні завади успішно пригнічуються методами вінерівської фільтрації. При наявності інформації про ІХ приміщення та/або параметри шуму, застосування методу спектрального віднімання є найбільш доцільним. Без наявності інформації про час реверберації проводять сліпе придушення реверберації одним з методів: спектральним відніманням з виділенням пауз між словами, сліпою деконволюцією, методом максимальної правдоподібності.

Перелік Літератури

[1] Yoshioka T. "Making Mashine Understand Us in Reverberant Rooms", IEEE Signal Processing Magazine. – 2012, vol. 29, No. 6. – P. 114-126.
[2] Meihui Lu; Xuan Zhou; Nabih Jaber; Kun Hua; Mahdi Ali, "Speech enhancement using a critical point based Wiener Filter", Advances in Wireless and Optical Communications (RTUWO), 2017, pp. 175 - 179
[3] M. Khan; S. Mohsen; J. Chambers, "A new cascaded spectral subtraction approach for binaural speech dereverberation and its application in source separation" IEEE International Conference on Acoustics, Speech and Signal Proc. 2013, pp. 6566 - 6570 .
[4] Tomohiro Nakatani; Keisuke Kinoshita; Masato Miyoshi, "Harmonicity-Based Blind Dereverberation for Single-Channel Speech Signals", IEEE Transactions on Audio, Speech, and Language Processing
[5] K. Han, Y. Wang, and D. L. Wang, "Learning spectral mapping for speech dereverberation," in Proc. ICASSP, 2014, pp. 4661–4665.
[6] K. Furuya; S. Sakauchi; A. Kataoka, "Speech Dereverberation by Combining Mint-Based Blind Deconvolution and Modified Spectral Subtraction", 2006 IEEE International Conference on Acoustics Speech and Signal, 2006, p. I-I
[7] А.Н. Продеус, В.С. Дидковский, В.П. Овсяник, "Слепое измерение времени реверберации в системах автоматического распознавания речи", Харків, № 7(123), 2014, с.59-6

Выделение объектов на изображениях через морфологические преобразования

Янковский Александр Аркадьевич
Янковская Дарья Александровна

Харьковский национальный университет радиоэлектроники,
Харьков, проспект Науки, 14, 61166
oleksandr.yankovskyi@nure.ua

Анотация. *Предлагается процедура обработки изображений, позволяющая путем применения морфологических преобразований выделить на изображении отдельные элементы интереса, а затем подсчитать их количество*

Ключевые слова: *изображение, фильтр, пиксель, объект*

I. Введение

Одной из областей применения цифровой обработки изображений является анализ медицинских изображений, например срезы тканей, на которых необходимо обнаружить и выделить отдельные объекты (ОИ-объекты интереса). При большом количестве таких изображений возникает актуальная задача автоматизации их обработки. Для решения этих задач предлагается методика обработки изображений при помощи пакета MATLAB.

II. Решение проблемы и результат

Для выделения объектов на изображениях разработано много различных алгоритмов [1], [2]. К изображениям, используемым в данной работе, предлагается применить различные морфологические преобразования [3], которые отличаются невысокой сложностью и малым временем на обработку.

Исходное изображение (рис.1) в формате bmp сначала преобразуется в бинарное изображение методом бинаризации по нижнему порогу, что позволяет оставить на изображении объекты повышенной контрастности (рис.2).

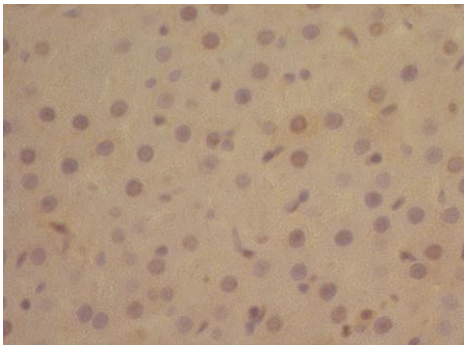


Рисунок 1 - Исходное изображение

После этого путем последовательного применения таких операций пакета MATLAB, как clean, dilate, close на изображении остаются только крупные объекты повышенной контрастности, которые и являются объектами интереса (рис.3).

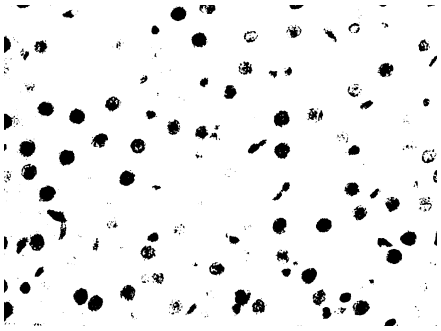


Рисунок 2 - Изображение после бинаризации по нижнему порогу с коэффициентом 128

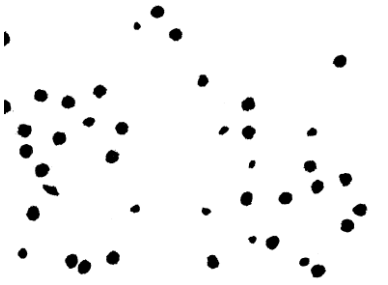


Рисунок 3 - Изображение после обработки

Далее при помощи других специальных функций MATLAB производится подсчет числа ОИ.

Список литературы

[1] Р. Гонсалес, Р. Вудс. Цифровая обработка изображений. СПб.: Питер, 2005. -1071 с.

[2] В.Т. Фисенко, Т.Ю. Фисенко. Компьютерная обработка и распознавание изображений: учебное пособие. –СПб.: СПбГУ ИТМО, 2008. -192 с.

[3] П.И. Рудаков, И.В, Сафонов. Обработка сигналов и изображений. MATLAB 5x. М.: ДИАЛОГ-МИФИ, 2000. – 416 с.

Исследование методов балансировки сетевой нагрузки

Ковалев Александр Олегович[1]

Партыка Станислав Александрович[2],

[1]*Харківський національний університет радіоелектроніки, пр. Науки 14, Харків, 61166, Україна, impwxxwp@gmail.com*

[2]*Харківський національний університет радіоелектроніки, пр. Науки 14, Харків, 61166, Україна, stanislav.partyka@nure.ua*

Анотация. *Рассматривается четыре метода балансировки нагрузки: случайный перебор, циклический перебор, кратчайшая очередь и кратчайшая очередь с устаревшей информацией о нагрузке. Также сравнивается средняя задержка систем для различных методов балансировки нагрузки.*

Ключевые слова: *балансировка нагрузки, случайный перебор, циклический перебор, кратчайшая очередь.*

I. ВВЕДЕНИЕ И ПОСТАНОВКА ЗАДАЧИ

Балансировка нагрузки является важным компонентом современной сетевой инфраструктуры и компьютерных систем [1]. Балансировку нагрузки можно определить как метод распределения рабочей нагрузки на несколько компьютеров или кластер компьютеров по сетевым каналам для достижения оптимального использования ресурсов, которое максимизирует пропускную способность и минимизирует общее время отклика [2].

II. ОСНОВНАЯ ЧАСТЬ

Рассматривается два основных типа балансировки нагрузки, которые используют информацию о системе для принятия решения:

– С актуальной информацией о состоянии.
– С устаревшей информацией.

В стратегии случайного распределения нагрузки входящее задание отправляется на сервер с вероятностью 1/N, где N - количество серверов. При использовании стратегии случайной балансировки нагрузки диспетчер не имеет информации о задании или состояниях сервера.

В стратегии циклического перебора задания отправляются на серверы. Эта стратегия выравнивает ожидаемое количество заданий на каждом сервере.

В стратегии кратчайшая очередь с актуальной информацией диспетчер отправляет задание на сервер с наименьшим количеством заданий в очереди. Если имеется несколько серверов с наименьшей длиной очереди, диспетчер случайным образом выбирает сервер из этого списка. Эта стратегия пытается выровнять текущее количество заданий на каждом сервере. Диспетчер также получает длину очереди серверов каждый раз, когда принимает решение.

В стратегии кратчайшая очередь с устаревшей информацией о нагрузке диспетчер также отправляет задание на сервер с наименьшим количеством заданий в очереди. Отличие от предыдущей стратегии состоит в том, что информация о состоянии системы обновляется с задержкой.

Результаты проведенных экспериментов приведены на рисунках 1 и 2.

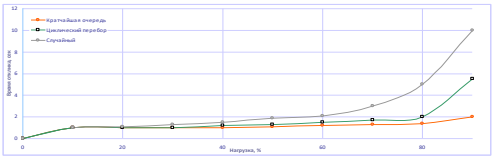


Рисунок. 1. Зависимость среднего времени отклика от загруженности системы

Из рисунка 1 видно, что стратегия кратчайшая очередь работает намного лучше, чем случайный выбор или циклический перебор.

Сравнивая среднее время отклика стратегии кратчайшей очереди с устаревшей информацией со случайной стратегией, можно заметить, что последняя лучше, даже если интервал обновления составляет всего 4 секунды. Но, с интервалом в 2 секунды между обновлениями стратегия кратчайшей очереди с устаревшей информацией работает лучше, чем случайный выбор, но все же уступает кратчайшей очередь с актуальной информацией.

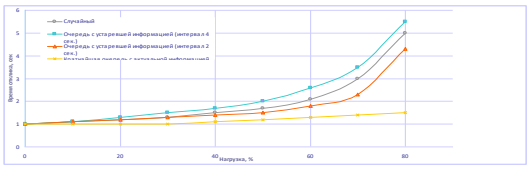


Рисунок. 2. Сравнение среднего времени отклика стратегий балансировки для случая обновления информации о состоянии системы с задержкой

III. ВЫВОДЫ

Рассмотрены четыре метода балансировки нагрузки с использованием имитационной модели, состоящей из одного балансировщика нагрузки и пяти серверов. Полученные результаты показывают, что стратегия кратчайшей очереди с актуальной информацией о загрузке сервера дает наименьшую задержку, как и ожидалось. Но в случае, если информация о состоянии системы значительно устарела, стратегия кратчайшей очереди работает хуже, чем случайная балансировка нагрузки.

СПИСОК ЛИТЕРАТУРЫ

[1] M. Alizadeh, T. Edsall, S. Dharmapurikar, R. Vaidyanathan, K. Chu, A. Fingerhut, V. T. Lam, F. Matus, R. Pan, N. Yadav, and G. Varghese, “CONGA: Distributed Congestion-aware Load Balancing for Datacenters,” SIGCOMM Comput. Commun. Rev., vol. 44, no. 4, pp. 503–514,

[2] J. Zhang, F. Ren, and C. Lin, “Survey on transport control in data center networks,” IEEE Network, vol. 27, no. 4, pp. 22–26, Jul. 2013.

Розробка БД опису поверхні візування в оптичному діапазоні на малих висотах

Єрьоміна Наталія Сергіївна
Паніматка Павло Віталійович

[1]*Харківський національній університет радіоелектроніки, пр. Науки 14, Харків, 61166, Україна,*nataliia.yeromina@nure.ua
[2]*Харківський національний університет радіоелектроніки, проспект Науки, 14, Харків, 61166,* Україна, panimatka@gmail.com

Анотація. *Запропоновано для побудови та корекції напрямку руху безпілотних літальних апаратів у повітряному просторі на основі оптичного аналізу та порівняння зображень з бортових систем огляду простору та фактичних зображень, що були зроблені раніше, а також задля визначення висоти польоту такого виду літальних апаратів і її корекції в поточному часі без втручання оператора. Також є корисним для систем, що використовуються для відслідковування нових об'єктів, що з'являються після початкових знімків місцевості.*

Ключові слова: *оптичний аналіз, OpenCV, AForge, система огляду, безпілотний літальний апарат, повітряний простір, місцевість.*

I. Вступ та постановка проблеми

Рішення багатьох задач, які забезпечують прийняття обґрунтованих управлінських рішень в різних областях економічної, політичної, військової та соціальної діяльності людини, ґрунтується на даних дистанційного зондування Землі (ДЗЗ).

У загальному випадку, дистанційне зондування визначають як процес або метод отримання знань про об'єкт, ділянці поверхні або явище шляхом аналізу даних, зібраних без контакту з досліджуваним об'єктом. Даний метод є одним з найбільш перспективним з точки зору набуття знань про стан поверхні Землі.

За статистикою 2018 року [1] використання безпілотних літальних апаратів збільшилось на 18%, зокрема і у військових цілях. Кожен літальний апарат має свої принципи управління, але з кожним роком у сфері розробки безпілотних літальних апаратів застосовується штучний інтелект, що дозволяє без застосування оператора побудувати маршрути до точки призначення, що була визначена раніше.

Рішення значної частини завдань моніторингу на основі даних дистанційного зондування поверхні землі базується на використанні методів обробки зображень. Під обробкою зображень будемо понімати процедури виділення особливостей на зображенні і їх ідентифікації на основі обраних характеристик.

Сучасні високоточні системи навігації ЛА базуються на комплексуванні інерційних навігаційних систем (ІНС) з системами супутникової корекції або з системами навігації по геофізичних полях (ГФП) Землі (кореляційно-екстремальними системами). Використання для корекції ІНС супутникових навігаційних систем - досить простий і ефективний спосіб, однак він має ряд недоліків, що полягає у низькій здатності протистояти перешкодам системи корекції і неавтономному функціонуванні комплексувальної навігаційної системи. Цих недоліків позбавлені кореляційно-екстремальні системи, що здійснюють визначення місце розташування ЛА в місцевій системі координат шляхом порівняння еталонного зображення, яке сформовано заздалегідь за вхідною відеоінформацією (наприклад, аеро- або космічного фотознімку), з поточним зображенням, яке формується в польоті ЛА. [2]

Основною метою розробки систем оптичного аналізу (візування) зображень місцевості для побудови маршрутів безпілотних літальних апаратів є повне або часткове виключення роботи оператори з процесу визначення шляху його руху, а також для збереження особового складу у разі застосування БЛА у військових цілях.

Мета роботи: розробка програмно-апаратного комплексу формування бази даних опису поверхні візування в оптичному (ТВ) діапазоні на малих висотах для безпілотних літальних апаратів.

II. Рішення проблеми та результати

Дані дистанційного зондування Землі (зображення земної поверхні і різні зареєстровані параметри земних об'єктів і явищ) отримують з допомогою на гою датчиків або знімальних систем. Під знімальною системою розуміють технічні засоби, за допомогою яких реєструють електромагнітне випромінювання. Залежно від місця установки знімальної системи вимірюють і реєструють випромінювання в наземних умовах, з повітряного (аеро-) літального апарату (носія). При отримані інформації про земну поверхню великої протяжності даний метод найбільш ефективний і оперативний.

Зображення, що отримані з бортових систем огляду безпілотного літального апарату представляють собою набір пікселів, що мають певний контраст та колір. Завдяки цьому візування об'єктів в різні пори роки ускладняються погодними умовами. Саме задля усунення цієї проблеми необхідно створювати базу даних опису поверхні візування.[3]

Основною проблемою на першопочатковому етапі обробки зображення є задача вибору ознак за якими буде розібране зображення. У задачі вибору ознак потрібно з отриманих вихідних даних виділити характерні властивості об'єктів, на основі яких сформувати простір описів таким чином, щоб в цьому просторі інші завдання розпізнавання вирішувалися б легше. Для цього на основі вихідних даних слід відокремити ознаки класів образів (або міжкласові ознаки) від внутрішньокласових ознак.

Так як кожне зображення представляє собою набір пікселів, що мають свої властивості, то вирішення цієї проблеми полягає у наступному:

- збір оптичних зображень однієї площини у різних ракурсах;

− прив’язка кожного із зображень до конкретних координат місцевості задля подальшого використання їх при побудові маршрутів безпілотних літальних апаратів;

− перетворення отриманих зображень у чорно-білу кольорову гамму задля розрізнення різних типів об'єктів місцевості за контрастністю;

− розбиття вихідного зображення на шматки, що місять N*N пікселів та присвоєння їм мітки, що дозволить ідентифікувати його в майбутньому;

− занесення до бази даних отриманої інформації.

Кожний етап обробки оптико-електронного зображення відбувається за допомогою програмного комплексу, що розроблений на основі бібліотек OpenCV та AForge для прискореної обробки.

Програмний комплекс складається із бази даних, що містить основну інформацію про прийняті зображення та програмного забезпечення, що необхідно для обробки та виділення основної інформації із зображення.

Метою візування зображення у цьому проекті є визначення основних контурів та порівняння їх із зображеннями, що будуть отримані в майбутньому при побудові маршрутів безпілотних літальних апаратів. Візування даним способом основане на визначенні контурів об'єктів, що зустрічаються на зображенні та порівнянні кольорових просторів із прототипом зображення.

Обробка зображення складається з декількох етапів. Першим етапом є перетворення його кольорового простору на чорно-білий. (у разі якщо оптичне обладнання з якого надходить графічна інформація дозволяє робити кольорові знімки). Це необхідно для подальшого прискорення обробки інформації. Другий етап полягає у визначенні контурів об'єктів на зображенні методом Фрімена. Він полягає у визначені контурів за допомогою цепних кодів, що представляють границі об’єкта у вигляді послідовності відрізків прямих ліній у вигляді прямих ліній відповідної довжини та напрямку. В основі цього представлення полягає 4- або 8- зв’язна решітка. Довжина кожного відрізка визначається здатністю решітки, а напрямки задаються обраним кодом. [4,5]

Також другий етап полягає у розбитті зображення на шматки, що мають певну кількість пікселів і розмір. Задля подальшого їх індексування і можливості розпаралелювання операції порівняння двох зображень на графічний процесор із збільшенням швидкості. Кожна частинка такого зображення індексується і відноситься саме до того зображення з якого біла взята, а безпосбередньо саме зображення відноситься до певних координат, що визначаються апаратурою і також заносяться до бази даних. Тобто при необхідності побудови маршрутів у динамічному режимі, за наявності на борту необхідних обчислювальних потужності безпілотний літальний апарат має можливість визначати маршрут самостійно без втручання оператора і корегувати його за необхідністю.

Третій етап є занесення отриманих результатів до бази даних і створення необхідних залежностей між усіма частинами. На цьому етапі головним фактором є швидкість обміну даними із базою даних. Від цього залежить швидкість обробки інформації, що поступає до центрального процесору літального апарату, який приймає рішення та навпаки із камер бортового огляду до БД із метою запису.

III. Висновки

Даний метод дозволяє створити, як контурний опис земної поверхні, так і опис поверхні, що базується на формуванні кольорового простору зображення із подальшим його порівнянням із фактичним зображення.

Недоліками методу візування в оптичному діапазоні є наступні:

− Неможливість використання в нічний час доби, що є суттєвим недоліком;

− Необхідна велика кількість зображень однієї площини поверхні під різними ракурсами, задля подальшого застосування отриманих даних і отримання точних результатів;

− Застосування апаратури, що здатна обробляти дані бортових систем огляду (на даний момент має високу вартість);

− Неточність визначення висоти до об’єкта за рахунок використання методу контрастного визначення.

До основних позитивних моментів даного методу візування можна віднести наступні:

− Можливість визначення об'єктів із заданою точністю, тобто можна виділити, як ділянки земної поверхні, так і окремі об’єкти (мости, будинки та інші);

− Часткове виключення оператора з процесу збору інформації;

− Використання даних для інших систем, що повинні використовувати дані з бортових систем огляду безпілотного літального апарату за допомогою загальної бази даних;

В результаті аналізу отриманих даних було виявлено те, що метод інтерполяції, який застосовується при визначенні відношення тієї чи іншої частини зображення до певного кольорового спектру є найбільш оптимальним, але вносить певний коефіцієнт помилки при визначенні.

Отримані вихідні результати роботи програмно-апаратного комплексу дуже залежать від вхідного опису сигналу відповідного об’єкту, який необхідно знайти, і способу у відповідності з яким цей сигнал представлений на зображенні, що спостерігається. Інакше поставлена завдання, що покладається на цю розробку втрачає сенс.

Джерела посилань

[1] Беспилотный летательный аппарат БПЛА (дрон) – 2019 – із преси

[2] Щербинин В. В., Построение инвариантных корреляционно-экстремальных систем навигации и наведения летательных аппаратов – 2011. - С. – 11-20.

[3] Комарова А. Ф., Журавлева И. В., Яблоков В. М. Открытые мультиспектральные данные и основные методы дистанционного зондирования в изучении растительного покрова // Принципы экологии. - 2016. - № 1. - С. 40–74.

[4] Фурман Я. А., Юрьев А. Н. , Яншин В. В. Цифровые методы обработки и распознавания бинарных изображений. - 1992. – С. 42-50.

[5] Фурса Н. Е. Метод поиска объектов на изображении с помощью контурного анализа по заданным характеристикам их контуров. Із преси.

Using of Global Positioning System navigation services in automated fare collection systems

Yeromina Nataliia Serhiyivna[1]
Shapa Lyudmila Serhiyivna[2],
Budko Anna Oleksiyivna[3]

[1]*Kharkiv National University of Radio Electronics, 14 Nauky Ave, Kharkiv UA-61166, Ukraine, nataliia.yeromina@nure.ua*
[2]*Kharkiv National University of Radio Electronics, 14 Nauky Ave, Kharkiv UA-61166, Ukraine, liudmyla.shapa@nure.ua*
[3] *Kharkiv National University of Radio Electronics, 14 Nauky Ave, Kharkiv UA-61166, Ukraine, anna.budko@nure.ua*

Abstract. *The purpose of the work is the optional expansion of the automated fare collection system in public transport of the city of Kharkiv to improve the transport network based on the use of GPS tracker. The following methods are used: process modeling using the IDEF0 charts. The proposed expansion of the automated payment system for public transport in the city of Kharkiv can be applied without changing the hardware base of the system, and will also achieve results such as increasing road safety, reducing time and energy resources costs for travel, improving vehicle comfort, increasing the competitiveness of carriers, improving public transport image.*

Keywords: *automated fare collection system, automatic payment systems, GPS, electronic travel document, IDEF0.*

I. INTRODUCTION AND PROBLEM STATEMENT

Nowadays, the lives of most citizens of the world is closely connected with the use of information systems. Due to the significant advances in information technology, the transport sector is undergoing significant changes: from smart ticket payments to new initiatives multimodal mobility and autonomous vehicles. A wide range of publications on this subject emphasizes the importance and relevance of this study Thus, the work of Carmelo R. G. and Ricardo Perez describes an automatic payment system based on various mobile communication and information support devices that reduces operating costs through the use of local communication infrastructures and general-purpose devices. A. Gusev's and V. Sergeev.'s approach is to supplement the existing concept with the components of internal control for autonomous elements [3].

Nowadays, automatic payment systems are introduced in many countries of the world, including Ukraine. One of the leading companies in the world involved in the manufacturing of equipment for the automated fare collection is the Czech Microelectronics Company.

One of the latest projects where the hardware and software solutions of Microelectronics Company have been used, is the project "Eticket" in the city of Kharkiv. The system of the single electronic ticket of Kharkiv has an architecture similar to that implemented in the Czech Republic and other large cities of the world.

To represent the transactions exchange process between the server and validation device, the model of data exchange between the server and validation device has been made, which is represented in notation IDEF0 (Fig. 1). This model allows to understand how transactions occur in the system for further improvement.

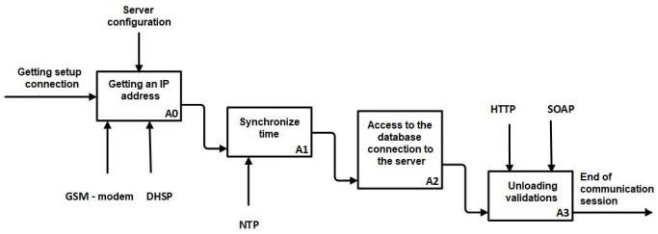


Figure 1 The model of data exchange between the server and validation device.

In such systems, for the provision of communication through GSM channels, the power of local telecommunications operators is used, which imposes certain restrictions on the volume, speed and data transmission volumes. Within this system, a tariff plan with a traffic restriction of 700 MB per month is used for each vehicle.

The current system analyzes the data exchange between the server and the validator for a complete 90-minute communication cycle.

The following main stages of data exchange can be distinguished:

1. Getting the IP address.
2. Time synchronization.
3. Access to the database connection.
4. Upload validation.

At the first stage of obtaining an IP address, the network protocol DHCP is used. The device asks for an address to the server. The server, in return, receives the message of the device, defines the necessary configuration of the client in accordance with the initial settings and sends it to the device. At this stage, the device must select one of the configurations and send a request to the server. The server confirms the request and the device may apply the settings.In total, during the session, approximately 30 packets of a total volume of 9,000 bytes are transmitted.

The second step is to synchronize the current time with the server on the device for the correct transaction record. One time synchronization session consists of 12 packets, 8 of which are directed to the server and 4 to the client. The total packet size in one session is 1080 bytes. Access to the database connection takes place once every 15 minutes.

Transmission of transactions to the server occurs every 90 minutes. Packet data transfer is used, namely the cross-platform SOAP protocol, which can be used in conjunction with other data transfer protocols. SOAP provides additional safeguards for the confidentiality and data integrity, and also offers built-in repetitive logic to offset unsuccessful data

exchange attempts. One packet size is 1192 bytes.

The total amount of data uploaded to the server during one complete loop of communication is 150 kilobytes, and 70 kilobytes loaded on the device.

Thus, in order to ensure full functioning, the system uses only 220 kilobytes during one communication loop. Taking into account the dynamics of the growth in the number of transactions, one can predict that at a maximum load, the Internet traffic of one device will be about 500 megabytes. This provides the potential for the expansion of the functionality and additional download link.

II. Problem solution and Results

To improve the system, it is suggested to introduce a navigation GPS system. The use of modern programmable controllers as part of the equipment makes the system unlimitedly flexible, opens up many opportunities for expansion of the system itself, as well as opportunities to provide it with additional functions. Existing hardware features allow to combine multiple systems into one software and hardware complex. This will make possible not only to track the movement of vehicles, but also to optimize the route network based on the analysis of paid trips, passenger traffic and passenger behavioral models.

Using the GPS module, it is planned to receive information about the location of the transport and transmit it to the processing center [5]. Based on transport location information, bindings of statistics on the number of transactions to the transport route and its schedule can be utilized using certain algorithms to programmatically adjust the transport route, its traffic and idle time. Also, this system can be equipped with sensors for monitoring of transport resources, which will provide information on energy costs and the possibility of their usage optimisation.

The existing hardware of the AFC system has the necessary tools to obtain, store and process the necessary transaction information. Each unit of ground-based public transport is equipped with an on-board computer OCU-10. It, in return, is equipped with GPS and GSM antennas. GSM communicates with the processing center, where the recording of information processing in real time occurs.

After analyzing the capacity of the communication channel, it can be stated that this system has the ability to use a certain amount of traffic to transmit GPS coordinates from the device.

The transmission of one coordinates pair with system information takes 263 bytes. When sending GPS coordinates, every 10 seconds, in the current operating mode of vehicles, traffic consumption per month is about 50 megabytes. This is 9% of the total traffic, taking into account the transfer of GPS coordinates, and allows to use the system's functionality without changing the tariff plan.

To improve the software of an existing hardware base, the following features may be provided by the system:

1. Creation of a timetable for routes.
2. Operational control and management of vehicles on routes.
3. Control of the vehicles' availability in the section of each route in accordance with the approved schedule.
4. Availability of tools for detecting deviations from planned schedules on the line.
5. Traffic monitoring on the routes of controlled vehicles in real time.
6. Visualization of the location of all vehicles on the electronic plan of the area.
7. Control of driver's working time on the line.
8. Ability to load vector graphs of roads.
9. Storage and processing of navigation and telemetry data obtained from vehicles.
10. Receiving report data on the transport work performance.
11. View and analysis of the data in the archive, resolving controversial situations.

In future it is planned to expand the functionality of the system by introducing navigation for the driver, and an information board for passengers. Using the existing GPS tracker as the basis, passengers can be automatically notified about the route and its stops. For the driver it is planned to create a navigation program that will control the speed of transport and its route using data from traffic sensors and will provide guidance to the driver on optimal route decisions and speeds.

Referring to the information on the driver's working time on the line, it is possible to introduce a payroll system for employees in accordance with the data in the transport system. It can be achieved by improving the software, namely, by the implementation of algorithms that are based on the data from all routes for a certain period of time from the archive.

III. Conclusions

The existing automated fare payment system is flexible and has the ability to expand and align with other systems, using only its own hardware base, by improving the software. Implementation of the GPS navigation system will cause a 9% increase in channel traffic, which is entirely within the current system and will not require additional financial costs.

The use of additional functions based on GPS navigation will increase the competitiveness of the system and in the long run will allow to transfer the entire system of vehicles management and monitoring, as well as workers, into an electronic automated system.

References

[1] C. R. García, A. Quesada-Arencibia, T. Cristóbal, G. Padrón, F. Alayón. Systematic Development of Intelligent Systems for Public Road Transport, Sensors, 16(7), 1104, 2016.

[2] A. V. Gusev, V. V. Sergeev Public Transportation Automated Fare Collection Systems Design, Indian Journal of Science and Technology, 9 (47), pp. 1-7, 2016.

[3] A. A. Nepogozhev, S. A. Kemerova. Implementation of transport card to increase the level of fare collection in urban areas, in Generation of Future: Young Scientists View Collection of scientific articles of the 4th International Youth Scientific Conference, India, 2015, 147-50.

[4] S. M. Nasution, E. M. Husni, A. I. Wuryandari. Prototype of train ticketing application using Near Field Communication (NFC) technology on Android device, in Proc. International Conference on System Engineering and Technology, Bandung, Indonesia, 2012, pp. 1-6.

[5] Seo, Jiwon and Walter, Todd. Future dual-frequency GPS navigation system for intelligent air transportation under strong ionospheric scintillation, IEEE Transactions on Intelligent Transportation Systems, volume 15, issue 5, April, 2014, pp. 2224 – 2236.

[6] F. Z. Aralbaev, O. M. Kharkiv. Development of public transport on the basis of the new system of payment of fares, Bulletin of the OGU, 2014, No. 8, pp. 199-204.

Модифицированные карты Кохонена в реконфигурируемых сенсорных системах

Михаль Олег Филиппович,
Дяченко Владислав Александрович

Харьковский национальный университет радиоэлектроники, пр. Науки 14, Харьков, 61166, Украина,
vladyslav.diachenko@nure.ua

Аннотация. *При реализации задач экологического мониторинга окружающей среды, применяется распределённая обработка информации, не предполагающая соподчинения и синхронизации действий. Кроме того, децентрализация допускает реконфигурируемость состава и связей информационного комплекса. Поддержание надёжности системы на удовлетворительном уровне предполагает «интеллектуальное наполнение», с совмещением в одном элементе нескольких функций. Объём информационного потока целесообразно минимизировать с применением принципов кластеризации. Для реализации предложена модифицированная карта Кохонена, поддерживающая параллельный циклический процесс обучения. Рассмотрено три последовательных этапа эксплуатации, охватывающие, соответственно, начальное обучение, текущее дообучение и компенсацию временного тренда.*

Ключевые слова: *карты Кохонена, распределённая обработка, централизованная обработка .*

I. Введение и постановка задачи

В различных предметных областях (ПО), в частности в связи с задачами экологического мониторинга окружающей среды, применяется распределённая обработка (РО) информации [1]: распределённый сбор, накопление, хранение, предобработка и пересылка.

II. Решение проблемы и результаты

Целесообразность РО диктуется распределённым характером ПО. Централизованная обработка (ЦО) менее эффективна, поскольку предполагает дополнительные ресурсные и временные затраты на пересылку информации. В ряде случаев это не приемлемо в связи с ограниченным временем актуальности информации. Кроме того, ключевая особенность ЦО – преимущественно последовательное выполнение действий. РО – изначально распараллелена, т.к. преимущественно не предполагает соподчинения и синхронизации действий. Интерес к РО обусловлен развитием автономных (самоорганизующихся, самоподдерживающихся, либо ресурсно-ограниченных) систем, в которых в течении продолжительного времени информация может сниматься с набора сенсоров, каждый из которых не достижим или ограничен в возможности обслуживания (профилактики, восстановления, калибровки и др.). Для соответствующих ПО целесообразны реконфигурируемые комплексы сбора и предобработки информации. Отдельные сенсоры индивидуально вырабатывают свой ресурс или отрабатывают свой цикл до самовосстановления, после чего теряются (выводятся из эксплуатации), либо «берут паузу» на самовосстановление. Функциональный ресурс системы при этом сокращается, вследствие чего реализуется реконфигурирование связей между сенсорами. При превышении критического уровня потери функциональности (дефицит функционального ресурса не компенсируется реконфигурацией системы), система должна «дозасеиваться» новыми партиями сенсоров. Достаточно очевидно, что надёжность системы может поддерживаться на удовлетворительном уровне при надлежащем «интеллектуальном наполнении» элементов (сенсоров). Целесообразно совмещение в одном элементе нескольких функций: сбор информации, накопление, предобработка, хранение, организация связи и пересылка информации. Объём информационного потока должен быть минимизирован, поэтому предобработка должна включать обобщение и уплотнения, а сбор информации - распознавание и сведение к соотнесению с типовыми объектами или состояниями, т.е. кластеризация. Для реализации указанного, предложены модифицированные карты Кохонена (МКК), поддерживающие параллельный циклический процесс обучения [2].

III. Выводы

Рассматривается три этапа эксплуатации МКК в составе системы с РО: изначальное обучение (исходная кластеризация состояний) сенсора, автономное дообучение «бортовой» МКК сенсора после «высеивания» в пространстве ПО, корректировка (обратная связь) МКК для учёта (компенсации) старения сенсора. Таким образом, второй и третий этапы учитывают, соответственно, пространственный и временной аспекты эксплуатации системы РО.

Перечень литературы

[1] G. Churyumov, V. Tkachov, V. Tokariev, V. Diachenko METHOD FOR ENSURING SURVIVABILITY OF FLYING AD-HOC NETWORK BASED ON STRUCTURAL AND FUNCTIONAL RECONFIGURATION // Информационные технологии и безопасность. Материалы XVIII Международной научно-практической конференции ИТБ-2018. – К.: ООО "Инжиниринг", 2018. – с. 145 - 159

[2] Дяченко В.А., Михаль О.Ф. Интеллектуальный аспект обучения модифици-рованных самоорганизующихся карт Кохонена // Бионика интеллекта: науч.-техн. журн. – Х.: Изд-во ХНУРЭ, 2015. – Вып. 2 (85). – С. 35-40.

Генеративно-соревновательная конвертации голосовых данных

Михаль Олег Филиппович,
Логвин Антон Алексеевич

Харьковский национальный университет радиоэлектроники, пр. Науки 14, Харьков, 61166, Украина,
logvin.anton.work@gmail.com

Аннотация. *В рамках задачи создания речевого интерфейса для задачи преобразования голоса сравниваются два метода: GAN и DNN. MCD выбран в качестве показателя оценки. Показано, что метрика очень чувствительна, но слабо коррелирует с реальным качеством, воспринимаемым человеком.*

Ключевые слова: *voice conversion, deep neural network, text-to-speech, generative-adversarial networks, Mel-cepstral distortion.*

I. Введение и постановка задачи

Концептуальное требование к человеко-машинному интерфейсу (ЧМИ) – максимальная комфортность, естественность и приближение к характеристикам межчеловеческого взаимодействия. Затраты значительных творческих усилий на разработки в этом направлении – обусловлены тем, что качество ЧМИ – это более низкая утомляемость (продолжительное сохранение работоспособности) персонала. Одновременно это снижение вероятности ошибок операторов, и повышение эффективности всей человеко-машинной системы [1].

II. Решение проблемы и результаты

Важной составляющей общей проблематики разработки ЧМИ является речевой интерфейс. В информационном плане, речевой канал человека существенно меньше по объёму, чем зрительный. Но в плане важности (ценности) передаваемой по нему информации, - соотношение противоположное. Объяснение этому следующее. Поскольку человек – существо социальное, многие важные задачи решаются группами людей. Часто, группа бывает разделена в пространстве, так что каждый индивид получает уникальную информацию. Реальны ситуации, при которых только один индивид получает информацию, критическую для всей группы (опасность или, наоборот, существенный выигрыш). Тогда речевой канал – важное средство передачи критической (сигнальной или командной) информации. Результат – выигрыш всей группы. Масштабы применения компьютеров в качестве усилителей человеческого интеллекта становятся столь значительными, что группа - становится человеко-машинной [2]. Отсюда важность речевого человеко-машинного интерфейса - комфорт передачи критической информации.

Ключевая составляющая проблемы - задача конвертации голоса (voice conversion). Традиционное решение - глубокие нейронные сетей (DNN - deep neural network) в качестве акустических моделей для TTS (text-to-speech) и VC (voice-conversion). Они могут достаточно точно моделировать соотношение между входными данными модели и звуковыми характеристиками. Но речевые параметры имеют тенденцию к сверх-сглаживанию, что снижает качество речи.

Рассматривается - использование генеративно-состязательной сети (GAN - generative-adversarial networks), которая. представляет собой модель, воспроизводящую сложную взаимосвязь между вектором входных данных случайного шума и выходных параметров с помощью состязательного процесса. Используются две подмодели: генератор (получить на вход случайный шум и сгенерировать данные) и дискриминатор (показывает вероятность того, что данные, поданные на вход, получены из тренировочного датасета или созданы генератором.). В качестве метрики оценивания испытана MCD (Mel-cepstral distortion).

III. Выводы

Кепстральные преобразования демонстрируют высокую чувствительность, но вцелом MCD не позволяет выделить преимущества GAN, непосредственно воспринимаемых на слух. В последующей работе для оценки качества синтезированной речи следует использовать MOS (mean opinion score) - численную меру оцениваемого человеком общего качества события или опыта.

Перечень литературы

[1] Михаль О.Ф. Информационный аспект организации индивидуальной творче-ской человеческой деятельности. // Информатика, математическое моделирование, экономика: Сборник научных статей по итогам Третьей Международной научно-практической конференции, г. Смоленск, 24-26 апреля 2013 г. В 3-х томах. Том 2 – Смоленск: Смоленский филиал Российского университета кооперации, 2013. – С. 81-88.

[2] Михаль О.Ф. Эволюционирование мультиагентной системы как аналог формирования индивидуального человеческого интеллекта // Бионика интеллекта: научн. техн. журнал. - 2016. - 2 (87). - С. 42-47.

Распределённые базы данных применительно к задачам управления системами интернета вещей

Михаль Олег Филиппович,
Лукашёв Сергей Андреевич

Харьковский национальный университет радиоэлектроники, пр. Науки 14, Харьков, 61166, Украина,
serhii.lukashov@nure.ua

Аннотация. *Интернет вещей - это концепция вычислительной сети физических объектов, оснащенной встроенными технологиями для взаимодействия друг с другом или с внешней средой. В рамках этой концепции рассматриваются вопросы проектирования распределенных баз данных применительно к организации систем управления отдельными сегментами Интернета вещей.*

Ключевые слова: *интернет вещей, распределенные базы данных.*

I. Введение и постановка задачи

Интернет вещей (ИВ) - (IoT - internet of things) – есть глобальная сеть подключенных к интернету физических устройств («вещей»), оснащенных сенсорами и устройствами передачи информации. Устройства в ИВ могут быть подключены к центрам управления и обработки информации. В связи с ИВ, организация таких сетей рассматривается как явление, способное перестроить экономические и общественные процессы. Поэтому актуальным является технический аспект - исследования по проектированию и использованию распределенных баз данных (РБД) в связи с концепцией ИВ [1].

II. Решение проблемы и результаты

Среда, в которой разворачивается ИВ может быть охарактеризована как многоцелевая информационная структура. В ней прикладная область есть реальный мир, «заселённый» подключёнными к ИВ «вещами». По мере разрастания числа «вещей», она видоизменяется. Информация о прикладной области есть контент ИВ: записи в РБД, совокупность которых является «статической частью» ИВ. Транзакции внутри РБД - «динамическая часть» ИВ. Она реализуется в процессоре, с которым пользователи работают через два интерфейса: рабочий и реконфигурационный. Пользователи ИВ - по крайней мере 4 группы: (1) люди-потребители услуг ИВ; (2) «вещи»- потребители услуг ИВ; (3) люди-операторы (исполнители), работающие в сфере ИВ и (4) «вещи», реализующие ИВ. 1 и 2 работают через рабочий интерфейс, 3 и 4 – через реконфигурационный. Сведение людей и «вещей» в единый список отражает тот факт, что «вещи», фигурирующие в ИВ, наделены известной долей интеллекта (smart), т. е. компьютеризированы, т. е. по определению являются усилителями функций человеческого интеллекта [2]. ИВ есть интеллектуализация человеческого окружения, т. е. перенос туда часть человеческих интеллектуальных функций. Процесс этот необратим (никто не будет (не сможет) «забирать» эти функции назад, потому что это будет сознательный отказ от определённых аспектов комфортности окружения) и по своим темпам – не соизмерим с процессом эволюции человеческого мозга. Поэтому у человечества – нулевые шансы, что оно будет «умнеть» быстрее, чем компьютеризируемое им человеческое окружение. Поэтому уход человечества в боковую (не основную) ветвь эволюции разума – вопрос реально обозримого времени. В рамках концепции ИВ, люди (как социально-культурное явление) рассматривают в настоящее время вопросы проектирования РБД применительно к организации систем управления отдельными сегментами ИВ. Но, как и всякая концепция, ИВ ограничен во времени уже в силу того, что он ограничен в своём концептуальном развитии возможностями человеческого мозга.

III. Выводы

Достаточно очевидно, что проектирование РБД и использования веб-технологий для интерфейсов приложений возможны только до определённого уровня сложности [3]. Эти функции будут постепенно и плавно перенесены на компьютерные системы, которые будут поддерживать более высокий уровень сложности, и это будет знаменовать смену носителя самой концепции ИВ, т.е. уход человечества в боковую ветвь развития.

Перечень литературы

[1] Михаль О. Ф. Глобальный системный контекст развития ЭВМ // Информати-ка, математическое моделирование, экономика: Сборник научных статей по итогам Второй Международной научно-практической конференции, г. Смо-ленск, 20 апреля 2012 г. В 3-х томах. Том 1 – Смоленск: Смоленский филиал АНО ВПО ЦС РФ "Российский университет кооперации", 2012. – с. 38-47.

[2] Михаль О.Ф. Синтез модели клеточного автомата на сети Петри. Часть I. Гносеологический аспект. // Информатика, математическое моделирование, экономика: Сборник научных статей по итогам Третьей Международной науч-но-практической конференции, г. Смоленск, 24-26 апреля 2013 г. В 3-х томах. Том 2 – Смоленск: Смоленский филиал Российского университета кооперации, 2013. – С. 89-94.

[3] Михаль О.Ф. Синтез модели клеточного автомата на сети Петри. Часть II. Масштабируемая структура. // Информатика, математическое моделирование, экономика: Сборник научных статей по итогам Третьей Международной научнопрактической конференции, г. Смоленск, 24-26 апреля 2013 г. В 3-х томах. Том 2 – Смоленск: Смоленский филиал Российского университета кооперации, 2013. – С. 94-103.

Адаптивные клеточные автоматы к задачам моделирования динамических систем

Михаль Олег Филиппович,

Севостьянова Елена Николаевна

Харьковский национальный университет радиоэлектроники, пр. Науки 14, Харьков, 61166, Украина,

olena.sevostianova@nure.ua

Аннотация. *Обсуждаются перспективы клеточных автоматов как аппарата для моделирования поведения кластерных систем. Предложены к рассмотрению иерархические клеточные автоматы. Концептуально разработана двухмерная двухуровневая схема. Ожидаемые результаты обсуждаются для перспективных направлений моделирования.*

Ключевые слова: *клеточные автоматы, иерархические клеточные автоматы.*

I. Введение и постановка задачи

Перспективность применения клеточных автоматов (КА) для моделирования поведения кластерных систем обусловлена следующим. Кластер есть объединение нескольких однородных элементов, рассматриваемое как самостоятельная единица, обладающая определёнными свойствами. Принадлежность элементов к кластерам понимается как систематизация, классификация, и др (статический аспект кластеризации). Работа с элементами при этом сводится к соотнесению их с определёнными кластерами. Представляет интерес поведение кластерных систем (КС) в динамике: формирование, рост, эволюционирование, деградация. Статический аспект при этом становится набором временных срезов динамического аспекта. Представляют интерес поведенческие модели КС, минимально затрагивающие конкретику прикладной области. В этом - «изобразительные средства» КА варьируются в широких пределах, базируясь на малых наборах правил [1].

II. Решение проблемы и результаты

Интересны иерархические КА-структуры (ИКА). Окружающая действительность (внешний мир, живая природа, социальные структуры, техника, информационные системы) организована иерархично. Соответственно, моделирование элементов окружающего мира целесообразно именно на ИКА. В многоуровневом варианте, поле ИКА подразделено на соседствующие не пересекающиеся ячейки. В матричной интерпретация, это битовое поле размером M□N ячеек; каждая ячейка размером mi□nj элементов, где i ∈ (1, 2, …, M), j ∈ (1, 2, …, N). Ячейки изображают отдельные кластеры; поле вцелом – всю ИКС. Кластеры могут быть разных размеров (параметр модели). Некоторые битовые поля могут содержать «1», обозначающую конкретный кластерный признак. В зависимости от условий моделирования, «1» могут перемещаться внутри ячеек (случайно или детерминировано); проходить «сквозь стенки ячеек» (переходить из данной ячейки в соседнюю); «отражаться от стенок» (оставаться в своей ячейке); раздваиваться (превращаться в два экземпляра). При столкновениях, «1» могут сливаться или рекомбинировать. В выборе вариантов правил поведения «1» есть значительная свобода; следовательно, имеется возможность параметрического расширения модели.

Изучаемыми характеристиками модели являются «населённости» отдельных кластеров. Один из ожидаемых эффектов – достижение состояния насыщения при неполном заполнении ячеек ИКА. Интересно так же изучение эволюции заполнения кластеров от единственной «1» до «насыщения». Одно из известных прикладных явлений, которое может быть смоделировано в рассматриваемой системе, – «закон Амдала» – наличие порога прироста производительности многопроцессорной вычислительной системы с общей памятью. Развитием изучения этого явления может быть моделирование на ИКА трафика компьютерных сетей [2].

III. Выводы

Текущее состояние – разработана концепция, программно реализованы (этап отладки) ключевые элементы, идёт планирование машинных экспериментов.

Перечень литературы

[1] Севостьянова Е.Н., Михаль О.Ф. Разработка концепции моделирования динамики формирования и эволюционирования кластерных систем на клеточных автоматах. // Комп'ютерні інтелектуальні системи та мережі. Матеріали XI Всеукраїнської науково практичної WEB конференції аспірантів, студентів та молодих вчених (21-23 березня 2018 р.). – Кривий Ріг: ДВНЗ «Криворізький національний університет», 2018. – с. 31-34 ..

[2] Севостьянова Е.Н., Михаль О.Ф. Моделирование динамики эволюционирования кластерных систем на клеточных автоматах // Друга міжнародна науково-технічна конференція "Комп'ютерні та інформаційні системи і технології". Збірка наукових праць. Харків: ХНУРЕ. 2018. - С. 53-54.

Локально-параллельное построение четкого множества, среднеквадратически минимально удаленного от исходного нечеткого

Михаль Олег Филиппович,
Федоренко Константин Игоревич

Харьковский национальный университет радиоэлектроники, пр. Науки 14, Харьков, 61166, Украина, mesomix@gmail.com

Аннотация. *Рассматривается локально-параллельная (ЛП) версия алгоритма построения функции принадлежности отдельного множества, среднеквадратичного минимального расстояния от исходного нечеткого множества. Запись ЛП состоит из смежных непересекающихся битовых сегментов. Эффективность алгоритма ЛП, по сравнению с последовательным, растет пропорционально количеству сегментов.*

Ключевые слова: *локально-параллельная, функция принадлежности, нечеткое множеств, четкоге множество.*

I. Введение и постановка задачи

Сохранение баланса черного - белого (ч/б) при преобразовании серого (тонового) изображения в контрастное ч/б, - актуально, поскольку обеспечивает сокращение объема информации при сохранении основного содержания. В более широком контексте, преобразование гладкого профиля функции принадлежности (ФП) μ нечеткого множества (НМ) μнм в ступенчатый (дискретный) профиль ФП четкого множества (ЧМ) μчм, есть задача принятия четких решений при нечетких исходных данных.

II. Решение проблемы и результаты

В теории НМ имеется теорема: обычное, традиционное ЧМ, построенное по правилу if (μнм ≤ 0,5) then (μчм = 0) else (μчм = 1), минимально (в среднеквадратическом смысле) удалено от исходного НМ. На основе этой теоремы может быть построен алгоритм оптимального уплотнения серого изображения в ч/б. Согласно определению ФП, μ ∈ [0, 1] описывает в теории НМ степень принадлежности элемента (в нашем случае – значение пиксела серого изображения) к некоторому множеству (оттенкам серого). Ситуация μ = 1 соответствует полной принадлежности; μ = 0 – непринадлежности. Частичная принадлежность описывается дробными значениями μ.

Человеческий глаз способен различать только несколько десятков градаций серого. Поэтому в реальных технических системах целесообразно перейти от непрерывного ряда возможных значений ФП к дискретному набору значений. Тогда - конкретное значение «степени серости» реально может быть описано двоичным числом длиной, допустим, 5 – 6 бит. В настоящее время преобладают 64-битные компьютеры, поэтому целесообразно представить фрагмент изображения, содержащий 10 – 12 пикселов, в виде единого регистрового представления (РгП). В нём соседствуют без пересечения 5-ти – 6-ти битовые сегменты. Такое представление информации называется локально-параллельным (ЛП) [1]. В ЛП-представлении значения ФП μнм и μчм хранятся в сегментах РгП.

Алгоритм, реализующий логику минимальной среднеквадратической удалённости, включает разделение исходного РгП на два, содержащих чётные и нечётные сегменты. Далее эти РгП вычитаются из образцовых РгП-констант, содержащих в соответствующих сегментах значения, соответствующие μ = 0,5. Превышение уровня 0,5 приводит к заимствованию из старшего разряда (младшего разряда соседнего левого сегмента), где в РгП-константе предусмотрительно стоит специальная «резервная» единица. Картина расходования «резервных» единиц позволяет построить маски, по которым из исходного РгП формируется «ч/б – РгП» согласно (1).

III. Выводы

На текущем этапе – концепция алгоритма разработана, программное обеспечение отлажено. Согласно плану экспериментов, исследуется выигрыш в производительности в зависимости от параметров модели. Эффективность ЛП алгоритма по сравнению с последовательным растет пропорционально числу сегментов [2]. Выигрыш по времени - пропорционально числу сегментов РгП.

Перечень литературы

[1] Михаль О.Ф. Локально-параллельное моделирование в рамках парадигмы системы массового обслуживания // Повышение конкурентоспособности социально-экономических систем в условиях трансграничного сотрудничества регионов: Всероссийское научное периодическое издание по итогам III Всероссийской научно-практической интернет-конференции с международным участием. – Ялта: РИО ГПА (филиал) ФГАОУ ВО «КФУ им. В.И. Вернадского» в г. Ялте, 2016. – С. 158-160.

[2] Федоренко К.И., Михаль О.Ф. Сравнение последовательнго и локально-параллельного вариантов алгоритма построения функции принадлежности чёткого множества, среднеквадратически минимально удалённого от исходного нечёткого множества //20-й Юбилейный Международный молодёжный форум «Радиоэлектроника и молодёжь в XXI веке». Сб. Материалов форума. Т. 5. - Харьков: ХНУРЭ, 2016. - С. 224-225.

Automation of the Educational Process in Ukraine Higher Military Education Institutions

Kalachova Vironika Valeriyivna,
Pichugin Mikhail Fedorovych,
Kolomiytsev Oleksiy Volodymyrovych,
Misyura Oleg Mykolayovych,
Trystan Andriy Viktorovych,
Lazebnyk Sergiy Volodymyrovych,
Babenko Oleksandr Ivanovych,
Pylypenko Vitaliy Mykolayovych,
Kryzhanivskyy Igor Mykolayovych,
Hrytsenko Lyudmyla Anatoliyivna

Kharkiv National Air ForceUniversity, 77/79 Sumska Str, Kharkiv UA-61023, Ukraine, info@hups.mil.gov.ua

Abstract. *Kharkiv National Air Force University is conducting research on improving the effectiveness of training and assessment of the its personnel, based on the use of innovative information technologies, organization and implementation of distance learning. At present, the main information technologies for automation of learning and realization of its distance form which were developed and implemented in KhNAFU with the purpose of effective specialists training increase are: the informational and educational environment «DIALOG»; the universal system for the development and conducting of computer tests; the complex of designing the academic schedule «CASCAD». In addition, the learning process successfully uses the distance learning system with the open source code – MOODLE. Thus, the educational establishment, from the point of view of automation and application in the educational process of modern information technologies fully prepare to integration in educational space of European Union and to implementation of the European norms and standards in education and science Armed Forces of Ukraine.*

Keywords: *information technologie, distance learning, computer test, program complex for designing the schedule, distance learning system, automated testing control.*

I. Introduction and Problem statement

Global informatization, development of telecommunication technologies and facilities of the computing engineering significant changes in the forms of educational process. The role of professional and continuous education is growing, without interruption from the main work activity. All this contributes to the development and implementation based on information technology, distance forms and distance learning systems and automation of learning process in general [1].

The introduction of distance learning in the process of training and retraining of specialists in the educational system of Ukraine is due to a number of reasons: the aspiration of Ukraine to integrate into the European Union and the introduction of European norms and standards in its education and science; the intensity of the development of science requires constant improvement of professional knowledge and skills of specialists of different branches, directions and specialties; only distance learning technologies are able to provide timely correction of the content of training military specialists at the expense of high speed updating of knowledge in the information and educational environment; high economic efficiency of distance learning [1-3].

Kharkiv National Air Force University (KhNAFU) is conducting research on improving the effectiveness of training and assessment of the its personnel, based on the use of innovative information technologies, organization and implementation of distance learning (DL) [2, 3].

II. Problem solution and Results

The main information technologies for automation of learning and realization of its distance form which were developed and implemented in KhNAFU with the purpose of effective specialists training increase are: the informational and educational environment «DIALOG»; the universal system for the development and conducting of computer tests; the complex of designing the academic schedule «CASCAD». In addition, the learning process successfully uses the distance learning system with the open source code - MOODLE [1-10].

As a result of conducting research on increasing the effectiveness of combat training through the use of distance learning technologies, the informational and educational environment «DIALOG» has been developed, which allows: to plan training by distributing subjects by type of training; to study as a group according to the subjects for which they are studying; organize classes in accordance with the requirements of the orders of the Ministry of Defense of Ukraine regarding the training of military specialists; to carry out automated control of testing of those who learn with automatic fixing of time and results of passing tests; control the process of learning by the average score for the group, the course through the system of statistical data generation (Fig. 1) [2, 3].

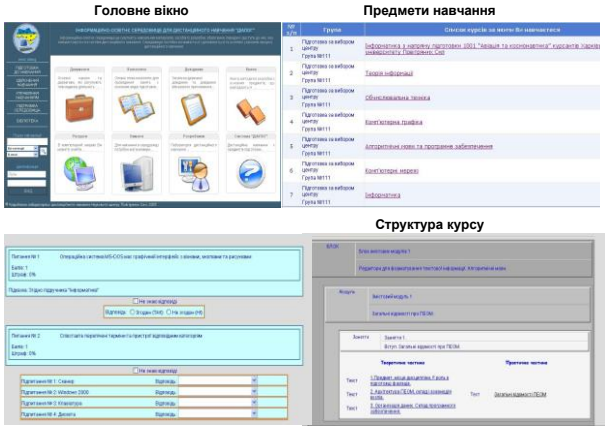


Figure 1. The specialized informational and educational environment «DIALOG» for distance learning

The universal system for the development and conducting of computer tests has been developed and implemented. The developed software application allows to solve the following tasks: locally, on separate PCs, to develop computer tests and conduct testing and self-control of those who study; choose the types of answers to questions (with one correct answer, with a few correct answers, with a response in the form of a record); divide the questions by category and type of answers and give the corresponding number of points for the correct answer; to randomly distribute questions by categories; use as a matter of a variety of document fragments (graphic, formulas, etc.) from other programs (MS Word, MS Excel, etc.); enter type of time limit and time limit; to pass the test and return to the questions; at the end of the test, analyze the responses (Fig. 2) [3-7].

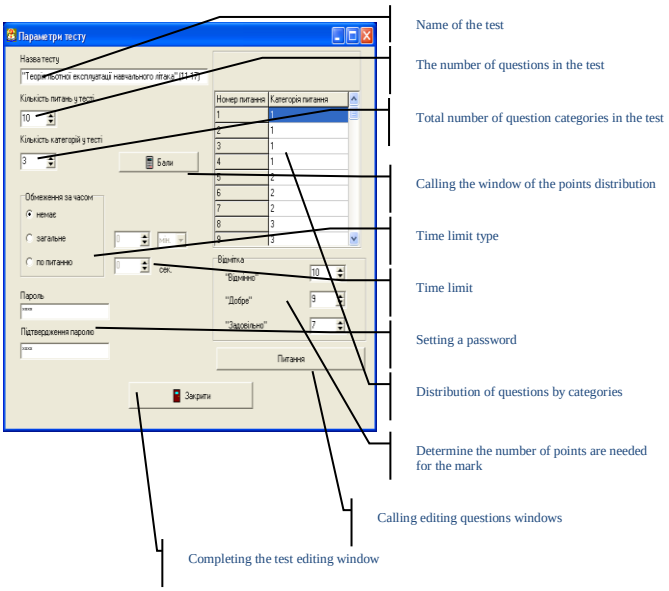


Figure 2. The window for creating (editing) the test parameters of a universal system for developing and conducting computer tests

Also, the MOODLE (Modular Object-Oriented Dynamic Learning Environment), a modular object-oriented learning environment, also known as a learning management system or a virtual learning environment, is deployed and used by the KhNAFU. To ensure work, it can be installed on a web server on its own computer or hosting company (Fig. 3-4) [1, 2].

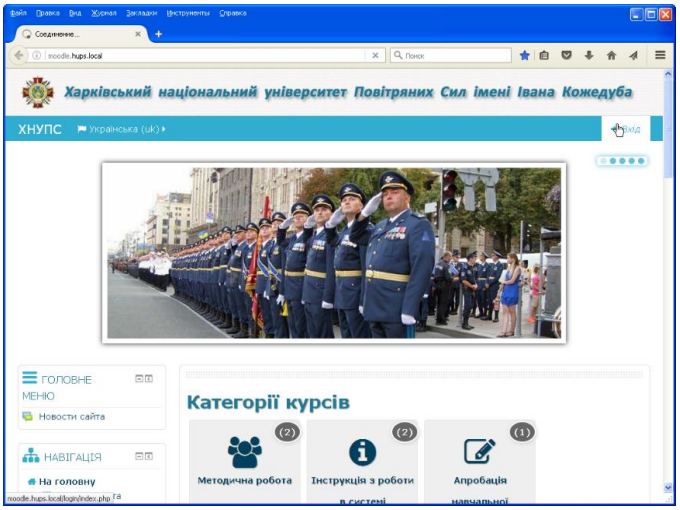


Figure 3. The system MOODLE, deployed on the server of the university

Figure 4. The system MOODLE scheme of work

The main advantages of the software systems developed and actively used at the KhNAFU and responsible for assessing knowledge («DIALOG», the universal system for the development and conducting of computer tests, MOODLE) are: automation of knowledge control processes for those learning; exclusion of "human factor", impartiality of evaluation; automatic fixing of test results; automatic statistical processing of test results and the formation of accounting records for personnel training [1-10].

The developed program complex of the automated system of designing the lessons schedule is deployed at the work places of the educational departments of the faculties and the department of the university and is successfully used during the planning of the educational process at the university (Fig. 5) [8-10].

The main advantages of the developed software complex are: it is an unique software product, created at the university, which fully corresponds to the content of all stages of the planning of training sessions for the semester; automatic control of the formation lessons schedule according to the

defined criterias of the quality of the lessons planning; automatic fixing of all user actions to change data; automated formation of reporting (statistical) documents for the planned learning process.

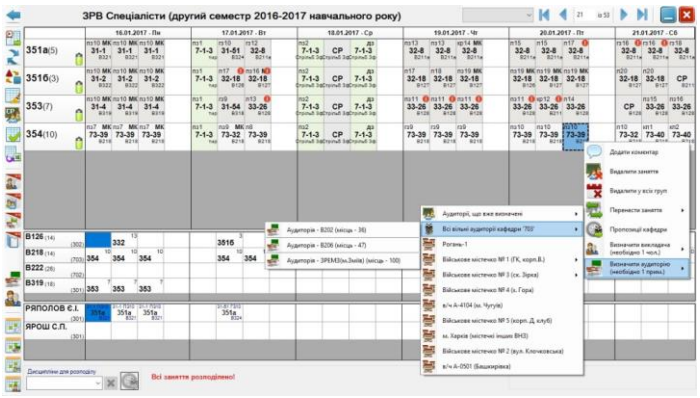


Figure 5. User interface program complex of automated system of designing the lessons schedule «CASCAD»

Perspective directions of improvement of the program complex «CASCAD» are: expansion of the created software complex functionality due to the development of new modules: the account of participants in the educational process; account of the success and ranking of university cadets (students); expansion of the list of accounting documents; development of procedures for the automatic formation of the basic optimized lessons schedule for the semester, taking into account the given restrictions (using genetic algorithms); creation of software modules of management and operative adjustment of curricula directly during the educational process; creation of an complex system of automated control of the Higher Military Educational Institution (based on the integrated components: personnel, logistics, planning and management of the educational process, financial support, etc.) [8-10].

III. CONCLUSIONS

Thus, it is necessary to mark that existing on current time in KhNAFU a educational-methodical base, hardware software and highly skilled scientifically-pedagogical composition of university, allow with a complete confidence to talk that educational establishment, from the point of view of automation and application in the educational process of modern information technologies fully prepare to integration in educational space of European Union and to implementation of the European norms and standards in education and science both Armed Forces of Ukraine and the Ukraine in general.

REFERENCES

[1] Distance learning. Fundamentals, concepts, perspectives. (the neck is given to the Ministry of Education and Science of Ukraine letter № 1 / II-10437 dated December 22, 2009) / Romanenko I.O., Sumtsov D.V., V.V. Kalachova, Suk O.P. // Tutorial. Kharkiv: NTU "KhPI", 2010, 276 p.

[2] Ways of modeling the system of distance learning of a higher educational institution in the context of reforming the educational system of Ukraine / V.V. Kalachova, T.O. Ivakhnenko, O.M. Nosik // Systems of information processing. - Kh. KhAFU, 2012. - № 3 (101). - P. 258-260.

[3] Intelligent Subsystems for Testing Knowledge for Distance Learning of Military Professionals / V.V. Kalachova, M.M. Kolmykov // New technologies - for airspace protection / Eighth scientific conference of KhAFU April 13-14, 2012 Abstracts - Kharkiv: KhAFU, 2012. - P. 132-133.

[4] Probabilistic-informational approach on the way of solving the task of assessing the level of combat training of the authorities of the Armed Forces of Ukraine / I.O. Romanenko, S.V. Dudenko, O.P. Babenko, V.V. Kalachova // Collection of scientific works of Kharkiv Air Force University. - Kh.: KhAFU, 2013. - №. 1 (34). - P. 36-39.

[5] Ways of realization of information technology for assessing combat training of military commanders of the Armed Forces / I.V. Ruban, S.S. Tkachuk, V.V. Kalachova, A.M. Nosik, A.M. Tkachov // Science and technology of AFAFU. - Kh.: KhAFU, 2013. - №. 4 (13). - P. 14-17.

[6] The method of integral assessment of the degree of attestation and the structural algorithm of software testing / K.S. Smelyakov, S.V. Alekseev, I.O. Romanenko, O.P. Babenko, I.V. Ruban, V.V. Kalachova // Collection of scientific works of KhAFU. - H. KhAFU, 2013. - № 2 (35). - P.120-126.

[7] Theoretical and informational model of the automated system for assessing combat training of military command units of the Armed Forces / I.V. Ruban, S.S. Tkachuk, V.V. Kalachova // Science and technology of AFAFU. - Kh. KhAFU, 2013. - № 3 (12). - P. 22-26.

[8] Mastering the skills of working with the software complex "Cascade" - as a way to optimize the work of the Secondary Education and European Integration of Higher Education of Ukraine / Kalachova V.V., Misyura O.M., Tretyak V.F., Kuzhel I.E., Trublin O.A., Shigimagha N.V., Shkurupiy S.S. // Educational and methodical collection of KhNAFU. - Kh. KhNAFU, 2018. - № 1 (147). - P. 38-47.

[9] Analysis of the features of development, operation and further development of the complex of programs of the automated system of designing the academic schedule "Cascade" / O.M. Misyura, M.F. Pichugin, S.V. Alekseev, V.V. Kalachova, O.A. Trublin // Systems of information processing. - Kh.: KhNAFU, 2017. - № 4 (150). - P. 193-198.

[10] Features of the development of the interface design of the complex program of the automated system for designing the schedule of classes at the Kharkiv National Air Force University "Cascade" / M.G. Tishchenko, O.M. Misyura, V.F. Tretyak, V.V. Kalachova, O.A. Trublin // Collection of scientific works of KhNAFU. - Kh. KhNAFU, 2018. - № 3 (57). - P. 144-151.

Approach to protecting video informational resource in the infocommunication component of critical infrastructure

Ryabukha Yuriy Mykolaiovych[1]
Vlasov Andrii Volodimirovych[1,2],
Severinov Oleksandr Vasyliovych[2]
Mazin Petro Krasnoslavovych[1]
Tretiak Viacheslav Fedorovych[1]

[1]*Kharkiv National University of Air Force by named I. Kozhedub, 77/79 Sumstska street, Kharkiv UA-61023, Ukraine, vav_and@i.ua*

[2]*Kharkiv National University of Radio Electronics, 14 Nauky Ave, Kharkiv UA-61166, Ukraine*

Abstract. *Is presented approach to the protection video information resource in infocommunication component of critical infrastructure that directed toward the development of the technology of processing video information resource for the purpose of the guarantee of its information security, improvement in the protection of resource itself and its service information, based on the development of the complex of the methods of data processing resource components.*

Keywords: *coding, video stream, video frame, semantic significant, processing, compact representation.*

I. Introduction and Problem statement

Complex application of data of infocommunication systems, allows to increase significantly dynamism, flexibility and management efficiency. Thus, the problem of information security and protection of the processed information resource cannot be solved without improvement of the existing technologies of processing and protection of information resource, and introduction of new technologies.

Actual are requirements: ensuring high-quality providing video data, efficiency of delivery of a video information, ensuring necessary level of safety and protection of video information resource.

Thus, as show researches [1-3] by the most significant threats to security to video information resource there are threats of availability and integrity, and from the point of view of ensuring protection – interception, opening and recognition of a resource.

Therefore, the complex problem of protection of a dynamic video information resource in an infocommunication component of control systems of objects of critical structure with simultaneous ensuring information security of this resource, is actual scientific applied research.

II. Problem solution and Results

It is offered to conduct researches and to develop technology of processing of video information resource which will realize the following methods:

- automatic detection and allocation of semantic significant information of the video frames (on the basis of the cascade scheme of processing of a video stream);
- classifications of degree of a semantic saturation of the video frames (or structural unit of a video stream) on the basis of their hierarchical clustering (both in temporary, and in spectral and spatial areas);
- estimates of information intensity of a video stream taking into account its structure and the executed classification semantic video frames saturations (fragments or macro blocks);
- structural processing of the video frames (its macro blocks) with application of selective approaches for decrease in intensity of the transferred video data with use of decisive rules in spectral space (taking into account identification and closing of significant structural units, and also coordination of future code designs);
- differential processing of the transformed submission of the video frames (coding of the video frames with adaptation of parameters depending on a class of a semantic saturation);
- defense of dynamic video information resource with forming of a few channels of treatment and transmission of video stream in obedience to classification of semantic maintenance of macro blocks of video frames;
- reconstruction of a video stream (video images) on the basis of decoding of channels taking into account a class of a semantic saturation of video images (fragments, macro blocks), intra personnel selection of structural units of a basic shot, the created channel for steganography and the introduced enciphering methods.

Complex development and application of these methods will allow to develop technology of processing of video information resource and to improve protection of video information resource and office information in an infocommunication component of critical infrastructure with providing necessary (not below set) the level of confidentiality and availability of a resource, and also saving (control) of key (semantic significant) information.

Process of formation of a video stream is based on consecutive creation of a chain of the video footage of different type. The type of frames of a video stream is meant as a way of coding and storage of information on the next frame differing from each other in existence or lack of dependences of this frame from previous and the subsequent.

Thus, the video stream consists of consistently created groups of the video frames. Each group of the video frames consists of three types of the video frame: intra (I-frame), predicted (P-frame) and bi-predicted (B-frame) [4].

It is offered to make the analysis and processing of structural unit of a frame for the brightness components, and to carry out procedures of closing (enciphering) and coding for all components (macro blocks) of a frames.

The block diagram is submitted of the offered technology of processing of video information resource in an infocommunication component of critical infrastructure on the Fig. 1.

Processing can be realized at different stages of formation, processing and transfer of video data, namely:

1) encryption of video stream (all operations on the decline of intensity of stream and anti jamming encryption are executed with the already hidden view data);

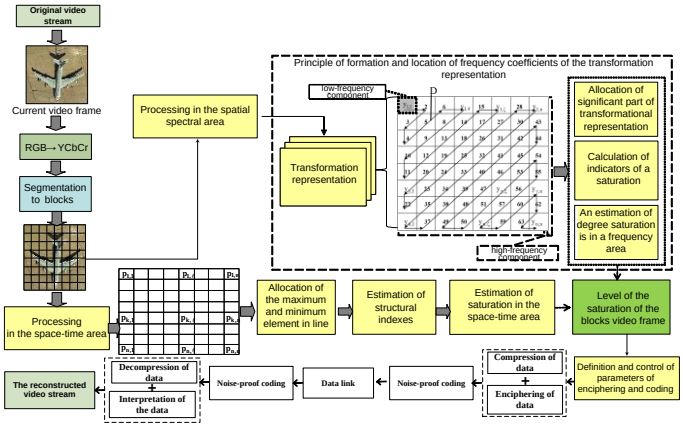


Figure 1. The block diagram of the offered technology of processing of video information resource

2) after compression submission of video data is created (before the coded video stream gets to a communication channel);

3) in the course of coding (algorithms of enciphering are integrated into the standardized process on processing of initial video data for decrease in their intensity).

For the removal of lacks of every variant it is suggested to use selective approach (data are closed in the process of their encryption). Such realization is real to development and introduction in the handling systems of data, where realization of programmatic additions and their integration are assumed in a video codec. For this variant encryption and encipherement are executed for basic data as far as the receipt of them on treatment.

To eliminate the maximum amount of redundancy in video stream processing, it is proposed to use the basic I-frame, since it contains the maximum amount of information, and other types of frames contain up to 70% of references to it [1, 2]. At the same time, developed methods for processing and hiding video data (for covert channel), will be based on the concealment of only I-frames. Thus, complete hiding of the entire video sequence with its minimum redundancy is ensured.

The processing process can be implemented at different stages of the formation, processing and transmission of video data, namely:

1) before encoding the video stream (encryption algorithms are applied to the newly created (uncoded) source video data; all operations to reduce the intensity of the stream and error-correcting coding are performed with already hidden video data);

2) after the compression representation of the video data has been formed (before the encoded video stream enters the communication channel);

3) in the encoding process (encryption algorithms are integrated into a standardized process for processing the original video data to reduce their intensity (at various stages of compression)).

The option of encrypting the source data before encoding has the following disadvantages:

- does not take into account the reduction of redundancy in the source video data;

- after encoding, an increase in the initial intensity of the video stream occurs as a result of the destruction of its structure due to pre-encryption;

- an increase in the intensity of encoded encrypted video data entails an increase in the time required to transmit this data in the communication channel.

The option of hiding the video stream after its compression allows reducing the preliminary redundancy of the original video stream and reducing the processing time (including encryption). It provides a high level of information closure, but at the same time they have significant drawbacks:

- in case of errors in the communication channel, error propagation occurs;

- cryptographic processing is subject to the entire video information flow, which increases the total processing time of the generated video data on the transmitting side and the processing time of video data on the receiving side.

Therefore, to eliminate these shortcomings, it is proposed to use a selective approach (an option in which data is closed in the process of encoding it). This approach is real to the development and implementation of data processing systems, where it is possible to implement software additions and integrate them into a video codec. For this option, encoding and encryption are performed for the original data as they are received for processing.

In the process of forming a video information stream in the implementation of a selective approach is achieved:

- raising the information content of the transmitted structures and reducing the initial intensity;

- eliminates redundancy (reduces the amount of information) that can be used in cryptanalysis;

- decreases the encryption time by reducing the length of processed messages.

The selection mechanism means closing not the entire video frame, but only its significant components.

A significant component is understood to be such a component of a video frame that carries the greatest semantic and structural information content. In the process of automatic selection of significant components, it is proposed to take into account the structural features of video stream formation.

For the selection of significant structural units are invited to identify the most informative, in terms of structural and semantic content, the components of the base frame. Since the luminance component of the video frame carries the most complete information, it is proposed to identify significant structural units on the basis of the luminance components. Therefore, the decision to close the structural unit is proposed to be carried out according to the results of the analysis of the information component of the aggregate of the blocks of the luminance component.

To determine the energy saturation of blocks, it is proposed to introduce the concept of blocks of three types:

- slightly saturated blocks (blocks in which there are uniform sections of the image);

- average saturation (blocks in which there are minor differences between the pixels, respectively, smooth transitions of contrast are present);

- highly saturated blocks (blocks in which there are sharp transitions of brightness and contrast of the image). [6]

It is proposed to evaluate the structural and semantic information content of the structural unit (macroblock) from the standpoint of spectral characteristics [3, 7] or on the basis of metrics [6, 7].

A system of indicators has been developed for identifying the most significant blocks of the brightness component of a video frame according to the degree of semantic and structural saturation based on the assessment of indicators: in the space-time domain and in the space-spectral domain [8].

To improve the classification of fragments of video frames (macroblocks), it is proposed to use a two-basis principle, which covers the spatial-temporal and spatial-spectral representation of a video frame [6-8].

The mechanism of selection is meant as closing not of all video frames, but only its significant components [5].

The significant component is understood as such component of the video frame which bears in itself the greatest semantic and structural informational content. In the course of automatic selection of significant components it is offered to consider structural features of formation of a video stream [6-8].

For selection of significant structural units it is offered to reveal the most informative, in respect of the structural and semantic contents, components of a basic frame [6]. As the fullest information is born by the brightness a component, significant structural units are offered to be revealed on its basis. Decision-making on closing of structural unit is offered to be carried out by results of the analysis of information component of set of blocks of the brightness component of the video frame.

For definition of a power saturation of blocks it is offered to enter classification of blocks of three types:

- poorly saturated blocks (blocks at which there are uniform sites of the image);
- an average saturation (blocks in which there are insignificant differences between pixels, respectively are present smooth transitions of contrast);
- strongly saturated blocks (blocks at which there are sharp transitions of brightness and picture contrast) [7].

It is necessary to develop system of indicators for identification of the most significant blocks of the brightness component of the video footage on degree of a semantic and structural saturation on the basis of an assessment of indicators: in space-time area and in spatial spectral area [1, 4, 6, 7].

It is offered to apply selective methods of enciphering to increase of a noise stability of all video stream, and owing to simple realization of these methods and small computing expenses. At unauthorized interception of such video stream with mistakes, in process to interpretation the quantity of these mistakes will only increase.

The analysis of various options of selective enciphering showed that the most effective is enciphering after a stage of transformational transformation [1, 4, 7].

It is necessary to develop the main stages of formation of a binary code of the ciphered significant structural unit which are based on three technological components for development of a method of coding of significant structural unit (macroblocks of frame).

- the first component consists in formation of a binary code of value components of transformation representation for the image block;
- the second component consists in formation of a code design of the structural unit of the basic video frame which is subject to enciphering;
- the third component consists in formation of matrixes of a binary code of significant structural unit of the same size, as an enciphering key.

It is proposed to develop the method of the decoding of closed video stream on the basis of the selection (development of the closed significant structural units) of base video frame. for this is proposed to decode the closed base video frame taking into account the determination of the significant structural units.

It is offered to improve a method of a compression of video images on the basis of differential processing of the transformed representation of shots according to the offered classification of semantic significant fragments and to carry out coding with adaptation of parameters of a compression depending on value of a class of a saturation and existence of the built-in steganografichesky container [6, 7].

III. Conclusions

Thus, methodological bases of protection of video information resource in infocommunication component of critical infrastructure the processing of video information resource (development of a complex of the interconnected methods) directed on development technology for the purpose of ensuring its safety, improvement of protection of the resource and office information of all video stream are formulated.

References

[1] V.V. Barannik, V.P. Polyakov, “The encoding of the transformed image in info-communication systems”, Kharkiv, 2010, 212p.

[2] Vlasov A.V., Barannik V.V., Akimov R.V. "Method of increasing availability and integrity of video information resources / XIIth International Conference" ["Modern problems of radio engineering, telecommunications and computer science", TCSET'2014], (Lviv- Slavske, Ukraine, February 25 – March 1, 2014) / Lviv: 2014. – p. 532.

[3] V.Barannik, S. Podlesny, A. Krasnorutskyi, A. Musienko, V. Himenko, "The ensuring the integrity of information streams under the cyberattacks action", 2016 IEEE East-West Design & Test Symposium (EWDTS), Yerevan, 2016, pp. 1-5.

[4] V.V. Barannik, V.V. Larin "Methodology of creation of cryptographic transformations on the basis of methods excluding redundancy". - International Conference TCSET’2010 [Modern problems of radio engineering, telecommunications and computer science] (Lviv-Slavsko, Ukraine, February 23 – 27, 2010)/Lviv Polytechnic National University, 2010. – P. 312.

[5] Ding Z. "GPU accelerated interactive space-time video matting"/ Z. Ding, H. Chen, Y. Gua, Q. Peng//In Computer Graphics International. – 2010. – P. 163-168.

[6] A.V. Vlasov, V.V. Lukin, D.A. Komolov "Coding of information resources of systems of a video conferencing for increase of their safety" //Radio electronics and informatics. – 2013. – No. 2. – Page. 44 – 48.

[7] A.V.Vlasov, A.V. Shiryaev "Method of coding of video images with masking for increase of safety of video information resources" // Radio-electronic and computer systems. – 2013. – No. 3. – Page. 65 – 73.

[8] A.V. Vlasov "Estimation of quality methods disguise images for detection edge contours" // Science-Based Technologies. – 2013. – № 2 (18). – pp. 193 – 197.

Analysis of Approaches to Big Data Optimization and Processing

Heorhii Kuchuk,
Andriy Kovalenko,
Igor Ruban

Kharkiv National University of Radio Electronics,
14 Nauki ave., Kharkiv, 61166, Ukraine,
kuchuk56@ukr.net, andriy_kovalenko@yahoo.com,
ihor.ruban@nure.ua

Abstract. *Big Data always possess pretty high degree of dimensionality. Nowadays there are certain methods aimed at reduction of such dimensionality in order to represent them in a lower dimensional space to effectively process them. The paper represents results on performed analysis of modern methods related to Big Data dimensionality reduction.*

Keywords: *Big Data, dimensionality, reduction, representation, scaling.*

I. INTRODUCTION

Analytics of Big Data is one of the most challenging problems nowadays. It mostly deals with large random data sets generated by completely random nature. Various types of computations typically are not efficient to such sets. One of the most efficient ways of data processing is in using parallelism.

But, since Big Data are high-dimensional data, it is practically impossible to process them directly, even considering certain processing method. First step in simplification of their processing can be reduction of such dimensionality. Result of dimensionality reduction is representation of Big Data in a lower dimensional space [1].

II. ANALYSIS OF MODERN METHODS

First analyzed method was a method of Principal Component Analysis (PCA) [2]. Idea behind the PCA is in searching for several, typically linear, combinations to represent the given data, while trying to minimally loose the information. In this way, it considers various optimization problems, each of them in a form of matrixes, vectors and appropriate projections. So, two following results are achieved using PCA:

- derivation of a subspace where the projections of original data are represented in the best of possible ways;
- derivation of projections that preserve as much variance as possible.

Second method was a method of multidimensional scaling [3]. It allows lowering a multidimensional space using the distance matrix in a way such that their pairwise distances are preserved. In a case when the data have a low-dimensional structure, a technique of Non-linear Dimensionality Reduction can also be used in the scope of multidimensional scaling, which allows detecting the proper structure of the data.

In this method, the Euclidean distance is constructed between data points. The method achieves good results if data points do lie near a linear subspace. In addition, the method is applicable to multiple data points, which have a low dimensional structure anyway. In such case, the geodesic distance of points should be considered instead of Euclidean distances. In multidimensional space at closely spaced points, some projections can be distant from each other.

This method has such disadvantages. The method is sensitive to the choice of the size of the neighborhood. For larger radius, it is possible to skip the low dimensional structure of data. A very small choice of radius leads to disconnected graph. Moreover, computational complexity of the method can be quite large.

Another one analyzed method was a method of diffusion maps [4]. It allows non-linear dimensionality reduction or feature extraction while capturing the geometry of the data set. The main idea is to construct a weight function on the basis of connection between data. To implement the method, a data model is built based on a sample. To build a diffusion map it is required to run the following steps. First step consists of construction a weighted graph on the data. The vertices of the graph are data points, the edge weight is the distance between its vertices. The distance is determined by the weight function. The selected function should satisfy three properties: symmetry, non-negativity and locality. In the second step, the weights matrix of the constructed graph is analyzed. Eigenvectors of this matrix are also being calculated. The third step is in sampling attachment in a lower dimensional space. The eigenvectors obtained using this function represent the data in a lower dimension.

The most important results, devoted to both features and application of the above methods are presented.

III. CONCLUSIONS

The paper represents results on Big Data dimensionality reduction. In such a way, several modern methods were analyzed: method of Principal Component Analysis, method of multidimensional scaling and method of diffusion maps. Results related to each of the methods are presented, as well as their main features and restrictions.

REFERENCES

[1] G. Kuchuk, A. Kovalenko, I.E. Komari, A. Svyrydov, V. Kharchenko. *Improving big data centers energy efficiency: Traffic based model and method*. Studies in Systems, Decision and Control, vol 171. Kharchenko, V., Kondratenko, Y., Kacprzyk, J. (Eds.). Springer Nature Switzerland AG, 2019. Pp. 161-183.

[2] Afonso S. Bandeira. *Ten Lectures and Forty-Two Open Problems in the Mathematics of Data Science*. NYU, 152 p. http://www.cims.nyu.edu/~bandeira/TenLecturesFortyTwoProblems.pdf, October, 2016.

[3] R. Mathar. *Multidimensionale Skalierung: mathematische Grundlagen und algorithmische Aspekte*. Teubner-Skripten zur mathematischen Stochastik. Teubner, Stuttgart, 95 p., 1997.

[4] R. Talmon, I. Cohen, S. Gannot, R. Coifman. Difusion Maps for Signal Processing: A Deeper Look at Manifold-Learning Techniques Based on Kernels and Graphs. *IEEE Signal Processing Magazine*, 30(4), pp. 75-86, July 2013.

ТЕХНОЛОГІЇ ЗАБЕЗПЕЧЕННЯ НАДІЙНОСТІ ТА БЕЗПЕКИ ФУНКЦІОНУВАННЯ КОМП'ЮТЕРНИХ ТА ІНФОРМАЦІЙНИХ СИСТЕМ

Virtual Private Network and its use in secured corporative networks

Hrushak Serhii Serhiivich[1],

Pavlenko Cynthia Serhiivna[2]

[1]*National Aviation University, 3 Lesia Kurbasa avenue, Kiev UA-03148, Ukraine, sg.grusha@ukr.net*

[2]*National Aviation University, 29D Nizhinska street, Kiev UA-03058, Ukraine, neesmu13@gmail.com*

Abstract. *Today information security concerns stand as the main topic in many computer-related fields. This work tries to present an effective method of secured data transmission inside and outside of corporative networks. How to establish information flow and be sure that unauthorized parties will not be able to see it? Virtual Private Network can be used to solve this and many other problems.*

Keywords: *network; transmission of data; security; VPN; SSH.*

I. Introduction And Problem Statement

Corporative network – a group of computers in a building or in a particular areas, which are all owned by the same company or institutions. Day by day, flow of data between those computers increases. As a result, need in secured, wide, reliable and secured data transmission channel between them also increase. Theft of sensitive and private information can damage company reputation and cause financial damage.

This work will tell about solving security problems in corporative networks. Main services that are involved:

- Confidentiality;
- Integrity;
- Authentication;
- Availability;
- Anti-replay.

II. Problem solution and Results

Virtual Private Network (VPN) is secure, reliable and logical connection that is created over a public network (Internet) [1]. CISCO defines a VPN as an encrypted connection between private networks over a public network [2]. It extends the private network across shared or public network. It enables a computer to send or receive data safely through shared or public network. To achieve this Secure Shell protocol can be used.

SSH is a low-cost, software-based solution for keeping prying eyes away from the data on a network [3]. Whenever data is sent by a computer to the network, SSH automatically encrypts it. When the data reaches its intended recipient. SSH automatically decrypts it. The result is transparent encryption: users can work normally, unaware that their communications are safely encrypted on the network. In addition, SSH uses modern, secure encryption algorithms and is effective enough to be found within mission-critical applications at major corporations. SSH covers such services as: authentication, encryption, integrity.Let's describe workflow of a corporate network that have VPN. Employee turn on computer and connects to VPN-server. This can be done, for example, with OpenVPN [4]. OpenVPN is an open-source commercial cross-platform software that implements VPN techniques to create secure point-to-point or site-to-site connections in routed or bridged configurations and remote access facilities [5]. OpenVPN consists of two base software products: client and server. Employees use client. OpenVPN server is a implementation of VPN server. Any authentication on OpenVPN server requires pair of SSH-keys: public and private. SSH-keys is a set of random-generated raw bytes, that are used in public-key cryptography. What is encrypted with private key can be decrypted with public key.

Public key lays on server side. Private key lays on client operating system side. Public key can be loaded via any ssh-agent (PuTTY, SecureCRT, etc.). Before accessing network, client tries to connect to server. Any data before transmission encrypts with private key. Server accept that data and tries to decrypt it with a presented public keys. If decryption succeed, server authenticates user and authorizes him. After this process, user can access any corporate services (Fig. 1).

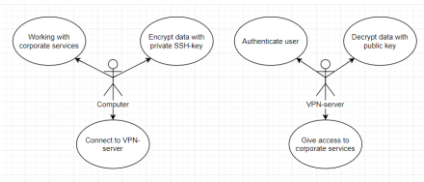


Figure. 1. Use-case diagram for computer and VPN-server

For the sake of security, the most corporate services should be accessible only for those, who are connected to corporate VPN and, as a result, have one specific external IP address. Those who are not connected to corporate VPN will not be able to access corporate services (Fig. 2).

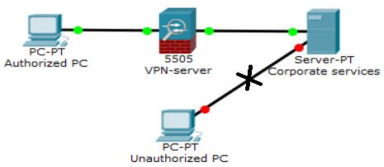


Figure. 2. Basic concept of corporate services availability

III. Conclusions

VPN allows employees to securely access their company's private network or data. Company's data or services for business operations can be accessed only through VPN connection. It prevents leaks of sensitive information to unauthorized parties.

VPN and SSH together is a powerful tool to cover most of main services involved in secured data transmission.

There are plenty of tools that allows to build secured corporative network with VPN: OpenVPN, PuTTY, etc.

References

[1] Zeeshan Ashraf , Virtual Private Networks in theory and practice, Beau Bassin: Shcolars' Press, 2018, p. 202.

[2] G. De Laet and G. Schauwers, "Network security fundamentals", Cisco Press, 2005.

[3] Daniel J. Barrett, Richard Silverman, SSH, Secure Shell: The Definitive Guide, USA: O'Reilly, 2001, p. 558.

[4] Eric F. Crist and Jan Just Keijser, Mastering OpenVPN, Birmingham: Packt Publishing, 2015, p. 364.

[5] Jan Just Keijser, OpenVPN Cookbook, 2nd edition, Birmingham: Packt Publishing, 2017, p. 400.

Модель порушника інформаційного простору в об’єктах критичної інфраструктури

Гвоздьов Роман Юрійович ,

Харківський національний університет радіоелектроніки, пр. Науки 14, Харків, 61166, Україна
roman.hvozdov@nure.ua

Заболотний Володимир Ілліч

Харківський національний університет радіоелектроніки, пр. Науки 14, Харків, 61166, Україна
volodymyr.zabolotnyi@nure.ua

Анотація. *В роботі розглядається загрози інформації в об’єктах критичної інфраструктури, напрями дій порушника та типові загрози критичної інформації.*

Ключові слова: *порушник, загроза, інформація, автоматизована система.*

I. Вступ. Постановка Завдання

Забезпечення надійності та безперешкодності роботи автоматизованих систем обробки інформації в об’єктах критичної інфраструктури є невід’ємною складовою функціонування держави.

Важливим етапом під час проектування комплексних систем захисту інформації є визначення моделі порушника. Опис моделі порушника безпеки інформації в інформаційно-телекомунікаційній системі має містити формалізований або неформалізований опис дій порушника, який відображає його практичні та теоретичні можливості, апріорні знання, час та місце дії тощо[1].

II. Рішення задачі

Дії порушника спрямовані на порушення властивостей інформації: конфіденційності, цілісності, доступності інформації, спостереженості та керованості автоматизованої системи[1].

Стосовно автоматизованої системи порушники можуть бути зовнішніми або внутрішніми. Модель порушника повинна визначати:

1) можливу мету порушника та її градацію за ступенем небезпеки для автоматизованої системи;

2) категорії осіб, із яких може бути порушник;

3) передбачення про кваліфікацію порушника;

4) передбачення про характер його дій.

Критичною загрозою функціонування об’єктів критичної інфраструктури є порушення цілісності та доступності інформації.

Одним із напрямків дій порушника спрямовані на дестабілізацію ситуації країни шляхом унеможливлення інформування населення країни, унеможливлення інформування вищого керівництва країни щодо надзвичайних ситуацій, нанесення збитків шляхом знищення матеріальних та інформаційних цінностей[1]. Вищеописані шляхи дій порушника являються критичними, бо можуть спричинити паніку у всіх шарах населення.

Можливі способи здійснення загроз відносяться до фізичного та логічного доступу порушника до критичної інформації.

До фізичного доступу можна віднести здійснення загрози каналами спеціального впливу шляхом формування полів і сигналів з метою руйнування системи захисту або порушення цілісності інформації[2].

До принципу логічного доступу відносять несанкціонований доступ шляхом підключення до апаратури та ліній зв’язку, маскування під зареєстрованого користувача, подолання заходів захисту з метою використання інформації або нав’язування хибної інформації, застосування закладних пристроїв чи програм та вкорінення комп’ютерних вірусів[2].

Наведемо спрощену класифікацію атак:

1) використання технічних засобів задля формування полів і сигналів з метою блокування засобів зв’язку;

2) віддалена відмова в обслуговуванні - атаки, що дозволяють порушити функціонування системи або перезавантажити комп’ютер через мережу (в тому числі через Інтернет).

3) підкуп персоналу, служби безпеки, інженерного складу для отримання необхідної інформації; нанесення збитків шляхом знищення матеріальних та інформаційних цінностей.

III. Висновки

З урахуванням викладеного можна виділити наступні складові створення ефективної системи захисту:

- нормативно-правова база;
- організаційні та організаційно-технічні заходи;
- науково-методична база;
- створення штатного підрозділу служби захисту інформації

Мета організаційно-технічних засобів може бути досягнута побудовою системи захисту інформації, що є організованою сукупністю методів і засобів забезпечення технічного захисту інформації. Технічний захист інформації здійснюється поетапно:

1) визначення й аналіз загроз;

2) розроблення системи захисту інформації;

3) реалізація плану захисту інформації;

4) контроль функціонування та керування системою захисту інформації

Посилання

[1] НД ТЗІ 2.6-001-11 «Порядок проведення робіт з державної експертизи засобів технічного захисту інформації від несанкціонованого доступу та комплексних систем захисту інформації в інформаційно-телекомунікаційних системах»

[2] НД ТЗІ 3.7-003-05 «Порядок проведення робіт із створення комплексної системи захисту інофрмації в інформаційно-телекомунікаційній системі

Метод предотвращения внедрения источников угроз в электронные системы

Горбачев Валерий Александрович [1]

Пономаренко Ольга Евгениевна [2]
Коткова Оксана Николаевна [3]
Абдулрахман Котаеба Батиаа [4]

[1,2,3,4] *Kharkiv National University of Radio Electronics, 14 Nauky Ave, Kharkiv UA-61166, Ukraine,*
valeriy.gorbachov@nure.ua, olha.ponomarenko@nure.ua

Аннотация. *Широко распространенный аутсорсинг изготовления интегральных микросхем повышает уязвимость к угрозам безопасности. В работе рассматривается подход, который включает в себя схему обфускации оборудования для защиты проекта от различных форм атак. Аппаратная обфускация – это метод, с помощью которого интегральная схема модифицируется, чтобы преднамеренно скрыть свою функциональность и структуру. В работе рассматривается обфускация монитора безопасности.*

Ключевые слова*: аппаратная закладка; монитор безопасности; аппаратная обфускация, реинжиниринг интегральных схем.*

I. Введение И Постановка Задачи

Современные методы предотвращения внедрения аппаратных закладок (АЗ), а также методы обнаружения АЗ перед этапом практического использования ИС, не могут обеспечить полную гарантию того, что ИС или электронная система свободны от АЗ. В отличие от методов обнаружения, методы предотвращения угроз АЗ объединяют методы, которые препятствуют внедрению АЗ. Одним из способов гарантирования, что в ИС не будет внедрена АЗ, является жесткое управление жизненным циклом разработки ИС на всех его этапах. Это важное звено в стратегии эффективной защиты. Этапами жизненного цикла разработки ИС являются этапы: составления спецификации, проектирования, изготовления, тестирования и сборки. Известно, что только этапы спецификации и тестирования могут быть не уязвимыми внедрением АЗ. Все другие этапы, на практике, уязвимы из-за зависимости от сторонних поставщиков IP модулей, от инструментов проектирования и от процесса проектирования и производства. В настоящее время актуальной является проблема обеспечения безопасного функционирования системы при наличии АЗ.

II. Решение Проблемы И Результаты

Используемая в работе концепция реконфигурируемой логики, позволяет значительно усложнить злоумышленнику доступ к структуре и функциональности проекта.

Основной концепцией проектирования и разработки защищенных систем является концепция МБ - механизм проверки обращений [1]. МБ — это концепция контроля доступа абстрактной машины, которая опосредует все обращения к объектам субъектами. МБ позволяет разработчикам интегрировать аспект безопасности в процесс проектирования системы, а не пытаться добавить

его позже. Предлагается выделить определенный компонент в электронной системе, который реализует ее защитные функции. Этот подход скрывает функциональные и/или схематические детали от разработчиков на ненадежных этапах цикла проектирования.

Работа посвящена обфускации (obfuscation) МБ, которая обеспечивает ключевое свойство МБ: невозможность обойти МБ. В работе предлагается метод обфускации МБ, основанный на многоуровневой композиции структурной модели системы [2]. Рассматривается применение реконфигурируемой логики логики для обфускации МБ для платформы SoC. Чтобы скрыть МБ, соответствующее ядро может быть запрограммировано с использованием информации о конфигурации на более поздних и надежных этапах проектирования.

III. Выводы

В работе рассмотрен метод защиты электронной системы от различных форм атак, который включает в себя аппаратную обфускацию проекта. Этот метод может рассматриваться как превентивная мера, скрывающая часть проекта от злоумышленника. Эта часть проекта является МБ, поэтому ее обфускация не позволяет злоумышленнику получить функциональность и исходную структуру проекта. Для своей реализации, метод требует аппаратно-программируемых функций во время выполнения цикла проектирования ИС. Таким образом, обеспечивается одно из основных свойств МБ: защита от несанкционированного доступа. Предложенный в работе формализм позволит проектировать сложные электронные системы, особенно на платформе SoC и NoC, функционирующие в присутствии АЗ.

Список литературы

[1] M. Bishop. Computer Security: art and science. Addison Wesley. ISBN 0-201-44099-7. 2002.

[2] V. Gorbachov, A. K. Batiaa, O. Ponomarenko and Y. Romanenkov, “Formal transformations of stuctural models of complex network systems,” in 2018 IEEE 9th International Conference on Dependable Systems, Services and Technologies DESSERT’2018, Conference proceedings, Kyiv, 2018, pp. 473–477

Підходи до підвищення криптостійкості методів приховування стегоповідомлення у тексті

Тарасенко Ярослав Володимирович

Черкаський державний технологічний університет, бул Шевченка 460, Черкаси, 18006, Україна, yaroslav.tarasenko93@gmail.com

Анотація. *Робота присвячена пошуку дієвих підходів до підвищення криптостійкості таких напрямів застосування алгоритмів вбудовування стегоповідомлення в англомовний текст, як вбудовування цифрових водяних знаків, ідентифікаційних номерів та заголовків. В результаті дослідження існуючих підходів підвищення надійності та криптостійкості цих алгоритмів було виявлено їх недоліки, зокрема нестабільність роботи в умовах застосування сучасних методів протидії комп'ютерній лінгвістичній стеганографії. На основі дослідження підходу підвищення криптостійкості шляхом повторення цифрового водяного знаку визначаються підходи по підвищенню криптостійкості згаданих стегоалгоритмів, а також рекомендації щодо напрямків подальшого вдосконалення існуючих підходів.*

Ключові слова: *криптостійкість стегоалгоритмів, комп'ютерна лінгвістична стеганографія, цифрові водяні знаки, вбудовування стегоповідомлення у текст, підвищення надійності стегоалгоритмів.*

I. Вступ і Постановка Завдання

На сьогоднішній день, все більшого поширення набуває протидія несанкціонованій прихованій передачі стегоповідомлення. І це очікувано, адже приховування самого факту передачі повідомлення спричиняє певні небезпеки, зокрема спілкування незаконних організацій, несанкціонована передача та збереження інформації та багато інших. Однак, методи стеганографії мають на меті не лише організацію незаконного каналу зв'язку, але і ряд областей застосування, що забезпечують захист інформації, зокрема захист від копіювання (захист авторського права), прихована анотація документів та аутентифікація [1]. В той же час, засоби, що покликані для протидії методам приховування повідомлення можуть бути використані зловмисниками для порушення прав громадян.

Крім передачі повідомлення, існують наступні напрями застосування стегоалгоритмів: вбудовування цифрових водяних знаків (ЦВЗ), ідентифікаційних номерів та вбудовування заголовків [2]. Основна проблема полягає у знаходженні балансу між забезпеченням протидії передачі повідомлень та уникненням видалення маркеру ЦВЗ для захисту авторських прав.

В той час, як текстова інформація займає провідне місце в обміні даними, передача даних у тексті ускладнена тим, що при статистичному дослідженні легко виявити найпростіші методи вбудовування ЦВЗ. Тому текстова інформація є надійним контейнером, за умови, що використовується семантична надлишковість. В той же час, свою ефективність для протидії вбудовуванню стегоповідомлення у текст на основі семантичних підходів, довів метод семантичного стиснення текстової інформації [3].

Отже, наразі існує потреба в розробці підходів для підвищення криптостійкості методів приховування ЦВЗ у текстових даних, для підвищення ефективності існуючих підходів по підвищенню криптостійкості стегоалгоритмів в умовах застосування засобів протидії приховування стегоповідомлення, а також в забезпеченні захисту ЦВЗ, заголовків чи ідентифікаційних номерів від навмисного чи випадкового видалення за умови одночасного забезпечення захисту від можливого використання методів комп'ютерної лінгвістичної стеганографії зловмисниками.

II. Рішення і результати

Оскільки існують такі методи приховування стегоповідомлення у текстовому контейнері: синтаксичні та семантичні [4], саме на принципах синтаксичної та семантичної надлишковості тексту і будується формування стегосистеми, а, відповідно, і вбудовування ЦВЗ, заголовків чи ідентифікаційних номерів.

Виходячи з [5], стійкість ЦВЗ забезпечується побудовою несиметричних систем ЦВЗ з використанням одного з типів однонаправленої функції, недоліки якої компенсуються використанням додаткових мір по підвищенню достовірності ЦВЗ, що передаються. Однак, в стегосистемах, використання цих же способів підвищення достовірності ускладнено [5]. З цього слідує, що використання методів руйнування саме стегосистеми матиме високу ефективність і при використанні ЦВЗ чи інших методів маркування стегоконтейнеру. Один з найдієвіших методів підвищення криптостійкості прихованого ЦВЗ (в тому числі у тексті) полягає у багаторазовому повторенні знаку для підвищення імовірності його захисту від руйнування за принципом багаторазового повторення сигналу, який застосовується в радіотехніці для оптимального прийому і зменшення впливу шумів [6]. Однак, в результаті аналізу, було виявлено, що він не ефективний в рамках використання спеціалізованого програмного забезпечення, що реалізує метод семантичного стиснення текстової інформації для протидії комп'ютерній лінгвістичній стеганографії.

Експеримент проводився на основі уривку тексту Ернеста Хемінгуея «Старий та море» в оригіналі, розміром 50 кБ. В цей текст було багаторазово приховано маркер ЦВЗ на основі таких методів лінгвістичної стеганографії, як синтаксичні та семантичні [4]. При цьому, завдяки лінгвістичним методам було вбудовано ЦВЗ, ідентифікаційний номер та заголовок, розмір яких не перевищував 1 біт. Результати обробки тексту з використанням методу

семантичного стиснення текстової інформації для кожного з цих типів вбудовування інформації з кількістю залишеніх біт наведено в таблиці 1.

Таблиця 1. Дослідження методу підвищення криптостійкості стегоалгоритмів вбудовування ЦВЗ у текст в умовах протидії шляхом семантичного стиснення

№ експе-рименту	Кількість ЦВЗ, заголовків чи номерів			
	Синтаксичні методи		Семантичні методи	
	Вбудовані в текст	Залишені після обробки	Вбудовані в текст	Залишені після обробки
1	2	1	2	0
3	5	0	5	2
4	8	0	8	1
5	12	0	12	3
6	10	2	10	1
7	15	0	15	0
8	18	0	18	0

Аналіз показав, що підхід до підвищення криптостійкості шляхом повторення водяного знаку [6] не ефективний в рамках використання методу семантичного стиснення текстових даних, а імовірність збереження хоча б одного знака надто низька та нестабільна

Таким чином, основуючись на принципах функціонування згаданого методу, на тому факті що для дослідження тексту використовується інтенсіональна логіка та дискурсний аналіз тексту [3], існуватимуть перелічені далі шляхи підвищення ефективності вбудовування маркеру ЦВЗ у текст, які, при цьому не надають можливості імовірному зловмиснику вбудовувати повноцінне стегоповідомлення.

1. ЦВЗ слід використовувати в ключових семантичних елементах основного тексту, які неможливо модифікувати. Такий підхід може забезпечити захист від видалення стегоповідомлпення шляхом семантичного стиснення, при тому не надаючи зловмиснику можливості приховати повідомлення цілком, оскільки 1-2 бітів занадто мало для його приховування, однак достатньо для вбудови маркера водяного знака.

2. Обов'язкова дискурсна перевірка семантики тексту задля виявлення найбільш стійких місць для приховування даних, та визначення подальшої імовірної модифікації тексту засобами, направленими на руйнування стегосистеми.

3. Використання інтенсіональної логіки для приховування ЦВЗ у структурному семантичному елементі шляхом визначення світів семантики, в яких цей елемент набуває тотожних значень. Це забезпечить стабільність вбудовування ЦВЗ, та неможливість руйнації стегосистеми. А наявність надто невеликої кількості таких елементів забезпечить захист від передачі повноцінного стегоповідомлення.

4. Використання принципів семіотики для вбудовування ЦВЗ на основі знакової системи. Це зумовлено тим фактом, що на ряду з синтаксичними та семантичними методами згаданими раніше, приховування повідомлення проводиться також на основі особливостей символів [7]. А те, що семіотичні принципи базуються на семантичній інтерпретації відповідних знаків, дозволить підвищити криптостійкість ЦВЗ, при цьому знакова система, що не приверне зайвої уваги є надто невеликою для використання її зловмисником.

III. Висновки

Для підвищення криптостійкості методів приховування стегоповідомлення у тексті, слід перш за все, маркер вбудовувати в ключовий семантичний елемент тексту, крім того, проводити дискурсну перевірку семантики тексту, використовувати елементи інтенсіональної логіки для приховування ЦВЗ та використовувати принципи семіотики. Такі підходи хоч і не стовідсотково забезпечать захист від видалення ЦВЗ, проте значно підвищать ефективність його вбудовування, при цьому не надавши зловмиснику можливості пересилання повноцінного повідомлення. Це означає, що авторські права та інші позитивні аспекти використання стеганографії будуть збережені, і, при цьому не зросте небезпека від можливого використання методів стеганографії зловмисником.

Отже, шляхи вдосконалення існуючих методів підвищення криптостійкості вбудовування ЦВЗ полягають у використанні їх із зазначеними підходами в комплексі.

Перелік посилань

[1] Горпенюк А.Я. Дослідження та порівняльний аналіз стеганографічних методів для впровадження даних у цифрові файли / А.Я. Горпенюк, А.О. Стороженко // Вісник Національного університету «Львівська політехніка». Серія: Автоматика, вимірювання та керування, 2012. – № 741. – С. 176-179.

[2] Калашніков М.В. Вбудовування цифрових водяних знаків у аудіофайли зі стисненням без втрат / М.В. Калашніков, О.О. Яковенко, Н.І. Кушніренко // Вісник Національного університету «Львівська політехніка». Серія: Автоматика, вимірювання та керування, 2014. – № 806. – С. 83-87.

[3] Тарасенко Я.В. Метод семантичного стиснення текстової інформації для протидії комп'ютерній лінгвістичній стеганографії / Я.В. Тарасенко, О.Б. Півень, І.М. Федотова-Півень // Наука і техніка Повітряних Сил Збройних Сил України, 2018. – № 3 (32). – С. 68-78.

[4] Rakhi A review on steganography methods / Rakhi, S. Gawande // International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering, 2013. – Vol.2, Issue 10. – P. 4635-4638.

[5] Грибунин В.Г. Цифровая стеганография / В.Г. Грибунин, И.Н. Оков, И.В. Туринцев. – Москва : СОЛОН-ПРЕСС, 2009. – 263 с.

[6] Бахрушина Г.И. Внедрение водяных знаков в изображения на основе принципа многократной передачи сигнала / Г.И. Бахрушина, И. С. Терешко, А.П. Бахрушин // Электронное научное издание «Ученые заметки ТОГУ», 2015. – Том 6, № 4. – С. 698 – 709.

[7] Очнев Д.В. Цифровые водяные знаки как метод защиты текстовых печатных документов / Д.В. Очнев, Е.С. Чиркин // Психолого-педагогический журнал Гаудеамус, 2012. – № 2 (20). – С. 148-149.

Аналіз ефективності методів боротьби з DOS-атаками в комп'ютерних системах

Єрьоміна Наталія Сергіївна
Харківський національній університет радіоелектроніки, пр. Науки 14, Харків, 61166, Україна,nataliia.yeromina@nure.ua

Земскова Альбіна Олексіївна
Харківський національній університет радіоелектроніки, пр. Науки 14, Харків, 61166, Україна, albina.zemskova@nure.ua

Анотація. *В обчислювальній техніці атаки відмови в обслуговуванні (DoS) є однією із складних проблем у поточному Інтернеті. Успішна атака дозволяє блокувати доступ користувачів інформаційних систем до ресурсів різних серверів, які можуть деактивувати всю систему. В даний час в світі існують рішення, які знижують негативний вплив DoS-атак, але ці дорогі способи мають ряд недоліків, які обмежують їхню здатність при використовуванні. Метою цієї роботи є аналіз використання різних методів для запобігання DoS-атаки.*

Ключові слова: *Dos-атака, методи боротьби, аналіз методів.*

I. ВСТУП І ПОСТАНОВКА ЗАВДАННЯ

Сучасний комп'ютерний світ являє собою різноманітну сукупність систем обробки інформації для вирішення багатогранного кола проблем, пов'язаного з різними областями людської діяльності. Чим складніше поставлена задача тим більш критичним стають такі характеристики як надійність та безпека інформаційних ресурсів, задіяних в процесі збору, накопичення, обробки і передачі комп'ютерних даних.

На сьогоднішній день для забезпечення безпеки ряд компаній користуються різним програмним забезпеченням не замислюючись про ступінь захисту того чи іншого засобу. Збій або недоступність інформаційного сервера тягне величезні фінансові втрати. Останнім часом стала особливо актуальною проблема DoS-атак. Їх потужність збільшилася майже в 3.5 рази [1] тільки за четвертий квартал 2014 року.

DoS (Denial of Service – відмова в обслуговуванні) – хакерська атака на обчислювальну систему з метою довести її до відмови, тобто створення таких умов, при яких легальні користувачі системи не зможуть отримати доступ до наданих системних ресурсів (серверів), або цей доступ ускладнений [2]. Такі атаки дозволяють довести до відмови практично будь-яку систему, не залишаючи юридично значимих доказів.

На даний момент виділяють 4 типа DoS-атак [3]:

- атака на насичення смуги пропускання;
- атака, що призводить до нестачі системних ресурсів;
- атака, що використовує помилки програмування;
- атака на DNS-сервера.

II. РІШЕННЯ І РЕЗУЛЬТАТИ

Існують різні системи виявлення вторгнень, які дозволяють виявляти DoS-атаки по відомим сигнатурам, розпізнаючи аномальну поведінку системи. Одні компанії використовують статичні засоби захисту до початку самої атаки, вибудовуючи спеціальні фільтри. На підходах до сервера (найближчому маршрутизаторі) повинна бути встановлена система аналізу трафіку, яка дозволить своєчасно дізнатися про початок атаки і вчасно вжити заходи для її запобігання. Інші – зберігають базу даних сигнатур вже відомих DoS-атак. Виробляючи при цьому моніторинг всієї системи по сигнатурам, можна зафіксувати початок DoS-атаки. Але цей спосіб не так ефективний, тому що при появі будь-якої нової DoS-атаки дана база сигнатур безкорисна. Ще один спосіб виявлення початку DoS-атаки являє собою виявлення аномальної поведінки в системі. Поточний стан системи в реальному часі порівнюється з її нормальним станом, тобто з тим, коли спостерігається звичайна динаміка трафіку і продуктивність самого сервера [3]. Інше більш-менш ефективне рішення полягає в купівлі дорогих хардварних систем CiscoTrafficAnomalyDetector і CiscoGuard. Працюючи разом, вони можуть подавити атаку, яка починається, але, як і більшість інших рішень, заснованих на навчанні та аналізі станів, дають збої. Всі ці способи допомагають захиститися лише від деяких видів DoS-атак. Хакери, націлені «звалити» той чи інший сервер, аналізують захист і вигадують інші способи впливу на неї, посилюючи атаку, або зовсім вдаючись до іншого методу.

III. ВИСНОВКИ

Приватні підходи надто ресурсозатратні і в силу величезного розмаїття DoS-атак, не забезпечують систему повноцінним захистом. Але правильна класифікація – це перший крок до створення комплексного розширювального апарату, здатного детектувати, вживати необхідні заходи до початку атаки і, в деяких випадках, повністю захищати систему від них. Також варто враховувати той факт, що за останній час збільшилася потужність DoS-атак, а разом з цим збільшилися і витрати на її реалізацію. Тому, не маючи 100% захисту від них, але ґрунтуючись на існуючій класифікації DoS-атак можна вибудувати захист своєї системи так, що дані атаки стали б просто економічно невигідними. Для цього, по мірі можливості, необхідно мати всі відомі способи захисту системи від атак. Важливо зловити момент і почати активні дії. Допоможе в цьому постійне спостереження за маршрутизатором, підключеним до зовнішньої мережі (аналіз графіків NetFlow).

ПЕРЕЛІК ПОСИЛАНЬ

[1] *J. Yuan, K. Mills*. Monitoring the Macroscopic Effect of DDoS Flooding Attacks. IEEE Transactions on dependable and secure computing. , Senior Member, IEEE. M., 2012 – 12 p.

[2] *Douligeris*, *A. Mitrokotsa*. DDoS Attacks and defense mechanisms: a classification. P., 2013 – 24 p.

[3] M. J. Hashmi, M. Saxena, Dr. R. Saini. Classification of DDoS Attacks and their Defense Techniques using Intrusion Prevention System. Research Scholar, Singhania University, Pacheri Bari, Jhujhunu, R. 2013. – 8 p.

Порівняльний аналіз методів аутентифікації по біометрії

Ніжніченко Олександра Костянтинівна

Харківський національний університет радіоелектроніки
пр. Науки 14, Харків,61166, Україна,
oleksandra.nizhnichenko@nure.ua

Анотація. *Аналіз показує, що аспекти безпеки даних набувають з кожним днем все більшого значення, створення надійних методів розпізнавання особистості стає все більш актуально. Існують методи розпізнавання, в якості яких можна розглядати сукупність ідентифікаційних карт, які стосуються соціального страхування або паролі, не можуть бути абсолютно надійними.*

Ключові слова: *біометрична аутентифікація, біометрична ідентифікація, надійність, FAR, FRR.*

I. Вступ. Постановка задачі

Останнім часом підвищуються вимоги до безпеки доступу до ресурсів інформаційних систем. Існує велика різноманітність методів ідентифікації та багато з них отримали широке комерційне застосування. На сьогодні в основі найбільш поширених технологій верифікації та ідентифікації лежить використання паролів і персональних ідентифікаторів або документів типу паспорта, водійських прав.

Однак такі системи дуже вразливі та можуть легко постраждати від підробки, крадіжки та інших факторів. Тому все більший інтерес викликають методи біометричної ідентифікації, що дозволяють визначити особу людини за його фізіологічним характеристикам шляхом розпізнання по заздалегідь збереженим зразкам.

Біометрія - сукупність методів ідентифікації та аутентифікації користувачів на основі їх поведінкових або фізіологічних характеристик [1] . У свою чергу методи біометричної ідентифікації поділяють на:

1. Статичні, засновані на фізіологічних ознаках людини, присутніх з нею протягом всього життя:
   - ідентифікація по відбитку пальця;
   - ідентифікація по обличчю;
   - ідентифікація по райдужній оболонці ока;
   - ідентифікація по геометрії руки;
   - ідентифікація по термограми особи;
   - ідентифікація по ДНК;
   - ідентифікація на основі акустичних характеристик вуха;
   - ідентифікація по малюнку вен.
2. Динамічні беруть за основу поведінкові характеристики людей, а саме підсвідомі русі в процесі повторення будь-якої звичайної дії: почерк, голос, хода:
   - ідентифікація по голосу;
   - ідентифікація по рукописному почерку;
   - ідентифікація по клавіатурного почерку
   - та інші.

Існують також комбіновані системи ідентифікації, що використовують кілька біометричних характеристик, що дозволяє задовольнити найсуворіші вимоги до надійності і безпеки систем контролю доступу [2].

II. Вирішення проблеми та результати

Одним з методів аутентифікації та ідентифікації, що найбільше розвивається, є ідентифікація по біометричним характеристикам. Біометрія оптимальна у використанні тим, що користувачеві не треба запам'ятовувати інформацію ідентифікації та аутентифікації. За останні роки розроблено більше десятка методів ідентифікації.

Зі збільшенням популярності таких методів ідентифікації постає питання про їх надійності та завадостійкості. Для визначення ефективності системи контролю і керуванням доступу на основі біометричної ідентифікації використовують наступні показники:

- FAR - коефіцієнт помилкового пропуску;
- FMR - ймовірність, що система невірно порівнює вхідний зразок з невідповідним шаблоном в базі даних;
- FRR - коефіцієнт помилкової відмови;
- FNMR - ймовірність того, що система помилиться у визначенні збігів між вхідним зразком і відповідним шаблоном з бази даних;
- графік ROC - візуалізація компромісу між характеристиками FAR і FRR;
- коефіцієнт відмови в реєстрації (FTE або FER) - коефіцієнт безуспішних спроб створити шаблон з вхідних даних (при низьку якість останніх);
- коефіцієнт помилкового утримання (FTC) - ймовірність того, що автоматизована система не здатна визначити біометричні вхідні дані, коли вони представлені коректно;
- місткість шаблону - максимальна кількість наборів даних, які можуть зберігатися в системі.

Головними, для оцінки будь-якої біометричної системи, є два параметри:

- FAR (False Acceptance Rate) – коефіцієнт помилкового пропуску, тобто відсоток виникнення ситуацій, коли система дозволяє доступ користувачу, незареєстрованим в системі.
- FRR (False Rejection Rate) – коефіцієнт помилкової відмови, тобто відмова в доступі справжньому користувачеві системи [3-4].

Таблиця 1. Коефіцієнти помилкового пропуску та відмови для різних систем біометричного доступу

Біометрична система керування доступу використовує:	FAR	FRR
Відбиток пальця	0,001%	0,6%
Розпізнавання 2D	0,1%	2,5%
Розпізнавання обличчя 3D	0,0005%	0,1%
Райдужна оболонка ока	0,00001%	0,016%
Сітківка ока	0,0001%	0,4%

Біометрична система керування доступу використовує:	FAR	FRR
Відбиток пальця	0,001%	0,6%
Розпізнавання 2D	0,1%	2,5%
Розпізнавання обличчя 3D	0,0005%	0,1%
Райдужна оболонка ока	0,00001%	0,016%
Сітківка ока	0,0001%	0,4%
Малюнок вен	0,0008%	0,01%

Обидва параметри розраховуються на основі методів математичної статистики [5]. Чим нижче ці показники, тим вище точність розпізнання об'єктів. Це означає, що такі системи контролю доступу будуть використовуватися на важливих об’єктах комп’ютерної мережі. Підвищити обидва показники надійності можна тільки принциповим удосконаленням біометричної методики.

III. Висновки

Розглянутий підхід до аналізу ідентифікації дозволяє оцінити достовірність і надійність різних методів біометрії в порівнянні з іншими методами ідентифікації. Як показано в роботі, застосування біометрії дозволить вирішити проблему надійності та може підвищити достовірність ідентифікації суб'єктів при організації доступу до систем з числом користувачів, що вимірюється сотнями, а також до критично важливих систем як частина системи контролю та управління фізичним доступом або як додатковий фактор аутентифікації. Для широкого класу систем біометрична ідентифікація придатна для посилення захисту або як підвищення завадостійкості систем.

Перелік посилань

[1] Юсупов О. Р. Сравнительный анализ возможности использования технологий биометрической идентификации // Молодой ученый. — 2016. — №19. — С. 118-121.

[2] Биометрическая идентификация и аутентификация. - / [Электронный ресурс]. – Режим доступа: URL: http://www.techportal.ru/glossary/biometricheskaya_identifikaciya.html (дата звернення: 18.09.2017).

[3] А.Г. Сабанов, С. Г. Смолина, Сравнительный анализ методов биометрической идентификации личности, // Молодой ученый. — 2018. — №32. — С. 98-201.

[4] Т.Ю. Коржак Eason, Матеріали VII Міжнародної науково-технічної конференції молодих учених та студентів, Методи і засоби визначення ефективності біометричної ідентифікації в комп’ютерних мережах. - / [Электронный ресурс]. – Режим доступа: URL:http://elartu.tntu.edu.ua/bitstream/lib/27107/2/VII_MNTK_2018v2_Korzhak_T_Y-Methods_and_means_for_determining_87-88.pdf (дата звернення: 28.11.2018).

[5] Абдрахманов Р. Б., Баймешова А. Н., Амітова А. Т. До питання біометричної ідентифікації // Молодий вчений. - 2016. - №26. - С. 127-131. - URL https://moluch.ru/archive/130/36048/ (дата звернення: 17.11.2018).

The Deadlock Problem & Approaches to Its Solution

Zakabluk Maksym
Shevchenko Oleksii
Movsesian Iana

Kharkiv National University of Radio Electronics,
14 Nauky Ave, Kharkiv UA-61166, Ukraine
e-mail: maksym.zakabluk@nure.ua

Abstract. *The paper discusses the problem of resource deadlocks, as well as ways of preventing and avoiding them. It points out the importance of developing mechanisms to fight against deadlocks in operating systems and describes the approach to preventing deadlocks based on combining eventdriven and service-oriented architectures, asynchronous I/O, and a number of other architectural solutions and techniques.*

Keywords: *deadlock, event-driven architecture, serviceoriented architecture, asynchronous I/O, dynamically resizing a buffer, deadline for processing a message, timeout.*

I. Introduction And Problem Statement

Deadlocks are one of the characteristic problems of parallel systems in which several entities share several objects (resources). Despite the fact that research aimed at fight against deadlocks was started back in the late 1960s, this problem remains relevant today. The approaches to preventing deadlocks and avoiding them are most actively developing in flexible manufacturing systems (FMS) [1], but the threat of dead-end situations also remains in local computer networks of cars [2], wireless sensor networks [3], device drivers and any other parallel systems and applications with resource sharing.

The deadlock prevention is based on the use of attacks on one or more of Coffman's four conditions, and implies the design of a system whose architecture fundamentally excludes the possibility of deadlocks [4]. If the violation of the specified conditions for the occurrence of deadlocks implies their prevention during the operation of the system, the same goal can be achieved at the software design stage by verification, for which model checking [5], modeling, analysis of the description of the system in one of the formal languages (Funclet+, xGiotto, AFS etc.) and other methods can be used.

In case of evasion, the system avoids entering into deadlock conditions, but is not immune from them. Evasion can be realized with the help of the banker algorithm, supervisory control based on Petri nets, pi-calculus, process algebra, fuzzy logic, finite state machine theory, and other approaches. The exponential dependence of the number of possible states of the system on the number of its elements and the connections between them in a number of cases makes an integral verification of the systems impracticable, and approaches to preventing deadlocks and evading them in dynamics – impractical. The situation is even more complicated for systems with variable topology and composition, as well as decentralized control, which makes it urgent to develop mechanisms to fight against deadlocks in operating systems.

II. Problem Solution And Results

An effective attack on the conditions of mutual exclusion, holding and waiting, as well as cyclic waiting is possible due to the combination of Event-Driven Architecture (EDA) and Service-Oriented Architecture (SOA), non-blocking asynchronous I/O (Asynchronous I/O, AIO) and some other architectural solutions and techniques. In the case of the organization of software in the form of a set of services, you can get rid of the separation of resources as such: each resource corresponds to a separate service that processes customer requests, and only this service can hold the resource. However, the use of synchronous calls by services can lead to cyclic waiting, which can be avoided by buffering requests and using asynchronous I/O, which is characteristic of the event-driven architecture. In the case of combining EDA, SOA and AIO, the services exchange messages, and the receipt of the message is interpreted as an event. Services, in this case, can be described by a finite state machine model.

However, due to the limited size of message queues and the non-determinism of the flow of external events, even the system with the above-mentioned architecture is not immune from getting into deadlocks due to complete filling of queues. This problem can be avoided by dynamically changing the queue size, as well as comparing each message with a processing deadline, which allows you to periodically delete messages from queues that are no longer relevant for processing. In addition, each message has a deadline for processing the system in real time by scheduling the execution of handlers using the EDF (Earliest Deadline First)algorithm, as done, for example, in the COSMIC middleware.

In the case of the description of services by the model of the finite state machine, deadlock situations are possible due to the circular waiting of messages, which can be avoided by comparing each state of the automaton with a certain timeout - the maximum permissible time in the given state. At the end of the timeout (which is interpreted as an event), the machine goes into one of the other possible states.

III. Conclusions

The above-mentioned architectural solutions have a number of advantages over conventionally traditional approaches to the designing of operating systems, and realize the deadlock prevention as their non-main function.

REFERENCES

[1] J.-P. Lopez-Grao, J.-M. Colom and F. Tricas, “The deadlock problem in the control of Flexible Manufacturing Systems: An overview of the Petri net approach”, Proc. 2014 IEEE Emerg. Technol. Fact. Autom., pp. 1–12, 2014.

[2] J. Xu, Z. Zheng and M. R. Lyu, “CGA-based deadlock solving strategies towards vehicle sensing systems”, Eurasip J. Wirel. Commun. Netw., pp. 1–11, 2014.

[3] N. Akiyama, A. Ikeda and T. Miyazaki, “Deadlock-free Behavior Definition for Wireless Sensor Nodes Using Formal Verification”, Commun. ACM, vol. 21, no. 8, pp. 666–677, 2017.

[4] Tanenbaum, Modern Operating Systems, 3rd ed. London: Pearson Education, 2009.

[5] E. M. Clarke, O. Grumberg and D. Peled, Model Checking, 1st ed. zal

Аналіз небезпеки впровадження вірусного програмного забезпечення в зображення

Гриньов Ростислав Сергійович
Харківський Національний Університет Радіоелектроніки, пр. Науки, 14, Харків UA-61166, Україна, rostgrin@gmail.com

Сєвєрінов Олександр Васильович
Харківський Національний Університет Радіоелектроніки, пр. Науки, 14, Харків UA-61166, Україна, oleksandr.sievierinov@nure.ua

Анотація. *У доповіді розглянута небезпека можливості впровадження вірусів в файли зображень з метою подолання засобів захисту.*

Ключові слова: *віруси; проникнення; подолання системи захисту; вірус у зображенні; IDS; IPS.*

I. Вступ

Комп'ютерні віруси несуть серйозну загрозу як для простих користувачів, так і для великих фірм і компаній. Сьогодні існує величезна різноманітність комп'ютерних вірусів. Створюються нові методики їх приховування і поширення. Найбільш частим є використання стеганографії для приховування вірусного програмного забезпечення в файлах.

В наш час для забезпечення захисту конфіденційних даних організацій використовуються антивірусне програмне забезпечення, системи виявлення вторгнень (IDS), системи запобігання вторгнень (IPS), брандмауери та фаєрволи. Проте навіть вони не можуть гарантувати захисту.

II. Вирішення проблеми та результати

Зловмисники можуть впроваджувати вірусне програмне забезпечення в зображення для обходу антивірусів, IDS/IPS і пісочниць. Перш ніж вірус буде запущений на комп'ютері співробітника, його проаналізує багато пристроїв (рисунок 1).

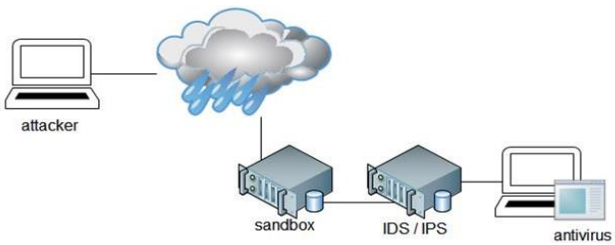


Рисунок 1 – Візуалізація шляху вірусу до цільового комп'ютера

Більшість методів аналізу включають використання відбитків і аналіз поведінки в пісочниці, а саме: перевірка поточного домену, перевірка запущених процесів, перевірка обсягу пам'яті, перевірка розміру диска, перевірка часу безвідмовної роботи.

Пісочниці аналізуватимуть тільки виконувані файли, бібліотеки DLL, документи Word, аплети Java. Більшість із засобів захисту просто не звертають уваги на зображення або інший безпечний тип файлу. Оскільки вважають, що немає причин витрачати процесорний цикл на аналіз зображення.

При дослідженні формату BMP найбільшу увагу привертають поля Size (розмір файлу BMP в байтах), XpelsPerMeter та YpelsPerMeter (горизонтальна та вертикальна роздільна здатність, пікселів на метр) та зарезервовані поля, адже вони є ненадійними. Звичайний заголовок BMP починається з подібного рядка 42 4D XX XX XX XX 00 00 00 00. Так наприклад відкривши зображення чорного прямокутника в hex-редакторі ми побачимо наступний заголовок (рисунок 2).

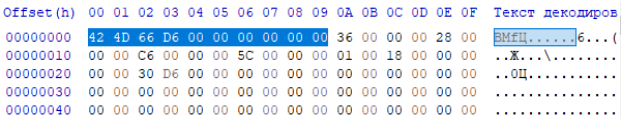


Рисунок 2 – Початок заголовку зображення.

Так, наприклад, можна впровадити вірус у зображення формату BMP, таким чином, що користувач не помітить нічого підозрілого. Він не побачить ніяких дивних пікселів на зображенні. Справа в тому, що штучно зменшивши висоту зображення на декілька пікселів в заголовку можна приховати спотворені пікселі, але людина цього не помітить.

Ін'єкція можлива через те, що байти, які вказують на тип файлу, з яких і починається файл, BM в ASCII, в шістнадцятковому вигляді – 42 4D, при конвертації в інструкції асемблера не призводять до помилки виконання, а подальші 8 байт заголовка ніяк не впливають на інтерпретацію зображення (рисунок 3). Ці 8 байт можна заповнити будь-якими інструкціями асемблера, наприклад, записати в них jmp-інструкцію, яка вкаже на вірус, що зберігається в зображенні (рисунок 4).

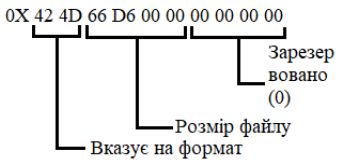


Рисунок 3 – Заголовок зображення.

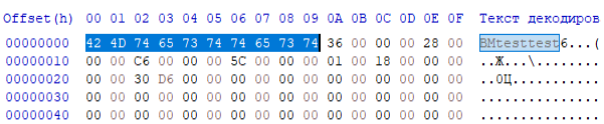


Рисунок 4 - Зображення зі зміненим заголовком.

Як вже згадувалося раніше заголовок файлу BMP починається з 0x 42 4D, що вказує на тип файлу (BM). При конвертації в інструкції асемблера отримаємо, що 42 – це inc edx, а 4D – dec ebp. Це означає, що якщо ці інструкції будуть передувати коду програми, то вони не викличуть збоїв та не мають команд переходів.

В hex-редакторі змінемо значення декількох останніх рядків (рисунок 5). Оскільки зображення було повністю чорним то значення дорівнювали 00.

Offset(h)	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Текст декодирован
0000D560	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
0000D570	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
0000D580	00	00	54	68	69	73	20	70	6C	61	63	65	20	69	73	...This place is
0000D590	65	6E	6F	75	67	68	20	74	6F	20	61	63	63	6F	6D	enough to accom
0000D5A0	6F	64	61	74	65	20	6D	61	6C	69	63	69	6F	75	73	modate malicious
0000D5B0	63	6F	64	65	2C	20	77	68	69	63	68	20	77	69	6C	code, which wil
0000D5C0	20	62	65	20	68	69	64	64	65	6E	20	69	6E	20	74	l be hidden in t
0000D5D0	65	20	69	6D	61	67	65	2E	20	42	75	74	20	64	75	he image. But du
0000D5E0	20	74	6F	20	74	68	65	20	63	68	61	6E	67	65	73	e to the changes
0000D5F0	74	68	65	72	65	20	77	69	6C	6C	20	62	65	20	6E	there will be n
0000D600	74	69	63	65	61	62	6C	65	20	76	69	73	75	61	6C	oticeable visual
0000D610	64	69	73	74	6F	72	74	69	6F	6E	73	2E	20	49	66	distortions. If
0000D620	61	72	74	69	66	69	63	69	61	6C	6C	79	20	72	65	artificially re
0000D630	75	63	65	20	74	68	65	20	68	65	69	67	68	74	20	duce the height
0000D640	66	20	74	68	65	20	69	6D	61	67	65	2C	20	74	68	of the image, th
0000D650	6E	20	74	68	65	79	20	63	61	6E	20	62	65	20	68	en they can be h
0000D660	64	64	65	6E	2E											idden.

Рисунок 5 – Змінене зображення.

Відкривши отримане зображення ми побачимо, що у правому верхньому куті з’явилися спотворені пікселі (рисунок 6).

Рисунок 6 – Збільшений правий кут зміненого зображення

Скориставшись hex-редактором ми можемо змінити висоту зображення і приховати спотворені пікселі (рисунок 7).

Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F
00000000	42	4D	74	65	73	74	74	65	73	74	36	00	00	00	28	00
00000010	00	00	C6	00	00	00	5B	00	00	00	01	00	18	00	00	00
00000020	00	00	30	D6	00	CC	00	00	00	00	00	00	00	00	00	00
00000030	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000040	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00

Рисунок 7 – Штучне зменшення висоти зображення на 1 піксель.

Після цих маніпуляцій відкривши зображення ми не помітимо нічого дивного (рисунок 8).

Рисунок 8 – Зображення зі штучно зменшеною висотою

Щоб виконати код, що зберігається в зображенні, можна використати набір команд PowerShell.

Основна небезпека подібних зображень з вірусами полягає в тому, що для виявлення загрози необхідно використовувати нестандартні методи. Можна змінити налаштування засобів захисту, щоб вони перевіряли всі типи файлів, але це суттєво сповільнить або навіть повністю паралізує роботу всієї інформаційно комунікаційної системи. Крім того, використання подібних інфікованих зображень може сильно ускладнити розбір інциденту інформаційної безпеки в організації. По-перше, системи безпеки можуть не відреагувати на вірус і виявити факт проникнення буде дуже складно. По-друге, якщо факт проникнення буде встановлений, буде майже не можливо з’ясувати як саме воно відбулося. Це обумовлено тим, що в першу чергу працівники відділу безпеки будуть з’ясовувати які виконувані файли, бібліотеки DLL, документи Microsoft Office, файли PDF потрапили в систему та використовувалися останнім часом. А через те, що не відома навіть приблизна дата проникнення, обсяг інформації, яку треба обробити значно зросте. В цьому випадку ніхто з працівників не буде досліджувати файли зображень.

III. Висновки

Важливо пам'ятати, що віруси можуть заражати не тільки виконувані файли і динамічні бібліотеки, а й файли зображень, аудіо та відео.

Оскільки зображення не можна запустити, як виконуваний файл, то і засоби захисту і технічні фахівці можуть легковажно ставитися до його вмісту та знехтувати цією загрозою. Однак такий файл може нести серйозну небезпеку. Необхідно уважно ставитися до налаштування систем запобігання вторгнень. І більш ретельно проводити розслідування інцидентів інформаційної безпеки.

Список літератури

[1] Ф.Файтс, П.Джонстон, М.Кратц "Комп'ютерний вірус: проблеми і прогноз", Москва, "Мир", 2013

[2] Мостовий Д.Ю. «Сучасні технології боротьби з вірусами».

Сімейство цифрових підписів SPHINCS

Марухненко Олександр Сергійович,
Харківський національний університет радіоелектроніки, пр. Науки 14, Харків, 61166, Україна
oleksandr.marukhnenko@nure.ua

Халімов Геннадій Зайдулович
Харківський національний університет радіоелектроніки, пр. Науки 14, Харків, 61166, Україна
gennadykhalimov@gmail.com

Анотація. *В роботі розглядається сімейство алгоритмів ЕЦП на основі геш-функцій SPHINCS, представники якого, SPHINCS+ та Gravity-SPHINCS, є кандидатами у конкурсі перспективних постквантових криптоалгоритмів NIST. Проаналізовано їх складові компоненти, переваги та недоліки.*

Ключові слова: *цифровий підпис, геш-функція, SPHINCS, постквантова криптографія.*

I. Введення. Постановка Завдання

Більшість сучасних асиметричних криптосистем побудовані на обчисленнях в кільцях, полях простих чисел і групах точок еліптичних кривих, їх стійкість базується на складності рішення задач факторизації (RSA), дискретного логарифма в полі (DSA) або групі точок еліптичної кривої (ECDSA). Всі перераховані завдання можуть бути вирішені з використанням квантового комп'ютера достатньої обчислювальної потужності. З метою аналізу та стандартизації нових криптосистем NIST в 2016 році оголошує про початок відкритого конкурсу. У першому раунді бере участь ряд алгоритмів, що базуються на різних алгебраїчних структурах - гратах, ізогеніях, геш-функціях і ряді інших. Представлено два алгоритми цифрового підпису на основі геш-функцій - SPHICS + [1] і Gravity SPHINCS [2], які є незалежними модифікаціями раніше розробленого алгоритму SPHINCS [3]. Завданням статті є аналіз та порівняння цих алгоритмів.

II. Рішення задачі

Серйозним недоліком перших розроблених алгоритмів цифрового підпису на базі геш-функцій є їх «одноразовість», тобто кожна пара ключів може бути використана для підпису тільки одного повідомлення. Рішення було запропоновано Мерклі і базується на використанні так званих геш-дерев або дерев Мерклі [4]. Геш-деревом називають повне бінарне дерево, в листові вершини якого поміщені геші від блоків даних, а внутрішні вузли містять геш-значення від конкатенації значень в дочірніх вершинах. Кореневий вузол дерева містить геш від усього набору даних, тобто геш-дерево є односпрямованої геш-функцією.

Як листя дерева виступаю геш-значення відкритих ключів одноразових підписів, наприклад ЦП Вінтерніц. Відкритим ключем є корінь дерева. Для підтвердження того, що використовуваний в підпису відкритий ключ OTS належить даному дереву, до підпису додається шлях аутентифікації - елементи дерева, необхідні для проходження від заданого листа до кореня дерева, № одноразового ключа, що був використаний, і сам відкритий ключ OTS. Таким чином перевірка підпису складається з двох етапів - перевірка підпису по відкритому ключу, аутентифікація ключа. В алгоритмах, в яких відкритий ключ повністю обчислюється з підпису (WOTS), немає необхідності передавати використаний ключ, що дозволяє зменшити розмір підпису.

Для зниження вимог до геш-функції можуть бути використані випадкові бітові маски, що накладаються на вузли перед гешуванням.

Для створення дерева з кількістю листків, не рівною ступені двійки, використовується концепція L-дерева: якщо у вузла немає правого сусіда, то даний вузол без змін переноситься на наступний рівень дерева.

SPHINCS працює з гіпердеревом висоти h, що складається з d рівнів дерев висоти h/d. Кожне з цих дерев виглядає наступним чином: листя дерева - $2^{h/d}$ коренів L-дерев, кожне з яких стискає відкритий ключ WOTS+. Відповідно, деерево можна розглядати, як пару ключів, що може бути використана для підпису $2^{h/d}$ повідомлень. Гіпердерево розділено на d рівнів. На рівні $d-1$ міститься одно дерево. На рівні $d-2$ міститься $2^{h/d}$ дерев. Корені цих дерев підписуються за допомогою пар ключів WOTS+ дерева на рівні $d-1$. В загальному випадку рівень i складається з $2^{(d-1-i)(h/d)}$ дерев, корені яких підписуються ключами WOTS+ дерев з рівня $i+1$. Нарешті, на рівні 0 кожна пара ключів WOTS+ використовується для підпису відкритого ключа HORST. Кажуть, що SHINCS має «віртуальну» структуру, оскільки усі елементи гіпердерева визначаються обраним ініціалізатором ГПВЧ та бітовими масками і уся структура ніколи не обчислюється. Ініціалізатор (seed) – частина секретного ключа, що використовується для псевдовипадкової генерації ключів гіпердерева.

В алгоритмі SPHINCS для псевдовипадкової генерації ключів використовується проста схема адресації. Адреса – бітовий рядок довжини $a = \lceil \log(d+1) \rceil + h$. Адресу пари ключів WOTS+ отримують шляхом кодування рівня дерева, до якого вона належить як log(d+1) – бітовий рядок (використовуючи $d-1$ для верхнього рівня з одним деревом. Потім надається індекс дерева на рівні у вигляді $(d-1)(h/d)$ -бітового рядка (дерева нумеруються зліва направо, починаючи з 0). Адресу пари ключів HORST отримують за допомогою адреси пари ключів WOTS+, яка використовується для підпису даного відкритого ключа, встановлюючи d як значення шару в адресному рядку.

Секретний ключ - два випадкових значення SK_1, SK_2, розмір яких визначається параметрами системи. SK_1 використовується для псевдовипадкової генерації ключів, SK_2 - для генерації непередбачуваного індексу і рандомізації геша повідомлення при створенні підпису.

Відкритий ключ - бітові маски (використовуються в WOTS +, HORST і L-деревах), корінь дерева шару d-1.

Підпис повідомлення являє собою підпис HORST, підписи коренів проміжних дерев, шляхи автентифікації. Структура алгоритму SPHINCS+ схожа зі структурою SPHINCS, проте були змінені деякі внутрішні компоненти, особливо схема багаторазової підпису. Основні відмінності:

1) Захист від багатоцільової атаки, яка полягає у застосуванні різних геш-функцій для кожного виклику - параметризованих геш-функцій. При кожному виклику використовуються різні ключі і різні бітові маски, які псевдовипадково генеруються на основі адреси виклику і відкритого значення.

2) Стиснення відкритого ключа WOTS+ без використання L-дерев. Замість них використовується параметризована геш-функція.

3) Заміна алгоритму HORST на FORS (Forest Of Random Subset). Ключова пара FORS складається не з єдиного монолітного геш-дерева, а з k дерев висоти log(t). Листя цих дерев - геші t секретних елементів, секретний ключ складається з kt елементів. Відкритий ключ - параметризований геш від конкатенації коренів всіх дерев. Значна відмінність від HORST полягає в отриманні набору значень секретного ключа для кожного індексу, отриманого з повідомлення. Подібний підхід дозволяє використовувати менші параметри, що збільшує швидкодію і зменшує розмір підпису.

4) Верифікований вибір індексу: у SPHINCS ключова пара HORST, що використовується для підпису повідомлення визначалася псевдовипадково згенерував індексом. Через використання секретного значення, перевіряючий не міг переконатися в коректності індексу. Даний недолік робив можливою багатоцільову атаку, в SPHINCS + він був усунутий за рахунок генерації індексу разом з дайджестом повідомлення.

Були представлені три варіації алгоритму SPHINCS+:

- SPHINCS+-SHA3 (використовує SHAKE256),
- SPHINCS+-SHA2 (використовує SHA2)
- SPHINCS+-Haraka (використовує коротко-входову геш-функцію Haraka).

Алгоритм Gravity-SPHINCS також є поліпшенням вихідного SPHINCS. У первинному варіанті для підписування безпосередньо повідомлень використовується алгоритм HORS, що має такий недолік: при збігу бітових рядків в геш-значенні повідомлення в підпису повторно використовується один і той же елемент ключа, що призводить до зниження стійкості. У Gravity-SPHINCS використовується модифікований алгоритм - PORS (PRNG to obtain a random subset), системні параметри і методи генерації ключів залишаються без змін, алгоритм підпису стає наступним:

1) Обчислюється геш повідомлення та и розбивається на k блоків по τ біт: $H_c(M) = (h_0, h_1, ..., h_{k-1})$
2) Якщо $h_i = h_j$, $i > j$, h_i відкидається та генерується новий блок довжини τ біт, що додається у кінець повідомлення, операція повторюється доти, доки усі блоки не будуть унікальними. Генерація нових блоків здійснюється ГПВП, що було ініціалізовано поатковим повідомленням.
3) Обчислюється підпис аналогічно HORS.

Для одночасної аутентифікації декількох листків дерева Мерклі автори використовують алгоритм Octopus, що дозволяє також прибрати надмірність шляхів автентифікації.

Алгоритми цифрового підпису на основі геш-функцій є перспективним напрямком постквантової криптографії, на конкурсі NIST вони представлені рішеннями Gravity-SPHINCS і SPHINCS +.

Gravity-SPHINCS і SPHINCS + - це два різних поліпшення вихідного алгоритму SPHINCS. Обидва змінюють схему багаторазового підбору HORST, використовувану в SPHINCS, різними її варіаціями. Це призводить до підписів змінної довжини для Gravity-SPHINCS і підписам фіксованої довжини для SPHINCS +. Однак, часто більш короткі підписи змінної довжини вимагають більше обчислювальних витрат на створення і перевірку.

Обидва алгоритми змінюють спосіб обчислення індексу використовується схеми багаторазової підпису. Різними методами вони досягають того, що індекс може бути перевірений верифікатором, подібної можливості не було в алгоритмі SPHINCS. Нарешті, Gravity-SPHINCS використовує припущення, що виявлення колізій для квантових комп'ютерів відбувається так само повільно, як пошук другого прообразу, при певних припущеннях про час доступу до пам'яті. Отже, Gravity-SPHINCS трохи спрощує процес гешування за рахунок зниження безпеки від стійкості до колізій внутрішньої геш-функції. Навпаки, SPHINCS+ знижує вимоги до стійкості по обчисленню другого прообразу (використовуються різні припущення про геш-функції, використовуваної для стиснення повідомлення в обох пропозиціях).

III. Висновки

Таким чином, схеми спроектовані принципово однаково, але відрізняються реалізацією певних блоків алгоритму. Вибір однієї з схем повинен здійснюватися з урахуванням конкретних вимог до використовуваної підпису.

Посилання

[1] Daniel J. Bernstein, Christoph Dobraunig, Maria Eichlseder, Scott Fluhrer, Stefan-Lukas Gazdag, Andreas Hulsing, Panos Kampanakis, Stefan Kolbl, Tanja Lange, Martin M. Lauridsen, Florian Mendel, Ruben Niederhagen, Christian Rechberger, Joost Rijneveld, and Peter Schwabe. SPHINCS+ – Submission to the NIST's post-quantum cryptography standardization process, 2017.

[2] .Jean-Phillippe Aumasson and Guillaume Endignoux. Gravity-SPHINCS – Submission to the NIST's post-quantum cryptography standardization process, 2017.

[3] Daniel J. Bernstein, Daira Hopwood, Andreas Hülsing, Tanja Lange, Ruben Niederhagen, Louiza Papachristodoulou, Peter Schwabe, and Zooko Wilcox O'Hearn. Sphincs: practical stateless hash-based signatures. Cryptology ePrint Archive, Report 2014/795, 2014.

[4] Ralph Merkle. A certified digital signature. In Gilles Brassard, editor, Advances in Cryptology – CRYPTO '89.

ІНФОРМАЦІЙНИЙ ЗАХИСТ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ УКРАЇНИ

Меленті Євген Олександрович

Інститут підготовки юридичних кадрів для СБУ НЮУ ім. Я. Мудрого, м. Харків, вул. Мироносицька, 71, Україна

Анотація. *В доповіді запропоновано використовувати модель загроз для типового об'єкту критичної інфраструктури при визначенні рівня захищеності об'єктів критичної інфраструктури й оцінці таких об'єктів на предмет уразливості систем безпеки. Використання такого підходу дозволить систематизувати можливі інциденти, з'ясувати причини, фактори їх виникнення та виробити ефективні заходи протидії та забезпечення стійкості функціонування об'єктів критичної інфраструктури.*

Ключові слова: *кібербезпека; шкідливе програмне забезпечення; інформаційна безпека держави; кібернетична загроза..*

I. Вступ

З кожним роком в світі збільшується кількість кіберзлочинів та кібератак. Нажаль, така тенденція не оминула й Україну. Відзначається значне зростання інтенсивності кібератак, здійснюваних на інформаційно-телекомунікаційну інфраструктуру в Україні. Протягом останніх років кібератак через мережу Інтернет зазнавали інформаційно-телекомункаційні системи державних установ, великих компаній, фінансових установ, політичних партій та засобів масової інформації, інформаційна інфраструктура об'єктів військового управління. В таких умовах необхідно підвищувати рівень захищеності критичної інфраструктури від терористичних посягань і диверсій в інформаційному просторі.

II. Вирішення проблеми та результати

З метою вирішення окресленого кола питань та вироблення дієвого механізму протидії диверсійно-підривній діяльності іноземних спецслужб у березні 2016 року введено в дію Стратегію кібербезпеки України, а у жовтні 2017 року підписано Закон України «Про основні засади забезпечення кібербезпеки України» [1], яким визначено основи протидії підривній діяльності в кібернетичній сфері. Прийняття закону надало можливість створення в Державній службі спеціального зв'язку та захисту інформації Центру реагування на кіберзагрози. Також у 2018 році на базі Служби безпеки України спільно з НАТО сформовано Ситуаційний центр забезпечення кібербезпеки, головними завданнями якого є запобігання кібератакам, встановлення їхнього походження та формування пропозицій із протидії їм. Як визначено статтею 19 Закону України «Про національну безпеку» [2], Служба безпеки України забезпечує державну безпеку, здійснюючи: протидію розвідувально-підривній діяльності проти України; боротьбу з тероризмом; контррозвідувальний захист державного суверенітету, конституційного ладу і територіальної цілісності, оборонного і науково-технічного потенціалу, кібербезпеки, економічної та інформаційної безпеки держави, об'єктів критичної інфраструктури; охорону державної таємниці. Таким чином, протидія розвідувально-підривній діяльності на об'єктах критичної інфраструктури в інформаційній сфері є однією з важливих задач, які покладаються на Службу безпеки України. Слід навести приклад масованої атаки комп'ютерного вірусу PetyaA на українські фінансові установи, урядові організації та медіа компанії, локальні мережі, великі промислові об'єкти влітку 2017 року. Така кібернетична загроза паралізувала роботу зазначених установ та організацій на тривалий час. Для мінімізації загроз державним інформаційним ресурсам Службою безпеки України, зокрема Департаментом контррозвідувального захисту інтересів держави у сфері інформаційної безпеки, у взаємодії з іншими правоохоронними органами України та міжнародними партнерами здійснено заходи щодо локалізації розповсюдження шкідливого програмного забезпечення.

В розрізі становлення й розвитку єдиної національної системи захисту об'єктів критичної інфраструктури неодмінно слід приділити увагу питанням забезпечення інформаційної безпеки та кіберзахисту таких об'єктів, що в свою чергу вимагає вироблення дієвої протидії таким загрозам. Отже, для встановлення пропорційності та адекватності заходів кіберзахисту реальним та потенційним ризикам по-перше, необхідно визначити рівень інформаційної захищеності таких об'єктів критичної інфраструктури. Враховуючи набутий позитивний досвід, до цих заходів доцільно залучити представників Служби безпеки України в якості експертів для проведення комплексної оцінки кіберзагроз щодо об'єктів критичної інфраструктури (насампред, кібертероризм та кібердиверсії). По-друге, необхідно унормувати порядок проведення зазначених перевірок та визначення рівня захищеності об'єктів критичної інфраструктури, виявлення уразливих місць в системі безпеки. Зазначену процедуру, повноваження та завдання Служби безпеки України в сфері захисту об'єктів критичної інфраструктури доцільно врахувати в новій редакції Закону України «Про Службу безпеки України» [3].

III. Висновки

В доповіді запропоновано використовувати модель загроз для типового об'єкту критичної інфраструктури при визначенні рівня захищеності об'єктів критичної інфраструктури й оцінці таких об'єктів на предмет уразливості систем безпеки. Використання такого підходу дозволить систематизувати можливі інциденти, з'ясувати причини, фактори їх виникнення та виробити ефективні заходи протидії та забезпечення стійкості функціонування об'єктів критичної інфраструктури.

Список літератури

[1] Закон України. Про основні засади забезпечення кібербезпеки України // [Електронний ресурс].-Режим доступу: http://zakon. rada. gov. ua. – 2017.

[2] Про національну безпеку України: Закон України від 21.06.2018 № 2469-VIII. URL: http://zakon5.rada.gov.ua/laws/show/2469-19.

[3] [Закон України «Про Службу безпеки України» : від 25.03.1992 р. // Закони України. – К. : Книга, 1997. – Т. 3. – С. 141–152.

Аналіз безпеки даних на основі платформи Samsung Knox

Нечволод Костянтин Вадимович
Сєвєрінов Олександр Васильович

Харківський Національний Університет Радіоелектроніки, пр. Науки, 14, Харків UA-61166, Україна,
kostiantyn.nechvolod@nure.ua
Харківський Національний Університет Радіоелектроніки, пр. Науки, 14, Харків UA-61166, Україна,
oleksandr.sievierinov@nure.ua

Анотація. *У доповіді розглянуто можливі вразливості та атаки на систему Samsung Knox.*

Ключові слова: *віруси; проникнення; подолання системи захисту; KNOX; MDM; ROOT OF TRUST.*

I. Вступ

Використання свого власного пристрою є новою, стрімко набираючою поширеність, тенденцією серед підприємств, яка спрямована на підвищення мобільності і продуктивності працівників за допомогою власних смартфонів. Погрози та небезпеки для підприємств також стрімко ростуть. Однак такі погрози можливо пом'якшити за допомогою запуску програмного забезпечення в «захищеному контейнері» на персональному пристрої. В даній роботі описані основні загрози для смартфонів, захист від них за допомогою Samsung Knox, яка є реальним засобом для задовільнення сучасних потреб бізнеса.

II. Вирішення проблеми та результати

Зараз одними з найпоширеніших загроз для мобільних пристроїв є:

– використання для доступу до глобальної мережі через незахищені точки доступу Wi-Fi, в яких можлива атака MITM(людина посередині);

– можливість крадіжки або втрати пристрою, яка дозволить зловмиснику отримати повний фізичний доступ до пристрою;

– шкідливе програмне забезпечення, яке може бути встановлено не навмисно самим користувачем і яке буде тихо збирати усю потрібну зловмиснику інформацію та навіть робити фото, відео та аудіо фіксацію усього, що трапляється навколо пристрою.

Однак остання загроза є найменш вірогідною через сам принцип побудови системи Android, де кожен додаток виконується відокремлено від інших та отримати доступ до даних іншої програми без отримання прав root неможливо.

Захист від цих загроз в системі Knox реалізовано комплексними заходами перевірки стану пристрою, справжності всіх складових операційної системи та використання для збереження конфіденційних даних в окремому, так званому, контейнері. Цей контейнер засновано на віртуалізації на самому пристрої і втілює ідею роботи багатьох «Віртуальних пристроїв», маючих свої власні ім'я, ізольованих один від одного на одному фізичному пристрої.

Захист за умови підключення до незахищених мереж забезпечується за допомогою використання окремого VPN для середовища Knox, а саме окремих додатків, для більшого захисту даних.

Захист даних при втраті пристрою з одного боку забезпечується криптографічними методами, а саме шифруванням, та за допомогою дистанційного блокування пристрою, визначення його місцезнаходження по координатах мережі та різноманітних супутникових систем навігації які підтримуються на пристрої. Та найголовніше – можливість повного видалення усієї інформації з втраченого мобільного пристрою.

Саме по собі шифрування даних пов'язано з апаратним забезпеченням Root of Trust та безпосередньою автентифікацією користувача, будь то графічний пароль, пін код, пароль або навіть біометричні засоби автентифікації, такі як сканування відбитка пальця, сітківки ока та сканування обличчя. Це забезпечує розшифрування даних тільки на тому пристрої, на котрому вони були зашифровані і тільки власником пристрою. Також використовується система DualDAR яка надає два варіанта шифрування для досягнення ще більшого рівня надійності.

Платформа Knox створює надійне середовище чотирма шляхами:

– Встановлює заснований на апаратному забезпечені Root of Trust, від якого залежать інші компоненти;

– Створює довіру під час завантаження системи за допомогою таких функцій, як Trusted Boot;

– Підтримує довіру під час користування пристроєм за допомогою захисту ядра в реальному часі;

– Доводить свою надійність за запитом за допомогою атестації працездатності пристрою.

Структура наведена на рис. 1

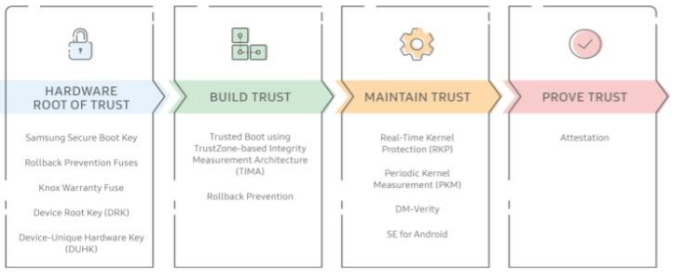


Рисунок 1-Загальна структура платформи Samsung Knox

Root of Trust створюється завдяки наступним крокам:

1. Генерується унікальний ключ для даного пристрою(DUHK) за допомогою апаратного генератора випадкових чисел;
2. Далі DUHK генерує і шифрує кореневий ключ пристрою(DRK) та ключ підтвердження Samsung(SAK). DRK і SAK включають код аутентифікації, який дозволяє

перевірити IMEI і серійний номер пристроїв. Це дозволяє користувачам отримати підтвердження того, що вони користуються саме с тим пристроєм, з яким повинні.
Використання DUHK доступно тільки для операційної системи TrustZone, яка використовує його для створювання наступних унікальних для кожного довіреного додатка ключів. DRK і SAK являються закритими ключами, які дозволяють довіреним додаткам підтверджують свою справність. Ці додатки глибоко інтегруються з апаратним забезпеченням для досягнення більшої безпеки.

3. Після запуска пристрою, Samsung використовує ключ безпечного завантаження(SSBK) для перевірки усього програмного забезпечення.

4. Програмне забезпечення перевіряє кожну функції. Платформи Knox, перед її запуском. Так як кожна перевірка складає ланцюг перевірок, яка починається з самої першої перевірки на апаратному Root of Trust, неважливо в який ланці була атака, система це виявить.

Для миттєвого блокування та недопущення запуску інших захищених частин системи, в платформі використовується так званий гарантійний запобіжник. Це одноразовий програмний запобіжник, який вказує на те, що пристрій ніколи не був в несанкційному стані. Якщо один з компонентів перевірки виявляє використання нелегітимних компонентів або якщо відключені деякі компоненти системи наприклад SELinux, система активує запобіжник.

Коли запобіжник активовано виконуються наступні міри безпеки:

– Не проходить перевірка працездатності пристрою;
– Видаляються усі ключі які використовуються для шифрування даних;
– Система Knox більше не працює на даному апаратному забезпечені, запобігаючи надання доступу до захищених даних, додатків всередині захищеного контейнера.

Унікальними особливостями системи Knox є те, що вона надає наступні ключові особливості:

– Визначення працездатності гарантовані для кожного пристрою завдяки кореневому ключу пристрою(DRK)
– Результати цієї перевірки легко співвідносяться з унікальними даними пристрою такими як IMEI або серійним номером.

Це все дозволяє IT-адміністраторам підприємства визначати який результат атестації пристрою відноситься до конкретного девайса без необхідності ретельної перевірки результатів з існуючими пристроями. В інших системах, які доступні на ринку, результати, надсилаються з окремих пристроїв, але IT-адміністратори не можуть чітко визначити пристрій по результату.

III. Висновки

Платформа Knox забезпечує IT-адміністраторам, адміністраторам безпеки можливість безпечного масового розгортання обладнання для мобільних пристроїв і швидкої інтеграції з існуючою бізнес-інфраструктурою і застосунками. Вона виконує багато перевірок для запобігання доступу до конфіденційних даних за наявності компрометації системи.

До недоліків можна віднести можливість використання цієї системи тільки на пристроях однієї компанії, закритість ісходного коду та неможливість відновлення працездатності системи після атак. Ще одним недоліком можна вважати доступ до деяких можливостей лише на платній основі.

Список літератури

[1] Samsung. WhitePaper: Knox Platform for Enterprise, 2018
[2] Kanonov U., Wool A. Sequre Containers in Android: the Samsung KNOX Case Study, 2016

Безпечне оновлення програмного забезпечення сучасних автомобілів

Фесенко Дмитро Олександрович

Харківський національний університет радіоелектроніки, пр. Науки 14, Харків, 61166, Україна
dmytro.fesenko@nure.ua

Халімова Світлана Володимирівна

Харківський національний університет радіоелектроніки, пр. Науки 14, Харків, 61166, Україна
svitlana.khalimova@nure.ua

Анотація. *The paper considers the possibilities of secure updating of car's ECUs, that connected with CAN network and can examine and controle all states of software update over different means of connection on different stages of update.*

Ключові слова: *система оновлення програмного забезепечення;автомобільна система; валідація даних; CAN мереж*

I. Введення. Постановка Завдання

Автовиробники почали випускати автомобілі з можливістю оновлення програмного забезпечення в автоматичному режимі через інтернет(технологія OTA), що відкриває нові можливості для проведення атак на компрометацію перепрограмування пристрою через мережу інтернет [1÷2]. Завданням статті є розробка системи, що контролює безпечність функціонування та оновлення ECU.

II. Рішення задачі

Більшість сучасних ECU оновлюються через мережеву шину CAN, де пристрій оновлення підключається до серверу обновлення до шини CAN в якості ECU і використовує існуючу можливість оновлення прошивки. В таких системах відсутня можливість валідації пристроїв відповідно до нового програмного забезпечення, що дає можливість при захоплені керування якимось ECU дозволяє підмінити оновлення ідентифікаторів пристрою. Іншою проблемою є повна довіра до даних, отриманих від сервера дилера, що може призвести до компрометації файлу оновлення. Таким чином під час розробки таких систем необхідно проводити додаткові кроки валідації, що будуть проводитися під час різних етапів оновлення програмного забезпечення системи, що фіксує зміни ідентифікаторів на основі технологій хешування параметрів недоліки існуючих методів на основі статистичних методів обробки повідомлень в мережі CAN для забезпечення надійного, безпечного та безперебійного управління програмними системами в автомобілях[3].

Виходячи з цього пропонується до використання система, що складається з ECU у вигляді мікрокомп'ютера, підключеного до мережі CAN автомобіля з функціональністю оновлення інших пристрої в мережі та моніторингу повідомлень для виявлення деструктивного впливу від скомпрометованих ECU, що буде працювати як система попередження вторгнення.

Система використовує функціонал перевірки станів частин інформації від серверу за допомогою перевірки функцій хешування та тестує роботу оновленого пристрою визначаючи повідомлення, що той відправляє на різні запроси.

Безпечна передача програмного забезпечення має велике значення для забезпечення успішного оновлення програмного забезпечення ECU. Для цього може виконуватися процес де OEM виробляє пакети оновлення мікропрограми, після чого OEM підписує пакет оновлення із захищеним закритим ключем. Сервер оновлення на стороні дилера запитує сервер, що підтримує OEM і завантажує оновлення програмного забезпечення через захищене з'єднання. Контрольна сума пакетів оновлення MD5 також передається для забезпечення завантаження оновлення програмного забезпечення не пошкоджено під час передачі. Система проводить перевірку цілісності завантаженого програмного забезпечення ECU за допомогою перевірки хеш-значення визначених даних з хеш-значенням, що отримується від серверу валідації. Відкритий ключ генерується на EOM для розшифрування пакета програмного забезпечення. Це гарантує, що пакет оновлення програмного забезпечення не буде змінено під час передачі через мережу інтернет або на сервері дилера. Система оновлення програмного забезпечення розшифровує пакет оновлення використовуючи відкритий ключ та перевіряє цілісність пакетів, після чого система оновлення програмного забезпечення ініціює оновлення програмного забезпечення для підключеного до ECU. Система гарантує цілісність процесу оновлення програмного забезпечення протягом всього циклу оновлення.

III. Висновки

Запропонована система дає необхідний контроль для належного управління програмним забезпеченням для різних автомобілів, що використовують для оновлення своїх систем, тестувати правильність оновлень та чи правильно вони працюють після проведення оновлень, чи не мають вони в собі деструктивних команд.

ПОСИЛАННЯ

[1] Mercedes Benz Workshop Manual S 430 4MATIC / електронний ресурс: https://workshop-manuals.com/mercedesbenz// — 2011.

[2] Smith C. Car Hacker's Handbook, A Guide for the Penetration Tester. San Francisco. 2016.-P.532

[3] Shanmugam K. Update Mechanism for Automotive ECU, /електронний ресурс:https://www.academia.edu/11130687/IJIRAE_Secure_Software_Update_Mechanism_for_Automotive_ECU// 2014.

Аналіз постквантової криптосистеми McEliece

Шипілов Дмитрій Віталійович,
Харківський національний університет радіоелектроніки, пр. Науки 14, Харків, 61166, Україна
dmyrtii.shypilov@*nure.ua*

Халімов Геннадій Зайдулович
Харківський національний університет радіоелектроніки, пр. Науки 14, Харків, 61166, Україна
gennadykhalimov@gmail.com

Анотація. *В роботі розглядається криптосистема McEliece, що заснована на теорії алгебраїчного кодування. Алгоритм асиметричного шифрування та алгоритм електронно-цифрового підпису, які засновані на криптосистемі McEliece визначаються перспективними для постквантової криптографії. Проаналізовано їх складові компоненти, переваги та недоліки.*

Ключові слова: *електронно-цифровий підпис, криптосистема McEliece, постквантова криптографія, хеш-функція.*

I. Введення. Постановка Завдання

McEliece – криптосистема з відкритими ключами на основі теорії алгебраїчного кодування запропонована Робертом Мак-Елісом у 1978 році. Це перша схема, яка використовує рандомізацію в процесі шифрування. Алгоритм використовує великий розмір ключових даних і не отримав відповідного визнання в криптографії. У проекті NIST, у 2016 він став кандидатом для постквантовой криптографії.

Алгоритм заснований на складності декодування повних лінійних кодів (спільне завдання декодування є NP-складним) і є стійким до атаки з використанням алгоритму Шора. Алгоритм використовує двійкові коди Гоппа. Алгебраїчний код, для якого відомий ефективний алгоритм декодування дозволяє виправляти t спеціально доданих помилок.

Криптосистема McEliece з кодами Гоппа не піддається сучасному криптоаналізу. Найбільш відомі атаки використовують алгоритм декодування множини даних [1÷3]. Завданням статті є аналіз складових частин криптосистеми McEliece та побудова на її основі електронного цифрового підпису.

II. Рішення задачі

1) Опис алгоритму асиметричного шифрування.

McEliece складається з трьох частин:

- алгоритму випадкової генерації ключа, результатом якого є відкритий та особистий ключі;
- алгоритму випадкового шифрування;
- детермінованого алгоритму розшифрування.

Текст повідомлення являє собою вектор довжини k над кінцевим полем $GF(\mathrm{q})$. Користувачі в системі спільно використовують параметри безпеки: n, k, t.

Генерація ключа:

- Аліса вибирає $[\mathrm{n},\mathrm{k},\mathrm{d}]$ – лінійний код, що виправляє t помилок. Потім для обраного коду розраховує породжуючу матрицю G розміром $k \times n$;
- для того, щоб вихідний код було складно відновити, Аліса генерує випадкову невироджену матрицю S розміром $k \times k$;
- Аліса генерує випадкову матрицю перестановки P розміром $n \times n$;
- Аліса обчислює матрицю $\hat{G} = S * G * P$;
- відкритим ключем є пара $(\hat{\mathrm{G}},\mathrm{t})$, а особистим – $(\mathrm{S},\mathrm{G},\mathrm{P})$.

Алгоритм шифрування.

Нехай Боб хоче передати повідомлення m Алісі, чий відкритий ключ $(\hat{\mathrm{G}},\mathrm{t})$. Основні кроки:

- Боб представляє своє повідомлення m у вигляді послідовностей двійкових символів довжини k;
- Боб генерує випадковий вектор помилок z довжини n та вагою t;
- Боб обчислює шифротекст як $c' = m * \hat{G} + z$ та передає його Алісі.

Алгоритм розшифрування.

Після отримання повідомлення c, Аліса виконує наступні дії для розшифрування повідомлення:

- обчислює зворотну матрицю P^{-1};
- обчислює $\hat{c} = c * P^{-1}$;
- використовує алгоритм декодування для коду $[\mathrm{n},\mathrm{k},\mathrm{d}]$, щоб отримати $\hat{m}$ з $\hat{c}$;
- обчислює $m = \hat{m} * S^{-1}$.

Перевірка коректності алгоритму.

Продемонструємо, що виконується головна властивість криптосистеми, тобто, що $D(\mathrm{E}(\mathrm{m})) = \mathrm{m}$. Боб надсилає $c = m * \hat{G} + z = m * S * \mathrm{G} * \mathrm{P} + \mathrm{z}$. Аліса обчислює $\hat{c} = c * P^{-1} = m * S * G + z * P^{-1}$. Оскільки P^{-1} – зворотна матриця перестановки, то вага $z * P^{-1}$ не більше ніж t. Код Гоппа матриці G виправляє до t помилок. Вага $\mathrm{wt}(\mathrm{m} * \mathrm{S} * \mathrm{G}, \mathrm{c} * \mathrm{P}^{-1}) \le \mathrm{t}$, тому Аліса отримає вірне повідомлення $\hat{m} = m * S$. Після цього Аліса обчислює вихідне повідомлення $m = \hat{m} * S^{-1} = m * \mathrm{S} * S^{-1}$.

Повна схема роботи алгоритму шифрування криптосистеми McEliece представлена на рис. 1.

2) ЕЦП, що ґрунтується на алгоритмі McEliece

ЕЦП заснований на алгоритмі McEliece складається з трьох частин:

- алгоритму випадкової генерації ключа, який формує відкритий та особистий ключі;
- алгоритму формування підпису;
- алгоритму перевірки підпису.

Хеш документа D, який необхідно підписати, представляє собою вектор довжини n над кінцевим полем $GF(q)$. Користувачі в системі спільно використовують параметри безпеки: n, k, t.

Рисунок 1 – Схема роботи алгоритму шифрування криптосистеми McEliece

Генерація ключа:

- Аліса вибирає $[n,k,d]$ – лінійний код, що виправляє t помилок. Потім для обраного коду розраховує породжуючу матрицю G розміром $k \times n$;

- для того, щоб вихідний код було складно відновити, Аліса генерує випадкову невироджену матрицю S розміром $k \times k$;

- Аліса генерує випадкову матрицю перестановки P розміром $n \times n$;

- Аліса обчислює матрицю $\hat{G} = S * G * P$;

- відкритим ключем є пара $(\hat{G}, t)$, а особистим – (S, G, P).

Формування ЕЦП:

- Аліса вибирає хеш-функцію $h()$, яка генерує n символів на виході. Таким чином, результат даної хеш-функції можна представити у вигляді синдрому і спробувати декодувати;

- вона обчислює хеш від документа $h(D)$;

- далі обчислюється $h(h(D) \| i)$, для $i = 0,1,2\ldots$ до тих пір, доки для деякого мінімально $i = i_{\min}$ буде можливо декодувати синдром одержуваний з обчисленого хешу;

- синдром $h(h(D) \| i_{\min})$ можна уявити як кодове слово з помилками обчислене для деякого A з помилками z ($h(h(D) \| i_{\min}) = A\hat{G} + z$);

- Аліса обчислює

$$h(h(D) \| i_{\min}) * P^{-1} = (A\hat{G} + z) * P^{-1} = A\hat{G} * P^{-1} + z * P^{-1} =$$
$$= A * S * G * P * P^{-1} + z * P^{-1} = A * S * G + z * P^{-1};$$

- застосовуючи швидкий алгоритм декодування Φ для $h(h(D) \| i_{\min}) * P^{-1}$ вона отримує: $\Phi(h(h(D) \| i_{\min}) * P^{-1}) \to A' = A * S$ та $z' = z * P^{-1}$;

- далі вона обчислює $A = A' * S^{-1} = A * S * S^{-1}$ та $z = z' * P = z * P^{-1} * P$;

- підписом документа D є параметри $(A, z, i_{\min})$.

Перевірка підпису:

- Боб обчислює $v_1 = h(h(D) \| i_{\min})$;

- потім він обчислює $v_2 = A * \hat{G} + z$;

- якщо $v_1 == v_2$ та $wt(z) \le t$, то підпис вірний.

Рисунок 2 – Схема роботи алгоритму шифрування криптосистеми McEliece

III. Висновки

В роботі виконано аналіз перспективних постквантових алгоритмів цифрового підпису заснованих на лінійних кодах. Запропоновано електронний цифровий підпис, що заснований на основі криптосистеми McEliece. Для забезпечення високої криптографічної стійкості алгоритму McEliece і ЕЦП на його основі необхідно використати коди з великими параметрами (n,k,d) і існує питання складності обчислень при декодування кодових слів.

Посилання

[1] Marco Baldi, Franco Chiaraluce, Roberto Garello, and Francesco Mininni. Quasi-cyclic low-density parity-check codes in the McEliece cryptosystem. In Proceedings of IEEE International Conference on Communications, ICC 2007, Glasgow, Scotland, 24-28 June 2007, pages 951–956. IEEE, 2007.

[2] Rafael Misoczki and Paulo S. L. M. Barreto. Compact McEliece keys from Goppa codes. In Michael J. Jacobson Jr., Vincent Rijmen, and Rei Safavi-Naini, editors, Selected Areas in Cryptography, volume 5867 of Lecture Notes in Computer Science, pages 376–392. Springer, 2009.

[3] Daniel J. Bernstein, Tung Chou, Tanja Lange, Ingo von Maurich, Rafael Misoczki, Ruben Niederhagen, Edoardo Persichetti, Christiane Peters, Peter Schwabe, Nicolas Sendrier, Jakub Szefer, Wen Wang. Classic McEliece: conservative code-based cryptography, 2017. – 38 c.

[4] Anja Becker, Antoine Joux, Alexander May, and Alexander Meurer. Decoding random binary linear codes in 2n/20: How 1+1 = 0 improves information set decoding. In David Pointcheval and Thomas Johansson, editors, Advances in Cryptology -EUROCRYPT 2012 - 31st Annual International Conference on the Theory and Applications of Cryptographic Techniques, Cambridge, UK, April 15-19, 2012. Proceedings, volume 7237 of Lecture Notes in Computer Science, pages 520–536. Springer, 2012.

Програмний комплекс для моделювання атак

Федюшин Олександр Іванович[1],

Левченко Денис Юрійович[2],

Лиско Віктор Іванович[3]

[1]*Харківський національний університет радіоелектроніки, пр. Науки, 14, м .Харків, UA-61166, Україна, oleksandr.fediushyn@nure.ua*

[2]*Харківський національний університет радіоелектроніки, пр. Науки, 14, м .Харків, UA-61166, Україна, denys.levchenko@nure.ua*

[3] *Харківський національний університет радіоелектроніки, пр. Науки, 14, м .Харків, UA-61166, Україна, viktor.lysko@nure.ua*

Анотація. *Розроблено програмний комплекс для моделювання атак в комп'ютерних мережах, що базується на використанні технологій віртуалізації та набору сценаріїв атак на мові програмування Python та її бібліотечних модулей. Запропоновані моделі дозволять отримувати науково-обґрунтовані організаційно-технічні рішення при проведенні аудиту, впровадження яких сприятиме підвищенню рівня інформаційної безпеки організації.*

Ключові слова: *моделювання, мережеві атаки, пентест, віртуалізація, програмний комплекс, python.*

I. Вступ і Постановка Завдання

З кожним роком кількість та способи мережевих атак непомірно зростають, тому при проектуванні мережі варто враховувати найгірші сценарії – атаки на неї, що може призвести до порушення трьох базових принципів захисту даних [1]: конфіденційності, цілісності та доступності. Розробляти та будувати окремий сегмент мережі, ідентичний перспективному, лише для тестування, це, насамперед, економічно невигідно, тому для тестування перспективних мереж використовуються спеціальні комплекси.

На сьогоднішній день існують дві основні технології побудови середовища для моделювання атак [2,3] – це використання систем на зразок Honeypot («Пастка»), тобто організація ресурсу, що є приманкою для зловмисників, і другий варіант – побудова моделі реально функціонуючої мережі в межах віртуального середовища, яка отримала назву в літературних джерелах Insight («під наглядом»).

Honeypot є ресурсом, що без будь-якого впливу на нього є неактивним, він збирає невелику кількість інформації, після аналізу якої будується статистика методів, якими користуються зловмисники, а також визначається наявність якихось нових рішень, які згодом будуть застосовуватися в боротьбі з ними. Існують версії, що функціонують на виділених серверах, а також програмно-емульовані. В межах невеликої мережі достатньо обмежитися віртуальною системою або навіть одним віртуальним сервісом. У великих організаціях використовуються виділені сервери з повністю відтвореними на них мережевими службами. Зазвичай в конфігурації таких служб спеціально допускають помилки, щоб у зловмисника вдався злом системи. В ідеалі всі події в подібних системах повинні записуватися на рівні ядра. Типові продукти подібного семейства: HoneyWeb, Honeyd, BackOfficer Friendly, Honeypot Manager, Potemkin Virtual Honeyfarm. В більшості випадків подібні системи застосовуються для проведення аналізу реалізацій масштабованих хакерських атак по типу Black Hat, перевіряється функціонування антивірусних засобів на предмет атак хробаків, або бекдорів. Як правило такі системи є досить дорогими в експлуатації і є спеціалізованими, для широкого кола спеціалістів недоступними. Тому на практиці найбільш розпосюдженою є технологія використання віртуальних машин [4,5] для емуляції функціонування мереж з різними робочими станціями та базовими операційними системами (ОС). Можливості моделювання в подібних системах обмежуються лише обчислювальними властивостями процесора, оперативної пам'яті та розміром дискового простору.

Якщо ж додати до подібних систем можливості створення та реалізації сценаріїв атак на окремій мові програмування, то можна отримати універсальний інструмент для організації пен тестування системи.

Метою даної роботи. є розробка моделей та програмного комплексу, які надають можливість опису атак в умовах динамічно нестійкого зовнішнього середовища й забезпечують можливості автоматизованої розробки атак на цільові системи з метою оцінки їх безпеки.

Розв'язок даного завдання дозволить не тільки знизити час і вартість оцінки, але й підвищити точність виявлення вразливостей.

II. Рішення поставленої задачі

Віртуальні машини дають змогу швидко і без значних втрат розгорнути комп'ютерну мережу з бажаними характеристиками та з різним програмним забезпеченням, при чому це може бути як локальна мережа без доступу до основної ОС, так і мережа з доступом до інтернету.

Пентестінг охоплює безліч векторів: зовнішні (з інтернету, з використанням віддаленого доступу) і внутрішні (через бездротове корпоративне з'єднання, з використанням повноважень і знань гостя, рядового співробітника або співробітника IT департаменту). Головними етапами є: аналіз відкритих джерел, інструментальне сканування, аналіз/оцінка виявлених уразливостей і вироблення рекомендацій, підготовка звіту та аудит ІБ.

Тестовим стендом є віртуальна машина, зі встановленою операційною системою Windows 7 SP 1.

Засоби пошуку та експлуатації вразливостей зібрані у спеціальній операційній системі, призначеній для аналізу захищеності та проведення тестувань комп'ютерних систем на проникнення – ОС Kali Linux; як альтернатива можуть використовуватись: ОС BlackArch Linux; ОС Parrot Security OS; ОС BlackBox.

Для проведення аналізу використовується віртуальне середовище виконання Virtual Box, де встановлюються

віртуальні машини «жертви» та «нападника». В якості останнього використовується програмний комплекс на основі ОС Kali Linux із встановленим пакетом необхідного програмного забезпечення. Біля 300 open source security інструментів, організовані в наступні групи: “Information Gathering”, “Vulnerability Assessment”, “Exploitation Tools”, “Privilege Escalation”, “Maintaining Access”, “Reverse Engineering”, “RFID Tools”, “Stress Testing”, “Forensics”. В якості мови для реалізації типових сценаріїв атак використовується мова програмування Python.

Python дає можливість легко модифікувати кінцевий продукт, у даному випадку це розроблений програмний комплекс, для потреб конкретного користувача. Що, у свою чергу, дає можливість позбутися залежності від виробників, які пропонують додатки до своїх продуктів за суттєву доплату. Тобто, 1-2 кваліфікованих розробники, чи група студентів можуть реалізувати потрібний їм функціонал шляхом додавання модуля чи класу до існуючої програми.

Для повноцінного використання розробленого програмного комплексу для моделювання атак в мережі необхідно забезпечити наявність декількох компонентів.

По-перше, необхідно мати дистрибутив, образ віртуальної машини або ж встановлену операційну систему Kali Linux. Це дає можливість запустити програмний комплекс “Network Attack Trainer” без встановлення додаткових пакетів. Для нормальної роботи програми під операційними системами сімейства Windows необхідно встановити пакет Python та PIP (Python Package Index), що дозволить встановлювати і використовувати сторонні пакети Python.

Користувацький інтерфейс представлений двома вкладками (рис. 1, 2):

- Information gathering;
- Attack Execution.

На першій вкладці розташовані інструменти для виконання початкової фази мережевої атаки: модуль сканування мережі; модуль перевірки стану хоста; модуль сканування хоста.

Рис 1. Перша вкладка програмного інтерфейсу

Сканування мережі відбувається за допомогою модуля get_ips.py, що пінгує усі наявні хости у мережі, де знаходиться машина атакуючого, результати сканування виводяться у відповідне поле інтерфейсу програми.

Сканування хоста – це, перш за все збір інформації, що включає виявлення його вразливих місць та можливостей їх використання зловмисником за для своїх цілей чи матеріальної вигоди. Система має широкий набір утиліт для реалізації сканування.

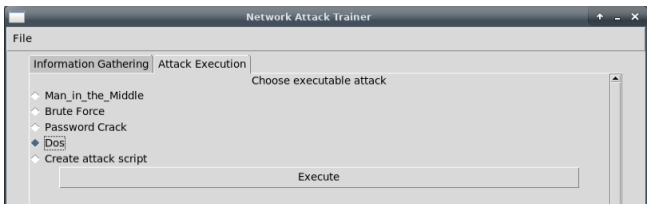


Рис 2. Друга вкладка програмного інтерфейсу

Головною метою роботи є розробка стенду, котрий би допомагав удосконалювати навички студентів. Його невід’ємною частиною є практичне написання коду мовою програмування Python, що є потужним інструментом для мережевого програмування, завдяки своїй простоті та можливості роботи з різними платформами.

Підпрограма атаки – скрипт, ґрунтується на даних сканування цільового хоста, що дає змогу визначити, ймовірно встановлену, на хості операційну систему, її версію, відкриті порти й сервіси запущені на них. Тип і деталі реалізації конкретної атаки, якщо вона не наявна в списку за замовчуванням, визначаються автором скрипта.

III. Висновки

Виявлення вразливостей є безперервним процесом і містить у собі виявлення вразливостей на етапі розробки та експлуатації системи. Пошуку вразливостей на етапі розробки систем приділяється значна увага, однак є недостатнім число засобів для моделювання подібних атак, особливо засобів, які можна використовувати в навчанні.

Розглянувши роботу комплексу та дослідивши найпоширеніші атаки можна зробити висновок, що будь-яка мережа має слабкі елементи та має недоліки, експлуатація яких, може призвести до втрати нею здатності зберігати цілісність, доступність та конфіденційність даних, що циркулюють в ній.

Звісно, застосувавши максимально можливі превентивні заходи, шанси на успішну реалізацію вразливості в мережі впадуть, але все врахувати фізично неможливо, тому розроблений програмний комплекс– “Network Attack Trainer” є чудовим плацдармом для імітації можливості здійснення найпоширеніших атак в проектованій мережі. Завдяки своїй гнучкості, вбудованому редактору коду і простоті використання, комплекс можна налаштувати під індивідуальні потреби.

Перелік Посилань

[1] V. Igure and R. Williams, “Taxonomies of attacks and vulnerabilities in computer systems”, Communications Surveys & Tutorials, IEEE, 10(1), pp.6-19. http://dx.doi.org/10.1109/COMST.2008.4483667.

[2] Rainer Bye, Stephan Schmidt, Katja Luther, and Sahin Albayrak. Application-level simulation for network security. In Proceedings of the First International Conference on Simulation Tools andTechniques for Communications, Networks and Systems, 2008.

[3] Jean-Vincent Loddo and Luca Saiu. Marionnet: A virtual network laboratory and simulation tool. In First International Conference on Simulation Tools and Techniques for Communications, Networks and Systems, 2008.

[4] Marcelo Picorelli Virtualization in software development and QA, 2006. WMWORLD 2006. http://www.vmworld.com.

[5] J.Mirkovic and P. Reiher A taxonomy of ddos attack and ddos defense mechanisms. ACM SIGCOMM Computer Communication Review, 34(2), 2004, pp.39-53.

Таксономія мережевих атак при проведенні пентест дослідження

Федюшин Олександр Іванович[1],

Лиско Віктор Іванович[2]

[1]*Харківський національний університет радіоелектроніки, пр. Науки, 14, м .Харків, UA-61166, Україна, oleksandr.fediushyn@nure.ua*

[2] *Харківський національний університет радіоелектроніки, пр. Науки, 14, м .Харків, UA-61166, Україна, viktor.lysko@nure.ua*

Анотація. *Проаналізовані типові таксономії мережевих атак з точки зору їх прикладного використання в задачах проведення аудиту безпеки інформаційних ресурсів організації за допомогою інструментів пентестингу. Запропонований багатовимірний підхід до їх класифікації, що базується на аналізі обставин проведення атаки, а також моделі порушника.*

Ключові слова: *таксономія, мережеві атаки, пентест, аудит безпеки, модель порушника.*

I. Вступ і Постановка Завдання

Кількість мережевих атак прямо пропорційна кількості потенційно небезпечного коду, що призводить до необхідності регулярного обстеження захищеності інформаційних ресурсів за допомогою засобів аудиту інформаційної безпеки. Метою надання послуг аудиту є визначення актуального стану захищеності інформаційних систем, що дає можливість подальшого усунення недоліків, вразливостей та поліпшення захищеності інформаційних систем від сучасних кіберзагроз.

Для повного розуміння потенційно вразливих систем та механіки можливих атак, доцільно проводити їх класифікацію. Власне класифікація атак – це їх розподіл по суміжних групах за визначеними критеріями. Класифікації, які також називаються таксономіями, є ієрархічним структуруванням поля знань в основні групи і підкатегорії.

Сьогодні в літературі можна знайти численні підходи до класифікації атак. Найчастіше використовуються одновимірні та ієрархічні розподіли, а багатовимірні – досить рідкісні.

Проаналізувавши їх можна прийти до висновку, що багато існуючих таксономій [1-5] розроблені для конкретних областей (наприклад, криптопротоколів або бездротових сенсорних мереж, WSN), або взагалі не застосовуються на практиці. Наприклад, Neumann представив таксономію, засновану на 26 видах атак, які були згруповані в дев'ять категорій, такі як апаратні зловживання, обходи та активні зловживання. Але через відсутність загального виміру, можливо, що інші класи атак могли бути виключені. Через це Lindquist і Johnson використали результат атаки для розташування атак і побудували три класи, а саме експозицію, DoS і помилковий вихід. Інший підхід використовується Кумаром (Kumar, 1995). Там класи таксономії будуються на основі особливостей сигнатур (існування, послідовність, частковий порядок, тривалість, інтервал). Хоча ця таксономія дозволяє виявляти відомі атаки, ідентифікація відповідної уразливості неможлива. Тому таксономія може бути використана для моніторингу безпеки, але не для системного аналізу. Інші автори [2] дають вичерпний огляд подальшої систематики на основі системи виявлення вторгнень (IDS). Численні інші спеціалізовані таксономії атаки доступні, наприклад, фокусуючись на DDoS (Mirkovic & Reiher, 2004), веб-атаках (Álvarez & Petrović, 2003) або досліджуючи конкретні атаки, такі як атаки відтворення [3-6].

Оскільки чіткої і однозначно визначеної класифікації не існує, у зв'язку з постійним розширенням векторів атак, то цілком логічно розробити власний метод таксономії атак на окремі групи і відповідні їм підгрупи, орієнтуючись на потреби спеціалістів, що проводять аудит із застосуванням методів та підходів пентестингу. Наведемо декілька фундаментальних причин, які були взяті до уваги при дослідженні проблемної області:

- незручність практичного застосування локальних класифікацій окремих компаній чи груп системних адміністраторів;
- вищезгадана локальність класифікацій, що виключає поширення в складених класифікаціях чи то професійних колах;
- суб'єктивність створення таксономій без коректної стандартизації їх декларування.

II. Рішення поставленої задачі

Метою надання послуг з аудиту безпеки є:

- аналіз ризиків, пов'язаних з можливістю здійснення загроз безпеки щодо ресурсів інформаційних систем;
- оцінка поточного рівня захищеності інформаційних систем;
- локалізація вузьких місць в системі захисту інформаційних систем;
- оцінка відповідності інформаційних систем існуючим стандартам в області інформаційної безпеки;
- вироблення рекомендацій щодо впровадження нових та підвищення ефективності існуючих механізмів безпеки інформаційних систем.

Сьогодні, опис мережевих атак за єдиним атрибутом не дозволить охопити усі характеристики процесів, з яких складається атака, тому варто звернути увагу на багатовимірну їх класифікацію. Як приклад, розглянемо класифікацію, запропоновану Howard, J. D. в [6].

Вищенаведена класифікація мережевих та комп'ютерних атак містить п'ять критеріїв систематизації: доступ, інструменти здійснення атаки, об'єкти атаки, зловмисник і результати атаки. Під зловмисником, у даному контексті, розуміється модель порушника, інструменти як шлях та спосіб здійснення атаки, доступ – слабкі місця реалізації. Сутність цього

розподілу – орієнтованість на саму атаку, а не на спосіб її реалізації.

Наведені класифікації розроблені для DoS атак, але вони можуть допомогти ідентифікувати атакуючого, його можливості, цілі, вразливості та кінцеві результати. Також, вони можуть викрити слабкість архітектури системи, можливості для застосування експлойтів, самі експлойти, механізми зв'язку, ступінь автоматизації, вплив на жертву.

Для повноцінної класифікації атаки, необхідно систематизувати множину можливих типів зловмисників – розробити модель порушника, згідно з НД ТЗІ 1.1 – 003- 99, модель порушника – абстрактний формалізований або неформалізований опис порушника. Існує багато розроблених класифікацій порушника за різними критеріями [7-9], але головними є два, це технічні можливості потенційного порушника і перспективна мета його дій.

Представлена на рис. 1 класифікація базується на декількох послідовних питаннях, що стосуються мережевої атаки: хто, де, як і що атакує.

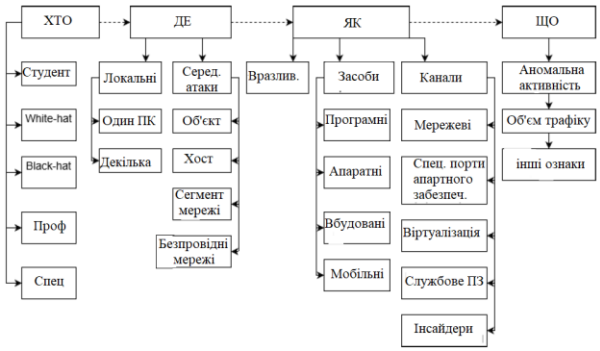


Рис 1. Класифікація за обставинами

Вищенаведена модель порушника дає чітку відповідь на перше запитання «хто?», щодо другого - «де?», то варто розуміти, що усі мережеві атаки мають свої географічні координати, незалежно від того, розподілені вони чи ні. Для визначення місця координації атаки доцільно використати розділення сутності другого питання на дві частини: локальні атаки і середовище атаки. Під локальною атакою мається на увазі атаки в локальних та закритих мережах, також інтернет речей, аналіз та спостереження за середовищем атаки дає можливість зрозуміти її природу, що є важливим аспектом при побудові ефективної політики безпеки та аналізі можливих загроз. Середовище атаки включає в себе:

– конкретні об’єкти (пристрої в мережі), які розглядаються як мета атаки; результатом є пошкодження чи знищення конкретного пристрою в мережі, яскравим прикладом є атака на комп’ютерну систему автомобіля Тесла[10];
– атаки на хости, зловмисник захоплює виділений комп’ютер, з подальшим захопленням мережі, чи використанням захопленого хоста як елементу ботнету;
– сегментна – атака на сегмент локальної обчислювальної мережі;
– в безпровідних мережах.

Основна проблема аналізу вразливостей мережі, це знайти усі способи і можливості реалізації атаки при відомій структурі та конфігурації досліджуваної комп’ютерної мережі. Цю проблему можна вирішити розділивши атаки за трьома критеріями: вразливості, які можна експлуатувати, засоби за допомогою яких реалізуються загрози та мережевий компонент, тобто наявність відкритих портів, тощо. Варто зосередити увагу на засобах, якими можуть користуватися потенційні порушники захищеного периметру:

– програмні засоби;
– апаратні;
– вбудовані програмні засоби;
– мобільні засоби.

За допомогою наведеного методу класифікації, адміністратор може дізнатися методи та цілі атакуючого і оцінити можливі наслідки протиправних дій.

III. Висновки

Класифікації, які також називаються таксономіями, є ієрархічним структуруванням поля знань в основні групи і підкатегорії. Виходячи з розподілу таксономії, слід детально розуміти характер різних класів. Застосовуючи їх систематично, можна виявити нові недоліки з захисті інформаційних ресурсів.

Таксономія повинна зосереджуватись на наступних властивостях:

– категорії взаємно виключаються, між категоріями немає перекриття;
– чіткі та недвозначні критерії класифікації;
– повторна класифікація повинна давати однакові результати;
– повинні бути зрозумілі та корисні;
– дотримуватися встановленої термінології.

Істотною перевагою такого підходу до класифікації мережевих атак є його простота та надійність, навіть недосвідчений системний адміністратор чи адміністратор безпеки зможе легко упорядкувати пул атак, з якими йому доводиться працювати. Моделювання подібних атак як упорядкованої множини загроз здійснюється значно простіше, оскільки структура моделі прямо залежить від структури атаки. Зокрема, такий підхід дає можливість використовувати невеликі, але змістовні моделі, які можна створити за допомогою програмних комплексів.

Перелік Посилань

[1] V. Igure and R. Williams, “Taxonomies of attacks and vulnerabilities in computer systems”, Communications Surveys & Tutorials, IEEE, 10(1), pp.6-19. http://dx.doi.org/10.1109/COMST.2008.4483667.
[2] F. Swiderski, W. Snyder, Threat modeling, Microsoft Press Redmond,WA, USA, 2004.
[3] B. Ng, A. Kankanhalli, Y. Xu, Studying users’ computer security behavior: A health belief perspective, Decision Support Systems 46, 2009, pp.815–825.
[4] J.Mirkovic and P. Reiher A taxonomy of ddos attack and ddos defense mechanisms. ACM SIGCOMM Computer Communication Review, 34(2), 2004, pp.39-53.
[5] G. Alvarez, S. Petrovic, A new taxonomy of web attacks suitable for efficient encoding, Computers and Security 22 (5), 2003, pp.435–449.
[6] J. D. Howard and T. A. Longstaff, “A common language for computer security incidents”, Sandia National Labs., Albuquerque, NM (US); Sandia National Labs., Livermore, CA (US) (No. SAND98-8667).
[7] Web security threat classification v2.0, Tech. rep., Web Application Security Consortium (2010).
[8] K. Hoffman, D. Zage, C. Nita-Rotaru, A survey of attack and defense techniques for reputation systems, ACM Comput. Surv. 42 (1), 2009, pp. 1–31.
[9] Tesla is Hacked [Електронний ресурс] / HackerJournal - Режим доступу: https://xakep.ru/2017/07/28/tesla-model-x-hack/

Аналіз забезпечення конфіденційності інформації в сучасних мессенджерах

Арчакова Альона Ігорівна
Харьковский Национальный Университет Радиоэлектроники, Пр-т Науки 14, Харьков 61166, Украина, alona.archakova@nure.ua

Сєвєрінов Олександр Васильович
Харьковский Национальный Университет Радиоэлектроники, Пр-т Науки 14, Харьков 61166, Украина, oleksandr.sievierinov@nure.ua

Анотація. *У доповіді розглянуті популярні серед користувачів України додатки для швидкого обміну повідомленнями та їх безпека. Особливу увагу було приділено методам забезпечення конфіденційности інформації, протоколу шифрування end-to-end encryption та розглянута схема його роботи на прикладі одного з мессенджерів., були перелічені деякі переваги та недоліки. Проведений аналіз мессенджерів на існуючі заходи захисту даних користувачів, таких як секретні чати, двохфакторна автентифікація та інші. Проведене дослідження показало, що однією з основних проблем безпеки мессенджерів є сервери,на яких вони розгорнуті. Тому одним із кращих рішень є децентралізація та підтримка наскрізного шифрування за замовчанням у кожному мессенджері*

Ключові слова: *end-to-end encryption, E2EE, мессенджери, Viber, WhatsApp, Telegram.*

I. Вступ

На даний час все більшу популярність набувають додатки для швидкого обміну повідомленнями - мессенджери. Підтвердженням тому є також їх різноманіття. Більшість користувачів вибирають мессенджер з точки зору зручності використання. І, на жаль, над безпекою мессенджера замислюються менш за все. В Україні найпопулярнішими мессенджерами є Viber, Facebook Messenger, WhatsApp і Telegram.

Не дивлячись на всі засоби безпеки, які використовуються мессенджерам для захисту конфіденційних даних, більшість з них не можуть забезпечити необхідний рівень конфіденційності.

У статті [1] продемонстровано, як зламати секретний чат Telegram, і важливим було те, що у користувача не відобразився паралельний активний сеанс з іншого пристрою.

Також у роботі [2] група дослідників змогла отримати доступ до акаунту WhatsApp і навіть змінювати зміст відправлених повідомлень.

Також немає ні якої гарантії, що конфіденційну інформація користувачів не буде збирати власник програмного забезпечення.

У мессенджерів, таких як Viber та WhatsApp, використовується кодова база Signal засновник протоколу end-to-end encryption, але на сайтах даних додатків є інформація про те, що уся інформація та повідомлення користувачів проходять через їх сервера, при тому, що це суперечить основної ідеї цього протоколу.

Таким чином, актуальним питанням є проведення аналізу засобів безпеки у сучасних популярних мессенджерах, а саме методів забезпечення конфіденційності інформації.

II. Забезпечення конфіденційності в сучасних мессенджерах

В найпопулярніших мессенджерах реалізована можливості шифрування повідомлень, спілкування в секретному чаті, верифікації користувачів. Важливими аспектами безпеки є конфіденційності листування та місце зберігаються повідомлення, передані файли - на сервері або на самому пристрої.

У якості шифрування велика частина додатків використовує наскрізне шифрування. Наскрізне шифрування (E2EE - end-to-end encryption) – спосіб передачі даних, в якому тільки користувачі, які беруть участь в спілкуванні, мають доступ до повідомлень. Таким чином, використання наскрізного шифрування не дозволяє отримати доступ до криптографічних ключів з боку третіх осіб. Це означає, що призначена для користувача інформація стає недоступною навіть серверів, передає дані. Шифрування і дешифрування відбувається на кінцевих пристроях користувачів. Крім того, дані залишаються зашифрованими, поки не будуть доставлені до місця призначення. Але така схема не дає повної безпеки, так як використовується асиметричне шифрування, яке вразливе: перш ніж зашифрувати якісь дані, їх необхідно передати по мережі, отримати ключ користувача, і при цьому обмін ключів йде через сервер. При такому шифруванні виходить, що головна вразливість - сервер.

У даного шифрування існують вразливості, такі як:

1) атака “Людина посередині”. Для запобігання атаки MITM деякі додатки використовують подвійну автентифікацію.

2) Безпека кінцевих точок, де пристрій користувача може буде вкрадений або зламаний.

Із важливих безпечних критеріїв кожного мессенджера можна виділити:

– централізованість, коли уся інформація користувача проходе через сервер та може на ньому лишатися (у зашифрованому виді);

– наявність end-to-end encryption. У деяких мессенджери ця настройка йде за умовчанням, у деяких її необхідно підключати самостійно;

– повідомлення про необхідність звірки відбитків end-to-end encryption. При старті E2EE-чатів деякі месенджери пропонують перевірити відбитки співрозмовників, інші не пропонують це відкрито. Але не всі месенджери мають функцію перевірки відбитків ключів.

Розглянемо докладніше засоби безпеки у популярних мессенджерах.

У Viber наскрізне шифрування використовується за замовчанням. Передача даних носить централізований

характер. У ньому є такі функції, як "Секретний чат", який можна запустити вручну. Особливостями секретного чату є повідомлення, які самознищуються, повідомлення про зроблені скріншоти і захист від пересилання повідомлень. При цьому, наскрізне шифрування не використовується, якщо ви працюєте з застарілою версією Viber.

Facebook Messenger хоч і користується великою популярністю, але в рейтингу з безпеки серед інших месенджерів виявився далеко в кінці списку. Побудований на основі відкритого протоколу MQTTУ. Централізований. В додатку підтримується наскрізне шифрування, але не за замовчуванням. Для включення шифрування повідомлень потрібно активувати "Секретний чат". Тобто звичайні чати незашифровані і вся інформація з листувань потрапляє на сервер, отримавши доступ до якого зловмисник може дізнатися про користувача абсолютно все. Функції повідомлень про необхідність звірки відбитків ключів не має.

WhatsApp використовує наскрізне шифрування за замовчанням, включно у секретних і групових чатах. WhatsApp не зберігає повідомлення на своїх серверах. Замість цього повідомлення зберігаються на телефоні, а потім на серверах, на яких користувач створює резервні копії телефону. Наприклад, якщо ви використовуєте iPhone, всі ваші повідомлення WhatsApp зберігаються в iCloud, якщо ви використовуєте його в якості резервної копії. Принцип наскрізного шифрування у мессенджері WhatsApp представлений на рис. 1

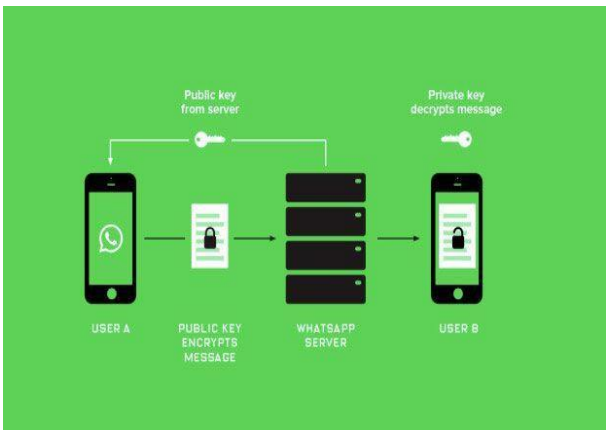


Рисунок 1 – Принцип наскрізного шифрування у мессенджері WhatsApp

1. Користувач А (точніше, його пристрій) запитує у сервера компанії, яка володіє програмою-месенджером, відкритий ключ.

2. Відбувається відправлення повідомлення від А до В, заздалегідь закодованого цим ключем.

3. Пристрій користувача виконує після отримання розшифровку повідомлення.

Telegram побудован на технології протоколу MTProto. Цей протокол був розроблений спеціально для Telegram і в основі протоколу лежить оригінальна комбінація симетричного алгоритму шифрування AES (в режимі IGE), протокол Діффі-Хелмана для обміну 2048-бітними RSA-ключами між двома пристроями та ряд геш-функцій. Вихідний код протоколу не є цілком доступним користувачу. Мессенджер є централізованим. Також Telegram використовує наскрізне шифрування виключно в Секретних чатах, які необхідно включати вручну. Функції повідомлень про необхідність звірки відбитків ключів не має. Повідомлення, фотографії, відео та документи зашифровані і зберігаються на серверах Telegram (за винятком повідомлень Секретного чату).

В сучасних месенджерах заявлена підтримка наскрізного шифрування, але у деяких вона не підтримується за замовчанням, що є вразливістю. Також однією с важливих проблем можна вважати сервери мессенджерів, через які зловмисник може перехватити необхідну йому інформацію. Одним із варіантів рішення проблеми є децентралізація. Також в якості методу захисту можна запропонувати розробникам увести обов'язкову функцію звірки ключів end-to-end encryption при старті обміну повідомленнями.

III. Висновки

Таким чином, проведений аналіз показав, що незважаючи на методи захисту інформації користувачів в сучасних мессенджерах, які популярні в Україні, існує небезпека витоку конфіденційних даних. Це обумовлено у першу чергу централізацією мессенджерів та відсутністю наскрізного шифрування у додатку за замовчанням.

На цей час найбільш захищеним мессенджером в України за показниками заходів безпеки, які включені за замовчанням, можна вважати Telegram. Другим за безпекою іде WhatsApp, якщо не враховувати збір великої кількості метаданих про своїх користувачів.

Список літератури

[1] Anglano C., Canonico M., Guazzone M. Forensic analysis of telegram messenger on android smartphones //Digital Investigation. – 2017. – Т. 23. – С. 31-49.

[2] Пользуетесь WhatsApp? Кажется, у вас проблемы // [Електроний ресурс] https://rg.ru/amp/2018/08/09/polzuetes-whatsapp-kazhetsia-u-vas-problemy.html Режим доступу 12.03.19

[3] N. Unger, S. Dechand, J. Bonneau, S. Fahl, H. Perl, I. Goldberg, and M. Smith, "Sok: Secure messaging," in S&P, 2015.

[4] N. Kobeissi, K. Bhargavan, and B. Blanchet, "Automated verification for secure messaging protocols and their implementations: A symbolic and computational approach," in EuroS&P, 2017.

ГНУЧКІ ІНТЕГРОВАНІ СИСТЕМИ ТА РОБОТОТЕХНІКА

Исследование влияние объёма нагретой зоны и интенсивности системы поверхностного охлаждения на максимальный перегрев радиоэлектронного аппарата

Синотин Анатолий Мефодиевич

Харківський Національний Університет Радіоелектроніки, просп. Науки 14, Харків, індекс 61166, Україна, Україна,anatolii.sinotin@nure.ua

Колесникова Татьяна Анатольевна

Харківський Національний Університет Радіоелектроніки, просп. Науки 14, Харків, індекс 61166, Україна, tatayna.kolesnykova@nure.ua

Стародубцев Николай Григорьевич

Харківський Національний Університет Радіоелектроніки, просп. Науки 14, Харків, індекс 61166, Україна nikolaj.starodubcev@nure.ua

Аннотация *В работе приведены результаты исследований влияния на максимальный перегрев аппарата интенсивности поверхностного охлаждения и величины объёма нагретой зоны*

Ключові слова: *візуальне керування, обробка зображень, системи комп'ютерного зору, оптимізація.*

I. Введение

При проектировании, необходимо выбирать элементную базу с наименьшей потребляемой мощностью и материалы с высокой температуростойкостью.

В случае необходимости использования отдельных элементов с малой допустимой температурой перегрева ϑ_o целесообразно выделять эти элементы в самостоятельную группу, чтобы не усложнять обеспечение заданного теплового режима конструкции прибора в целом и располагать подальше от центра, по возможности поближе к корпусу. Это замечание очень важно учитывать при выборе элементной базы электрической схемы, так как после задания конструктору электрической схемы он лишен возможности влиять на фактор рассеиваемой мощности и температуростойкости элементов схемы.

II. Основная часть

Для создания надежных и компактных радиоэлектронных аппаратов, наряду с разработкой оптимальных электрических схем, необходимо учитывать допускаемый температурный режим используемых элементов в разрабатываемой конструкции радиоэлектронного аппарата.

Максимальный перегрев радиоэлектронного прибора во многом зависит от его формы и его объёма. Влияние расположения тепловыделяющих элементов можно выразить через так называемый начальный параметр F_0

$$F_0 = \frac{P_0}{\vartheta_0} \cdot \frac{1}{4\lambda \cdot \sqrt[3]{V}} \cdot \frac{0{,}82A_0^3}{3\mu_0^2}; \qquad (1)$$

$$Bi_0 = \frac{K_0}{\lambda_0} \cdot \frac{1}{2} \cdot \sqrt[3]{V}, \qquad (2)$$

где P_o - суммарная мощность источников тепла, Вт;

ϑ_o - максимальный допустимый перегрев прибора, град; λ_o - эффективная теплопроводность при отсутствии теплостоков при газовом заполнителе, Вт/м.град; V - объём нагретой зоны, м^3; K_o - средний поверхностный коэффициент теплопередачи Вт/м^2 • град; A_o, μ_o - амплитуда и собственные значения характеристического уравнения при B_{I_o};

Начальный параметр F_0 характеризует тепловой режим следующей конструкции РЭА:

- нагретая зона имеет форму куба $\left(\xi_{X_o} = \xi_{Y_o} = \xi_{Z_o} = 1\right)$,

где $\xi_{l_o} = 2l_{mii} / 2l_i, i = X, Y, Z;$;

анизотропность по теплопроводности в объёме и теплообмену на поверхностях отсутствует $\left(\lambda_X = \lambda_Y = \lambda_Z = \lambda_o; K_X = K_Y = K_Z = K_o\right)$

- кондуктивные теплостоки отсутствуют $\left(\lambda_{max} = \lambda_o\right)$;

- мощность источников тепла распределена равномерно.

Начальный параметр F_0 можно минимизировать за счет уменьшения отношения P_{o/ϑ_o}, увеличения объема нагретой зоны V и интенсивности поверхностного теплообмена K_0.

Рассмотрим каждый фактор в отдельности.

Уменьшение отношения P_{o/ϑ_o} вызывает определенные требования к разработке электрической схемы аппарата.

Проведенные экспериментальные исследования показывают, что для одноблочных кубических конструкций аппаратов с размером $\sqrt[3]{v} \geq 0{,}5$ м минимизация начального параметра F_0 за счет увеличения объема нагретой зоны (плотности

размещения элементов) и перехода к более интенсивной системе поверхностного охлаждения $K_0 = \infty$ становится практически невозможной.

Наоборот, для конструкций размером $\sqrt[3]{V} \le 0{,}5$ м увеличение объема и рост K_0 приводят к уменьшению F_0 в три раза при $\sqrt[3]{V} = 0{,}1$м и на 50% при $\sqrt[3]{V} = 0{,}3$ м за счет изменения K_0 от 4 Вт/м^2-град до ∞. Практически уже при $K_o \ge 100$ Вт/м^2 град. наступает предельный случай, т. е. для аппаратов с газовым заполнением (с малой эффективной теплопроводностью $\lambda_o = 0{,}2$ Вт/м.град) нецелесообразно использовать жидкостные и другие более эффективные системы поверхностного охлаждения.

Предельная минимизация F_0 может быть осуществлена за счет применения вынужденного конвективного воздушного охлаждения (α = 10—100 Вт/м.град) [3].

Коэффициент теплопередачи

$$K_o = \frac{K^1 S_k / S}{1 + K^1 S_k / \alpha S}, \qquad (3)$$

где K_0 — коэффициент теплообмена через газовую прослойку от нагретой зоны к кожуху, Вт/м^2. град; α — коэффициент теплообмена между поверхностью кожуха и окружающей средой, Вт/м^2. град;

$S_к$, S - площади поверхностей кожуха и нагретой зоны, м^2.

Анализ выражения (4) и значений коэффициентов теплообмена для различных типов систем охлаждения [3] позволяет наметить два пути увеличения K_0 для минимизации параметра F_0 и синтеза конструкции с заданным тепловым режимом по максимальному перегреву. Первый путь — чисто конструктивный при небольших значениях K_0, т.е .для радиоэлектронных аппаратов, предназначенных функционировать в условиях естественного охлаждения воздухом.

Расчеты конструкций приборов [2] показали, что имеет место равенство проводимостей между нагретой зоной и кожухом, а также с окружающей средой:

$$K^1 \cdot S \approx \alpha \cdot S_K \qquad (4)$$

После подстановки (5) в (4) получим $K_O = \alpha \cdot S_K$ т.е. применение кожуха практически в 2 раза снижает эффективность поверхностного охлаждения.

При совмещении кожуха аппарата с нагретой зоной $(S_к = S)$, а $K^1 \to \infty$ и Ko = K.

Таким образом, чисто конструктивным путем, совмещая кожух прибора с нагретой зоной, можно увеличить K_0 в два раза.

При этом следует обеспечить хороший тепловой контакт между нагретой зоной и кожухом, например, применяя высокотеплопроводные пасты в стыках между платами (шасси), гранями кожуха и т.д. Рассмотренный метод наиболее эффективен тогда, когда требуется сохранить герметичность (пылезащищённость) аппаратуры.

Можно пойти и другим конструктивным путем: уменьшить влияние кожуха на интенсивность теплостоков за счет нарушения герметичности и обеспечения непосредственного контакта нагретой зоны с охлаждающим воздухом через перфорационные (жалюзи) отверстия. Тогда выражение для K_0 в первом приближении примет вид

$$K_0 = K^{\bullet}_0 (1 + S_{пер} / S_{k)}), \qquad (5)$$

где $S_{пер.}$— площадь перфорационных отверстий, м^2; K_o - определяется выражением (5). при $S_{пер.} = 0$. Отношение $S_{пер.} / S_K$ называется коэффициентом перфорации. Более строгий учет перфорации приведен в работе [3]. Практически уже при $S_{пер.} / S_K =$ 0,5 - 0,6 значение K_0 близко к K^*_o т. е. достигается предельный эффект минимизации F_0.

Рассмотренные конструктивные методы не позволяют существенно изменять коэффициент теплопередачи К. Для существенного изменения интенсивности теплообмена на поверхности нагретой зоны необходим переход от естественного к вынужденному поверхностному охлаждению путем продувки воздуха, т.е., требуются дополнительные изменения в конструкции аппарата. При этом согласно равенству (2) необходимо либо одновременно увеличить интенсивность теплообмена между нагретой зоной и кожухом (K^1), кожухом и окружающей средой α, либо предварительно совместить кожух с нагретой зоной $K^1 \to \infty$ В противном случае рост K_0 будет незначительным, несмотря на существенное увеличение α. Таким образом, во втором пути минимизации за счет увеличения K_0 предусматривается переход к новой системе охлаждения с предварительным совмещением кожуха с нагретой зоной, особенно в конструкциях с плотным монтажом.

III. Выводы

Практически изменение объема в 8 раз (на участке $\sqrt[3]{V} < 0{,}5$ м) приводит к уменьшению F_0 в три раза при K_0 = 4 Вт/м.град и в два раза при $K_0 = \infty$. Такое изменение объема может быть осуществлено за счет перехода от монтажа высокой плотности $(\eta_м \ge 1)$ к монтажу малой плотности $(\eta_м \approx 1)$.

Увеличение объема нагретой зоны за счет уменьшения плотности размещения элементов находится в противоречии с требованием минимизации размеров конструкции, поэтому может быть применено только в том случае, когда отсутствуют жесткие ограничения на размеры конструкции в техническом задании.

Список использованных источников

[1] Синотин А.М.Исследование точности метода многих точек для определения теплопроводности анизотропных материалов. // Автоматизированные системы управления и приборы автоматики. – 2004. – Вып.129. – С. 37 – 40.

[2] Майко И. М., Детинов Ю. М., Синотин А. М. О теплофизическом конструировании одноблочных радиоэлектронных аппаратов с заданным тепловым режимом.— Вопросы радиоэлектроники. Сер. ТРТО. 1974. вып. 1, С. 80—87.

[3] Дульнев Г. Н., Тарновский Н. Н. Тепловые режимы электронной аппаратуры.— Л.: Энергия, 1971.248 с.

[4] Лыков А.В. Теория теплопроводности. Госэнергоиздат. 1952. 392 с.

[5] Майко И.М., Синотнн А.М., Детинов Ю.М. О теплофизическом конструировании одноблочных радиоэлектронных аппаратов с заданным тепловым режимом.// Вопросы радиоэлектроники. ТРТО. 1974. № 1. С.14 -1

Model consistency of assembly elements in the modular type robot's constructions

Funkendorf Anastasiia
Yevsieiev Vladyslav

Kharkiv National University of Radio Electronics, 14 Nauky Ave, Kharkiv UA-61166, Ukraine, e-mail

The problem solution of the consistency functional elements checking in the modular type robot's constructions at the stage of their design is proposed. Developed corresponding mathematical models are presented.

Keywords: *robot, modular construction, element coherence, mathematical model.*

I. Introduction And Problem Statement

Modern designs of modular robots are becoming more widespread in various fields of human activity. This is due to their advantages in production, operation, maintenance and utilization, as well as much more flexible solutions than in the classical approaches to design.

At the design stages of these structures, the main problem that does not allow to realize the full automation of this process, is to check the coherence of the functional modules in the holistic device construction. This is a complex scientific and technical task of the present, which requires the development of new approaches and appropriate mathematical support for its solution.

II. Problem solution and Results

The structure of the robot's modular design of any destination can be represented by six functional modules, each of which can have a varied technical solution: manipulation module *Mnp* ; enclosure module *Bd* ; control module *Cnt* ; moving module *Mv* ; sensor module *Sen* ; module for communication with a people *Con* [1], [2].

Interconnections between the specified modules can be characterized by the parameters of mechanical P_M and electrical connections P_E . Then, the coherence structural elements of the design in holistic device is provided by matching the one module parameters to the another parameters module. Such a theory of relativity can be expressed mathematically in a generalized form, as:

$$R_{i,j} = \begin{cases} P_{Mi}^{j} : P_{Mj}^{i}; \\ P_{Ei}^{j} : P_{Ej}^{i}. \end{cases}, \qquad (1)$$

where i – the module for which the connection is made; j – the module with which it's being connected.

In case of particular compound parameters are coincidence, this index takes the value 1. If the inconsistency is due to one of the modules, or both, 0. In terms of programming, this approach can easily be implemented with boolean values and logical comparison operators [3], but can only function if a corresponding database exists. It should include all connections that can be used for individual function modules.

In accordance with the accepted structuring of specified type robots and the classification of modules, the mathematical model of consistency will have the form:

$$R = \begin{cases} P_{MMnp}^{Sen} : P_{MSen}^{Man}, P_{MMnp}^{Bd} : P_{MBd}^{Mnp}, P_{MMnp}^{Con} : P_{MCon}^{Mnp}, \\ P_{MMnp}^{Mv} : P_{MMv}^{Mnp}, P_{MMnp}^{Cnt} : P_{MCnt}^{Mnp}; \\ P_{MSen}^{Bd} : P_{MBd}^{Sen}, P_{MSen}^{Con} : P_{MCon}^{Sen}, P_{MSen}^{Mv} : P_{MMv}^{Sen}, \\ P_{MSen}^{Cnt} : P_{MCnt}^{Sen}; \\ P_{MBd}^{Con} : P_{MCon}^{Bd}, P_{MBd}^{Mv} : P_{MMv}^{Bd}, P_{MBd}^{Cnt} : P_{MCnt}^{Bd}; \\ P_{MCon}^{Mv} : P_{MMv}^{Con}, P_{MCon}^{Cnt} : P_{MCnt}^{Con}; \\ P_{MMv}^{Cnt} : P_{MCnt}^{Mv}. \\ P_{EMnp}^{Sen} : P_{ESen}^{Man}, P_{EMnp}^{Bd} : P_{EBd}^{Mnp}, P_{EMnp}^{Con} : P_{ECon}^{Mnp}, \\ P_{EMnp}^{Mv} : P_{EMv}^{Mnp}, P_{EMnp}^{Cnt} : P_{ECnt}^{Mnp}; \\ P_{ESen}^{Bd} : P_{EBd}^{Sen}, P_{ESen}^{Con} : P_{ECon}^{Sen}, P_{ESen}^{Mv} : P_{EMv}^{Sen}, \\ P_{ESen}^{Cnt} : P_{ECnt}^{Sen}; \\ P_{EBd}^{Con} : P_{ECon}^{Bd}, P_{EBd}^{Mv} : P_{EMv}^{Bd}, P_{EBd}^{Cnt} : P_{ECnt}^{Bd}; \\ P_{ECon}^{Mv} : P_{EMv}^{Con}, P_{ECon}^{Cnt} : P_{ECnt}^{Con}; \\ P_{EMv}^{Cnt} : P_{ECnt}^{Mv}. \end{cases} \qquad (2)$$

III. Conclusions

The presented models and offered solutions allow to solve a problem of automation design modular robot's, and also to checked the coherence of functional modules in the holistic construction. It can also facilitate the further construction of the connections table, which is a mandatory and integral part of the technical documentation necessary to provide an automated assembly process of modular type robot's constructions.

References

[1] Nevliudov, V. Yevsieiev, E. Razumov-Friesyuk, A. Funkendorf "Formalization models for solving automation problems of designing robots with modular structure", Systems of control, navigation and communication, 2017, pp. 36-38.

[2] I. Nevlyudov, A. Funkendorf, K. Khrustalev "Mathematical model technological process of robot's assembly with a modular type construction", Scientific notes of Ternopol State University named after Vernadsky. Series: Technical Sciences, vol. 29, 2018, pp. 197-203.

[3] S. Sahay Object-Oriented Programming with C++. Oxford University Press, 2006, 500 p.

Інтернет роботизованих речей: огляд концепції

Цимбал Олександр Михайлович

Харківський Національний Університет Радіоелектроніки, прос. Науки 14, Харків, індекс 61166, Україна, oleksandr.tsymbal@nure.ua

Бронніков Артем Ігорович

Харківський Національний Університет Радіоелектроніки, прос. Науки 14, Харків, індекс 61166, Україна, artem.bronnikov@nure.ua

Анотація. *В роботі проведено аналіз концепції IoRT (Інтернету Роботизованих Речей), а саме розвитку існуючих поглядів на розробку систем керування роботами, ефективності впровадження в існуючі гнучкі виробничі системи, інтеграції систем підтримки прийняття рішень.*

Ключові слова: *автоматизовані системи керування виробництвом, IoT, робототехніка, штучний інтелект.*

I. Вступ

У епоху впровадження концепції Industry 4.0 і цифрової трансформації виробництва, виробничі системи є ринком, на якому реалізуються більшість проектів промислових IT (IIoT). IoT є ключовим компонентом розвитку промисловості у всьому світі, який включає Industry 4.0 та промисловий Інтернет[1].

Інтернет робототехнічних речей – це нове бачення, яке об'єднує широке застосування сенсорів та робототехнічних об'єктів. Поєднання цих технологій та технологій Internet of Things сприятиме розвитку як сучасного Інтернету речей, так і існуючих робототехнічних систем, що дозволить створити нові потенційно перспективні виробничі сервіси.

II. Основні завдання концепції Robotic IoT

Початкова ідея IoT-робототехніки може простежуватися з розподілених, гетерогенних парадигм управління роботами, зокрема мережних та хмарних робототехнічних систем. Сам термін «Інтернет робототехнічних речей» (IoRT) був придуманий для позначення концепції, відповідно до якої дані датчиків з різних джерел отримуються, обробляються з використанням локальних і розподілених даних , а потім використовуються для керування та маніпулювання об'єктами у фізичному світі. Системи IoRT виникають завдяки широкому використанню сенсорних систем та технологій аналізу даних, із кінцевою метою у кращому виконанні завдань промислового та іншого призначення.

Хмарні обчислення та IoT є технологіями, які, хоча є не пов'язані напряму з робототехнікою, забезпечують створення розподілених робототехнічних систем. Технології IoT мають будуватися на трьох принципових елементах: широкому застосуванні датчиків у об’єктах роботизації та робочому просторі; на інтелектуальних підключених об'єктах, що використовують зв'язок між мехатронними системами; на засобах забезпечення аналітики даних та семантичних технологіях, що трансформують неоднорідні дані датчиків. Схематично це показано на рисунку 1.

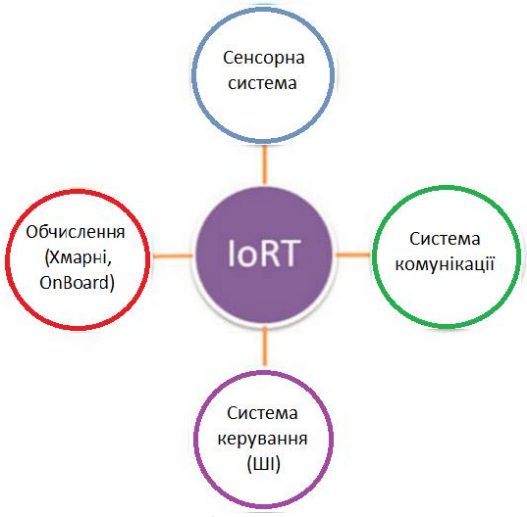


Рисунок 1 – Структура IoRT

В структурі IoRT хмарні обчислення забезпечують мережевий доступ за запитами до віртуалізованих апаратних ресурсів (обробки, зберігання) або послуг вищого рівня. Хмарна інфраструктура використається засобами IoT для розгортання масштабованих послуг платформи IoT, які регулюють доступ до даних датчиків (необроблених, оброблених або змішаних). Обробка потоків даних, що генеруються пристроями IoT в декількох централізованих центрах обробки даних, однак може виявитися певною проблемою системи реального часу, якщо виникатимуть затримки обробки інформації.

Хмарна парадигма була прийнята спільнотою робототехніки як засіб розвантаження ресурсомістких завдань, для обміну даними і знаннями між роботами, для забезпечення функцій реконфігурації роботів.

Технології використання датчиків і засобів аналітики даних з IoT можуть надавати роботам більш широкі можливості у порівнянні з бортовими системами, з точки зору простору, часу та типу інформації. Навпаки, розміщення вбудованих датчиків дозволяє розміщувати їх гнучко і динамічно, забезпечувати складні стратегії активного дослідження робочого простору.

Ключовим викликом IoRT є просторова і часова розподіленість. Перш за все необхідно запровадити методи отримання таких даних. В частині робіт [2] пропонується використати локальні бази даних для кожного об'єкта. При цьому дані організовуються в просторовій ієрархії, наприклад, об'єкт має позицію відносно робота, робот позиціонується в кімнаті і т.п. Інші автори [3] пропонують, щоб роботи надсилали конкретні запити на спостереження до розподілених

серверів, наприклад, щодо областей та об'єктів робочого простору.

Сенсорні системи також можуть бути організовані у розподілений спосіб. Наприклад, розподілені камери допомагають роботові знаходити зарядну станцію у великому середовищі.

III. Штучний інтелект в Robotic IoT

Ключовим компонентом здатності роботів сприймати інформацію є отримання знань про їх власне розташування із можливістю побудови або оновлення моделей робочого простору. Незважаючи на великий прогрес у цій галузі, самостійна локалізація все ще може бути складним процесом для переповненого або глобальному простору. В цьому сенсі використання GPS-датчиків обмежується особливостями самого стандарту (у варіанті цивільних систем) та проблемами із GPS у внутрішніх середовищах. При цьому використання IoT може суттєво покращити забезпечення формування інформації про «світ» робота.

Здатність рухатися є однією з фундаментальних характеристик мобільних робототехнічних систем. Наявність IoT забезпечує мобільні роботи додатковою інформацією про робочий простір, наприклад контролювати стан автоматичних дверей та ліфтів, положення інших мобільних об’єктів та устаткування.

Послуги платформи IoT можуть полегшити використання робототехніки в таких областях, як логістика постачання об’єктів, землеробство і моніторинг навколишнього середовища, виконання пошукових і рятувальних робіт, коли інфраструктура зв'язку може бути відсутня або пошкоджена, мобільним роботам може знадобитися взаємна комунікація на рівні спеціальних мереж і використання один одного в якості вузлів пересилання інформації.

Маніпуляційні роботи також є ключовим елементом технології IoT. Промислові роботи, або мобільні пристрої із маніпуляторами на борту роботи можуть захоплювати, піднімати, утримувати та переміщати об'єкти, застосовуючи систему відповідних датчиків.

Додаткова якість використання IoT у робототехніці полягає в отриманні особливостей об'єктів, включаючи ті, які не можна спостерігати за допомогою датчиків, але впливають на процедуру захоплення, зокрема на розподіл маси, наприклад, у заповненій чашці робота-асистента.

Автономність рішень роботі відноситься до здатності системи визначати найкращий хід дій для виконання своїх цілей і завдань. При цьому актуальними стають методи планування рухів на основі систем штучного інтелекту, використання прогностичних моделей навколишнього середовища та можливих дій роботів в них. Якість планів критично залежить від якості цих моделей та оцінки початкового стану. У цьому відношенні покращення ситуації може бути забезпечене застосуванням IoT. Наприклад, робот-пилосос може отримувати дані про перешкоди у приміщенні і адаптувати план своїх дій. IoT також розширює сферу автономії при прийнятті рішень, надаючи доступ до більшої кількості суб'єктів типу керованих ліфтів та дверей. Рішення полягає в тому, щоб зробити планування адаптивним і виконуваним у реальному часі.

Ще однією цікавою рисою використання IoT в роботехніці є здатність робота взаємодіяти фізично, когнітивно та соціально з користувачами, операторами або іншими системами. Технології IoRT можуть сприяти взаємодії людини з роботом на функціональних (командних і програмних) і соціальних рівнях, а також як засоби для телевзаємодії.

Функціональні можливості датчиків IoT можуть зробити взаємодію людини з роботом більш надійною. При цьому бажаним рівнем може бути використання природної мови спілкування, особливо для непрофесійних користувачів. Хоча це є основою для нечіткостей та невизначеностей. Іншим способом спілкування залишається мова жестів, наприклад, для вказання на об'єкти. В цьому випадку перспективним шляхом є поєднання систем комп’ютерного зору з датчиками на одязі оперативного персоналу підприємства.

Реакції оперативного персоналу у вигляді жестів, висловлення голосу або міміки обличчя можуть бути використані для оцінки емоційного стану користувачів змусити робота реагувати на них. Інтеграція з сенсорами IoT на тілі або одязі оператора може поліпшити оцінку рішення шляхом вимірювання фізіологічних сигналів частоти серцевих скорочень, провідності шкіри. Ці оцінки можіть бути основою для адаптації стратегії взаємодії робота, наприклад, в контексті розробки робота–асистента для соціальної або медичної сфери.

Пізнавальні здібності роботів на основі використання IoT суттєво збільшаться, якщо роботи зможуть розуміти взаємозв'язок між собою і навколишнім середовищем, оцінювати можливий вплив і наслідки своїх дій. Все це основою для таких аспектів пізнання, як мультимодальне сприйняття і соціальний інтелект.

IV. Висновки

Актуальною проблемою сучасних гнучких інтегрованих виробничих систем залишається забезпечення виконання виробничих функцій, спрямованих на підвищення ефективності виробництва за рахунок безперервності функціонування всієї системи.

Система управління, яка буде враховувати зміни робочого середовища і станів гнучкою виробничої інтегрованої системи повинна здійснювати нагляд за умовами виконання завдання і, при необхідності, адаптувати процес виконання виробничих функцій РТС.

В якості такої системи може виступати інтелектуальна система керування, побудована на принципах IoRT. Впровадження такої системи має істотно поліпшити характеристики систем управління робототехнічними системами, що входять до складу ГІПС.

Список використаних джерел

[1] The Internet of Things in manufacturing: benefits, use cases and trends // https://www.i-scoop.eu/internet-of-things-guide/internet-of-things-in-manufacturing.

[2] P. Simoens, M. Dragone, A. Saffiotti. The Internet of Robotic things: A review of concept, added value and applications. // International Journal of Advanced Robotic Systems. – January-February 2018, P. 1-11.

[3] О.М. Цимбал, А.І. Бронніков. Формування стратегій прийняття рішень в завданнях робототехніки // Матеріали V Міжнародної науково-технічної Інтернет-конференції Сучасні методи, інформаційне, програмне та технічне забезпечення систем керування організаційно-технічними та технологічними комплексами», 22 листопада 2018 С. 213-214.

ПРОЕКТУВАННЯ, ВПРОВАДЖЕННЯ ТА ЕКСПЛУАТАЦІЯ ІНФОРМАЦІЙНИХ СИСТЕМ ТА ТЕХНОЛОГІЙ

Analysis of the algebraic fractals generation time on GPU and CPU

Barkovskaya Olesia Yurievna[1],

Poroshenko Anton Igorovich[2]

[1]*Kharkiv National University of Radio Electronics, 14 Nauky Ave, Kharkiv UA-61166, Ukraine, olesia.barkovska@nure.ua*

[2]*Kharkiv National University of Radio Electronics, 14 Nauky Ave, Kharkiv UA-61166, Ukraine, anton.poroshenko@nure.ua*

Abstract. *The aim of this work is to reduce the time spent on generation of algebraic fractals using as example the Mandelbrot set. As a result, it was established that time needed for fractal image generation depends on limit of maximum number of iterations and on the scale of image. The highest fractals generation speed is achieved on GPU processing using a block size of 64 threads with acceleration up to 220 times compared with CPU processing. Increasing number of threads in the blocks leads to increasing of image generation time.*

Keywords: *PyCUDA; fractals; image; fragment; block; Mandelbrot.*

I. Introduction And Problem Statement

Fractals are widely used in various fields of science. In computer graphics fractals are used to describe textures of the natural objects, such as plants, land and sea surfaces, clouds, snow. They are also used for creation of images and landscapes.

Big amount of algebraic calculations required for fractals creation makes this task time-consuming, but at the same time suitable for execution on a graphics card [1]. Main requirements for tasks solved on graphics processors are: explicit data parallelism, no data dependencies and the necessity to solve the problem in a short time [2].

The aim of this work is to reduce the time generation of algebraic fractals using as example the Mandelbrot set.

To achieve this goal, following tasks should be solved: analysis of time for fractals creation on CPU and GPU, depending on maximum number of possible iterations, for which the condition for creation the colorized Mandelbrot set is reached; analysis of configurations of computational CUDA kernel for generation of a Mandelbrot set on a GPU.

II. Problem solution and Results

Fractal images are created using simple algebraic calculations [3], in which complex objects are created using several coefficients while following recursion principle [4] (system reproduces itself), which simplifies work with computer graphics, but leads to an increasing in the number of calculations to expand the colormap for each iteration [5].

To accomplish the task at the CPU (Intel (R) Core (TM) i5-7300HQ CPU @ 2.50GHz), the Python language and the NumPy package were used. To accomplish the task using computing power of the GPU (Nvidia GeForce 1060 With Max-Q Design, chip microarchitecture is GP106), the PyCUDA Python package is used.

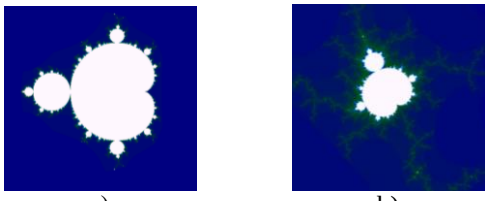
Analysis of time generation of the full Mandelbrot set (Fig. 1a) and of the fragment 100 times smaller (Fig. 1b) was performed by conducting tests at various maximum number of iterations.

The result of the work is given in Tab. 1.

Results show that the maximum acceleration of 220 times is achieved on a small block size with the number of threads equal to 64.

Table 1. Comparison of generation time of the Mandelbrot set

Scale	Maximum number of iterations	Time, s			
		CPU	On GPU, with block size		
			64	256	1024
Full image, 3x3	5	0.44	0.002	0.005	0.02
	400	4.15	0.05	0.16	0.51
	1000	10.2	0.12	0.27	1.18
Fragment, 0.03x0.03	5	0.41	0.002	0.005	0.01
	400	2.27	0.02	0.09	0.27
	1000	3.87	0.16	0.32	0.5



a) b)

Figure. 1. Mandelbrot set: a) full set, b) fragment

III. Conclusions

As a result, it was established that time needed for fractal image creation depends on limit of maximum number of iterations and on the scale of image. The highest fractals generation speed is achieved on GPU processing using a block size of 64 threads with acceleration up to 220 times compared with CPU processing. Increasing number of threads in the blocks leads to increasing of image generation time.

REFERENCES.

[1] Eric Brainville CPU/GPU Multiprecision Mandelbrot Set December 2009.

[2] K. Pingali D. Nguyen M. Kulkarni M. Burtscher M. A. Hassaan R. Kaleem T.-H. Lee A. Lenharth R. Manevich M. Mendez-Lojo D. Prountzos X. Sui "The tao of parallelism in algorithms" Proc. PLDI 2011.

[3] B Mandelbrot: The fractal geometry of nature Freeman and Co. San Francisco. Calif 1982

[4] Eric Brainville CPU/GPU Multiprecision Mandelbrot Set December 2009.

[5] Sui Tao, Tian Ming-hao and Zhang Ze-yang, "Research on high-periodic attracting points in Mandelbrot set," Proceedings of 2011 International Conference on Computer Science and Network Technology, Harbin, 2011, pp. 20

Технология Позиционирования Мобильного Объекта Для Виртуальных Пространств Больших Торговых Центров

Саенко Владимир Иванович[1]
Коваленко Александр Игоревич[2]

[1,2]Kharkiv National University of Radio Electronics, 14 Nauky Ave, Kharkiv UA-61166, Ukraine, [1]vladimir.sayenko@nure.ua, [2]kovalek96@gmail.com

Abstract. *A location service of indoor-navigation for a mobile device in large public buildings is offered. The service uses a technology that is based on the usage of Bluetooth beacons. The beacons are installed in these buildings. The technology describes a scheme of preparing and transferring location information. Some solutions on correcting the beacon's signal accuracy are offered too. As a result, this approach gives enough accuracy to solve the problem at an acceptable level of financial costs*

Keywords: *indoor positioning; indoor navigation; Beacon-based positioning system; geolocation; location calculation algorithm.*

I. Введение и Описание Проблемы

Для современного человека понятие «виртуального пространства» становится все привычнее. Каждый пользователь смартфона, неосознанно формирует свое собственное виртуальное пространство, которое интегрируется с другими. Пользователь привыкает к определенному сервису и желает, чтобы его конфигурация и качество не менялись на при каких изменениях внешних условий. Появление крупных публичных центров (например, молы) часто приводит к нарушению привычных персональных виртуальных пространств. Типичным явлением является сложность нахождения друг друга в таких центрах. Причина – нестабильность и или невозможность GPS навигации и позиционирования. Часто люди с трудом могут найти друг друга в этих центрах. Многоэтажность, многокомнатность, закрытость создают реальные сложности локального навигационного позиционирования посетителя.

Задача исследования методов и технологий позиционирования мобильного объекта (indoor-навигации) для разных виртуальных пространств больших закрытых публичных центров является актуальной

Решение данной задачи находит множество применений: возможность быстро найти ближайшую стойку регистрации в здании аэропорта, свободное место на парковке, экспонат в музее, отдел и полку с нужным товаром в магазине, а также получить его описание на экране телефона и многое другое.

Применение средств indoor-навигации предоставляет новые инструменты для маркетинга. Например, проходя мимо магазина, человек может моментально узнать о проводимых акциях, мероприятиях, предоставляемых услугах, благодаря всплывающему сообщению на экране своего телефона. При этом все предложения будут учитывать его интересы, за счет информации о его прошлых покупках. Появляется возможность сбора и анализа статистической информации, основанной на перемещении пользователя в торговом центре. Такой анализ позволяет понять, какие отделы и товары пользуются повышенным интересом.

Традиционные системы навигации не могут решить данную проблему из-за достаточно высоких (около 10 м) показателей погрешности, а также невозможности получения данных со спутника внутри помещений.

Решение может быть найдено при использовании дополнительной внутренней локации. Такие технологии могут быт основаны на использовании WiFi источников [6], или технологий на основе Bluetooth.[1, 2, 3, 4]

II. Описание Технологии

Предлагается использование подхода, основанного на Bluetooth-маячках Beacon. Подход включает технологию, которая предполагает установку маячков внутри здания в ключевых точках. Они производят широковещательную рассылку с заданной периодичностью, содержащую идентифицирующую их информацию. Пользовательское приложение циклично получает эти данные, определяет координаты маячков по базе данных относительно помещения, и на основе силы сигнала определяет своё местоположение. Также данный подход позволяет добавлять Beacon на требующие идентификации объекты.

Рассмотрим формат данных, отправляемых маячком:

Преамбула (4 байта) – префикс пакета, позволяющий установить, что данное устройство является Beacon-маячком. Преамбула состоит из 4х полей: идентификатор компании (2 байта), тип (1 байт) и длина данных (1 байт).

Proximity UUID (16 байт) – идентификатор группы Beacon-маячков.

Major (2 байта) – идентификатор набора маячков внутри одной группы. То есть внутри группы маячков, идентифицируемой UUID, может быть несколько подгрупп, каждая из которых идентифицируется по номеру Major.

Minor (2 байта) – номер, идентифицирующий маячок внутри Major.

TX Power (2 байта) – эталонное значение мощности маячка, представляющее собой силу сигнала на расстоянии в 1 метр от маячка. Измеряется и записывается в маячок 1 раз при его производстве. Данная константа используется при определении расстояния от пользователя до маячка.

Совместное использование pUUID, Major, Minor позволяет нам однозначно идентифицировать маячок, а также определять по таблице соответствия маячков их координатам, координату самого маячка.

В рамках технологии реализован способ определения положения в пространстве, основанный на вычислении координат маячков, которые определяются на основе информации рассылаемой Beacon, перечисленной выше, такой как: pUUID, Major, Minor, TX Power. Также данный подход включает в себя метод вычисления расстояние до маячков, реализованный с помощью параметра RSSI (Received Signal Strength Indicator) [5], который вычисляется пользовательским Bluetooth-приёмником на основе силы принимаемого сигнала. Чем выше значение этого параметра – тем ближе маячок. Для определения расстояния до маячка используется текущее значение RSSI, а также эталонный TX Power для коррекции.

При определении позиционирования могут возникнуть ошибки из-за присутствия крупных экранирующих объектов по направлению от маячка до устройства или наличия поблизости поверхностей, состоящих из материалов, отражающих радиосигнал. Для повышения точности предлагается усреднить значение RSSI с каждого из маячков, настроить их на выдачу данных с максимальной частотой, после чего накапливать данные в буфере и с определённой периодичностью считать средний показатель RSSI. Предлагается выбрать три маяка с лучшими средними показателями RSSI и определить по координатам этих маячков положение в пространстве с помощью трилатерации. При трилатерации используется известное местоположение двух и более объектов и измеренное расстояние между каждым из опорных объектов (Beacon маячков) и устройством, для которого определяется местоположение. Для точного и однозначного определения относительно местоположения точки или объекта на двумерной размерности требуется, по меньшей мере, три опорные точки (информация с трёх Beacon-маячков с лучшими средними RSSI). Так как расчеты проводятся в двумерном пространстве, а расстояние до маячков в трёхмерном, если разница по оси Z между наблюдателем и маячками ощутима, требуется строить проекции на оси X, Y. Далее искомое расстояние находится по теореме Пифагора.

В плане физической реализации маячки являются Bluetooth 4.0 LE устройствами. Это означает, что их роль может выполнять любое устройство, оснащённое BLE-чипом. Например, это могут быть смартфоны на базе Android, а также iPhone, iPad, обычные ноутбуки и т.д., использующие специальное приложение, реализующее функции Beacon-маячка. Типичный Beacon-маячок, компактен и способен проработать от одной батарейки до трех лет. Схемотехнически он состоит из батарейки и Soc (System on chip), представляющий собой микроконтроллер, в который загружается прошивка для реализации функции Beacon-маячка, и периферийный модуль Bluetooth LE. Дальность действия маячка – в среднем 10 метров (варьируется от 15см до 40м в зависимости от модели и настроек). Периодичность выдачи данных настраиваемая, стандартное значение – 200мс. Маячок является простым устройством, который только выдаёт в эфир свои данные, используя Bluetooth профиль GATT, при этом к нему не обязательно выполнять подключение.

При практической реализации предложенного подхода следует помнить, что эта технология не предоставляет никаких средств безопасности. Это решение не подходит для работы с конфиденциальными данными, ведь злоумышленник может сканировать эфир в режиме реального времени, на предмет обнаружения искомого маячка. Также злоумышленник может нарушить ориентирование по заранее расставленным в помещении маячкам, выставив собственный с измененными значениями pUUID, Major, Minor. В итоге, данную технологию следует использовать в подходящих сценариях, а также учитывать необходимость средств защиты.

Преимуществом данной технологии является достаточно высокая точность, простота идентификации объектов. Недостатком является необходимость покупки специализированного оборудования (маячков или устройств выполняющих их роль) и контроля за источниками его питания. В результате данный подход даёт достаточную точность решения проблемы при приемлемом уровне финансовых затрат.

III. Заключение

В работе рассматривается технология позиционирования мобильного объекта для разных виртуальных пространств. Технология основана на использовании сигналов от маячков Bluetooth, установленных внутри закрытых публичных центров (зданий). Данное решение находит множество применений, начиная от места на парковке и заканчивая отделом и полкой с товаром в магазине, а также возможностью получить его описание на экране телефона. Также в этой работе обсуждаются способы корректировки точности сигнала маяка.

В результате используемый подход и технология дают достаточную точность для решения рассмотренной проблемы при приемлемом уровне финансовых затрат.

Список Источников

[1] Wang, Y., Yang, X., Zhao, Y., Liu, Y. & Cuthbert, L. 2013. ‘Bluetooth Positioning using RSSI and Triangulation Methods’. Consumer Communications and Networking Conference, pp. 837 – 842.

[2] Lau, E. & Chung, W. 2007. ‘Enhanced RSSI-Based Real-Time User Location Tracking System for Indoor and Outdoor Environments’. International Conference on Convergence Information Technology, 2007, pp. 1213 – 1218.

[3] Zhou, S. & Pollard, J.K. 2006. ‘Position Measurement using Bluetooth’. IEEE Transactions on Consumer Electronics, vol. 52, no. 2, pp. 555 – 558.

[4] Faragher, R. & Harle, R. 2015. ‘Location Fingerprinting with Bluetooth Low Energy Beacons’. IEEE Journal on Selected Areas in Communications, vol. 33, no. 11, pp. 2418 – 2428.

[5] Chowdhury, T. I., Rahman, M. M., Parvez, S., Alam, A. K. M. M., Basher, A., Alam, A. & Rizwan, S. 2015. ‘A multi-step approach for RSSi-based distance estimation using smartphones’. 2015 International Conference on Networking Systems and Security, pp. 1 – 5.

[6] Саенко В.И., Волчанецкий И.С. Мобильный сервис определения местоположения пользователя в закрытых публичных центрах/ Матеріали другої міжнародної науково-технічної конференції «Комп’ютерні та інформаційні системи і технології». 2018. – с.115-116.

Прискорений пошук та заміна тексту в текстовому документі

Зайцева Софія Геннадіївна[1],
Барковська Олеся Юріївна[2]

[1]Харківський національний університет радіоелектроніки, пр.Науки, 14, м.Харків,61166, Україна, zaytsevasg@gmail.com
[2]Харківський національний університет радіоелектроніки, пр.Науки, 14, м.Харків,61166, Україна, olesia.barkovska@nure.ua

Анотація. *У роботі розроблено програмний застосунок для створення й зміни текстових файлів із функцією прискореного пошуку, а також пошуку та заміни фрагментів тексту в існуючому документі. Отримані результати показали, що зі збільшенням розміру слова для пошуку прямопропорційно зменшується час на його пошук через задіяння більшої кількості ядер. Такі самі результати були отримані для функції пошуку та заміни елементів.*

Ключові слова: *текст; пошук;заміна; редактор; прискорення.*

I. ВСТУП. ПОСТАНОВКА ЗАДАЧІ

Основними вимогами до текстових редакторів є можливість форматування та редагування тексту, створення і відкриття текстових документів, проведення пошуку по документу і виконання автозаміни. Також повинна бути можливість збереження тексту в файл, інтуїтивно зрозумілий інтерфейс для користувача. Наданим умовам задовольняє багато існуючих редакторів, але недоліком, який присутній у більшості розглянутих редакторів є відсутність можливості перекладу тексту, а також повільне виконання пошуку та заміни тексту у великому текстовому файлі.

Метою роботи є розробка програмного застосунку, призначеного для створення й зміни текстових файлів (вставки, видалення та копіювання тексту, заміни змісту), виводу на друк, перекладу фрагментів тексту, а також прискореного пошуку фрагментів тексту в існуючому документі.

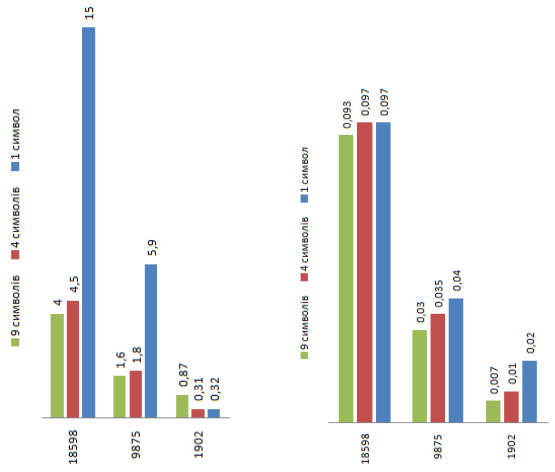
Для досягнення поставленої мети мають бути вирішені наступні завдання: аналіз методів прискореного пошуку тексту; аналіз методів прискореної заміни фрагментів тексту; впровадження багатопотокової реалізації пошуку та заміни тексту у текстовий редактор; забезпечення можливість перекладу певного фрагменту тексту.

II. РІШЕННЯ ПОСТАВЛЕНОЇ ЗАДАЧІ. АНАЛІЗ РЕЗУЛЬТАТІВ

Послідовний пошук та заміна елементів базуються на наступних етапах: виконується послідовне порівняння запитаних елементів з елементами вихідного текстового файлу; після співпадіння першого символу перевіряється наступний і так далі, доки не буде досягнуто останній символ із пошукового запиту. Прискорення запропонованої послідовної реалізації пошуку та заміни тексту виконувалось із використанням бібліотеки паралельних задач TPL [1,2] завдяки динамічному масштабуванню ступеня паралелізму для ефективного використання усіх доступних процесорів [3-5].

Тестування функції пошуку та пошуку і заміни елементів було проведено на різному наборі даних. Для початкового тексту було обрано три документи розміром 1, 5 та 10 сторінок.

Також було проаналізовано вплив розміру слова (1, 4 та 10 символів у слові), яке має бути знайдено, на час виконання операції при послідовній та паралельній реалізації. Результати наведені на рис.1.



а) б)

Рисунок 1. Результати застосування паралелізму: а) при пошуку текстового фрагменту; б) при пошуку та заміні тексту

III. ВИСНОВКИ

Отримані результати показали, що зі збільшенням розміру слова для пошуку прямопропорційно зменшується час на його пошук через задіяння більшої кількості ядер. Такі самі результати були отримані для функції пошуку та заміни елементів. Також можна побачити, що функція пошуку та заміни елементів відбувалася значно швидше. Це пояснюється тим, що використовується більш трудомістка графічна операція зміни кольору тексту.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЬ

[1] M. Posadas, “Mastering C# and .NET Framework,” Packt Publishing Ltd, 2016., 560p.

[2] A.Freeman, “Pro .NET 4 Parallel Programming in C#”, Apress, 2010, 328p.

[3] L. Skovajsová, "Long short-term memory description and its application in text processing," 2017 Communication and Information Technologies (KIT), Vysoke Tatry, 2017, pp. 1-4. doi: 10.23919/KIT.2017.8109465

[4] S. Lakhara and N. Mishra, "Desktop full-text searching based on Lucene: A review," 2017 IEEE International Conference on Power, Control, Signals and Instrumentation Engineering (ICPCSI), Chennai, 2017, pp. 2434-2438. doi: 10.1109/ICPCSI.2017.8392154.

[5] X. Hei, J. Zhang, B. Wang, H. Jin and N. Giacaman, "Parallelization using task parallel library with task-based programming model," 2014 IEEE 5th International Conference on Software Engineering and Service Science, Beijing, 2014, pp. 653-656. doi: 10.1109/ICSESS.2014.6933653.

Модульна архітектура програмного забезпечення при роботі з Big Data на основі Node.js

Росляков Ігор Миколайович[1]
Барковська Олеся Юріївна[2],

[1]*Kharkiv National University of Radio Electronics, 14 Nauky Ave, Kharkiv UA-61166, Ukraine, ihor.rosliakov@nure.ua*
[2]*Kharkiv National University of Radio Electronics, 14 Nauky Ave, Kharkiv UA-61166, Ukraine, olesia.barkovska@nure.ua*

Анотація. *У роботі розглянута проблема низької ефективності та продуктивності архітектурних рішень, створених із використанням програмної платформи Node.js. Для визначення можливості підвищення ефективності та продуктивності архітектурних рішень було досліджено вплив багатопоточності та наявності індексування полів таблиць БД при пошуку даних на час обробки запиту. Отримані результати показали, що використання багатопоточності з використанням індексування підвищують ефективність та продуктивність до 5 разів.*

Ключові слова: *Node.js; Big Data; база даних; архітектура; клієнт; сервер.*

I. Введення. Постановка задачі

Програмне забезпечення використовуючи програмну платформу Node.js [1] набуває стрімкого розвитку. В теперішній час важливу роль відіграє швидкість обробки , оскільки значно збушується кількості інформації що обробляється. Однак, в багатьох програмних продуктах використовуються архітектурні підходи, які не можуть забезпечити велику швидкість для отримання та використання Big Data [4], як у десктопних, так і у мобільних реалізаціях системи. Тому, кожен програміст, що розробляє такі системи, використовує базову структуру програмних продуктів та адаптує її під поставлене завдання. Це призводить до подальшої модернізації та вдосконалення програмного продукту, але може призвести до зниження швидкості обробки та унеможливлює масштабування. Використання програмної платформи Node.js із врахуванням архітектурних особливостей програмного забезпечення в подальшому може забезпечити можливість розширення функціоналу додатків.

Наведені фактори зумовлюють актуальність створення архітектурного рішення для розробки програмних продуктів, в яких необхідна обробка Big Data та надається можливість розробнику:

- Додавати нові архітектурні модулі для постійної модернізації системі;
- Мати швидкий доступ для зміни архітектурного рішення при необхідності зберігання великої кількості інформації.

Метою роботи є підвищення ефективності та продуктивності архітектурних рішень, використовуючи програмну платформу Node.js.

Для досягнення мети мають бути вирішені наступні задачі: проаналізовано вплив багатопоточності при пошуку даних в БД на час обробки запиту; проаналізовано вплив наявності індексування полів таблиць БД при пошуку даних на час обробки запиту.

II. Рішення поставленої задачі

Для вирішення поставленої задачі було створено веб-додаток, що включає в себе клієнтську та серверну частини, а також базу даних (рис.1).

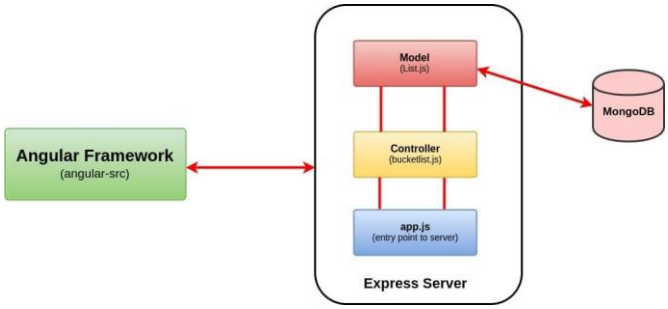


Рисунок 1. Логічна структура розробленого програмного продукту

Клієнтська частина веб-додатку створена за технологіями веб-розробки Angular 7 [2]. Серверний додаток розроблено використовуючи програмну платформу Node.js.

Архітектура серверної частини побудована з урахуванням розділення модульної структури:

- Модуль бізнес логіки який відповідає за взаємодію маж поведінкою об’єктів предметної області. А саме взаємодія інтерфейсів сервісів з частковою або повною реалізацією їх.
- Модуль Data Access в якому пердставленно абстракні інтерфейсі для організації роботи с типами в базі даних а також механізму збереженняю Що дає можливість використання без урахування механізму типу самої бази данних.

Перевірка ефективності та продуктивності додатку виконана при наступних вхідних даних:

- Дані отримані за допомогою безкоштовного сервісу books.google.com в розмірі 100 000 книжок;
- У якості бази даних (БД) для збереження інформації використано MongoDB [3].

Під ефективністю програмного продукту (ПП) розуміємо кількість оброблених даних під час пошуку.

Під продуктивністю ПП розуміємо швидкість обробки пошукового запиту на сервері в розробленому архітектурному рішенні.

При аналізі результатів враховувались такі показники:

- Однопоточні операції при пошуку даних в БД;
- Багатопоточні операції при пошуку даних в БД;
- Використання індексів в таблицях БД;
- Відсутність індексування в таблицях БД.

Шляхом тестування запиту при використанні однопоточних операцій при пошуку даних в БД та

відсутності індексування було становлено, шо для пошукового вибору даних в кількості 50000 книг відповідь від серверу надійшла за 69.12с. (рис.2).

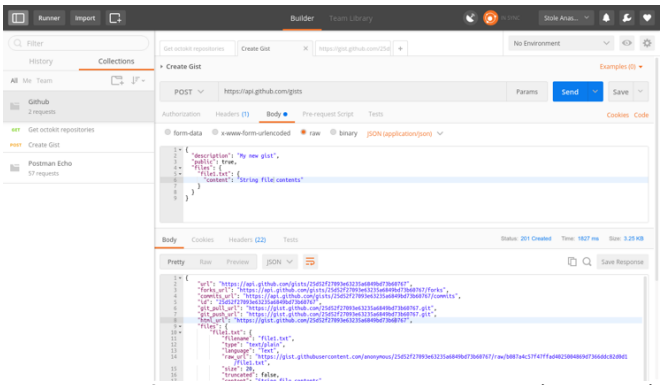


Рисунок 2. Отримання результату за умов відсутності індексу та однопоточності

Враховуючи результат тестування можна сказати, що пошук в БД займає значну частину часу. Це призводить до затримок відображення даних у веб-додатку.

Саму тому було проведено тестування із використанням багато поточних операцій та індексування полів в таблицях БД при пошуку даних за умов того ж самого пошукового запиту до серверу. За результати цього також було оброблено 50000 книг і відповідь надійшла за 12.25с (рис.3).

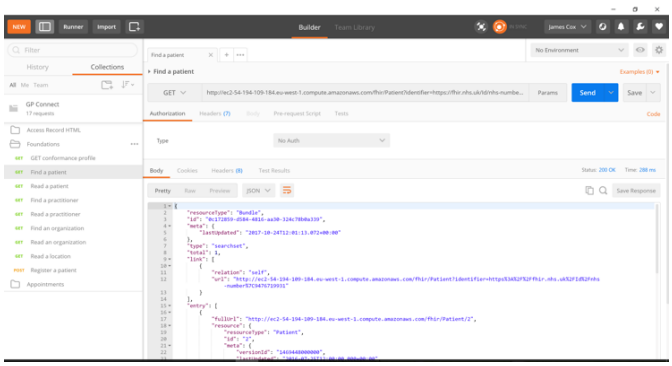


Рисунок 3. Отримання результату за умов індексування полів таблиць БД та використання 4 потоків

Результати аналізу продуктивності та ефективності ПП для усіх проведених тестів наведені у табл.1.

Розрахунок досягнутого прискорення при реалізації із використанням одного потоку виконується у відповідності з формулою (1):

$$S_{thr} = \frac{T_1}{T_{thr}}, \quad (1)$$

де T_1 - час відповіді від сервера при однопоточності, T_{thr} - час відповіді від сервера при кількості потоків рівній thr з індексуванням.

Розрахунок досягнутого прискорення при реалізації із використанням більш ніж одного потоку виконується у відповідності з формулою (2):

$$S^i_{thr} = \frac{T^i_1}{T^i_{thr}}, \quad (2)$$

де T^i_1 - час відповіді від сервера при однопоточності, T^i_{thr} - час відповіді від сервера при кількості потоків thr з індексуванням.

Таблиця 1. Розрахунок досягнутого прискорення при обробці запитів

Умови тестування		2000 результатів		50000 результатів	
Кількість потоків	Індексація	Час відповіді від сервера	Приско-рення	Час відповіді від сервера	Приско-рення
1	-	19.2	-	69.12	-
1	+	14	-	63	-
2	-	10	1.92	45	1.3
2	+	7.5	1.86	40.77	1.54
4	-	6.9	2.78	22.1	3.12
4	+	2.5	5.6	12.25	5.14

Запропоноване рішення має наступні можливості:

- Масштабування модульного доповнення архітектурного рішення;
- Гнучке налаштування або зміна конфігурації системи при роботі з базою даних;
- Зручний інтерфейс для зміни кількості потоків, що обробляють запити;
- Зручний інтерфейс для автоматичного зберігання статистики запитів та витраченого часу на їх обробку у вигляді графіків та таблиць.

III. ВИСНОВКИ

В ході виконання роботи було проаналізовано вплив багатопоточності та наявності індексування полів таблиць БД при пошуку даних на час обробки запиту та отримані наступні результати: збільшення кількості потоків призводить до збільшення прискорення у 5 разів, як при тестуванні на 2000 елементів пошукової вибірки, так і 50000 елементів пошукової вибірки.

Використання багатопоточності в розмірі 4 потоків та індексування таблиць забезпечить підвищення ефективності та продуктивності архітектурних рішень, використовуючи програмну платформу Node.js.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЬ

[1] Azat Mardan, “Practical Node.js: Building Real-World Scalable Web Apps ”, 2nd ed., Apress, 2018, 505pp.

[2] John Kocer, “Angular 7: By Example (Part One Book 1)”, Amazon KDP Publish;, 2018, 429pp.

[3] Deepak Vohra, “Pro MongoDB Development”, Apress; 1st ed., 2015, 506pp.

[4] A. Jamil, M. Abdullah, M. A. Javed and M. S. Hassan, "Comprehensive Review of Challenges & Technologies for Big Data Analytics," 2018 IEEE International Conference on Computer and Communication Engineering Technology (CCET), Beijing, 2018, pp. 229-233. doi: 10.1109/CCET.2018.8542219

Аналіз методів забезпечення масштабованості та продуктивності серверного додатку

Сас Владислав Анатолійович[1]

Барковська Олеся Юріївна[2],

[1]*Kharkiv National University of Radio Electronics, 14 Nauky Ave, Kharkiv UA-61166, Ukraine, vladyslav.sas@nure.ua*

[2]*Kharkiv National University of Radio Electronics, 14 Nauky Ave, Kharkiv UA-61166, Ukraine, olesia.barkovska@nure.ua*

Анотація. *Надана робота присвячена аналізу методів, які забезпечують масштабованість та продуктивність серверного додатку, а саме: аналізу продуктивності існуючих ORM та серверних фреймворків, аналізу та реалізації паттернів та принципів проектування. Отримані результати показали переваги Dapper, оскільки даний ORM має найбільшу швидкість обробки запитів та надає можливість відображати результат запитів у об'єкти, що є основою для подальшого використання цього відображення.*

Ключові слова: *сервений-додаток; масштабованість; продуктивність; ORM; паттерн;* Angular 4; Entity Framework Code First; *ASP.Net Web Api 2.*

I. Введення. Постановка задачі

Продуктивність програми є головною проблемою при розробці корпоративної програми, особливо коли одночасний доступ до додатку намагаються отримати тисяч користувачів. Під продуктивністю додатку розуміємо кількість оброблюваних запитів в секунду (RPS) і швидкість їх виконання (TTFB - Time to First Byte) [1]. Під масштабованістю системи розуміємо пул можливостей для збільшення RPS. Головними підходами для збільшення гнучкості, розширюваності та швидкості обробки запитів є використання певних ORM та обробка запитів за допомогою Server-side web application Frameworks [3].

Метою роботи є забезпечення масштабованості та продуктивності серверного додатку, для чого перш за все має бути проведений аналіз існуючих ORM для .Net platform та пошук найшвидшої ORM.

II. Вирішення поставленої задачі

Серед ORM, які впливають на продуктивність та масштабованість серверного додатку виділяють: EntityFramework, NHibernate, Dapper, ADO.NET [2].

Кожне з наведених відображень має свої переваги та недоліки. Щоб визначитись з питанням, яка з ORM є найкращою, в роботі виконано аналіз їх функціональності у відповідності з наступники критеріями: можливість нативних запитів, простота роботи, контроль з'єднання з базою даних, час обробки запиту. Наявність нативних запитів впливає на можливість взаємодії з БД за допомогою SQL запитів, взаємодії з конструкціями T-SQL такими як процедури, представлення, функції та інші. Під простотою роботи розуміємо кількість роботи для обробки запиту. Контроль з'єднання з базою даних забезпечує можливістю користувачу впливати на процес з'єднання з БД. Під простотою оновлення структури БД розуміємо автоматичне оновлення структури БД за допомогою коду або міграцій. Час обробки запиту визначаємо як:

$$T_{RPS} = T_{conn} + T_{proc},$$

де T_{conn} – час відкриття та закриття з'єднання , T_{proc} – час обробки запиту

Таблиця 1. Переваги та недоліки різних ORM

	Entity Framework	NHibernate	Dapper	ADO.NET
Наявність нативних запитів	-	+	+	+
Простота роботи	-	+	+	+
Простота оновлення структури БД	+	-	-	-
Контроль з'єднання з БД	-	+	+	+
Час обработки запиту	-	-	+	+

При аналізі часу обробки запитів було виконано ряд досліджень на тестовому додатку. Дослідження проводились на локальному сервері із внесенням змін у складність запитів. Результати роботи із різними ORM наведені на рисунку 1.

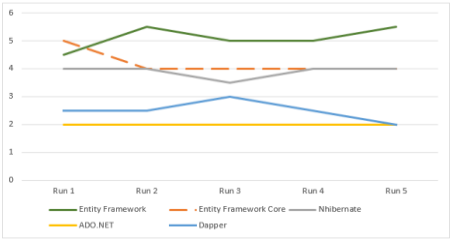


Рисунок 1. Швидкість оброки SELECT-запиту в ORM

III. Висновки

Аналіз графіку демонструє перевагу Dapper, оскільки даний ORM має найбільшу швидкість обробки запитів та надає можливість відображати результат запитів у об'єкти, що є основою для подальшого використання цього відображення. Недоліком Dapper є складність оновлення структури БД, але це не є основним на даному етапі, тому що у нас вже є структура БД та подальші оновлення ми зможемо здійснити мануально, головною є перенос запитів у процедури, щоб уся логіка запитів була на рівні БД, це дає нам самодостатність та безпечність БД.

Перелік джерел посилань

[1] R.Miller, J. Lerman, "Programming Entity Framework: Code First", O'Reilly Media, Inc., 2011, 159pp.

[2] C. Xia, G. Yu and M. Tang, "Efficient Implement of ORM (Object/Relational Mapping) Use in J2EE Framework: Hibernate," 2009 International Conference on Computational Intelligence and Software Engineering, Wuhan, 2009, pp. 1-3. doi: 10.1109/CISE.2009.5365905

[3] Wei Zhang, Linna Zhao, "Analysis and design of persistent layer in object-oriented application program based on ORM," Proceedings of 2011 International Conference on Computer Science and Network Technology, Harbin, 2011, pp. 1711-1713. doi: 10.1109/ICCSNT.2011.6182297

About Designing Information System of Information Warfare

Kereselidze Nugzar

Sukhumi State University, 61 A.Politkovskaya street, Tbilisi 0168, Georgia ,nkereselidze@sou.edu.ge

Abstract. *In the following work it is proposed to investigate the Information Warfare of antagonistic parties using the Information System. The information system appears to be designed based on the objectives of the Information Warfare study. The objectives of the study can be: establishing the patterns of the Information Warfare; the selection of its control parameters; establishment of manageability; development forecasting; development of recommendations, etc... In accordance with these goals, stages and subsystems are defined during the design of the Information Warfare Information System.*

Keywords: *Information Warfare; Information System; Mathematical model; Computer model.*

I. Introduction And Problem Statement

For several decades humanity has used new forms of conflict, from which Information warfare occupies an important role. Since 1976, when American researcher Thomas Rona (Rona T. P., "Weapon Systems and Information War", Boeing Aerospace Co.,Seattle, WA, 1976.) first used the term ''Information warfare'' a lot of important things have happened towards this direction: An important role has been given to discovering ''Information Warfare'' threats in Leader countries' national securities and preventing them, Scientific researches and publications have been qualitatively and quantitatively increased towards ''information warfare''. One of the important directions in information warfare is the Information flows generated by controversy in the open channels (electronic, print media, the Internet or other means). The aim of the information warfare can be: A) humiliating the image of the opponent country – painting it as an enemy, discrediting the government, demoralization of armed force personnel and civilians. B) Argumentation to justify possible future military actions, forming a public opinion inside and outside the country. C) To resist the geopolitical ambitions of the opposing side and other. A strong information correlation and future military action between the countries has been recorded. The study of information warfare created between opposing parties, establishment of its regularity, management capabilities and determination of control parameters, Information Warfare Development forecast, development of various types of scientific recommendations and other, occur as avoidance to essential information warfare transforming into military action in defense of human life, ecology and resources of different types. Mathematical and computational methods seem to be an effective way to research these problems. Using mathematical and computer models to describe the object of research and study it, including intensive production of computer experiments represent a precondition of creating a deep**,** comprehensive computer system of information warfare in financial and other resource-limited conditions [1-4].

The object of the proposed project is researching the information warfare process between the opposing sides. Information warfare is discussed in terms that the antagonistic sides' open channels - the media, the Internet and other means are used to disseminate information discrediting each other. This process involves a third party, such as an international organization - the peacemaking side, which, by using open channels, calls antagonistic sides to lower the rhetorical persistence, or even stop the information warfare.

The presented work is created with the help of Shota Rustaveli National Science Funding of Georgia Grant YS17_78.

II. Problem solution and Results

To design an information system of Information Warfare it is necessary to carry out the following investigation phases - steps and to create the corresponding subsystems: To get a discrediting part of information flows spread by opposing sides, for which the synergistic efforts of philologists, sociologists, psychologists and diplomats create an opposing typical terms and phraseology base, the so-called Key Data of confrontation. An analogous framework for the peacemaking side will be created, in which the key terms and phraseology characteristic of calls for peace will be stored.

Ensuring the monitoring system on the information spread by the information warfare subjects or spread on behalf of them**,** for which the search engine is considered to be of use. At this point, for each of the subjects, there is a temporary base for general activities. In the base structure the information dissemination time, author, author's political or any other type of status fields is essential.

Taking out the general activities of temporary bases on the first stage with the help of key data. The software product is used for this process. As a result we will have specific activity bases for every subject. It is possible that the second and the third stages can be carried out simultaneously, the ability - inability to afford this will be clearer on realization.

Establish the amount of information spread from specific activity bases which were made for information warfare subjects and for which in the first stage, a created synergistic group will establish the so called "weight" of existing terms, phraseologies. "Weight" is determined towards the source of the information as well. The result will be the amount of information spread in the context of information warfare by according subjects in specific moments of time. To give an example, for the first time t spread of information by the antagonistic side is $N_1(t)$, the spread of the other antagonistic

party - $N_2(t)$ number of information. While the number of information the peacekeeper side releases is $N_3(t)$.

Information warfare mathematical model is created to connect the fourth stage $N_1(t)$, $N_2(t)$ and $N_3(t)$ ratios with each other. In fact, creating several models of the information warfare in reality with their level of adequacy is needed; the models can be described in various ways. In general, we will get a model library. For each model except $N_1(t)$, $N_2(t)$ and $N_3(t)$, we can have parameters that go inside them $\alpha, \beta, \lambda, \gamma, ...$ which have a specific semantic load when making a model. For example: aggressiveness coefficient, peace readiness index, quality and other peacekeeping activity.

In the models, which were created on the fifth stage, giving a specific information warfare $\alpha, \beta, \lambda, \gamma, ...$ parameters. For which expertly defined $N_1(\cdot), N_2(\cdot), N_3(\cdot)$ values will be for different times and with their help, by using different methods determining the parameters of the process. After this from several models we will select the model (parameters with specific meanings), which is the most adequate in describing the informational warfare. At this point this also becomes a kind of learning process; it is possible to imitate different types of information warfare with different specific values and predetermining parameters for them. It is not excluded that when describing the real information warfare, the learning process could be useful. At this point, we are actually choosing, selecting a mathematical or computer model for the information warfare.

Analysis of the model chosen on the sixth stage. It allows us to forecast the process of information warfare. This requires to solve an appropriate mathematical model and to find the following $N_1(\cdot), N_2(\cdot), N_3(\cdot)$ values for time moment – the future. On this stage, if $N_1(t)$ and $N_2(t)$ have big values, then the information warfare might transfer into a ''hot'' phase. On expert's level, it is preferable that they were national security specialists; also, the process of information warfare should be scaled in the terms of threat and be given proper levels. Let`s say M is the maximum technological level of antagonistic sides and they can only spread M information in one minute. Then, if $N_1(t)$, $N_2(t) \in [90\%M, M]$ threat level is red, and $N_1(t)$, $N_2(t) \in [80\%M, 90\%M)$ - is orange and so on. Of course, bringing these levels are less effective, if an action plan for national security won't be written about each relevant level**.** In this case, we should consider the results of the eighth and ninth stages.

Governing parameters in parameters and model manageability establishment for selected model, in the best case, determining specific values for control parameters, for which ending process of the information warfare with the activity of the peacekeeping side in any terms will end optimally. To achieve the goal of this stage, it is necessary to solve the Chilker type optimal control task.

Analysis of the obtained results from the eighth stage and working out recommendations for peacekeepers.

Automation of the first 9 steps, packing them into a software product and determine the orders of the (AISOIW - Automated Information System of Information Warfare) and training of the operators.

III. CONCLUSIONS

With Automated information system of information warfare - (AISOIW) it will be possible to study the progress of information warfare - to determine aggressiveness of the antagonistic sides, peacekeeping activities and to determine if this activity will be enough to avoid outbreaks of the information warfare. With the help of (AISOIW) it will be possible to determine the minimal level of activity for peacekeepers and above these levels peacekeepers calls are, in reality, effective on antagonistic sides and aims to suppress the war. In fact, it is possible to determine the effectiveness of peacekeeping operations and to determine whether the peacekeepers only operate for actions, or if they really want to achieve the goal by activity. Determining the effectiveness of peacekeepers will allow the organizations to avoid unreasonable costs and also will not let the information warfare develop into a hot phase, and thus avoid catastrophic results for people, infrastructure, ecology and more caused by military activities. (AISOIW) will allow the peace process to optimize the necessary recommendations. Also, it is possible to model and experiment on a specific information warfare with its parameters. Use of applied mathematics, computer science, including information systems for working out new social tasks is interesting for even these sciences, because as a result we get new problems and resolving these problems develop these sciences. For example, during the peace process optimization a new type of task was raised - Chilker [5,6], in which achievable state for antagonistic parties - achieving zero happens at different moments of time and also these "times" are free. Creating a software product for this new task in the limits of (AISOIW), with a high-level interface and activity has a scientific-practical value.

REFERENCES

[1] T. Chilachava, N. Kereselidze, Continuous linear mathematical model of preventive information warfare, Sokhumi State University Proceedings, Mathematics and Computer Sciences vol. 7, 2009, Tbilisi, pp. 91–112.

[2] N. Kereselidze, On The Ratios of The Information Technology Levels of The sides in A Generalized Mathematical Model of The Information War of Ignoring The Enemy, (In Russian), Proceedings of the XXI International Conference on Security Management Problems for Complex Systems, Russian Academy of Sciences, V.A. Trapeznikova, Institute of Applied Mathematics Mv Keldish, Moscow, December 18, 2013, pp. 173-175.

[3] N. Kereselidze, About One Problem of Mathematical Model of Information Warfare, (In Russian), Proceedings of the International Scientific Conference Dedicated to Academician I. Prangishvili's 85Th Anniversary "Information and Computer Technologies, Modeling, Control", Tbilisi, Georgia, November 3-5, 2015. Publishing House "Technical University", Tbilisi, 2015, pp. 411-414.

[4] N. Kereselidze, Mathematical and Computer Chilker Models in Information Warfare, (In Russian), journal "Information Wars", № 2 (36), 2016, pp. 18–26.

[5] N. Kereselidze, An Optimal Control Problem in Mathematical and Computer Models of the Information Warfare. Differential and Difference Equations with Applications : ICDDEA, Amadora, Portugal, May 2015, Selected Contributions**.** /Editors: Pinelas, S.**,** Došlá**,** Z.**,** Došlý**,** O.**,** Kloeden, P.E. (Eds.), Springer Proceedings in Mathematics & Statistics, 164, DOI 10.1007/978-3-319-32857-7_28, Springer, 2016, pp. 303-311.

[6] N. Kereselidze, Combined continuous nonlinear mathematical and computer models of the Information Warfare, International journal of circuits, systems and signal processing, Volume 12, 2018, pp. 220-228.

Технологические Решения Создания Internet Of Things Системы Для Мониторинга Состояния Водителя

Саенко Владимир Иванович[1]
Шилин Александр Сергеевич[2]

[1,2]*Kharkiv National University of Radio Electronics, 14 Nauky Ave, Kharkiv UA-61166, Ukraine,* [1]*vladimir.sayenko@nure.ua*
,[2] *oleksandr.shylin1@nure.ua*

Abstract. *A special service for drivers is offered. The service is a monitoring system based on the use of IoT technology. It is designed to control a driver health state. The service implementation system includes sensors, operating devices, a mobile application and a cloud app for extended transferring the information. The solutions could be used for any special system with operators.*

Keywords: *IoT; car service; mobile app; driver condition, monitoring system.*

I. ВВЕДЕНИЕ И ОПИСАНИЕ ПРОБЛЕМЫ

В наше время автомобили оснащаются мощными вычислительные платформами. Эта тенденция возрастает с введением автоматических функций безопасности и беспилотных машин. Графические процессоры, камеры, датчики, и сетевое оборудование – это лишь малая доля из того, чем оборудованы сегодня наши автомобили. Все более широкое использование имеют камеры, и программное обеспечение с использованием искусственного интеллекта, которое помогает анализировать состояние машины в режиме реального времени. Одним из важных направлений в развитии современной автомобильной индустрии является обеспечение безопасности водителя. Чаще всего решения направлены на контроль показателей состояния автомобиля, но не состояния водителя

Грузовик, легковой автомобиль, самолет, вертолет, аграрный комбайн, строительный кран, ручной катер - всеми этими устройствами все еще руководит человек - безусловно, самое слабое звено в системе. Проблема в том, что транспорт опасен не только для водителя\оператора или владельца, но и для окружающих. Ежедневно тысячи людей погибают из-за несчастных случаев: пьяных водителей, переутомленных пилотов, рассеянных крановщиков. Конечно, невозможно полностью избежать этих событий, но их можно значительно минимизировать, выявляя таких операторов еще до того, как нога нажмет на педаль газа. К технологиям, позволяющим решать данные проблемы относятся технологии Internet of Things (IoT). IoT - это современный достаточно молодой концепт, сущее которого в том, что любой из окружающих нас предметов можно окружить цифровыми устройствами и подсоединить к экосистеме, сети из таких же вещей [1]. Все молодые ветви имели или имеют свои детские проблемы. IoT не исключение: уже сегодня тысячи пользователей и компаний столкнулись с высокой фрагментацией платформы, отсутствием стандартизации [2] и огромными дырами в безопасности. Тем не менее, потенциальная выгода намного превышает возможные риски. Именно поэтому сотни компаний, в том числе транспортных, инвестируют в IoT, не собираясь останавливаться [3].

Для транспортных систем наблюдается неуклонный рост уровня автоматизации. Каждая новая модель автомобиля имеет все больше и больше электронных устройств. И двигаться в стремлении контролировать автомобиль пока есть куда. Но повышение безопасности за счет контроля водителя, его состояния, исправление его ошибок – это новая сфера исследований. Лишь недавно Volvo представила свою новую разработку, которая автоматически принимает решение об экстренном торможении [4]. Tesla – предложила полноценный автопилот. И это только начало, ведь все передовые автоконцерны стали уделять этому направлению свое внимание. Именно поэтому вопросы, которые рассматриваются в работе, нацеленные на диагностику не технический показателей автомобиля, а состояния водителя перед и во время поездки, что в перспективе поможет снизить количество ДТП.

II. ОПИСАНИЕ ТЕХНОЛОГИИ

Предлагаемые технологические решения для создания системы мониторинга состояния водителя основаны на использовании технологий Internet of Things.

В качестве параметров контроля используется комплекс показателей: содержание алкоголя в дыхании водителя, контроль открытости век, контроль положении головы, а также подсчёт количества попыток для вставки ключа в замок зажигания. На основе полученных данных система принимает решение о состоянии водителя. Взаимодействие с водителем осуществляется двумя способами. Если было замечено, что водитель закрыл глаза во время поездки, то воспроизводится громкий неприятный звук. Если было обнаружено, что состояние водителя неудовлетворительное, то выдается голосовое сообщение, советующее не садиться за руль или не продолжать поездку.

Расширенная структура системы, реализующая данный сервис, включает четыре компонента: физическую часть, обрабатывающее приложение, прикладное мобильное приложение и серверное приложение.

Физическая часть - это средства идентификации, измерения и передачи данных. Обрабатывающее приложение осуществляет сбор информации от

первичных устройств, анализ и формирование действия. Прикладная часть – это мобильное приложение для клиента. Серверное приложение - это специальное приложение, выполненное на основе облачного сервиса.

Разрабатываемая система, собирает данные в реальном времени, что требует от неё наличия датчиков и устройства, к которому они будут подключены. Для считывания показателей используются датчики алкоголя в воздухе аппаратно совместимые с выбранным компьютером, аналого-цифровой преобразователь, видеокамера, поддерживающая стриминг видеоряда, тончайшие кнопки (около 2мм), а также металлическая или пластиковая пластина с отверстием в центре под ключ зажигания.

Основные технологические решения для физической части целесообразно строить, исходя из принципов микросервисной архитектуры. В этом случае каждое физическое устройство отвечает за свой сервис. Парадигма данной архитектуры позволит наилучшим образом создать масштабируемую систему, это крайне необходимо в рамках рассматриваемого решения. Основным достоинством предложенного подхода является наличие готовых, открытых программных и концептуальных решений, доступных для использования без лицензий. К самой распространенной группе таких решений относится продукция на базе Arduino.

Обрабатывающая часть системы состоит из микроконтроллера (Arduino), или микрокомпьютера (Raspberry PI), к которому подключена вся периферия, на котором также выполняются все расчеты по принятию решений. При выборе базового контроллера Raspberry PI на нем должна быть установлена Unix-совместимая операционная система. Если будет выбран Arduino, то к нему не выдвигается специфических требований. Для Arduino программа обработки зашивается непосредственно в память микроконтроллера без установки промежуточных операционных систем. Все данные, собранные из этих устройств анализируются основным модулем для принятия решения о состоянии водителя.

Основной модуль выполняется как система с обучением, с реализацией базовых принципов. искусственного интеллекта. За основу принимается метод обучения с учителем. На базе принятого нейросетью решения система выдает рекомендации по целесообразности и безопасности управления транспортным средством.

Для создания мобильного приложения целесообразно использовать язык программирования Java, который является объектно-ориентированным и агрегирует преимущества данной концепции, а с другой стороны, имеет библиотеки, позволяющие удобно взаимодействовать компонентам физической системы и управляющего приложения. Эта технология является кроссплатформенной и позволяет создавать приложения под самые популярные платформы iOs и Android.

Серверное приложение является опционным компонентом, позволяющим осуществлять связь с дополнительными мобильными системами (например, мобильные устройства родственников).

Облачные сервисы в данном случае можно также использовать для хранения данных в виде базы данных. В простейшем случае для сохранения состояний система использует локальное хранилище. Эталонный вариант реализации – это использование внутреннего компьютера автомобиля. Для упрощения реализации может использоваться внутренняя память микроконтроллера, в том числе и для базы данных.

Для создания серверного приложения предлагается использовать облачные платформы с расширенной функциональностью. В частности облачное решение Amazon - AWS имеет три сервиса, состоящих из множества инструментов, которыми можно воспользоваться для построения IoT автомобильного сервиса: AWS IoT Core - платформа, которая позволяет подключенным устройствам легко и надежно взаимодействовать с облачными приложениями и другими устройствами.; AWS IoT Device Management - сервис, который упрощает безопасное размещение, организацию, мониторинг и дистанционное управление устройствами IoT; AWS Greengrass - это программное обеспечение, которое позволяет безопасно запускать локальные вычисления, обмениваться сообщениями и кэшировать данные для подключенных устройств [6].

Использовать ее можно не только в автомобиле, но и в любом другом транспорте или месте, где есть аккумулятор, и многое зависит от состояния и концентрации оператора.

III. Заключение

В работе рассматриваются технологические решения, направленные на построение системы мониторинга состояния водителя транспортного средства. Решения основаны на использовании набора контролируемых диагностических показателей состояния человека. Контроль осуществляется в реальном режиме времени. Результаты диагностики формируются в форме предупреждающих сообщений.

Предлагаемые решения могут быть использованы для реализации систем диагностики состояния человека, исполняющего обязанности оператора любых сложных систем. Реализации функций диагностики может быть не только предупреждающей, но и блокирующей.

Данный проект является дальнейшим развитием исследовательской тематики, проводимой на кафедре ИУС ХНУРЭ [5].

Список Источников

[1] Грингард С. Интернет вещей. Будущее уже здесь / Сэмюэл Грингард., [Текст] – Москва, 2016. – 188 с.

[2] Claire Rowland, Elizabeth Goodman, Martin Charlier, Ann Light, Alfred Lui. Designing Connected Products. – O'Reilly Media, Inc., 2015. – 400 с.

[3] Алексей Лагутенков. Тихая экспансия интернета вещей // Наука и жизнь. – 2018. – № 5. – с. 38-42.

[4] 4. Sandeep Thorat, Sanket Thorve, Jaydatta Upase, Agampal Singh Dhupar. Design and Implementation of Automatic Emergency Braking System // INPRESSCO, 2016.

[5] Саенко В.И., Соловьев М.И. Простой iot сервис удаленной диагностики для пользователя автомобилем/ Матеріали другої міжнародної науково-технічної конференції «Комп'ютерні та інформаційні системи і технології». 2018. – с.117-118.

[6] Rossman J The Amazon Way on IoT: 10 Principles for Every Leader from the World's Leading Internet of Things Strategies / John E. Rossman., 2016. – 168 с

Автоматизована інформаційна система для ведення щоденника тренувань

Кобзар Марія Станіславівна[1]

[1] *Харківський національний університет радіоелектроніки, пр. Науки, 14. Харків, 61166, Україна.*
E-mail: mariia.kobzar@nure.ua

Іващенко Георгій Станіславович[2]

[2] *Харківський національний університет радіоелектроніки, пр. Науки, 14. Харків, 61166, Україна.*
E-mail: heorhii.ivashchenko@nure.ua

Анотація: *Представлена робота присвячена проблемам розробки кросплатформеного мобільного додатку для ведення щоденника тренувань. Використані технології Xamarin.Forms, SQLite, Syncfusion. Додаток легко масштабується і адаптується для різних завдань і видів тренувань.*

Ключові слова: *щоденник тренувань, мобільний додаток, вправа, програма тренування, Xamarin, SQLite.*

I. ВСТУП І ПОСТАНОВКА ЗАВДАННЯ

У сучасному світі набуває поширення прагнення заняття спортом і популяризується ведення здорового способу життя. Рух і фізична активність, що включає в себе спеціальні фізичні вправи (наприклад, фітнес), з урахуванням вікових та фізіологічних особливостей людини, є одним з основних елементів здорового способу життя, а ведення щоденника тренувань – невід'ємна частина тренувального процесу, яка забезпечує безпечність тренувань для здоров'я та поліпшує спортивні показники.

Повсюдне поширення мобільних технологій спрощує ведення щоденника тренувань за рахунок мобільності та оперативності роботи. Існуюче програмне забезпечення дозволяє зберігати інформацію про попередні та майбутні тренування і вправи, що плануються, а також аналізувати і складати свій, більш ефективний план тренінгу з урахуванням власного рівня фізичної підготовки.

У роботі був проведений порівняльний аналіз існуючих додатків для спрощення організації тренувань, а також були виявлені їх основні недоліки: відсутність необхідного функціоналу та наочного календаря для планування тренінгу, обмеженість можливостей налаштування, відсутність локалізації, обмежена база тренувань, а також наявність платного контенту і реклами та закритий вихідний код.

II. ПРОПОЗИЦІЯ ЩОДО ВИРІШЕННЯ

Вирішенням проблеми управління тренуваннями є розробка конкурентоспроможного мобільного додатку, який забезпечує універсальність і можливість адаптації для різних завдань і видів тренувань.

Запропоноване рішення представляє собою мобільний кросплатформений додаток, реалізований на платформі Xamarin.Forms, що дозволяє створити універсальну розмітку сторінок одночасно для різних платформ, при цьому зберігаючи можливість настроювання поведінки сторінок, властивої кожній платформі окремо, що дозволяє скоротити час на розробку продукту, а також на його подальшу підтримку [1].

Додаток реалізує шаблон проектування MVVM (Model-View-ViewModel), який забезпечує меншу зв'язаність між компонентами і шар абстракції між бізнес-логікою програми та БД [2].

Для розробки програми використовувалася найбільш популярна СУБД для локальних додатків SQLite та бібліотека Syncfusion. Даний інструмент являє собою колекцію елементів для Xamarin.Forms, які дозволяють створити зручний графічний інтерфейс для створення сучасних мобільних додатків і забезпечують зручну взаємодію клієнта і додатку [3].

Розроблено модель даних, яка описує сутності вправи, програми тренувань та антропометричних показників. Для роботи з SQLite використовувалася бібліотека SQLite.NET, яка представляє собою ORM-рішення для Xamarin.Forms, а також забезпечує просту інтеграцію, безпеку і високу продуктивність роботи з базою даних [4].

III. ВИСНОВКИ

Запропоноване рішення має наступні можливості:

- формування власної БД тренувань і вправ;
- можливість додавання і редагування власних програм тренувань;
- використання календаря занять для відображення запланованих тренувань;
- внесення додаткових заміток;
- внесення рекомендацій до виконання вправ;
- калькулятор визначення фізичної форми;
- стеження за антропометричними даними;
- локалізований мовний інтерфейс;

Додаток поєднує в собі простоту графічного інтерфейсу користувача і насичений функціонал. Воно легко масштабується та адаптується для різних завдань і видів тренувань як досвідчених спортсменів, так і для тих, хто тільки починає активні тренування.

Реалізована на платформі Xamarin.Forms, інформаційна система підтримує операційні системи Android, iOS і Universal Windows Platform.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

[1] D. Hermes, N. Mazloumi, "Building Xamarin.Forms Mobile Apps Using XAML: Mobile Cross-Platform XAML and Xamarin.Forms Fundamentals," Bookmetrix, 2019, 218 p.

[2] P. Johnson, "Using MVVM Light with Your Xamarin Apps," Apress, 2017, 200 p.

[3] J. Karlsson, D. Hindrikes, "Xamarin.Forms Projects," Packt Publishing, 2018, 609 p.

[4] C.Petzold, "Creating Mobile Apps with Xamarin.Forms," 2nd Edition., Kindle Edition, 2014, 280 p.

Знання-Орієнтована Структуризація Управлінського Рішення в Системах Підтримки Прийняття Рішень

Левикін Віктор Макарович [1],
Чала Оксана Вікторівна[2]

[1]Kharkiv National University of Radio Electronics, 14 Nauky Ave, Kharkiv UA-61166, Ukraine, viktor.levykin@nure.ua
[2]Kharkiv National University of Radio Electronics, 14 Nauky Ave, Kharkiv UA-61166, Ukraine, oksana.chala@nure.ua

Анотація. *Розглянуто проблему підтримки прийняття рішень в умовах невизначеності на тактичному рівні організаційного управління. Вирішення даної проблеми пов'язано із побудовою множини альтернативних управлінських рішень, що містять послідовності управляючих дій із переходу від поточного до цільового стану об'єкту управління. Такі рішення формуються згідно формальних процедур та стандартів діяльності підприємства, а також з використанням персональних знань та досвіду особи, що приймає рішення. Тому управлінське рішення має знання-орієнтовану структуру. Запропоновано модель управлінського рішення у вигляді послідовності управляючих дій, що визначає послідовність станів об'єкту управління, а також темпоральних та контекстно-темпоральних залежностей між цими станами. Ці залежності задають послідовність виникнення у часі для пар станів об'єкту управління, а також зв'язки між станами підмножини елементарних об'єктів. Модель дає можливість сформувати нові управлінські рішення на основі темпоральних правил.*

Ключові слова: *управлінське рішення, підтримка прийняття рішень, темпоральна залежність, стани об'єкту управління.*

I. Вступ Та Постановка Задачі

Сучасні підходи до організаційного управління передбачають використання баз знань для підтримки управлінських рішень в умовах невизначеності при розв'язанні частково структурованих та неструктурованих задач на тактичному та стратегічному рівнях організаційної ієрархії. Невизначеність при прийнятті рішень є наслідком неповноти інформації про стан об'єкту управління, а також про зовнішні впливи на цей об'єкт.

Процес прийняття управлінських рішень передбачає вирішення задач пошуку та імплементації управлінського рішення. При вирішенні першої задачі послідовно виконується аналіз поточної ситуації та формування множини можливих управлінських рішень з переходу до цільового стану об'єкту управління. Друга задача передбачає вибір та реалізацію відібраного рішення особою, що приймає рішення (ОПР) [1].

На тактичному рівні організаційного управління використовуються системи підтримки прийняття рішень (СППР) на основі знань [2], а на стратегічному – системи підтримки дій керівника. СППР реалізує задачу пошуку управлінського рішення. Система підтримки дій керівника формує патерни вхідних даних щодо поточної ситуації, що є передумовою аналізу цієї ситуації та формування можливих управлінських рішень. В якості вхідних даних Управлінське рішення містить у собі послідовність використовуються результати роботи систем оперативного рівня.

управляючих дій із переходу від поточного до цільового стану об'єкту управління. Оскільки управлінські рішення формуються з використанням як формальних знань, що відображають процедури та стандарти підприємства, так і неформальних знань ОПР [3], то при вирішенні задачі пошуку рішення необхідно врахувати залежності між управлінськими діями, тобто розглядати знання-орієнтовану структуру цього рішення.

Таким чином, знання-орієнтована структуризація управлінського рішення для підтримки рішень в умовах невизначеності та тактичному рівні організаційного управління є актуальною задачею.

Існуючі підходи до знання-орієнтованої підтримки рішень базуються на використанні комунікативних методів вилучення причинно-наслідкових залежностей у ОПР або експертів у даній предметній галузі [4]. Однак отримання таких залежностей потребує великих витрат часу. Також ці каузальні залежності відображають специфіку конкретної організації, що потребує повторного використання комунікативних методів при переході до нової предметної області.

Для подолання недоліків наведених підходів доцільно замість каузальних використовувати темпоральні залежності [5]. Останні задають зв'язки між управлінськими діями у часі, тобто визначають знання-орієнтовану структуру управлінського рішення, і тому можуть бути побудовані автоматизованим способом .

Мета доповіді полягає в визначенні структури управлінського рішення з урахуванням темпоральних залежностей, що відображають послідовність управляючих дій. Для досягнення мети вирішуються такі задачі: визначення загальних характеристик управлінського рішення; визначення структурних елементів управлінського рішення та зв'язків між цими елементами.

II. Результати Дослідження

Управлінські рішення призначені для реалізації управління підприємством як організаційною системою, а також технологічними, економічними, інформаційними процесами на цьому підприємстві в умовах невизначеності щодо стану його внутрішнього та зовнішнього середовища.

Управлінські рішення будуються та реалізуються при виникненні проблемних ситуацій, які свідчать про невідповідність очікуваного та фактичного стану організаційної системи. На тактичному рівні управлінські

рішення впливають на процеси виробництва продукції та послуг з використанням матеріальних, трудових та інших ресурсів; розподілу ресурсів для забезпечення діяльності підприємства; обміну інформацією та знаннями для забезпечення ефективного функціонування підприємства; використання ресурсів та виробничої інфраструктури підприємства для виготовлення продукції.

Управлінські рішення формуються на основі знання-орієнтованих патернів. Узагальнений зв'язок між патернами прийняття рішень та призначенням цих рішень представлено у таблиці.

Таблиця. Зв'язок між патернами прийняття рішень та призначенням управлінських рішень

Патерни прийняття рішень	Результуючі рішення
1. Формальні правила виконання дій	Типові рішення без врахування поточного стану предметної області
2. Формальні правила виконання дій, базовий критерій ефективності дій	Спрощені рішення з метою скорочення часу їх виконання
3. Базова модель процесу/задачі	Рішення про послідовність дій, що відповідають прогнозованому стану предметної області
4. Розширена неформальними даними модель процесу/задачі	Прийняття рішення після уточнення або використання додаткових вхідних даних
5. Персональні знання щодо моделі процесу/задачі	Прийняття нових ефективних рішень, що не передбачені базовими правилам та моделями

Зазначимо, що формальні правила перших трьох рівнів можуть бути представлені як каузальними, так і темпоральними залежностями. Шаблони 4 та 5 рівнів базуються на неформальних персональних знаннях, вилучення яких традиційними методами потребує значних витрат часу експертів та інженерів знань. Однак вони можуть бути єдиним чином описані у вигляді сукупності темпоральних залежностей.

Розглянемо структуру управлінського рішення з урахуванням темпоральних залежностей між станами об'єкту управління.

Управлінське рішення П містить послідовність управляючих дій u_j^{j-1}, які визначають послідовність переходів між послідовними станами s_{j-1}, s_j об'єкту управління у моменти часу τ_{j-1} та τ_j відповідно:

$$u_j^{j-1} : s_{j-1} \to s_j,\ \tau_{j-1} < \tau_j, \tag{1}$$

$$\Pi = \left\langle u_1^0, ..., \mathrm{u}_j^{j-1}, \mathrm{u}_{j+1}^j, ..., \mathrm{u}_{aim}^J \right\rangle \Leftrightarrow \left\langle s_0, ..., \mathrm{s}_{j-1}, \mathrm{s}_j, \mathrm{s}_{j+1}, ..., s_J, s_{aim} \right\rangle. \tag{2}$$

Кожен стан s_j об'єкту управління визначається множиною значень α_j^k змінних a_j^k, які є атрибутами елементарних об'єктів – артефактів [6] Af_m:

$$s_j = \left\{ a_j^k : \forall a_j^k \ \exists Af_m \right\}. \tag{3}$$

Знання про реалізоване рішення П представлені темпоральними R та контекстно-темпоральними залежностями $R^{(A)}$:

$$R = \{r_1^0, ..., r_{j-1}^0, r_j^0, r_{j+1}^0, ..., r_J^0, r_{aim}^0, ..., r_{j+1}^j, ..., r_J^j, r_{aim}^j, ..., r_{aim}^j : \forall j\ \tau_{j-1} < \tau_j\}, \tag{4}$$

$$R^{(A)} = \left\{ r_j^{(A)} : \forall s_j \forall a_j^k \in A\ a_j^k = \alpha_j^k, a_{j-1}^k \neq \alpha_j^k \right\}. \tag{5}$$

Темпоральні залежності визначають зв'язки між станами об'єкту управління в цілому, без виділення окремих артефактів. Зазначимо, що значення властивостей цих артефактів в моменти часу τ_j визначають стани s_j. Кожна залежність виду r_{j+1}^j задає зв'язок у часі між парою послідовних станів s_j та s_{j+1}, а залежності виду s_j – зв'язки між парою станів, між якими є інші стани. Контекстна залежність $r_j^{(A)}$ визначає умови виникнення стану s_j, оскільки враховує властивості атрибутів артефактів, що змінюються в момент виникнення цього стану. Іншими словами, контекстна темпоральна залежність задає зв'язки між станами, пов'язані із зміною контексту. Контекст у даному випадку представлений апріорно визначеною підмножиною артефактів.

III. Висновки

Запропоновано модель управлінського рішення у вигляді послідовності управляючих дій, що визначає послідовність станів об'єкту управління. Відношення між цими станами задаються темпоральними залежностями та контекстними темпоральними залежностями. Перші задають послідовність виникнення у часі для пар станів об'єкту управління. Контекстні темпоральні залежності визначають зв'язки у часі між станами для підмножини елементарних об'єктів – артефактів та відображають зміну контексту виконання управляючих дій.

Практичне значення отриманих результатів полягає у можливості побудови множини альтернативних управлінських рішень на основі визначених темпоральних правил. Вказані правила визначають знання-орієнтовану структуру управлінського рішення, що є інваріантною до предметної області.

Перелік Посилань

[1] K. C. Laudon, J. P. Laudon, "Essentials of Management Information Systems". Prentice-Hall, Inc, 2007, 586 p.

[2] C.K. Oduoza. "Decision support system based on effective knowledge management framework to process customer order enquiry", in Chiang, S. Jao(Eds), Decision Support Systems, INTECH, Croatia, 2010, p. 406.

[3] O. Kalynychenko, S. Chalyi, Y. Bodyanskiy , V. Golian, N. Golian, "Implementation of search mechanism for implicit dependences in process mining" 2013 IEEE 7th International Conference on Intelligent Data Acquisition and Advanced Computing Systems (IDAACS), Institute of Electrical and Electronics Engineers (IEEE), 2013. Available at: www/URL:https://doi.org/10.1109/idaacs.2013. 6662657.

[4] Dalkir K. "Knowledge Management in Theory and Practice", Burlington, Massachusetts: Elsevier Butterworth-Heinemann, 2005, 372 p.

[5] V. Levykin, O. Chala "Method of determining weights of temporal rules in markov logic network for building knowledge base in information control system", EUREKA: Physics and Engineering, 2018, №.5, pp. 3-10. DOI: http://dx.doi.org/10.21303/2461-4262.2018.00713.

[6] D. Cohn, R. Hull, "Business artifacts: A data-centric approach to modeling business operations and processes", bulletin of the IEEE Computer Society Technical Committee on Data Engineering, 2009, vol. 32(3), pp.1–7.

Analysis of Requirements for Explanations of Recommendations in E-Commerce Systems

Leshchynskyi Volodymyr Oleksandrovich [1],
Leshchynska Irina Oleksandrivna [2]

[1]*Kharkiv National University of Radio Electronics, 14 Nauky Ave, Kharkiv UA-61166, Ukraine, volodymyr.leshchynskyi@nure.ua*

[2]*Kharkiv National University of Radio Electronics, 14 Nauky Ave, Kharkiv UA-61166, Ukraine, iryna.leshchynska@nure.ua*

Abstract. *The problem of explaining the recommendations of goods and services in the e-commerce system is considered. It has been shown that it is necessary to analyze the indicators to evaluate the explanations to the recommendations and to formulate requirements for these explanations. As a result of the analysis, the groups of indicators characterizing the interaction of users and owners with the system of e-commerce are highlighted, as well as an opportunity to evaluate the usefulness of explanations for consumers. The requirements for explanations in the e-commerce system are formulated. The implementation of these requirements is evaluated using selected indicators groups.*

Keywords: *recommendations, explanations, recommender subsystems, personalization of sales, e-commerce.*

I. Introduction And Problem Statement

Recommendations in e-commerce systems look like relevant list of goods and services for the current user [1]. When constructing these recommendations, the similarity of goods or users is analyzed. For formation of such a list the reference subsystem is used. It uses two types of input data. Firstly, the ratings of the goods formed by the user of the electronic commerce system are taken into account. Secondly, information is used on the choice of the consumer of certain goods.

Recommendations make it possible to form a personal set of goods of interest to the current consumer. It simplifies customer search and increases sales of e-commerce systems.

However, to improve the efficiency of consumer choice, the explanation of the proposed recommendations is used. Such explanations help to simplify the selection and purchase of goods as they can better understand whether the proposed product meets their needs [2]. As a result, consumer confidence in the e-commerce system increases. It uses this system for further purchases.

The use of explanations gives an opportunity to withstand artificial changes in the rating. Such changes are used by intruders to promote certain products and services [3]. This may lead to false recommendations that are not in line with his interests.

Approaches to construction recommendations in e-commerce systems are intensively developing during the current decade. Opportunities for standard explanations of recommendations are used in the Amazon e-commerce system. For today, key efforts in this direction are aimed at simplifying explanations for the consumer [4].

This indicates the importance of analyzing the requirements for explaining the recommendations in order to determine the properties of these explanations that simplify the choice for the consumer.

II. Problem solution and Results

The purpose of this report is to define the requirements for explaining the recommendations in order to identify the relationship between the characteristics of the explanation and the choice of the consumer.

To achieve the goal you need to solve the following tasks:

– the analysis of the characteristics of recommendations in e-commerce systems;

– the integration of existing criteria for assessing explanations of recommendations;

– the analysis and additions to the existing requirements for the explanation of the recommendations, taking into account the indicators of their assessment.

The criteria for assessing the explanation are given in [5]. The specified criteria are intended for a qualitative assessment of how the recommendation subsystem works, how the user interacts with this subsystem, whether the user can trust the recommendations, or makes the explanation given to choose specific products and services, or increases the speed of consumer choice, etc.

The conducted analysis of the criteria allows you to select the following groups:

– The indicators of interactive interaction with the user based on the explanation of the recommendations issued;

– The indicators of support for the user's choice in the e-commerce system;

– The indicators to assess the convenience of using explanatory recommendations.

The first group includes indicators: transparency, scrutability, trust.

The transparency indicator is designed to assess whether the recommendation subsystem helps the user to understand how the recommendations were generated [5]. Was the similarity between the users used, or the similarity between the goods is taken into account.

Such an indicator is used, in particular, in expert systems. The conclusions in such systems are realized through a logical conclusion on heuristic rules. Such rules may have inaccurate or false cause-and-effect dependencies obtained as a result of knowledge extraction from experts in a given subject area. Therefore, the clarity of the explanation enables the user to make sure that there are no inconsistencies in the received recommendations regarding the goods and services.

The evaluation of this indicator is to establish the user's understanding of the scheme of work of the advisory subsystem. Interviews with users of the e-commerce system are conducted to test the understanding.

Scrutability gives you an opportunity to take into account that the user can change his interests [8]. That is, depending on the received explanations the user can specify the list of necessary goods and services.

The sequence of the formation and clarification of explanations using these indicators includes the following steps:

1) Formation of recommendations in the e-commerce system;

2) Formation of explanations of recommendations;

3) check the understanding of the explanations by the user; the expert is conducting an examination through a user survey;

4) Clarification of the explanation by the expert.

The difficulty in using such an indicator lies in the fact that it reflects the personalized understanding of the current user. That is, you need to perform a cyclical refinement of the recommendations for a set of users. Otherwise, new consumers will not have an accurate understanding: how the list of goods and services was formed.

The trust indicator [3, 5] is intended to assess the degree of trust of users to the recommendations received, as well as the process of forming these recommendations.

The peculiarity of using this indicator is that users trust the subsystem of recommendations in case they choose the recommended goods or services.

To determine this indicator, an e-commerce user survey is conducted. The disadvantage of this approach is that trust does not always depend on user behavior. Therefore, it is additionally necessary to identify implicit factors that relate trust and consumer behavior. An alternative approach to determining consumer confidence is to count the sessions of interaction with the e-commerce system.

In general, the first set of indicators gives an opportunity to evaluate the interaction of the user - system of e-commerce from the user's side.

The second set of metrics is designed to evaluate the user's interaction with the e-commerce system from the owner of this system. This group contains effectiveness, persuasiveness.

The first indicator determines the effect of the explanations received on the choice of the product or the refusal of the consumer's choice. Efficiency is estimated as an increase in the number of sales using explanations compared to the number of sales based on recommendations without explanation.

The second indicator determines the more precise choice of goods by the consumer as a result of the received explanations. For example, explanations are effective if the buyer chose a new product, new season clothes, a higher quality product with a higher price, etc.

E-commerce rankings are used to evaluate this indicator before and after providing explanations. Also, a metric that determines an increase in the amount of purchases after receiving an explanation, an increase in purchases since the explanation, an increase in purchases for the selected product group, etc. can also be used.

The last set of indicators is intended to assess the capabilities of the advisory subsystem from the consumer's point of view. This group contains efficiency and satisfaction.

The first indicator is designed to estimate the cost of time to make decisions by the consumer. That is, the more efficiency, the faster the user chooses goods and services.

This indicator is primarily intended to measure interactive recommendations. The formation of interactive recommendations is a multi-step process. At each step, as a result of interaction with the consumer, the recommended list of goods and services is specified. Therefore, this indicator is calculated as the total time for finding recommendations. You can also estimate the number of refinement cycles for interactive recommendations with explanations in comparison with the number of cycles of detailing recommendations without explanation. The use of this indicator makes it possible to implement adaptive formulation of explanations of recommendations. That is, to reduce the time of refinement, the user can only get the most important explanations in this state. This reduces the time spent by the user of the e-commerce system.

The satisfaction indicator [5] is designed to evaluate the ease of use of the e-commerce system. The assessment of satisfaction is traditionally performed by conducting a survey of users. Also, for this evaluation, consumer comments about the work of the e-commerce system are used.

The integral estimate is calculated as the ratio of positive and negative comments. Also, when determining satisfaction, it is advisable to take into account the relationship between the number of pages viewed and the quantity or amount of selected goods. Then the metric is calculated as the ratio of the number of items viewed for one purchase without explanation and using explanations. Obviously, the effect of explanations on satisfaction increases with the decrease of this indicator.

The analysis of indicators for assessing explanations of recommendations in e-commerce systems shows that recommendations should meet the following requirements:

1) Ability to interactively refine the recommendations using the transparency, scrutability metrics under the threshold of trust.

2) Increase the effectiveness rate with the minimum value of persuasiveness.

3) Increase satisfaction with a given threshold of efficiency.

The combination of these requirements allows determining the parameters of interaction between the consumer and the owners of the electronic commerce system, and then optimizing all other metrics.

III. CONCLUSIONS

The analysis of indicators for assessing explanations of recommendations in the system of e-commerce is carried out. As a result of the analysis, indicators for assessing explanations of recommendations are grouped into groups that characterize the interaction of users with the e-commerce system, owners with the e-commerce system, as well as the usefulness of explanations for consumers. Based on the integration of indicators, requirements for explanations in the e-commerce system are formulated.

REFERENCES

[1] C. Aggarwal “Recommender Systems: The Textbook”, New York: Springer, 2017, 498 p.

[2] S. Cleger-Tamayo, J. M. Fernandez-Luna, J. F Huete “Explaining neighborhood-based recommendations”, in The 35th International ACM SIGIR conference on Research and development in information retrieval, ACM, 2012, pp. 1063–1064.

[3] I. Shilling “Attack detection for recommender systems based on credibility of group users and rating time series”, https://doi.org/10.1371/journal.pone.0196533 [Published: May 9, 2018].

[4] F. Gedikli, D. Jannach, M. Ge “How should i explain? A comparison of different explanation types for recommender systems” in International Journal of Human-Computer Studies, 2014, № 72(4), pp. 367–382.

[5] N. Tintarev, J. Masthoff “Evaluating the effectiveness of explanations for recommender systems”, in User Modeling and User-Adapted Interaction, 2012, № 22(4), pp.399–439.

Побудова Багатошарового Ситуаційного Представлення Вибору Споживача Рекомендаційної Системи

Чалий Сергій Федорович [1],

Прібильнова Інна Борисівна [2]

[1]*Kharkiv National University of Radio Electronics, 14 Nauky Ave, Kharkiv UA-61166, Ukraine, serhii.chalyi@nure.ua*

[2]*Kharkiv National University of Radio Electronics, 14 Nauky Ave, Kharkiv UA-61166, Ukraine, inna.butsukina@nure.ua*

Анотація. *Розглянуто проблему підтримки вибору споживача товарів та послуг шляхом формування рекомендацій у вигляді упорядкованого за рейтингом переліку товарів, що можуть бути цікавими цьому споживачеві. Запропоновано комбінувати підходи на основі характеристик споживача та характеристик товарів на основі ситуаційного представлення вибору споживача у вигляді багатошарового графу. Кожен шар є дводольним графом, який визначає зв'язок користувача з товарами та послугами на різних рівнях деталізації або з урахуванням відомих характеристик цих товарів. Запропоновано підхід до побудови ситуаційного представлення на основі виявлення близькості споживачів на кожному шарі. Підхід дає можливість відібрати підмножини цікавих для споживача товарів та послуг за комплексом їх характеристик, в тому числі на різних рівнях опису.*

Ключові слова: *рекомендаційна система, рекомендації на основі контенту, рекомендації на основі близькості користувачів, багатошаровий граф.*

I. Вступ Та Постановка Задачі

Рекомендаційні системи спрощують вибір споживачів в системах електронної комерції. Вони формують рекомендації у вигляді упорядкованого переліку цікавих для споживача товарів та послуг [1].

Підходи до формування такого переліку використовують оцінки схожості споживачів або товарів [2]. Однак існуючі підходи не враховують ситуативність вибору споживача. Остання може бути визначена на основі комбінації властивостей товарів та споживачів, що робили покупки на заданому інтервалі часу.

Зазначене свідчить про актуальність побудови ситуаційного представлення вибору споживача.

Метою роботи є розробка підходу до побудови багатошарового представлення вибору споживача з урахуванням комплексу характеристик товарів та послуг.

II. Результати Дослідження

Запропонований підхід поєднує item-based user-based підходи до опису вибору споживача в рекомендаційних системах та базується на ситуаційному представленні вибору споживача. Кожна ситуація вибору може бути розглянута у аспекті схожості характеристик товару, які вибирає споживач, а також у аспекті схожості споживачів. Тому ситуаційне представлення має вигляд дводольного багатошарового графу. Кожен шар містить вершини, що відповідають споживачам, та вершини, що відповідають властивостям товарів. Шари зв'язані між собою через вершини, що відповідають споживачам.

Дводольний граф кожного шару містить вершини типів $User_i$ та $Item_j$. Вершини першого типу задають властивості споживача, а другого – товарів та послуг. Дуги графу визначають тип зв'язку. Наприклад, для першого, базового шару графу використовуються такі типи зв'язку:

– $Rating_{ij}$ у випадку, якщо споживач $User_i$ у відгуку поставив оцінку конкретному товару $Item_j$;

– $Quantity_{ij}$, тобто кількість покупок товару $Item_j$ споживачем $User_i$ у випадку відсутності зворотного зв'язку.

Послідовність побудови наведеного ситуаційного представлення містить у собі такі фази.

Фаза 1. Відбір споживачів, що є близькими за інтересами. Відбір виконується на основі порівняння оцінок або покупок товарів. Критерієм схожості користувачів є відмінність оцінок в межах одного балу, або покупка тих же товарів. В якості метрики доцільно використати відношення схожих оцінок або покупок до загального масиву оцінок (покупок). Дана фаза виконується для кожного шару ситуаційного представлення вибору споживача.

Фаза 2. Упорядкування товарів за рейтингом на кожному шарі ситуаційного представлення. В результаті виконання даної фази виникає можливість запропонувати споживачеві вибір товарів за різними їх характеристиками та на різних рівнях групування цих характеристик.

Фаза 3. Інтеграція рекомендацій, що отримані на фазі два. На даній фазі можливим є використання двох стратегій: виділення рекомендацій на основі перетину або об'єднання переліків товарів та послуг для кожного шару ситуативного представлення.

III. Висновки

Запропоновано підхід до побудови багатошарового ситуаційного представлення вибору споживача рекомендаційної системи, який дозволяє поєднати вибір схожих споживачів на основі врахування комплексу характеристик товарів та послуг.

Перелік Посилань

[1] F. Ricci, L. Rokach, B. Shapira "Recommender Systems Handbook", Springer, 2011, 1008p.

[2] C. Aggarwal "Recommender Systems: The Textbook", New York: Springer, 2017, 498 p.

Метод логічно-інформаційного представлення технічного завдання для автоматизованої системи проектування ПП

Євсєєв Владислав В'ячеславович
Харківський національний університет радіоелектроніки, пр. Науки 14, Харків, 61166, Україна, vladyslav.yevsieiev@nure.ua

Демська Наталія Павлівна
Харківський національний університет радіоелектроніки, пр. Науки 14, Харків, 61166, Україна, nataliia.demska@nure.ua

Бортнікова Вікторія Олегівна
Харківський національний університет радіоелектроніки, пр. Науки 14, Харків, 61166, Україна, viktoriia.bortnikova@nure.ua

Анотація. *В роботі розглянуто метод уявлення технічного завдання у вигляді безлічі взаємозалежних параметрів, які в сумі дають можливість окреслити ПП, що розробляється, запропонована логічна-інформаційна структура, наведено приклад конструкції листа ТЗ для мови програмування Pascal.*

Ключові слова: *проектування, програмний продукт, технічне завдання.*

I. Вступ

Аналіз сучасних систем автоматизованого проектування програмних продуктів (ПП) [1] показав, що використання багатомодульного підходу дозволить зменшити навантаження на систему, збільшити максимальну точність проектування на базі незалежної обробки даних в кожному модулі, проводити аналіз і дослідження отриманих результатів, вносити корективи на кожному етапі проектування, що дасть можливість відстежувати виникнення помилок на всіх етапах проектування технічного завдання (ТЗ) аж до етапу генерації вихідного коду.

II. Розробка структури технічного завдання

Запропонована нова модель життєвого циклу «Jump» заснована на максимально повному заповненні ТЗ спільно замовником і розробником. Лист ТЗ повинен представляти вимоги до ПП, що розробляється, повністю описувати його функціональність, специфіку і додаткові функції які можна буде інтерпретувати в запити до бази знань за допомогою запропонованих математичних моделей і методів прийняття рішень [2].

Виходячи з цього, був розроблений метод уявлення ТЗ у вигляді безлічі взаємозалежних параметрів, які в сумі дають можливість окреслити ПП що розробляється на базі простої природної мови в інтуїтивно зрозумілому форматі, на базі стандартних прикладних програмних рішень, які узгоджуються з міжнародним форматом експорту/імпорту даних, при цьому мати структуроване представлення даних.

Аналіз таких прикладних програм показав, що для зручного представлення даних ТЗ підходить MS Excel (формат файлу *.xls), який дозволяє представляти дані у вигляді жорстко структурованих таблиць з прив'язкою до кожного осередку необхідних параметрів. Також MS Excel дає можливість розширення ТЗ до будь-яких необхідних обсягів вхідної інформації, в залежності від складності розроблюваного ПП і його функціональних рішень.

Структуризація ТЗ відповідно до запропонованих рішень можна уявити як складнопідрядну структуру з прив'язкою до подій, які виникають при роботі з інтерфейсом користувача. На рис. 1 представлено структурно залежне логічно-інформаційне уявлення ТЗ. Представлена концепція побудована на застосуванні графічних елементів інтерфейсу як базового носія інформації про проектований ПП.

Під $Form_1$ розуміється головна форма програми, яка характеризується сукупністю основних блоків: «$Form_1$ *propertied and evens*», «*Components on* $Form_1$ *strcture*». Блок «$Form_1$ *propertied and evens*» складається з взаємозв'язаних структурних елементів: «*Main propertied*»: параметри $mp_1,\ldots, mp_n \rightarrow$ «*Properties parameters*»: значення $pp_1,\ldots, pp_n$. Кожному mp_1 відповідає одне значення pp_1, яке може приймати значення в вигляді n де $n=1,2,3,..,m$, логічних операцій (*false, true*) або зарезервованих параметрів опису значень під певну мову високого рівня програмування (Top, Batten, и т.д.). Набір таких параметрів строго обмежений і несе в собі інформацію про умови візуального відображення $Form_1$ для користувача. Блок «*Main events*» являє собою сукупність подій me_1, $me_2,\ldots,me_n$, які можна накласти на $Form_1$ при обробці дій над нею у вигляді «*Create form*», «*Close form*» і т.п., набір подій і параметрів у вигляді програмного коду строго визначений для кожної мови і середовища розробки. Кожному події me_1, $me_2,\ldots,me_n$ відповідає подія ea_1, $ea_2,\ldots,ea_n$ блоку «*Events on action whit Form*» який може приймати значення у вигляді функцій і процедур взаємодії з користувачем, які описані у вигляді програмного коду обмеження використання [3], такі як на блок «*Main events*», або на подію me_1, $me_2,\ldots,me_n$.

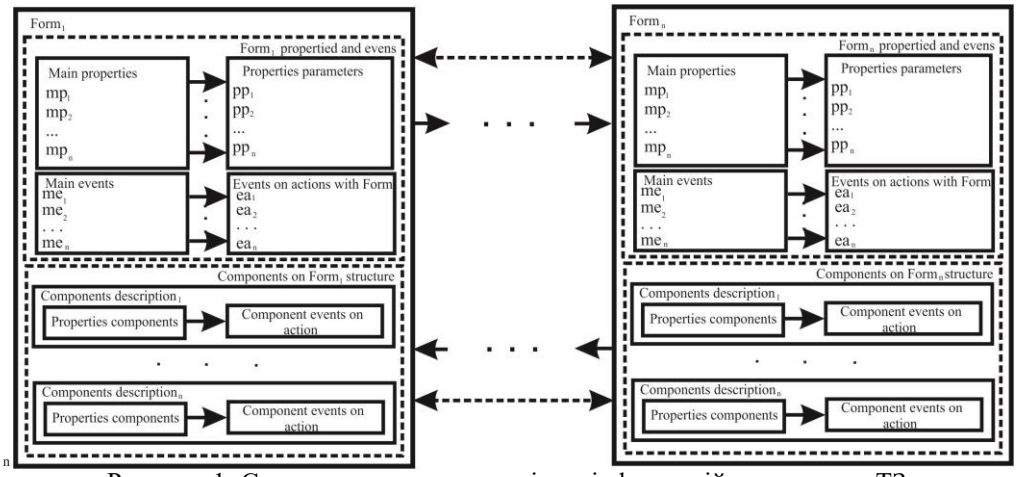


Рисунок 1. Структурно залежне логічно-інформаційне уявлення ТЗ

Кожний *Form₁* має нескінченний набір «*Components on Form₁ structure*» і являє собою структуру *Form₁* у вигляді дерева побудови, де кожен елемент дерева являє собою набір візуальних компонентів призначених для роботи з даними і елементами групування (елементи вводу (Edit), відображення даних (Grid), елементи інтерфейсу (Menu), елементи групування (Group). Кожен елемент в блоці «*Components description₁*», представляє взаємозв'язок «*Properties components*» → «*Components events on action*» і ґрунтуючись на запропонованій структурі «*Properties components*» має такі ж властивості як і елемент «*Main propertied*», але при цьому «*Components events on action*» володіє нескінченною варіацією дій (звернення до БД, розрахунки, закриття форми, і т.д). Залежно від загальної структури побудови ПП (кількість елементів *Form₁*) необхідно врахувати передачу глобальних змінних і функцій переходу між вікнами, внаслідок чого взаємодія між елементами *Form* має бути враховано в рамках всього процесу розробки продукту. В середньому кількість елементів *Form* може коливатись від 1…25-30 і вище, а також вони можуть викликатися спливаючими всередині головної *Form₁* і посилатися на неї.

Ґрунтуючись на запропонованій логічно-інформаційній структурі і середовищем проектування ТЗ наведемо приклад конструкції листа ТЗ для мови програмування Pascal (середовище розробки Red Studio X5) (рис. 2). Фрагмент блоку «*Form₁ propertied and evens*» → «*Main propertied*» та «*Properties parameters*», «*Main evens*» → «*Evens on action with Form₁*» наведено на рисунку 3, а фрагмент блоку «*Components on Form₁ strcture*» → «*Components description₁*» на рисунку 4.

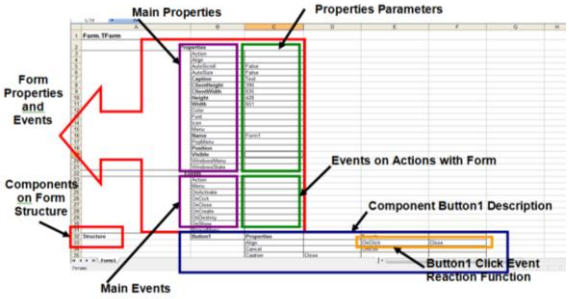


Рисунок 2. Фрагмент ТЗ для мови Pascal в середовищі розробки Red Studio X5

1	Form1.TForm		
2	Properties		
3		Action	
4		Align	
5		AutoScroll	False
6		AutoSize	False
7		**Caption**	Test
8		**ClientHeight**	390
9		**ClientWidth**	635
10		**Height**	428
11		**Width**	651
12		Color	
13		Font	
14		Icon	
15		Menu	
16		**Name**	Form1
17		PopMenu	
18		**Position**	
19		**Visible**	
20		WindowsMenu	
21		WindowsState	
22	Events		
23		Action	
24		Menu	
25		OnActivate	
26		OnClick	
27		OnClose	
28		OnCreate	
29		OnDestroy	
30		OnShow	
31		PopupMenu	

Рисунок 3. Фрагмент блоку «*Form₁ propertied and evens*» → «*Main propertied*» та «*Properties parameters*», «*Main evens*» → «*Evens on action with Form₁*»

31		PopupMenu			
32	Structure	Button1	Properties		Events	
33			Align		OnClick	Close
34			Cancel		OnExit	
35			Caption	Close		
36			Font			
37			Height	25		
38			Left	552		
39			Top	357		
40			Width	75		
41			DropDownMenu			

Рисунок 4. Фрагмент блоку «*Components on Form₁ strcture*» → «*Components description₁*»

III. Висновки

Запропоноване рішення дозволяє спростити структуру листа ТЗ, використовувати інтуїтивно зрозумілий опис елементів *Form₁*, врахувати дерево побудови і всі елементи необхідні для візуалізації та роботи з даними, також запропонований метод дає можливість вести проектування на формальній мові, що спрощує роботу з замовником шляхом безпосередньої участі його при складанні ТЗ.

Список використаних джерел

[1] Лавріщева, К. М., & Стеняшин, А. Ю. (2013). Індустріальний підхід до розробки і виконання прикладних систем в гетерогенних розподілених середовищах. In *International Conference «Parallel and Distributed Computing Systems* (pp. 196-204).

[2] Невлюдов, І. Ш., Євсєєв, В. В., & Демська, А. І. (2018). Розробка синтаксичної та семантичної моделі мови визначення і опису даних предметної області // II Міжн. нук.-техн. конф. «Виробництво & Мехатронні системи» (M&MS-2018). – Харків, 2018. – 2018. – С. 48–53.

[3] Евсеев, В. В. (2011). Применение программных метрик кода на раннем этапе жизненного цикла программного обеспечения. *Восточно-европейский журнал передовых технологий*, (1 (2)), 19-21.

Узагальнена модель моніторингу та управління експлуатацією інформаційної системи

Левикін Віктор Макарович[1]
[1]Харківський національний університет радіоелектроніки, пр. Науки 14, Харків, 61166, Україна, viktor.levykin@nure.ua

Євланов Максим Вікторович[2]
[2]Харківський національний університет радіоелектроніки, пр. Науки 14, Харків, 61166, Україна, maksym.ievlanov@nure.ua

Неумивакіна Ольга Євгеніївна[3]
[3]Харьковский национальный университет радиоэлектроники, пр. Науки 14, Харьков, 61166, Украина, olga.neumyvakina@nure.ua

Петриченко Олександр Вячеславович[4]
[4]Харьковский национальный университет радиоэлектроники, пр. Науки 14, Харьков, 61166, Украина, oleksandr.petrychenko@nure.ua

Abstract. *The main problems of representation of information system design architectural framework are considered. The task of modeling an architectural framework for knowledge-oriented development of information systems is formulated. A theoretical-category model of an architectural framework is proposed. The main way of practical implementation of the architectural framework model is proposed.*

Keywords: *architectural framework, information system, generating pattern, model, theory of cathegories.*

I. Вступ Та Постановка Задачі Моделювання Моніторингу Та Експлуатації Web-Базованої Інформаційної Системи

Сучасні стратегії розвитку IT-компаній передбачають перевід переданих у експлуатацію інформаційних систем до розряду так званих «дійних корів» – IT-продуктів, підтримка та супроводження яких вимагає від IT-компанії значно менших фінансових витрат, ніж прибутки від підприємств-споживачів цих IT-продуктів, які надходять до IT-компанії. Тому головною метою управління експлуатацією інформаційних систем та їх компонентів є підвищення ефективності експлуатації цих систем та їх компонентів одним з наступних шляхів:

а) підвищення при сталих витратах прибутків від експлуатованих інформаційних систем за рахунок пропонування функціональних можливостей цих систем новим споживачам або пропонування вже існуючим споживачам нових функціональних можливостей, які раніше були відсутні у експлуатованих інформаційних системах;

б) скорочення при сталих прибутках витрат на експлуатацію інформаційних систем та їх компонентів за рахунок пошуку та розробки нових, ближчих до оптимуму сценаріїв, моделей, методів, алгоритмів, та версій компонентів цих систем.

Вирішення такої задачі управління експлуатацією інформаційних систем та їх компонентів вручну є дуже складним. Тому виникає необхідність автоматизованого вирішення задач моніторингу та управління експлуатацією компонентів інформаційних систем, які дозволили б підвищити прибуток IT-компанії-постачальника цих систем за рахунок підвищення ефективності експлуатації їх компонентів.

Особливо важливою ця задача стає для управління експлуатацією web-базованих інформаційних систем, головною особливістю яких слід вважати відсутність будь-яких клієнтських частин і розміщення основних компонентів системи на одному чи кількох серверах. Ця особливість спричиняє значне підвищення навантаження на серверну частину системи порівняно з класичними клієнт-серверними інформаційними системами.

Тому основною задачею даного дослідження є розробка узагальненої моделі, яка буде визначати головні архітектурні особливості інформаційної технології моніторингу та управління експлуатацією web-базованих інформаційних систем.

II. Розробка Узагальненої Моделі Моніторингу Та Експлуатації Web-Базованої Інформаційної Системи

Основні особливості процесів управління експлуатацією будь-яких інформаційних систем і технологій на теперішній час викладено в стандарті ISO 20000. Цей стандарт є міжнародним процесно-орієнтованим стандартом управління IT-послугами. Мета створення цього стандарту полягала в створенні універсальних критеріїв, за допомогою яких будь-яка фірма чи служба, що надає IT-послуги, зможе оцінювати їх ефективність та виконання вимог замовників з врахуванням їх бізнесу [1, 2].

В цілому роботи з моніторингу та управління експлуатацією web-базованою інформаційною системою та її окремими компонентами зазвичай розглядаються як окремі варіанти IT-проекту. Цей IT-проект ініціюється під час виконання технічних процесів життєвого циклу системи, пов'язаних з організацією експлуатації інформаційної системи та супроводження цієї системи IT-компанією-розробником.

Тому в загальному випадку задачу управління експлуатацією web-базованої інформаційної системи слід розглядати як окремий випадок задачі управління IT-проектом, яка в загальному випадку буде мати такий вигляд:

$$F_{Pr} = \sum_{i=c+1}^{e} r^{Pr}(K_i^{f_{Pr}}) \to max, \quad (1)$$

$$F_U = \sum_{i=c+1}^{e} r^{U}(K_i^{f_U}) \to max, \quad (2)$$

при виконанні умов

$$\begin{cases} \sum\limits_{i=c+1}^{e} \alpha_i^{Pr}\, pay(PM(K_i^{f_{IS}}, K_i^{f_{Pr}})) \geq pay^*(PM(K_i^{f_{IS}}, K_i^{f_{Pr}})); \\ \sum\limits_{i=c+1}^{e} \beta_i^{Pr}\, t(PM(K_i^{f_{IS}}, K_i^{f_{Pr}})) \leq t^*(PM(K_i^{f_{IS}}, K_i^{f_{Pr}})); \\ \sum\limits_{i=c+1}^{e} \gamma_i^{Pr}\, q(PM(K_i^{f_{IS}}, K_i^{f_{Pr}})) \geq q^*(PM(K_i^{f_{IS}}, K_i^{f_{Pr}})), \end{cases} \quad (3)$$

$$\begin{cases} \sum\limits_{i=c+1}^{e} \alpha_i^{U}\, pay(PM(K_i^{f_{IS}}, K_i^{f_{U}})) \leq pay^*(PM(K_i^{f_{IS}}, K_i^{f_{U}})); \\ \sum\limits_{i=c+1}^{e} \beta_i^{U}\, t(PM(K_i^{f_{IS}}, K_i^{f_{U}})) \leq t^*(PM(K_i^{f_{IS}}, K_i^{f_{U}})); \\ \sum\limits_{i=c+1}^{e} \gamma_i^{U}\, q(PM(K_i^{f_{IS}}, K_i^{f_{U}})) \geq q^*(PM(K_i^{f_{IS}}, K_i^{f_{U}})), \end{cases} \quad (4)$$

де $K_i^{f_{Pr}}$ – представлення на рівні знань функціональної вимоги tr_i^f з точки зору постачальника IT-послуг; $K_i^{f_U}$ – представлення на рівні знань функціональної вимоги tr_i^f з точки зору споживача IT-послуг; $PM(K_i^{f_{IS}}, K_i^{f_{Pr}})$ – функція розрахунку обсягу робіт зі створення інформаційної системи з точки зору постачальника IT-послуг; $PM(K_i^{f_{IS}}, K_i^{f_U})$ – функція розрахунку обсягу робіт зі створення інформаційної системи з точки зору споживача IT-послуг;

Детально елементи цільових функцій розглянуто у [3].

Головною відмінністю управління експлуатацією інформаційної системи від управління її проектуванням слід визнати надходження під час експлуатації від споживача IT-послуг системи до постачальника IT-послуг цієї ж системи запитів на зміни (request for change, RFC). Ці RFC визначають не тільки нові функціональні вимоги до експлуатованої інформаційної системи, а й нові нефункціональні вимоги до цієї ж системи. При цьому основними цілями управління експлуатацією інформаційної системи за [2] слід вважати:

а) зведення кількості RFC, які надходять від споживача IT-послуг, до необхідного мінімуму, який визначається впливом зовнішніх для споживача факторів чи довгостроковою програмою розвитку IT-інфраструктури споживача;

б) зведення кількості RFC, які не були виконані постачальником IT-послуг або у виконанні яких постачальником IT-послуг споживачу IT-послуг було відмовлено, до нуля.

Тоді функції цілі (1) та (2) можна представити у вигляді:

$$F_{Pr} = \begin{cases} \sum\limits_{i=c+1}^{e} K_i^{tr_{Pr}}(RFC_i) \to min; \\ \sum\limits_{i=c+1}^{e} \overline{K}_i^{tr_{Pr}}(RFC_i) \to 0. \end{cases} \quad (5)$$

$$F_U = \begin{cases} \sum\limits_{i=c+1}^{e} K_i^{tr_U}(RFC_i) \to min; \\ \sum\limits_{i=c+1}^{e} \overline{K}_i^{tr_U}(RFC_i) \to 0. \end{cases}, \quad (6)$$

де RFC_i – і-й запит на зміну експлуатованої інформаційної системи; $K_i^{tr_{Pr}}(RFC_i)$ – представлення на рівні знань вимоги на зміну експлуатованої інформаційної системи з точки зору постачальника IT-послуг; $K_i^{tr_U}(RFC_i)$ – представлення на рівні знань вимоги на зміну експлуатованої інформаційної системи з точки зору постачальника IT-послуг; $\overline{K}_i^{tr_{Pr}}(RFC_i)$ – представлення на рівні знань вимоги на зміну експлуатованої інформаційної системи, яку постачальник IT-послуг не зміг виконати; $\overline{K}_i^{tr_U}(RFC_i)$ – представлення на рівні знань вимоги на зміну експлуатованої інформаційної системи, у виконанні якої споживачу IT-послуг було відмовлено постачальником IT-послуг.

Аналогічно змінюються і системи обмежень (3) та (4).

III. Висновки

Використання узагальненої моделі як сукупності функцій цілей (5), (6) та змінених систем обмежень (3) і (4) дозволяє ставити та вирішувати задачу оптимального чи раціонального управління експлуатацією сучасних інформаційних систем (в тому числі – web-базованих інформаційних систем).

Використання для формалізації описів RFC представлень вимог на рівні знань дозволяє сформулювати та в подальшому вирішити проблему вибору оптимального чи раціонального набору показників експлуатації інформаційної системи чи її окремих компонентів. Моніторинг цих показників дозволить скоротити кількість RFC, що надходять від споживача IT-послуг до співробітників IT-компанії, яка є постачальником IT-послуг, за рахунок своєчасного автоматизованого чи автоматичного визначення інцидентів під час експлуатації системи та виявлення проблеми, що породила визначений інцидент.

Список Використаних Джерел

[1] Горобец, Н. ISO 20000: зрелое управление ИТ-услугами / Н. Горобец // Директор информационной службы. – 2006. – № 9. – С. 62–67.

[2] ГОСТ Р ИСО/МЭК 20000–1–2010. Информационная технология. Менеджмент услуг. Часть 1. Спецификация [Текст]. – М.: Стандартинформ, 2011. – 16 с.

[3] Левыкин В.М. Паттерны проектирования требований к информационной системе: моделирование и применение / В.М. Левыкин, М.В. Евланов, М.А. Керносов: монография. – Харьков: ООО «Компанія СМІТ», 2014. – 320 с.

Розробка концептуальної моделі сховища даних для вирішення задач Data Mining в інформаційних системах управління проектами

Васильцова Наталія Володимирівна[1]

Панфьорова Ірина Юріївна[2]

Корнєєва Євгенія Володимирівна[3]

[1]*Харківський національний університет радіоелектроніки, пр. Науки 14, Харків, 61166, Україна, nataliia.vasyltsova@nure.ua*

[2]*Харківський національний університет радіоелектроніки, пр. Науки 14, Харків, 61166, Україна, iryna.panforova@nure.ua*

[3]*Дніпровський державний проектний інститут житлового та цивільного будівництва «Дніпроцивільпроект», вул. Січеславська набережна 29-а, Дніпро, 49000, Україна, korneevae425@gmail.com*

Abstract. *The main problem of evaluating the maturity of the company's processes, which is based on the principles of project management, is formulated. As an example, we consider the problem of evaluating the maturity of an IT company, which occurs when the level of maturity of its processes increases. To solve the problem of developing a conceptual model of the project data warehouse, a process-based description of the IT project has been proposed. The main process groups and project management functions are highlighted.*

Keywords: *IT-project, process evaluation, data warehouse, maturity level, process-functional description.*

I. Вступ та постановка задачі розробки концептуальної моделі сховища даних про виконувані проекти

Майже кожна компанія, яка використовує в своїй діяльності проектні моделі та методи управління, стикається з необхідністю оцінювання своєї зрілості. Виконання такої роботи стає необхідним після виникнення у керівництва компанії за результатами аналізу поточної діяльності своїх підлеглих наступних питань:

а) «Чи існує «правильна» модель бізнес-процесів компанії?»;

б) «Як впровадити таку модель у своїй компанії?»;

в) «Які ризики виникають при переході на впроваджувану модель?»;

г) «Чи зможе компанія виконувати проект з максимальним вдоволенням вимог та дотриманням проектних обмежень?».

Головною проблемою, яка породжує ці питання, слід визнати неспроможність компанії виконувати проекти, складність яких перевищує деякий рівень (для кожної компанії свій).

Вирішення цієї проблеми полягає у створенні спеціальних інформаційних технологій та інструментальних засобів оцінювання зрілості бізнес-процесів компанії. Такі технології та засоби повинні, з одного боку, враховувати загальні правила вирішення задачі оцінювання зрілості, а з іншого боку – враховувати особливості предметної галузі, моделей і методів управління, які властиві підприємству, процеси якого оцінюються.

Цілі оцінювання зрілості процесів, які відбуваються в компанії, визначені на теперішній час стандартом ISO 15504 і формулюються таким чином [1]:

а) об’єктивне розуміння стану власних процесів компанії для їх поліпшення;

б) об’єктивне визначення придатності власних процесів компанії для конкретної вимоги або сукупності вимог;

в) об’єктивне визначення придатності процесів іншої організації для конкретного контракту або сукупності контрактів.

Очікувані вигоди від вирішення задачі оцінювання зрілості процесів компанії полягають у наступному [1]:

а) формування культури постійного поліпшення процесів і діяльностей компанії (оточення дружнього змагання для спеціалістів та компанії в цілому);

б) встановлення придатних методів для підтримки і супроводження цієї культури;

в) проектування процесів компанії для задоволення вимог бізнесу;

г) оптимізація ресурсів компанії.

Крім того, циклічне здійснення оцінювання зрілості процесів компанії є важливим інструментом розуміння ефективності технологічних процесів, які виконуються співробітниками компанії (в тому числі з використанням інформаційних систем і технологій).

Для досягнення визначених цілей та вигод в результаті оцінювання зрілості процесів компанії керівництво цієї компанії вимушено проводити аналіз великої кількості фактів щодо виконання окремих процесів і робіт проекту. Для вирішення задач подібного аналізу, а також для полегшення робіт з формування та прийняття управлінських рішень на основі результатів цього аналізу рекомендується використовувати спеціалізовані інформаційно-аналітичні системи або окремі функціональні модулі, що базуються на концепціях Data Mining та Process Mining [2].

Тому основною задачею даного дослідження є визначення особливостей розробки концептуальної моделі сховища даних, яке є основним елементом подібних інформаційно-аналітичних систем чи спеціалізованих функціональних модулів.

II. Результати дослідження особливостей побудови концептуальної моделі сховища даних про виконувані проекти

Розглянемо спочатку ситуацію виникнення необхідності вирішення задачі оцінювання зрілості

процесів компанії на прикладі підвищення рівня зрілості ІТ-компанії, яка займається випуском програмних продуктів.

Найбільш популярною моделлю оцінювання зрілості ІТ-компанії є базова модель Capable Maturity Model (CMM). Дана модель безперервно розвивалася з 1991 р. по теперішній час. Модель CMM передбачає виділення п'яти основних рівнів зрілості розробки програмних продуктів, причому для кожного з рівнів можна виділити свої головні особливості процесів проектування (ключові особливості процесів інжинірингу програмних продуктів) [3].

Найнижчим рівнем зрілості за моделлю CMM є початковий (перший) рівень. На цьому рівні здійснюється безпосереднє забезпечення виконання персоналом робіт ІТ-проекту зі створення програмного продукту. Особливостями процесів ІТ-компанії на цьому рівні є:

а) відсутність стабільних умов для створення якісного програмного продукту;

б) повна залежність результату ІТ-проекту від особистих якостей менеджера та досвіду програмістів;

в) відсутність гарантованості успіху наступних ІТ-проектів внаслідок успіху щойно виконаного ІТ-проекту;

г) різке падіння якості створюваного програмного продукту внаслідок звільнення менеджерів та програмістів;

д) зведення у стресових станах робіт з розробки програмного продукту до написання коду та його мінімального тестування.

При переході з першого на другий (повторюваний) рівень зрілості процеси ІТ-компанії повинні мати такі особливості:

а) впровадженні інформаційні технології управління ІТ-проектами;

б) планування та управління ІТ-проектом базується на накопиченому досвіді;

в) в ІТ-компанії існують стандарти на розробку програмних продуктів та забезпечується слідування цим стандартам;

г) в ІТ-компанії існує спеціальна група забезпечення якості;

д) у випадку необхідності ІТ-компанія може взаємодіяти з субпідрядниками.

Досвід переходу ІТ-компаній з першого на другий рівень зрілості вимагає виділення в системі управління ІТ-компанією таких ключових галузей управління процесами життєвого циклу програмного продукту:

а) управління вимогами до продукту;

б) планування ІТ-проекту;

в) відстеження ІТ-проекту;

г) управління діяльністю субпідрядників з розробки програмного продукту;

д) забезпечення якості програмного продукту;

е) менеджмент конфігурації програмного продукту.

В загальному випадку перехід на більш високий рівень зрілості процесів вимагає від ІТ-компанії виділення та охоплення нових ключових галузей управління шляхом створення нових функціональних задач формування та прийняття рішень з управління ІТ-проектом в цілому та його окремими галузями.

Ця особливість дозволяє визначити процес розробки концептуальної моделі сховища даних спеціалізованої інформаційно-аналітичної системи чи функціонального модуля оцінювання зрілості процесів ІТ-компанії як адаптацію типового процесно-функціонального опису ІТ-проекту до особливостей процесів конкретної ІТ-компанії.

В якості процесів виконання ІТ-проекту пропонується використовувати наведені в [4] такі групи процесів:

а) група процесів ініціації проекту;

б) група процесів планування проекту;

в) група процесів виконання проекту;

г) група процесів моніторингу та контролю проекту;

д) група процесів завершення проекту.

В якості функцій управління ІТ-проектом пропонується використовувати визначені в [4] основні аспекти управління проектом:

– управління інтеграцією проекту;
– управління змістом проекту;
– управління строками проекту;
– управління вартістю проекту;
– управління якістю проекту;
– управління людськими ресурсами проекту;
– управління комунікаціями проекту;
– управління ризиками проекту;
– управління закупівлями проекту;
– управління зацікавленими сторонами проекту.

Тоді типова концептуальна модель сховища даних спеціалізованої інформаційно-аналітичної системи чи функціонального модуля оцінювання зрілості процесів ІТ-компанії може бути представлена схемою типу «сніжинка». Вимірами цієї схеми будуть виступати описи наведених вище груп процесів та функцій управління ІТ-проектом розробки програмного продукту. Таблиця фактів цієї схеми буде базуватися на сукупності фактичних описів стану ІТ-проекту та програмного продукту під час виконання процесів зазначених вище груп з точки зору зазначених вище функцій управління ІТ-проектом.

III. ВИСНОВКИ

Отримані результати дозволяють сформулювати і в подальшому вирішити задачу створення типової спеціалізованої інформаційно-аналітичної системи чи функціонального модуля оцінювання зрілості процесів, яку можна буде використовувати для оцінювання зрілості процесів не тільки ІТ-компанії, але й будь-яких компаній та підприємств, що використовують в своїй діяльності принципи проектного управління.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

[1] ГОСТ Р ИСО/МЭК 15504-1-2009. Информационные технологии. Оценка процессов. Часть 1. Концепция и словарь. – М .: Стандартинформ, 2010. – 20 с.

[2] Барсегян, А.А. Технологии анализа данных: Data Mining, Visual Mining, Text Mining, OLAP / А.А. Барсегян, М.С. Куприянов, В.В. Степаненко, И.И. Холод. – СПб.: БХВ-Санкт-Петербург, 2008. – 384 с.

[3] Терехов, А. Современные модели качества программного обеспечения [Электронный ресурс] / А. Терехов // Сайт компании «Interface». – Режим доступа: http://www.interface.ru/fset.asp?Url=/misc/qs.htm. - Заголовок с экрана.

[4] Руководство к своду знаний по управлению проектами (Руководство PMBOK) – Пятое издание [Текст]. – Newton Square: Project Management Institute, Inc., 2013. – 586 с.

Застосування прецедентного підходу до розв’язання інцидентів в прикладній ІС

Шейна Олександр Віталійович[1],
Коптєв Олександр Олександрович[2]
Шеховцова Вікторія Іванівна[3]

[1,2,3]Харьковский национальный университет радиоэлектроники, проспект Науки 14, Харьков UA-61166, Украина,
[1]oleksandr.sheina@nure.ua,
[2]oleksandr.koptiev@nure.ua,
[3]viktoriia.shekhovtsova@nure.ua

Abstract. *On the basis of a case-law approach, solving problem situations at the apiary using automated classifier incidents and library precedents. The obtained evaluations on the results of the implementation of the proposed solution to the problem situation are used to rank the precedents in the basis of decisions, which subsequently optimizes the library of incidents and increases the efficiency of the use of the developed information system of decision-making.*

Keywords: *Incident, precedent, information system, decision-making, case-law approach.*

I. Вступ і постановка проблеми

Постановка задачі. Виробничі та життєві ситуації часто стикаються з великим різноманіттям проблемних інцидентів, що потребують швидкого та ефективного реагування. Неможливо передбачити всі фактори впливу, але можливо визначити ті, що трапляються найчастіше. Звідси виникає необхідність існування певної класифікації проблемних ситуацій. Така процедура повинна проводитись автоматично за встановленим алгоритмом. В кожній предметній області є своя специфіка, але принципи і підходи до цього процесу мають бути однаковими і вони потребують своєї формалізації. При умові правильного визначення класу проблемної ситуації необхідно зробити вірний вибір її розв’язання із різноманіття можливих альтернатив. Це інший бік процесу подолання інциденту – визначення прецеденту, що стане найкращим способом владнати інцидент. Задачею даного дослідження виступає розв’язання саме цієї проблеми.

II. Вирішення проблеми і результати

Результат. Велика кількість проблемних ситуацій та широкий спектр їх розв’язання ускладнюють загальну задачу та вимагають розроблення відповідного інструментарію для її вирішення. В якості предметної області було обрано підприємство з обслуговування пасіки та виробництва меду і бджоло продуктів. В узагальненому вигляді задача має вигляд, як представлено на рисунку 1. Діагностування інцидентів спирається на прецедентний підхід [1], що дозволяє поєднати за певними ознаками класифікатори інцидентів та прецедентів їх розв’язання [2].

Задачу можна розділити на декілька етапів:

1 етап. Діагностування інциденту та встановлення симптомів, що характеризують проблемну ситуацію.

2 етап. Встановлення коду інциденту для його однозначного ідентифікування в системі. Фрагмент однієї з гілок алгоритму визначення коду інциденту наведений на рис.2.

3 етап. Знаходження в бібліотеці прецедентів за визначеним кодом групи варіантів розв’язання інциденту.

Рисунок 1 – Узагальнений підхід до розв’язання проблемної ситуації

4 етап. Реалізація обраного варіанта дій та оцінка результату його втілення.

5 етап. Кореляційне корегування (ранжування) в групі прецедентів за оновленими оцінками результату.

Рисунок 2 – Фрагмент алгоритму визначення коду інциденту

III. Висновки

Запропонований підхід до вирішення поставленої задачі дозволив розробити програмний продукт, який дозволяє в автоматизованому режимі швидко знаходити оптимальні способи розв’язання інцидентів та корегувати базу прецедентів на основі отриманих результатів їх впровадження.

Список використаних джерел

[1] Smirnov V.A. A precedent approach to building models of the process of troubleshooting in the diagnosis of complex technical systems // V.A. Smirnov / Automated control systems. St. Petersburg: T-Comm №6. 2013. p. 73-78.

[2] Dorodnyh N.O., Nikolaichuk OA, Yurin A.Yu. Automated creation of production knowledge bases based on event trees // Information and mathematical technologies in science and management. - 2017. - №2 (6). -C.30-41.),

Експертне оцінювання при розробці спеціалізованих медичних інформаційних систем

Міхнова Аліна Володимирівна[1]
Міхнов Дмитро Кіндратович[2],
Чиркова Катерина Сергіївна[3]

[1] *Харківський національний університет радіоелектроніки, пр. Науки 14, Харків, 61166, Україна, alina.mikhnova @nure.ua*
[2] *Харківський національний університет радіоелектроніки, пр. Науки 14, Харків, 61166, Україна dmytro.mikhnov@nure.ua*
[3] *Харківський національний університет радіоелектроніки, пр. Науки 14, Харків, 61166, Україна, , kateryna.chyrkova @nure.ua*

Анотація. *Розглядається методика експертного оцінювання впливу даних на показники діяльності закладів служби крові, на які впливає повнота та достовірність даних інформаційного супроводу, для визначення проектних рішень з модернізації спеціалізованої медичної інформаційної системи. Експертне оцінювання передбачене на різних рівнях обробки даних інформаційного супроводу з урахуванням ступеню автоматизації обробки інформації та наборів даних, що впливають на показники діяльності.*

Ключові слова: *заклад служби крові, експертне оцінювання, спеціалізована медична система.*

I. Актуальність

Заклади служби крові (ЗСК) відносяться до галузи охорони здоров'я і займаються заготівлею компонентів крові та забезпеченням ними пацієнтів в лікувальних закладах.

На сьогоднішній день в більшості ЗСК інформаційний супровід процесів забезпечується спеціалізовані медичні інформаційні системи (СМІС) – це окремий клас медичних автоматизованих інформаційних систем, які дають можливість забезпечити дотримання вимог відповідно якості компонентів крові, дозволяють своєчасно виявляти та мінімізувати кількість помилок з причин людського фактору.

Оскільки на сьогоднішній день СМІС СК велика кількість і всі вони в різному ступені забезпечують автоматизацію процесів ЗСК. Відповідно оцінювання ефективності СМІС СК з точки зору впливу на цільові показники діяльності ЗСК є актуальною та складною задачею.

Відповідно питання вибору, прийняття та обґрунтування рішень щодо модернізації та впровадження СМІС СК потребує застосування методів системного аналізу, а саме методів експертного оцінювання. Експертні методи дозволяють ефективно застосувати емпіричний досвід фахівців галузи виробничої трансфузіології та сучасних інформаційних технологій при прийнятті рішень щодо модернізації або вибору СМІС СК в ситуаціях, коли повна математична формалізація таких рішень неможлива.

II. Вирішення проблеми та результат

Для формування переліку показників діяльності ЗСК, на які впливає повнота та достовірність даних інформаційного супроводу; їх коефіцієнтів значності в залежності від ступеню серйозності негативних наслідків для безпеки донорської крові; а також бінарних оцінок впливу даних інформаційного супроводу на показники діяльності ЗСК; коефіцієнтів важливості даних що впливають на відповідний показник діяльності ЗСК; коефіцієнтів ступеню автоматизації та достовірності отримання даних потребує залучення групи експертів та обробки інформації для отримання рішення [1-2].

Існує дві групи методів експертних оцінок: методи індивідуальних експертних оцінок та методи колективних експертних оцінок [3-4].

Методи колективних експертних оцінок передбачають отримання різнобічного аналізу всіх варіантів модернізації або вибору СМІС СК.

Для вирішення задачі визначення варіанту модернізації або вибору СМІС СК запропоновано наступну послідовність етапів проведення експертного оцінювання:

- Крок 1. Визначення групи експертів в галузі виробничої трансфузіології та інформаційних технологій;
- Крок 2. Формування бланків експертної оцінки переліку показників діяльності ЗСК та їх значності; впливу даних інформаційного супроводу на показники діяльності ЗСК; важливості даних відносно впливу на відповідний показник діяльності ЗСК; ступеню автоматизації та достовірності отримання даних;
- Крок 3. Обробка матеріалів колективної експертної оцінки. Остаточна оцінка визначається як середнє нормалізоване зважене значення оцінки.

Оцінки важливості виражаються в балах і можуть набувати значення від 0 до 1.

III. Висновки

Запропонована методика може бути використана при оцінюванні ефективності функціонуванні спеціалізованих медичних інформаційних систем закладів служби крові.

Перелік посилань

[1] Mikhnova A. Information support model of production transfusion processes / A. Mikhnova, D. Mikhnov, K. Chyrkova // Eastern-European Journal of Enterprise Technologies. – Х. – 2016. – 3/3 (81). – С. 36 – 43.DOI: 10.15587/1729-4061.2016.71673

[2] Міхнова, А. В. Метод формування організаційно-технічних структур сегментів ІС служби крові [Текст]: зб. наук. пр. / А. В. Міхнова, Д. К. Міхнов, К.С Чиркова // Системи обробки інформації. – 2015. – № 12 (137). – С. 156–160.

[3] Грабовецький Б. Є. Методи експертних оцінок: теорія, методологія, напрямки використання / Б. Є. Грабовецький. — Вінниця : ВНТУ, 2010. — 171 с..

[4] Петяк Ю. Ф. Методика опитування експертів для виявлення факторів інформаційної безпеки мобільних пристроїв / Ю. Ф. Петяк // Наукові записки [Української академії друкарства]. Серія : Технічні науки. - 2015. - № 1. - С. 23-29

ІНФОКОМУНІКАЦІЙНІ МЕРЕЖІ І ТЕХНОЛОГІЇ

Method to improve the quality of the local access point based on mixed polarization of MIMO antenna

Masocha Success Maregere
Martynchuk Alexander

Kharkiv National University of Radio Electronics, 14 Nauky Ave, Kharkiv UA-61166, Ukraine, oleksandr.martynchuk@nure.ua, joaomissamo@gmail.com

Abstract. *The given work is devoted to increase of carrying capacity of Wi-Fi channel with MIMO by use the mixed polarization antenna system and orthogonal data coding. We investigate how this depends on the array geometry and the electric field polarization. Moreover, we validate our theoretical predictions with measurements above a nearly perfectly flat surface*

Keywords: *Wi-Fi, MIMO, mixed polarization, orthogonal data coding.*

I. INTRODUCTION

Interest in using the properties of polarization of radio waves under interference has increased at the present time. The polarization can be constant, permanently existing in a certain orientation, or it can rotate with each wave cycle.

Polarization sometimes plays an important role in wireless communication systems. The orientation of the linear antenna, dipole, and vibrator corresponds to the polarization of radio waves received or transmitted by this antenna.

Thus, a vertical antenna receives and emits vertically polarized waves, and a horizontal antenna receives or emits horizontally polarized waves. The best short-range communication is achieved when the transmitting and receiving antennas (source and receiver) have the same polarization. The least effective short-range communication usually occurs when two antennas are located at a right angle (for example, one horizontal and one vertical). At large distances, the atmosphere can cause fluctuations in the polarization of radio waves, so the difference between horizontal and vertical becomes less significant.

Thus, an ideal vertical antenna receives and radiates vertically polarized waves, and a horizontal antenna receives or radiates horizontally polarized waves. Of course, the best short-range communication is achieved when the transmitting and receiving antennas (source and receiver) have the same polarization. Naturally, the least effective short-range communication usually occurs when two antennas are at right angles. At large distances, the atmosphere can cause fluctuations in the polarization of radio waves, so the difference between horizontal and vertical becomes less significant. Under the conditions of short-range communication, the influence of interference leads to the fact that the received wave becomes arbitrarily different from the polarization transmitted. In this connection, the reception and processing of orthogonal field components becomes relevant. It seems relevant further development of communication systems based on the signal of double polarization.

II. PROBLEM SOLUTION AND RESULTS

The diversity of transmitted polarizations is proposed as an alternative to spatial diversity in order to limit the aperture of antenna arrays at both ends of the radio link. It is proposed to consider the use of different combinations of polarization states of signals on the emission and reception. It expected to receive a combination of polarization, when the fluctuations of the main polarization signal channel will be minimal.

The spatial orientation of the electric field component is called polarization of the EM wave. The type of the polarization is defined by the mark that electrical field component 'draws' while the wave propagates.

For the Linear polarization direction of E is constant and does not change with time. The type of the linear polarization can be vertical, horizontal, or slant (±45º). Vertical polarization is Transverse electric (TE) polarization or parallel polarization. Horizontal polarization is Transverse magnetic (TM) polarization or perpendicular polarization. For the Elliptical polarization the direction of E changes according to ratio of Ez/Ey, if x is the direction of propagation.

For Circular polarization the amplitude of E is time-independent. The rotation of the polarization (either elliptical or circular) can be right-handed circular polarization (RHCP) (=counter clockwise) or left-handed circular polarization (LHCP) (=clockwise).

Actual transmitted signal characterized by the parameters of the polarization ellipse - the angle of ellipticity and orientation angle of semi-major axis of the ellipse. Then, omitting the factors - angular frequency, attenuation and range, the vector of the electric field near a transmitting antenna can represented in the form of the polarization vector of the emitted signal

III. CONCLUSIONS

Research results indicate the different propagation conditions at different polarizations at the two radiation patterns. Various orthogonal polarizations create different conditions improvement and development of troposphere communication systems. The research results indicate the need to manage the state of orthogonal polarizations, depending on the range and propagation conditions.

REFERENCES

[1] Martynchuk A.A., Loshakov V.A., Oliver L.M/. Development of a trans-horizon communication system based on dual polarization MIMO architecture // "Проблемы электромагнитной совместимости перспективных беспроводных сетей связи (ЕМС-2015). – Харьков: ХНУРЭ, 2015.

[2] Popovskii V., Loshakov V., Filipenko O., Martynchuk O., Drif A./ Results of development tropospheric communications system / 2015 Second International Scientific Practical Conference "Problems of Infocommunications. Science and Technology". –Kharkiv, ANPRE, 2015.

Current Trends in Using the Software-Defined WAN

Abdelfattah Mohamed

Kharkiv National University of Radio Electronics, 14 Nauky Ave, Kharkiv UA-61166, Ukraine, m.zaki178@gmail.com

Abstract. *The given work is devoted to the investigation the current trends of using the Software-defined WAN as a specific application of software-defined networking technology applied to WAN connections such as broadband internet, 4G, LTE, or MPLS. While connecting enterprise networks – including branch offices and data centers – over large geographic distances, SD-WAN simplifies the management and operation of a WAN by separating the networking hardware from its control mechanism.*

Keywords: *SD-WAN, broadband internet, enterprise network, cloud-based applications, network security.*

I. INTRODUCTION

SD-WAN consists of several technologies combined with newer improvements. Redundant telecommunication links connecting remote sites date back to the 1970s with X.25 links used for remote mainframe terminal access. Central management of those links with a greater focus on application delivery across the WAN started to become popular in the mid-2000s. SD-WAN combines the two, and adds the ability to dynamically share network bandwidth across the connection points. Additional enhancements include central controllers, integrated analytics and on-demand circuit provisioning, with some network intelligence based in the cloud, allowing centralized policy management and security.

Networking publications started using the term SD-WAN to describe this new networking trend as early as 2014. Software-defined WAN is quickly replacing traditional Wide Area Networks (WANs) as more enterprises realize the need to rethink networking for today's cloud-centric world. SD-WAN simplifies the way networks are designed, deployed and managed. It also brings powerful capabilities that increase the efficiency and agility of IT teams. In addition, SD-WAN devices can be installed without removing the existing network equipment and can be managed from a central console using a modern graphical user interface.

II. PROBLEM SOLUTION AND RESULTS

Considerable savings can be fulfilled by moving some or all traffic from MPLS to cost-effective broadband alternatives in a Hybrid WAN configuration. SD-WAN makes it easy to achieve cost savings by automatically splitting traffic between low-cost and highly-available WAN links based on business criticality. This is possible when the SD-WAN solution can identify traffic by application and steer it according to policy-based rules. While there is no doubt that cost savings is a key benefit of SD-WAN adoption, it's not always easy to recognize how much can you save and what is your true return on investment.

Software-defined WAN is making it simpler to set up and manage networks at branch offices despite their growing complexity and a lack of onsite IT staff. With zero-touch, rapid deployment, almost anyone can plug in an SD-WAN gateway and watch as it is discovered, provisioned, and brought online. One network engineer can administer dozens, maybe hundreds, of SD-WAN devices on an ongoing basis. This is made possible by policy-driven management, which translates business requirements into operational rules that are transmitted to all SD-WAN devices across the enterprise network.

Network performance is important for business-critical applications and unified communications – especially when applications run in the cloud. But not all network traffic needs to move quickly. Software-defined WAN combines traditional Quality of Service with the ability to steer the traffic of different applications and users onto appropriate paths. SD-WAN can also monitor the "health" of WAN links and automatically route traffic onto an alternate (backup) path when the primary path becomes congested. Nevertheless, that doesn't help if all available paths are bad. In this case, the WAN optimization can be used together with SD-WAN to improve performance across congested links and high-latency connections.

Software-defined WAN enhances **security** in several ways. SD-WAN can identify network traffic by source/destination, application, and users. Then it routes the traffic according to centrally-defined security policies that control access to zones and the Internet. SD-WAN gateways form connections between sites using VPN tunnels with advanced encryption. Many gateways come with a robust perimeter firewall that meets most security needs. Internet traffic that requires a firewall with advanced features can be backhauled through a central access point with stronger security or sent through cloud security provider.

III. CONCLUSIONS

It can be concluded that SD-WAN is used in connecting branch/remote sites directly to the Internet as the increasing reliance on cloud-based applications in most organizations is a driver for this use case. Setting up Internet break-outs from branch/remote offices is slow, inefficient, and error-prone when using traditional methods. SD-WAN drastically simplifies and speeds the process. You can quickly design a shadow appliance, which is a placeholder for a physical device, on the central management console. Then use zero-touch provisioning to bring the SD-WAN device online without the need for administrative action when it is plugged in at the remote/branch office.

REFERENCES

[1] G. Blokdyk. *Software-Defined WAN SD-WAN A Clear and Concise Reference*. 5STARCooks, 2018.

[2] G. Blokdyk. *SD-WAN A Complete Guide*. 5STARCooks, 2018.

[3] R. Naggi and R. Srivastava. *SD-WAN The Networking Blueprint for Modern Businesses*. Amazon Digital Services LLC, 2018.

[4] G. Blokdyk. *Sd-WAN and Security the Ultimate Step-By-Step Guide*. 5STARCooks, 2018.

[5] P. Goransson, C. Black, T. Culver. *Software defined networks: a comprehensive approach*. Morgan Kaufmann, 2016.

Квадратична модель оптимального управління чергами на інтерфейсах маршрутизаторів телекомунікаційних мереж

Лебеденко Тетяна Миколаївна

Харківський національний університет радіоелектроніки, пр. Науки,14, м. Харків, 61166, Україна, tetiana.lebedenko @nure.ua

Анотація. *Отримала розвиток квадратична модель оптимального управління чергами на інтерфейсах маршрутизаторів телекомунікаційних мереж, метою якої є узгоджене вирішення задач управління перевантаженням (Congestion Management), розподілу мережного ресурсу (Resource Allocation) та запобігання перевантаження (Congestion Avoidance). Розрахунок керуючих змінних, що відповідають за рішення перерахованих задач, відбувався в ході мінімізації квадратичної цільової функції, зваженої відносно класів потоків та черг. Перевагою моделі є можливість більш раціонального розподілу та використання мережного ресурсу та можливих відмов в обслуговуванні.*

Ключові слова: *управління перевантаженням, запобігання перевантаження, розподіл мережного ресурсу, якість обслуговування, управління чергами.*

I. Вступ

Як відомо, кількісні значення основних показників якості обслуговування (Quality of Service, QoS) багато в чому залежать від результативності вирішення задач по управлінню мережними ресурсами – інформаційними, буферними та канальними. При цьому поліпшення таких показників QoS як середня затримка, джиттер та кількість відкинутих пакетів безпосередньо залежить від використання механізмів управління чергами (Queue Management), важливе місце серед яких займають механізми Congestion Management, Resource Allocation та Congestion Avoidance [1-4]. Тому для практики актуальним є наявність теоретичних рішень щодо забезпечення узгодженого розв'язання таких інтерфейсних задач як розподіл потоків пакетів по сформованих на інтерфейсі маршрутизатора чергах з урахуванням класифікації переданих потоків, вимог до якості обслуговування та характеристик створюваних черг; розподіл пропускної здатності інтерфейсу між окремими чергами; а також запобігання перевантаження з превентивним (завчасним) обмеженням інтенсивності потоків, що надходять на інтерфейс маршрутизатора телекомунікаційних мереж (ТКМ). [5].

II. Квадратична модель оптимального управління чергами на інтерфейсах маршрутизаторів ТКМ

Зважаючи на це запропоновано математичну модель оптимального управління чергами на інтерфейсах маршрутизаторів ТКМ, яка дозволяє забезпечити узгоджене вирішення задач Congestion Management, Resource Allocation та Congestion Avoidance. Основу моделі складають умови забезпечення диференціації обслуговування потоків пакетів відповідно до класів потоків та черг (вимог до якості обслуговування); модифіковані умови збереження потоку, згідно з якими потоки пакетів можуть або бути спрямованими на обслуговування до однієї з черг інтерфейсу маршрутизатора або бути відкинутими з неї; умови щодо коректності розподілу пропускної здатності інтерфейсу між сформованими чергами та умов запобігання перевантаження. Розрахунок керуючих змінних, згідно до поставлених умов та обмежень реалізовано у ході вирішення оптимізаційної задачі, де цільова функція, зважена відносно класів потоків та черг, представлена квадратичною формою. Врахування та прив'язка до класів потоків та черг при вирішенні даної оптимізаційної задачі дозволяє забезпечити превентивне обмеження інтенсивності потоків пакетів за аналогією з механізмами запобігання перевантаження (RED, WRED) за рахунок можливості гнучкого регулювання напрямлення тих чи інших потоків до тих чи інших черг. Перевагою запропонованого рішення є більш справедливий, порівняно з лінійною формою цільової функції, характер розподілу та використання мережного ресурсу та можливих відмов в обслуговуванні [3-5]. Це пов'язано з тим, що у разі можливого перевантаження інтерфейсу відмови в обслуговуванні будуть стосуватися всіх без виключення потоків пакетів, але меншою мірою з високими значеннями класів, та меншою – з низькими.

III. Висновки

За результатами дослідження запропонованої квадратичної моделі оптимального управління чергами на ряді числових прикладів було підтверджено її адекватність та ефективність щодо узгодженого вирішення задач Congestion Management, Resource Allocation та Congestion Avoidance заснованому на класах.

Список літератури

[1] A. Monge, K. Szarkowicz, "MPLS in the SDN Era: Interoperable Scenarios to Make Networks Scale to New Services," 1st edition, O'Reilly Media, 2016.

[2] S. Alvarez. QoS for IP/MPLS networks. Cisco press, 2006.

[3] S. Lenas, S. Dimitriou, F. Tsapeli, V. Tsaoussidis, "Queue-management architecture for delay tolerant networking," in Wired/Wireless Internet Communications, 2011, pp. 470-482.

[4] O. Lemeshko, Ali S. Ali, M. Semenyaka, "Results of the dynamic flow-based queue balancing model research," in Proc. 2012 of Internatial Conference on Modern Problems of Radio Engineering Telecommunications and Computer Science (TCSET), 21-24 February. 2012, pp. 318-319.

[5] T. Lebedenko,A. Kholodkova, A. Al-Dulaimi. "Linear-Quadratic Model of Optimal Queue Management on Interface of Telecommunication Network Router," in Proc. 2018 of 3th International Conference on Information and Telecommunication Technologies and Radio Electronics (UkrMiCo), 10-14 September 2018, pp.1-4.

Метод ієрархічно-координаційної маршрутизації на рівні автономних систем IP-мережі

Лемешко Олександр Віталійович,
Ільяшенко Андрій Євгенович,
Мерсні Амаль

Харківський національний університет радіоелектроніки,
пр. Науки,14, м. Харків, 61166, Україна,
oleksandr.lemeshko.ua@ieee.org,
andy.ilyashenko@gmail.com,
amal.mersni@nure.ua

Анотація. *Запропоновано метод ієрархічно-координаційної маршрутизації на рівні автономних систем (Autonomous Systems, AS) IP-мережі. В основу метода покладено декомпозиційну модель маршрутизації. Новизною моделі є формулюванням умов взаємодії автономних систем IP-мережі, виконання яких гарантувало зв'язність шляхів, які проходять через множину AS. В рамках методу вихідна задача ієрархічно-координаційної маршрутизації сформульована як задача багаторівневої оптимізації, для розв'язання якої використано принцип цільової координації та методи лінійного програмування. Результати дослідження підтвердили ефективність запропонованих рішень.*

Ключові слова: *метод, маршрутизація, мережа, шлях, координація, рівень, трафік.*

I. Вступ

Для підвищення ефективності і гнучкості рішень щодо ієрархічної маршрутизації доцільно відмовитися від обмежень, пов'язаних з обов'язковим проходженням всіх міждоменних маршрутів через backbone, тобто зробити все домени мережі функціонально рівноправними. Така архітектура реалізована, наприклад, на рівні автономних систем IP-мереж, коли, в загальному випадку, шукані шляхи в мережі можуть проходити через довільне число AS [1]. Децентралізація розрахунку маршрутів в кожній окремій AS сприяє підвищенню масштабованості IP-мережі. Проте при використанні множини пригранічних маршрутизаторів між AS однозначність у децентралізованому виборі маршрутів втрачається, що може негативно вплинути на ефективність (продуктивність) мережі в цілому. Тому в даній роботі пропонується **м**етод маршрутизації на рівні автономних систем IP-мережі з введенням дворівневої ієрархії маршрутних рішень з координацією роботи AS для забезпечення зв'язності маршрутів, які проходять через множину таких систем.

II. Метод ієрархічно-координаційної маршрутизації на рівні автономних систем IP-мережі

В роботі запропонована декомпозиційна потокова модель ієрархічної маршрутизації, яка представлена умовами реалізації одно/багатошляхової стратегії маршрутизації, збереження потоку та запобігання перевантаження каналів зв'язку в кожній з автономних систем IP-мережі. Новизною моделі є, по-перше, модифікація умов збереження потоку для автономних систем трьох типів: відправника, одержувача пакетів і множини транзитних AS; по-друге, введення в її структуру умов взаємодії AS для забезпечення зв'язності маршрутів, які проходять через множину автономних систем IP-мережі. Модель орієнтована на підтримку маршрутних метрик, які реалізовані в сучасних протоколах IP-маршрутизації – RIP, IGRP, OSPF.

Синтезований метод ієрархічно-координаційної маршрутизації на рівні автономних систем IP-мережі базується на представленій декомпозиційній моделі. В межах метода завдання ієрархічної маршрутизації було зведено до оптимізаційної задачі лінійного програмування. Для забезпечення координованої роботи множини автономних систем щодо розрахунку зв'язних маршрутів, які проходять через множину AS, при розв'язанні сформульованої оптимізаційної задачі використано принцип цільової координації [2-4]. Він дозволив ввести дворівневу ієрархію розрахунків: нижній рівень відповідав за розрахунок маршрутів в окремих AS, а верхній – за координацію рішень нижнього рівня, спрямованої на забезпечення зв'язності розрахованих маршрутів між AS.

III. Висновки

Дослідження процесів ієрархічної маршрутизації, організованої за допомогою запропонованого методу, підтвердило його ефективність на ряді розрахункових прикладів. Доведена збіжність методу до оптимального рішення за кінцеву кількість ітерацій координаційної процедури. Швидкість збіжності методу визначала оперативність розв'язання маршрутних задач та обсяги переданої між ієрархічними рівнями службової інформації про стан мережі. Встановлено, що на збіжність методу впливали розміри мережі, зв'язність маршрутизаторів та AS мережі в цілому. Запропонований метод може бути використаний як математичне та алгоритмічне забезпечення при розробці перспективних протоколів ієрархічної маршрутизації в сучасних інфокомунікаційних мережах.

Список літератури

[1] D. Medhi, K.Ramasamy. *Network Routing*, Second Edition: Algorithms, Protocols, and Architectures (The Morgan Kaufmann Series in Networking) 2nd Edition. Cambridge, MA, USA: Elsevier Inc., 2018. 1018 p.

[2] М. Месарович, Д. Мако, И. Такахара. Теория иерархических многоуровневых систем. М.: Мир, 1973, 344 с.

[3] А.В. Лемешко, Е.С. Невзорова, К.М. Арус. "Анализ сходимости координационной процедуры при реализации иерархической маршрутизации в телекоммуникационной сети," Проблеми телекомунікацій, 2015, № 1 (16),. с. 54-71. URL: http://pt.journal.kh.ua/2015/1/1/ 151_lemeshko_coordination.pdf..

[4] А.В. Лемешко, Е.С. Невзорова, А.Е. Ильяшенко. "Разработка и анализ метода иерархическо-координационной междоменной маршрутизации в телекоммуникационной сети," Наукові записки Українського науково-дослідницького інституту зв'язку, 2016, №4 (44), с. 49-67.

Иерархический метод управления трафиком в сети MPLS-DiffServ

Невзорова Елена Сергеевна

Харьковский национальный университет радиоэлектроники, пр. Науки,14, г. Харков, 61166, Украина, olena.nevzorova.ua@ieee.org

Анотация. *В работе предложена потоковая модель и иерархический метод управления трафиком в сети MPLS-DiffServ. Использование потоковой модели позволило обеспечить согласованное решение задач маршрутизации и распределения пропускной способности каналов связи. С другой стороны, в основу предложенного метода положен принцип прогнозирования взаимодействий, что позволило ввести двухуровневую иерархию расчетов: нижний уровень отвечал за расчет маршрутных переменных, а верхний – за распределение канального ресурса.*

Ключевые слова: *управление трафиком, поток, маршрутизация, MPLS сеть, принцип предсказания взаимодействий*

I. Введение

Как показал проведенный анализ [1] важным направлением улучшения качества обслуживания (Quality of Service, QoS) в современных телекоммуникационных сетях (ТКС) является повышение уровня согласованности в решении отдельных задач по управлению трафиком. При этом числовые значения основных QoS-показателей, к которым относятся, прежде всего, скорость передачи, средняя задержка и вероятность потерь пакетов, во многом зависят как от объема канального и буферного ресурса, выделенного тем или иным потокам, так и от степени их сбалансированного использования. За решение данной задачи в современных телекоммуникационных сетях традиционно отвечают протокольные средства маршрутизации и распределения пропускной способности каналов связи, реализованные на принципах Traffic Engineering в рамках архитектурных моделей интегрированных (Integrated services, IntServ) и дифференцированных услуг (Differentiated Services, DiffServ) [2]. При этом как при маршрутизации потоков, так и распределении канального ресурса необходимо учитывать разнородность требований пользователей сети относительно заявленного уровня качества обслуживания, что обеспечивается соответствующей классификацией трафика и маркировкой (приоритезацией) пакетов.

II. Иерархический Метод Управления Трафиком в Сети MPLS-DiffServ

Предложенный метод основан на потоковой математической модели, использование которой позволило обеспечить согласованное решение задач маршрутизации и распределения пропускной способности каналов связи. Новизной предлагаемой модели является введение условий балансировки нагрузки в каналах связи сети в соответствии с их классом обслуживания и требованиями технологии Traffic Engineering. В рамках данной модели искомые решения получаются в ходе решения задачи нелинейного программирования. С целью понижения вычислительной сложности и повышения масштабируемости получения искомых решений без потери их адекватности обоснован выбор к использованию принципа прогнозирования (предсказания) взаимодействий, относящийся к теории иерархических многоуровневых систем управления [3, 4]. Реализация данного принципа предполагает введение двухуровневой иерархии расчетов. Нижний (первый) иерархический уровень отвечает за решение задач маршрутизации, а верхний (второй) – за распределение канального ресурса между потоками различных классов, а также координацию решений нижнего уровня. При этом удалось свести исходную достаточно размерную задачу нелинейной оптимизации к итерационному решению менее размерных задач линейного программирования без потери адекватности конечных решений [5, 6].

III. Выводы

В данной работе предложен иерархический метод управления трафиком в сети MPLS-DiffServ. На численном примере подтверждена сходимость метода к оптимальным решениям за конечное число итераций, а также его соответствие архитектуре DiffServ-TE с точки зрения обеспечения сбалансированной загруженности канального ресурса в соответствии с приоритетом и классом обслуживания переданных пакетов. Линейность решаемой оптимизационной задачи положительно сказывается на снижении вычислительной сложности практической реализации предложенного метода на контроллере программно-конфигурируемых сети.

Список литературы

[1] M. Barreiros and P. Lundqvist. *QOS-Enabled Networks: Tools and Foundations. Wiley Series on Communications Networking & Distributed Systems, 2nd Edition.* Wiley, 2016.

[2] I. Minei. *MPLS DiffServ-aware Traffic Engineering*. Juniper Networks, Inc., 2004. 24 p.

[3] M.D. Mesarovic, D. Macko and Y. Takahara. *Theory of hierarchical, multilevel, system*. Academic Press, New York and London, 1970.

[4] M. G. Singh and A. Titli. *Systems: Decomposition, Optimization and Control*. Pergamon, Oxford, 1978.

[5] О.В. Лемешко, та О.С. Невзорова. “Дворівневий метод маршрутизації з балансуванням пріоритетного розподілу канального ресурсу у програмно-конфігурованій телекомунікаційній мережі,” Радіотехніка : Всеукр. міжвід. наук.-техн. зб. Вип. 192, 2018. сс. 61-70.

[6] O. Lemeshko, O. Nevzorova, and A.M. Hailan. “Hierarchical Method of Routing and Resource Allocation in DiffServ-TE Network,” in 14th International Conference Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (TCSET’2018). 20-24 Feb. 2018. pp. 1014-1018.

Створення глобальної мережі розумних пристроїв на основі концепції Internet of Everything

Персіков Михайло Анатолійович,
Жерноклеєв Віктор Сергійович,
Рибінський Валентин Максимович

Харківський національний університет радіоелектроніки,
пр. Науки,14, м. Харків, 61166, Україна,
mihapersikov@gmail.com

Анотація. *Проведено аналіз розгортання глобальної мережі розумних пристроїв на основі концепції Internet of Everything. Виявлено необхідність забезпечення інтероперабельності між множиною різнорідних пристроїв за умови забезпечення конфіденційності та безпеки кінцевих користувачів. Запропоновано проводити розробку відповідних аналітичних моделей, здатних виявляти як зовнішні, так і внутрішні загрози в умовах, де будь-який пристрій може бути скомпрометованим.*

Ключові слова: *глобальна мережа, розумні пристрої, IoT, IoE, мережна безпека.*

I. Вступ

Сучасний стан розвитку інформаційного суспільства характеризується появою еволюційних обчислювальних технологій, що використовують Інтернет як засіб комунікацій. Ця інфокомунікаційна технологія, названа Internet of Everything (IoE), встановлює вільний потік інформації між різними взаємопов'язаними пристроями [1-5]. Використання IoE є багаторівневим і знаходить своє застосування практично у всіх сферах життя, починаючи від з'єднання між собою пристроїв розумних будинків до їх комунікацій з віртуальними середовищами для організації зв'язку між ними [1, 2, 5]. Хоча IoE використовується як інфраструктура для обміну інформацією, в той же час проблеми конфіденційності та питання безпеки кінцевих користувачів є надзвичайно актуальними [4, 5]. IoE має широкі можливості щодо інформаційного обміну, але це вимагає вживання відповідних заходів для його ефективного та безпечного впровадження та розповсюдження в значній мірі.

II. Забезпечення конфіденційності та безпеки в IoE

IoE є складною мережею, що складається з мільярдів ідентифікованих пристроїв, які взаємодіють один з одним для досягнення спільних цілей при застосуванні різних технологій на рівнях програмного, підпрограмного та апаратного забезпечення. При цьому всі фізичні пристрої формують апаратний рівень мережі, наприклад, на основі безпроводових технологій: пристрої з радіочастотною ідентифікацією (Radio Frequency Identification, RFID), сенсори, смартфони, розумний одяг (wearable technology) тощо [5]. Далі використовувані пристрої на апаратному рівні поділяються на три робочі процеси: пристрої зв'язку, датчики та ідентифікація. Обробка, візуалізація або інтерпретація необхідних даних керується програмним рівнем за допомогою спеціалізованого програмного забезпечення. Слід відмітити, що рівень підпрограмного забезпечення є сполученням між програмним та апаратним рівнями. Підпрограмний рівень відіграє найважливішу роль серед усіх трьох при впровадженні нового програмного забезпечення, організуючи сумісність апаратного рівня. На сьогодні проводиться достатньо розробок щодо впровадження IoE з урахуванням питань конфіденційності та безпеки, але все ще вимагає досліджень і нових рішень щодо вдосконалення мережної безпеки в рамках технології IoE [4]. Досягнення високої інтероперабельності між множиною пристроїв є ключовим завданням, оскільки вони є неоднорідними, що призводить до значної складності щодо вирішення питань конфіденційності та безпеки.

III. Висновки

Дослідження процесів розгортання глобальної мережі розумних пристроїв на основі концепції IoE призводить до висновків щодо необхідності врахування як зовнішніх, так і внутрішніх атак. При цьому використання особистих пристроїв IoE може бути застосовано саме для проведення інсайдерських атак. Отже, актуальною представляється розробка нових аналітичних моделей, здатних виявляти загрози, а також будувати інфокомунікаційні системи та мережі, стійкі до середовищ IoE, де будь-який пристрій може бути скомпрометованим.

Список літератури

[1] S. Cirani, G. Ferrari, M. Picone and L. Veltri. *Internet of Things: Architectures, Protocols and Standards*. 1 edition. John Wiley & Sons, 2018.

[2] D. Hanes, G. Salgueiro, P. Grossetete, R. Barton and J. Henry. *IoT fundamentals: Networking technologies, protocols, and use cases for the internet of things*. 1 edition. Cisco Press, 2017.

[3] M. Rao. *Internet of Things with Raspberry Pi 3: Leverage the power of Raspberry Pi 3 and JavaScript to build exciting IoT projects*. Packt Publishing Ltd, 2018.

[4] A. Gupta. *IoT Hackers Handbook: An Ultimate Guide to Hacking the Internet of Things and Learning IoT Security*. 1.0 edition. CreateSpace Independent Publishing Platform, 2017.

[5] A. Majeed, A.U. Haq, A. Jamal, R. Bhana, F. Banigo and S. Baadel. "Internet of everything (IoE) exploiting organisational inside threats: Global network of smart devices (GNSD)," in Proc. *2016 IEEE International Symposium on Systems Engineering (ISSE)*, 3-5 October 2016, pp. 1-7.

Оцінка нелінійних спотворень у радіотракті базової станції системи мобільного зв'язку

Селіванов Костянтин Олександрович[1],
Москалець Микола Вадимович[2]

Харківський національний університет радіоелектроніки,
пр. Науки,14, м. Харків, 61166, Україна,
[1]*sunright@yandex.ua*
[2]*mykola.moskalets@nure.ua*

Анотація. *У даній роботі проведені дослідження продуктів нелінійних спотворень у радіоприймальному тракті базової станції мобільного зв'язку з використанням адаптивної антенної системи. Проведено оцінку рівнів нелінійних спотворень за допомогою коефіцієнтів вищих гармонік і коефіцієнта субгармонік для різних видів нелінійностей, характерних для радіотрактів з використанням адаптивних антенних систем. За допомогою імітаційного моделювання отримані кількісні оцінки величини нелінійних спотворень сигналів при проходженні їх через нелінійні елементи адаптивної антенної системи, математичні моделі яких представлені характеристикою гістерезису.*

Ключові слова: *нелінійність, нелінійний елемент, коефіцієнти гармонік, нелінійні спотворення.*

I. Вступ

В адаптивних алгоритмах обробки сигналів, які використовуються в адаптивних антенних системах, при управлінні амплітудно-фазовим розподілом проявляються характерні для систем типу Уайта гістерезисні явища. Розглянуті системи є стохастичними динамічними системами. Збагачення спектра вхідного сигналу у нелінійному елементі (НЕ) є надзвичайно важливим явищем. З одного боку на ньому заснована робота цілого ряду радіотехнічних пристроїв, з іншого – через нелінійність характеристик виникають деякі небажані ефекти, які необхідно оцінювати та враховувати [1].

II. Оцінка продуктів нелінійних спотворень у адаптивних антенних системах

За допомогою імітаційного моделювання отримані оцінки величини нелінійних спотворень сигналів при проходженні їх через нелінійні елементи, математичні моделі яких представлені залежностями у вигляді системи рівнянь [2]:

$$y=\begin{cases} k\,x-kC_1-k\varepsilon\,sign\left(\dfrac{dy}{dt}\right)\ при\left(\dfrac{dy}{dt}\right)\neq 0\ \ i\ \ 0\le y\le k(C_2-C_1); \\ k\,x+kC_1-k\varepsilon\,sign\left(\dfrac{dy}{dt}\right)\ при\left(\dfrac{dy}{dt}\right)\neq 0\ \ i\ \ -k(C_2-C_1)\le y\le 0; \\ const \quad \begin{cases} при\ |y-k\,x+kC_1|\le k\varepsilon\ \ i\ \ 0\le y\le k(C_2-C_1); \\ або\ \ |y-k\,x-kC_1|\le k\varepsilon\ \ i\ \ k(C_2-C_1)\le y\le 0; \end{cases} \\ k(C_2-C_1)sign(y) \qquad при\ |x|\ge C_2+\varepsilon; \\ 0 \qquad при\ |x|\le C_1-\varepsilon,\ якщо\ C_1>\varepsilon, \end{cases} \tag{1}$$

Проведено машинний експеримент і для моделі (1) отримана залежність коефіцієнтів вищих гармонік і субгармонік від величини зони люфту при впливі на НЕ 10 гармонійних коливань рівномірно розподілених по всій смузі частот приймальної частини базової станції мобільної системи зв'язку. Необхідно відзначити, що паразитні складові спектру розташовуються в основному на кратних гармоніках, а саме на гармоніках основних частот. Так, як приклад, представлені графіки спектра корисних сигналів (рис.1а) і паразитних складових на виході НЕ (рис.1б).

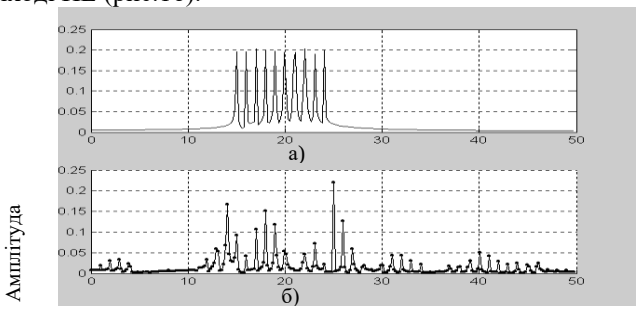


Рисунок 1. Спектр корисних сигналів і паразитних складових на виході НЕ

Як видно з отриманих залежностей, паразитні складові спектра, проникаючі в спектр каналу прийому базових станцій систем мобільного зв'язку, де здійснюється рівномірний розподіл частот, розташовуються саме на основних складових спектра і приймають значення, зіставні зі значеннями корисних сигналів.

III. Висновки

При прийомі випадкових сигналів, якими є сигнали зв'язку, дане явище може призвести до непередбачуваних і неконтрольованих ситуацій. Проведені дослідження дозволяють зробити висновок про те, що існуюча на сьогоднішній момент методика розподілу частот у системах мобільного зв'язку (рівномірний розподіл частот) не є оптимальною.

СПИСОК ЛІТЕРАТУРИ

[1] Москалец Н.В, Селиванов К.А., Никитенко Т.В. Анализ нелинейных искажений в радиотракте с применением различных методов оценки нелинейности. *Электронное научное специализированное издание «Проблемы телекоммуникаций».* 2011. № 2 (4). С. 150–161. URL:http://pt.journal.kh.ua/2011/2/1/112_selivanov_radio.pdf

[2] Yu.Yu. Kolyadenko. A Nonlinear Stochastic Model of Space-Time Processing Signals // Telecommunications and Radio Engineering, Vol. 52. № 10. 1998. pp. 49-52.

Підвищення відмовостійкості мереж засобами швидкої перемаршрутизації з балансуванням навантаження та профілюванням трафіка

Єременко Олександра Сергіївна,
Євдокименко Марина Олександрівна,
Шаповалова Анастасія Сергіївна

Харківський національний університет радіоелектроніки,
пр. Науки,14, м. Харків, 61166, Україна,
oleksandra.yeremenko.ua@ieee.org,
maryna.yevdokymenko@ieee.org,
anastasiia.shapovalova@nure.ua

Анотація. *Запропоновано оптимізаційну модель швидкої перемаршрутизації з балансуванням навантаження та профілюванням трафіка в телекомунікаційних мережах. Перевагою рішення є формулювання задачі як оптимізаційної, яка орієнтує на мінімізацію верхнього динамічно керованого порогу завантаженості каналів зв'язку та зваженої відносно пріоритету обслуговування інтенсивності потоків, що отримують відмови в обслуговуванні на границі мережі.*

Ключові слова: *відмовостійкість, резервування, швидка перемаршрутизація, балансування навантаження, профілювання трафіка.*

I. Вступ

Відомо, що рішення з підвищення відмовостійкості телекомунікаційних мереж (ТКМ) на основі реалізації швидкої перемаршрутизації базуються на резервуванні її елементів і пропускної здатності [1-3]. Таким чином, введення ресурсної надлишковості є платнею за підвищення надійності мережних рішень. Проте резервування мережного ресурсу в ході реалізації тієї чи іншої схеми захисту завжди негативно впливає на її продуктивність та рівень якості обслуговування в цілому. Тобто з підвищенням навантаження на мережу реалізація схем захисту елементів мережі, а особливо її пропускної здатності в ході швидкої перемаршрутизації може призвести до перевантаження. Як відомо, ефективним проактивним засобом боротьби з перевантаженням мережі є забезпечення збалансованого використання доступного мережного ресурсу на принципах концепції Traffic Engineering (ТЕ) [3, 4]. Дієвим реактивним методом боротьби з перевантаженням є профілювання трафіка, а зокрема обмеження його інтенсивності на границі мережі відповідно до пріоритету обслуговування пакетів [5]. Тому для практики дуже затребуваними є теоретичні рішення щодо забезпечення погодженого розв'язання мережних задач зі швидкої перемаршрутизації на принципах ТЕ та диференційованого обмеження трафіка.

II. Модель швидкої перемаршрутизації з балансуванням навантаження на основі ТЕ та диференційованим обмеженням трафіка

У зв'язку з цим запропоновано математичну модель швидкої перемаршрутизації з балансуванням навантаження на принципах ТЕ та диференційованим обмеженням трафіка в ТКМ. Основу моделі складають умови реалізації багатошляхової маршрутизації, модифіковані умови збереження потоку, які враховують пріоритетне обмеження трафіка на границі мережі у випадку її ймовірного перевантаження, викликаного, з одного боку, зростанням навантаження, а з іншого – реалізацією схем захисту елементів мережі та її пропускної здатності в ході швидкої перемаршрутизації, а також адаптовані під нові вимоги умови забезпечення захисту (резервування) вузла, каналу та пропускної здатності мережі. Перевагою запропонованого рішення також є формулювання задачі як оптимізаційної з критерієм оптимальності, який орієнтує на мінімізацію, по-перше, верхнього динамічно керованого порогу завантаженості каналів зв'язку, що відповідає вимогам концепції ТЕ, а, по-друге, зваженої відносно пріоритету обслуговування інтенсивності потоків, які отримують відмови в обслуговуванні на границі мережі. Лінійність сформульованої оптимізаційної проблеми забезпечувалась шляхом деякого розширення числа змінних, що розраховуються, які визначають верхній поріг для маршрутних змінних основного та резервного шляхів.

III. Висновки

Дослідження процесів швидкої перемаршрутизації з використанням запропонованої моделі на ряді числових прикладів підтвердило адекватність і ефективність отриманих на її основі маршрутних рішень як щодо забезпечення їх відмовостійкості та балансування навантаження, так і щодо заснованого на пріоритетах обмеження трафіка.

Список літератури

[1] R. White and E. Banks. *Computer Networking Problems and Solutions: An innovative approach to building resilient, modern networks 1st Edition*. 1 edition. Addison-Wesley Professional, 2018.

[2] J. Rak. *Resilient Routing in Communication Networks*. 1st edition, Springer, 2015.

[3] K. Golani, K. Goswami, K. Bhatt and Y. Park. "Fault Tolerant Traffic Engineering in Software-defined WAN," in *Proc. 2018 IEEE Symposium on Computers and Communications (ISCC)*, 25-28 June 2018, pp. 01205-01210.

[4] O. Lemeshko and O. Yeremenko. "Linear optimization model of MPLS Traffic Engineering Fast ReRoute for link, node, and bandwidth protection," in Proc. *2018 14th International Conference on Advanced Trends in Radioelecrtronics, Telecommunications and Computer Engineering (TCSET)*, 20-24 February 2018, pp. 1009-1013.

[5] O.V. Lemeshko, S.V. Garkusha, O.S. Yeremenko, and A.M. Hailan. "Policy-based QoS Management Model for Multiservice Networks," in Proc. *2015 International Siberian Conference on Control and Communications (SIBCON)*. 21-23 May 2015, pp. 1-4.

Тензорна модель швидкої перемаршрутизації із захистом рівня якості обслуговування

Євдокименко Марина Олександрівна,
Єременко Олександра Сергіївна,
Слейман Батуль

Харківський національний університет радіоелектроніки,
пр. Науки,14, м. Харків, 61166, Україна,
maryna.yevdokymenko@ieee.org,
oleksandra.yeremenko.ua@ieee.org,
sleimanbatoul@hotmail.com

Анотація. *Запропоновано тензорну модель швидкої перемаршрутизації із захистом рівня якості обслуговування в телекомунікаційній мережі. Новизна запропонованої моделі полягає в тому, що в умовах реалізації швидкої перемаршрутизації в мережі забезпечувався захист рівня обслуговування одночасно за показниками пропускної здатності, середньої міжкінцевої затримки та ймовірності втрат пакетів вздовж основного та резервного мультишляхів.*

Ключові слова: *тензорна модель, швидка перемаршрутизація, якість обслуговування, резервування, пропускна здатність, затримка, втрати пакетів.*

I. Вступ

Однією з важливих тенденцій розвитку телекомунікацій є проектування відмовостійких мереж, здатних зберігати свою високу ефективність в умовах ймовірних відмов комутаційного обладнання. Вирішення цієї наукової та прикладної задачі вимагає злагодженої роботи всього доступного функціоналу технологічних і протокольних засобів моделі взаємодії відкритих систем. Так, на мережному рівні ключова роль відводиться протоколам і методам швидкої перемаршрутизації, коли для передачі потоків пакетів розраховується не тільки основний, але й множина резервних маршрутів [1-2]. При цьому в ході швидкої перемаршрутизації важливо забезпечити захист рівня якості обслуговування вздовж цих маршрутів одночасно за множиною таких показників, як пропускна здатність, середня міжкінцева затримка та ймовірність втрат пакетів [3-5]. Тому рішення цієї важливої задачі вимагає розробки нових або вдосконалення існуючих математичних моделей і методів, які є теоретичною та алгоритмічно-програмною основою перспективних протоколів швидкої перемаршрутизації із захистом рівня якості обслуговування за множиною показників.

II. Тензорна модель швидкої перемаршрутизації із захистом рівня якості обслуговування

Для вирішення поставленої задачі використовувалась потокова модель швидкої перемаршрутизації [4], яка дозволяє забезпечити якість обслуговування за двома показниками: пропускної здастності та ймовірності втрат пакетів вздовж основного та резервного мультишляхів. Але відповідно до поставленої задачі для врахування такого важливого показника якості обслуговування як середня міжкінцева затримка пакетів, дана математична модель буде розширена за рахунок введення додаткової умови захисту цього показника, що, в свою чергу, є перевагою даного рішення. Тоді для введення додаткової умови захисту показника середньої міжкінцевої затримки було застосовано функціонал [6] тензорного моделювання процесів маршрутизації, завдяки якому виявилось можливим аналітично описати взаємозв'язок всіх введених основних показників якості обслуговування в мережі. Так, на підставі використання тензорної методології дослідження телекомунікаційна мережа була представлена двовалентним змішаним тензором в анізотропному просторі, який визначався структурою самої мережі. Метрика даного простору цілком залежала від типу потоків пакетів та дисциплін їх обслуговування на інтерфейсах маршрутизаторів мережі, а використання систем координат гілок мережі та незалежних контурів і вузлових пар дозволило забезпечити цілісний багатоаспектний розгляд телекомунікаційної мережі. Як результат, в рамках запропонованої моделі технологічна задача швидкої перемаршрутизації була сформульована в оптимізаційній формі з критерієм оптимальності та обмеженнями, якими виступали умови реалізації багатошляхової стратегії маршрутизації, умови збереження потоку, умови захисту каналу та вузла, умови захисту пропускної здатності мережі та умови забезпечення захисту рівня якості обслуговування за показниками ймовірності втрат пакетів і середньої міжкінцевої затримки вздовж основного та резервного мультишляхів.

III. Висновки

Для перевірки працездатності та адекватності запропонованої моделі було проведено експериментальне дослідження на ряді числових прикладів, в результаті якого були отримані основний і резервний мультишляхи, вздовж яких забезпечувався заданий рівень якості обслуговування за показниками пропускної здатності, середньої міжкінцевої затримки та ймовірності втрат пакетів.

Список літератури

[1] J. Rak. Resilient Routing in Communication Networks. 1st edition, Springer, 2015.

[2] D. Tipper. "Resilient network design: challenges and future directions." Telecommunication Systems, vol. 56, iss. 1, 2014, pp. 5-16.

[3] H. Hasan, J. Cosmas, Z. Zaharis, P. Lazaridis and S. Khwandah, "Development of FRR mechanism by adopting SDN notion," in Proc. 2016 24th International Conference on Software, Telecommunications and Computer Networks (SoftCOM), Split, 2016, pp. 1-7.

[4] O. Lemeshko, M. Yevdokymenko, O. Yeremenko, A.M. Hailan, P. Segeč and J. Papán. "Design of the Fast ReRoute QoS Protection Scheme for Bandwidth and Probability of Packet Loss in Software-Defined WAN," in Proc. 2019 15th International Conference the Experience of Designing and Application of CAD Systems in Microelectronics (CADSM), 26 February – 2 March 2019, pp. 3/72-3/76.

[5] O. Lemeshko, M. Yevdokymenko and Y. Anad Alsaleem Naors, "Development of the tensor model of multipath QoE-routing in an infocommunication network with providing the required Quality Rating," in Eastern-European Journal of Enterprise Technologies, vol. 5/2, iss. 95, 2018, pp. 40-46

.

Improvement quality of remote video surveillance by using the cloud CCTV technology

Ibrahim Araji
Martynchuk Oksana A.

Kharkiv National University of Radio Electronics, 14 Nauky Ave, Kharkiv UA-61166, Ukraine, ibrahim_araji@outlook.com, NTU "KhPI" 2, Kyrpychova str. 61002, Kharkiv, Ukraine oleksandr.martynchuk@nure.ua,

Abstract. *This work is devoted to the improvement of the quality of the remote video surveillance channel with the help of cloud-based video surveillance technology based on the use of polarization orthogonal antennas MIMO*

Keywords: *CCTV, Wi-Fi, MIMO, mixed polarization, orthogonal data coding.*

I. INTRODUCTION

.CLOUD technology based infrastructures can present significant advantages: lack of the necessary internal computing infrastructure; eliminates the lack of qualified personnel to install, maintain and troubleshoot; reliability.

It is the supplier that takes care of backup, business continuity, backup and disaster recovery. Significant cost scalability of CLOUD-based architecture appears: lack of initial investment; expected costs; pay only for what you use; Facilitate the increase or decrease in computing capacity, storage capacity and bandwidth on demand.

It seems relevant to further develop this technology, taking into account the possibility of using remote surveillance cameras. The positive effect can be based on the use of signals of double polarization and corresponding antennas.

II. PROBLEM SOLUTION AND RESULTS

The main features of the technology are as follows. Regardless of geography Unlimited tenants Accessibility of cloud architectures. A constantly growing number of cameras. Monitoring people is not available or almost impossible. Real waste of resources. Interesting events - only a small part of the recorded video. The data obtained using video surveillance has grown to almost unmanaged volumes.

The common misconceptions of CLOUD are not just remote storage or access to applications through a web browser. Why is cloud video storage impractical? The size of the data produced. The cost of storage and transfer. Limited available bandwidth.

Moving mountains around, very rare, like a golden spot lost in tons of stone. Miners do not move mountains of stone around! They bring mining equipment close to where gold ore is mined. And now what? Working with big data, cannot rely on much more efficient image compression algorithms, should rely on the boundary storage of high-quality HD video, should use video content analysis (VCA) to filter important footage (miniatures or short clips), describe significant events using Effectively searchable metadata.

Extracting interesting information on the site. Understanding is local and communication only when necessary. Smart cameras can filter out important events to reduce the amount of data sent to the data center, even with limited bandwidth. Motion Tracking Blob Motion Tracking and Trajectory Smoke Detection Fire Detection Face Detection Crowd Detection License Plate Recognition Detection of Lost and Found Motion Controls Controlling Origin, Blindness, Darkness Panic Detection Available Functions: Smart Products What you can do today.

Accurate image analysis: now possible, as it is done on RAW images from the sensor. Smart Products internal architecture. High resolution local storage and adaptive bandwidth external streaming. Broadband connection is not required. Bidirectional communication level, encrypted and automatic. Secure and reliable Internet connection Software for a virtualized data center with deployment in a private or public cloud. Control room wherever there is internet.

The further development of communication systems based on a double polarization signal is important. Transmit polarization diversity is proposed as an alternative to spatial separation in order to limit the aperture of the antenna arrays at both ends of the radio link. It is proposed to consider the possibility of using various combinations of polarization states of signals for radiation and reception. It is expected to receive a combination of polarization, when the fluctuations of the main signal of the channel polarization will be minimal.

Research results indicate different propagation conditions for different polarizations on two radiation patterns. Different orthogonal polarizations create different conditions for the improvement and development of tropospheric communication systems. Research results indicate the need to control the state of orthogonal polarizations depending on the distance and propagation conditions.

The investment and time required for the implementation of the described scenario, of course, is very long. Thus, it is important to develop effective ways of normalizing, combining and analyzing data from existing systems, while retaining most of the previous investments.

III. CONCLUSIONS

Research results indicate the possibility of increasing the communication range of a remote surveillance camera.

The basis is the study of various propagation conditions of radio waves at different polarizations. Different orthogonal polarizations create different conditions for the improvement and development of local communication systems.

REFERENCES

[1] Martynchuk A.A., Loshakov V.A., Oliver L.M/. Development of a trans-horizon communication system based on dual polarization MIMO architecture // "Проблемы электромагнитной совместимости перспективных беспроводных сетей связи (ЕМС-2015). – Харьков: ХНУРЭ, 2015.

[2] Popovskii V., Loshakov V., Filipenko O., Martynchuk O., Drif A./ Results of development tropospheric communications system / 2015 Second International Scientific Practical Conference "Problems of Infocommunications. Science and Technology". –Kharkiv, ANPRE, 2015.

Improving the quality of MIMO technologies of perspective communication channels when using polarized orthogonal data

Ayodele Tega Ajadi
Martynchuk Alexander

Kharkiv National University of Radio Electronics, 14 Nauky Ave, Kharkiv UA-61166, Ukraine, ayopauldele@gmail.com, oleksandr.martynchuk@nure.ua

Abstract. *In this article was derived method of finding the field components of the antenna signal and background noise, or processing in antenna with full polarization receiver. This will result to increase of bit rate of MIMO system on the basis of the use of polarization properties of signals, in the case of a real product. MIMO technology with orthogonal polarizing channels additional provides increase signal to noise ratio and therefore increase in bit rate in wireless net*

Keywords: *Wi-Fi, MIMO, mixed polarization, orthogonal data coding.*

I. INTRODUCTION

MIMO technology with orthogonal polarizing channels additional provides increase signal to noise ratio and therefore increase in bit rate in wireless [1].

MIMO is an important part of modern wireless communication standards such as IEEE 802.11n, ac (Wi-Fi), 4G, 3GPP Long Term Evolution, WiMAX.

II. PROBLEM SOLUTION AND RESULTS

The signal on the receiving party is recorded as follows:

$$X = H \cdot S + Z\,, \tag{1}$$

where S – matrix of transmitted signals; Z – matrix of a self-noise of the receiving elements of the antenna; X – matrix of the received signals; H – transformer matrix of the signals.

Most the simple and widespread matrix H is the Allamouti matrix.

Real antennae in MIMO technology can be represent like two input (top) and one output (bottom) antennae and this antennae can use at orthogonal polarization for better signal to noise ratio (SNR).

Its explain result of analysis differences of signal and noise polarizing parameters. Polarization is spatial - temporal characteristics of electromagnetic waves, it notes the spatial pattern of targeting vector voltage electric or magnetic field over the rotor vibration.

For homogeneous plane wave vector voltage electric and magnetic fields lie in the plane perpendicular to the direction of wave motion. Depending on whether parameters change (angle of orientation - β and angle of ellipse α) with the influence of polarization diagrams at time or remain constant, electromagnetic waves are divided into three groups: 1- completely polarized (polarization factor m=1); 2 - partially polarized (0<m<1); 3 – neutral or chaotic (m=0).

Consider the wave of elliptical polarization in the free linear basis and Ex, Ey orthogonal projection of the electric field vector E in the complex form. Represent wave in matrix form.

$$\vec{E_w}(t) = \begin{pmatrix} E_x(t) & E_y(t) \end{pmatrix}' \tag{2}$$

Polarization ellipse is defined by its shape (α), orientation axis (β) relative coordinate system selected and direction of rotation vector of the ellipse. The total form of wave is next

$$\vec{E_W}(t) = \begin{pmatrix} cos(\beta) & sin(\beta) \\ -sin(\beta) & cos(\beta) \end{pmatrix} \cdot \begin{pmatrix} cos(\alpha) & -j\,sin(\alpha) \\ -j\,sin(\alpha) & cos(\alpha) \end{pmatrix} \cdot \begin{pmatrix} E_0 \\ 0 \end{pmatrix} \cdot exp\{j(\omega \cdot t + \varphi_0)\} \tag{3}$$

Difference of polarization parameters between antennae and real signal described by loss of energy fact

$$P_{loss} = \cos^{-1}\left(\vec{E_S}, \quad \vec{E}\,in \right). \tag{4}$$

The dependence of throughput on SNR and given polarization losses for real conditions was calculated on the basis of the Shannon formula.

The results of the comparison of the real experiment of Alamouti / MRC algorithms with 2x2 multiplexing without antennas of orthogonal polarization indicate the following. We find that BER is close to 0.01 with a SNR of 10 dB for spatial multiplexing - QPSK and ML receiver (maximum likelihood).

Actual transmitted signal characterized by the parameters of the polarization ellipse - the angle of ellipticity and orientation angle of semi-major axis of the ellipse. Then, omitting the factors - angular frequency, attenuation and range, the vector of the electric field near a transmitting antenna can represented in the form of the polarization vector of the emitted signal

III. CONCLUSIONS

The result of the experiment means that the BR is better without loss of energy when the antennas are fully polarized. If BR is 11 MB / s with 10 dB SNR in real time and energy loss at 6 dB, then BR is 20 MB / s with 10 dB SNR and without energy loss due to polarization.

REFERENCES

[1] Martynchuk A.A., Loshakov V.A., Oliver L.M/. Development of a trans-horizon communication system based on dual polarization MIMO architecture // "Проблемы электромагнитной совместимости перспективных беспроводных сетей связи (EMC-2015). – Харьков: ХНУРЭ, 2015.

[2] Popovskii V., Loshakov V., Filipenko O., Martynchuk O., Drif A./ Results of development tropospheric communications system / 2015 Second International Scientific Practical Conference “Problems of Infocommunications. Science and Technology”. –Kharkiv, ANPRE, 2015.

Mobile info-communication systems and wireless 5G and 6G technologies

Tresor M.A.

Kharkiv National University of Radio Electronics, 14 Nauky Ave, Kharkiv UA-61166, Ukraine, mtumbeabitresor560@gmail.com, oleksandr.martynchuk@nure.ua,

Abstract. *This work is about the Wireless communication technologies Generation which is grown, advanced significantly in the mobiles telecommunications systems and networks*

Keywords: *NGN, 5G, 6G*

I. INTRODUCTION

The system is the first generation 1G, transmits in analog mode. To improve the quality of transmission, bandwidth and coverage of the signal system, the second generation of mobile 2G networks in digital mode has appeared, which marks a break with the previous technology. 3G opens the Internet and new multimedia services, 4G allows us to spread faster. But we have to introduce the next generation 5G, this is the fifth generation technology that will allow us to develop unimaginable digital services, it will be launched in 2020; and 6G, which is being researched in the future, this will be one of the greatest innovations in 2030, which is the actuality of the article.

II. PROBLEM SOLUTION AND RESULTS

This next stage of telecommunications will go far beyond accelerating data transmission speeds up to 10 Gigabits per second, opening new opportunities in transportation, medicine, manufacturing, many other industries and other areas of life. This technology dramatically improves the speed and consistency of 4G connections, higher spectral efficiency, better signaling and coverage over 4G, less latency in a millisecond, hundreds of thousands of wireless detection connections, running simultaneously. In addition to faster and more consistent wireless connection to users, 5G technology will contribute a great technological innovation in the vehicle industries with the driverless car; in medicine, allowing medical robots to become more common and doctors to perform more complex or difficult operations remotely; improving the efficiency of robots in manufacturing industries for wider use and with fewer errors. 3GPP (3rd Generation Partnership Project) is the body that regulates cellular standards, announced the first official standard of 5G, called the 5G NR standard (new radio), in December 2017. The 3GPP includes three groups of technical specifications (TSG) including RAN (radio access networks), SA (services and system aspects) and CT (core network and terminals). Qualcomm has always been involved in the development of 5G products and its research can be useful to 3GPP in designing the right standards. 5GPPP is considered as one of the pioneers of the standardization of the 5G protocol. These two groups are the most important groups for the development of 5G technology.

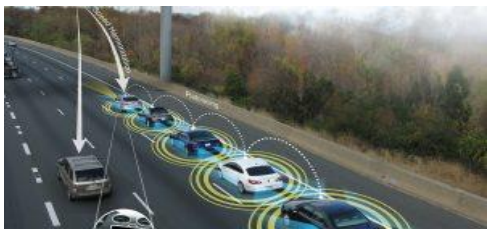


Figure 1. Driverless cars

Even if the 5G is not yet available, we can think about a future generation 6G, is proposed to integrate 5G with satellite networks for Global coverage, to resolve the needs of the user that the 5G will not be able to satisfy. In the next 10 years we will assist to a technological scandal, whose data transmission could go up to 1 Terabits per second. In 2018, the Center for Wireless Communications of the University of Oulu financed a project of the Academy of Finland "6 Genesis", research program that will be devoted to the conceptualization of 6G. In this program, new generations of mobiles will appear every 10 years, maybe around 2030 the 6G will be deployed. Another group of research from Terranova is working on a possibility of the 6G network connection that will be so fast and stable for 400 gigabits per second, transmission with a terahertz range.

III. CONCLUSIONS

In conclusion, we describing value of 5G performance in our daily life, with high data rate, reducing of latency, energy saving, cost reduction, higher system capacity, and massive device connectivity. The disadvantages of one this generation will be over by other which could be 6G. 5G will modernize the area of mobile telecommunication and wireless. This work demonstrates how it will be the types 5G applications. This initial design will allow us to experiment and look far as the result and how will be effective the 6G.

REFERENCES

[1] A. Banupriya,T Suba, K Rajalakshmi and S Rajasri, MILESTONE OF WIRELESS COMMUNICATION 1G TO 5G TECHNOLOGY March 2015.

[2] Rakesh Kumar Singh, Deepika Bisht and R.C. Prasad, Development of 5G Mobile Network Technology and Its Architecture, International Journal of Recent Trends in Engineering & Research,01 November 2017. 3. https://en.wikipedia.org/wiki/5G.

Аналіз методів оцінки надійності телекомунікаційних систем

Волотка Вадим Сергійович,
Бабін Вадим Вячеславович,
Бутенко Семен Олександрович

Харківський національний університет радіоелектроніки,
пр. Науки,14, м. Харків, 61166, Україна,
vadym.volotka@nure.ua,
vadym.babin@nure.ua,
semen.butenko@nure.ua

Анотація. *Метою дослідження надійності телекомунікаційних систем (ТКС) є прогнозування основних характеристик, їх функціонування при певних варіантах структурно-топологічної побудови і різних умов експлуатації. При цьому можуть використовуватися різні методи оцінки. Основна вимога – можливість отримання численних значень показників надійності.*

Ключові слова: *оцінка, надійність, аналіз, метод.*

I. Вступ

До теперішнього часу математична теорія надійності накопичила достатньо теоретичного і фактичного матеріалу, щоб гарантувати, що задачі обчислення показників надійності систем з розвиненою структурою в масі своїй мають комбінаторну складність, тобто, якщо використовувати терміни теорії складності алгоритмів, є NP-важкими [1]. Системи ТКС слід віднести до систем з розвиненою структурою, маємо на увазі структури розрахунку показників надійності. Основною принциповою причиною складності завдань розрахунку показників надійності є те, що цей розрахунок вимагає перерахування всіх елементів, що входять в структуру ТКС з безлічі. Оскільки точний аналітичний розрахунок показників надійносі систем з розвиненою струкутрою і з великим числом елементів практично неможливий, вдаються до наближеного оцінювання цих показників.

II. Методи оцінки надійності телекомунікаційних систем

Серед відомих найбільш популярними є такі моделі дослідження надійності ТКС:

- графова, яка використовується при розрахунках на етапах проектування та планування;
- модель, яка сама себе діагностує, при використанні якої зменшується обсяг службового трафіку.

Метод статистичного моделювання можна використовувати як засіб для перевірки і оцінки точності запропонованих наближених аналітичних методів. Це пов'язано з тим, що для складних структур сучасних ТКС точні аналітичні методи призводять до таких громіздких виразів, що практичне застосування їх стає неможливим. Тому, з одного боку, розвиваються наближені аналітичні методи, для яких завжди є актуальним питання про оцінку точності наближення, а з іншого - для багатьох систем на етапах проектування метод статистичного моделювання виявляється єдиним доступним методом. Якщо зіставити такі методи оцінки надійності ТКС, як метод мінімальних шляхів і мінімальних перетинів з методом статистичного моделювання, то можна сказати, що їх спільний недолік полягає в тому, що відповідно при великій кількості числа перетинів обчислення надійності стає трудомістким. А, наприклад, топологічний метод оцінки надійності таким недоліком не володіє. У нього такі особливості як відсутність обмежень на вигляд структурної схеми і простота обчислювальних алгоритмів. Багато практичні завдання оптимізації надійності, пов'язані з ТКС, можуть бути представлені у вигляді мережевої моделі. Запропоновано оцінювати надійність ТКС по апаратній та програмній частинам, розглядаючи їх незалежно один від одного. Для оцінки надійності апаратної частини ТКС на основі методу ізоморфізму запропоновано використовувати методи розрахунку надійності електронних засобів: приблизний, орієнтовний і остаточний. Визначено області використання вищевказаних методів і особливості застосування до розрахунку апаратної частини ТКС. Оцінку надійності програмних засобів доцільно проводити тими ж методами і з застосуванням таких же показників, що і апаратної частини. Більшість реальних ТКС, що забезпечують інформаційний обмін між великим числом територіально рознесених пунктів, має дуже складну структуру. Зв'язок між окремими пунктами інформаційної мережі може здійснюватися за багатьма можливих шляхів, включаючи транзит по цілому ряду пунктів. Суворий аналіз ТКС з довільною структурою, по суті, можливий лише методом прямого перебору. Кожен стан аналізується у відповідності до обраного критерію працездатності, що само по собі достатньо складно. До того ж навіть відносно прості реальні системи з числом елементів (каналів зв'язку і пунктів) близько 30-40 призводять до необхідності перебору мільйонів станів.

III. Висновки

Методи оцінки надійності ТКС орієнтовані на структури невеликого масштабу, а не для таких великих як ТКС. Головним недоліком цих методів є те, що при збільшенні розмірності мережі збільшується і громіздкість обчислень, виникають NP-повні задачі. Для розрахунку надійності мереж такого масштабу необхідно переходити з прямих методів розрахунку надійності до наближеної оцінки надійності всієї структури.

Список літератури

[1] Merle G., Roussel .-M., Lesage J.-J., Vayatis N. Analytical Calculation of Failure Probabilities in Dynamic Fault Trees including Spare Gates. – Proceedings of ESREL 2010 - European Safety a& Reliability Conference. September 2010.

[2] Boudali H., Dugan J.B. A continuous-time Bayesian network reliability modeling, and analysis framework. - IEEE Transactions on Reliability, vol. 55, No. 1, March 2006, pp. 86-97.

Виявлення DDoS атак статистичними методами

Радівілова Тамара Анатоліївна,
Тавалбех Максим Хаджем,
Глушаєв Денис Ярославович,
Заіка Максим Володимирович

Харківський національний університет радіоелектроніки,
пр. Науки,14, м. Харків, 61166, Україна,
tamara.radivilova@nure.ua, tavalbeh@icloud.com,
denys.hlushaiev@nure.ua, maksym.zaika@nure.ua

Анотація. *Запропоновано алгоритм виявлення вторгнень заснований на статистичних методах аналізу аномалій. Перевагою алгоритму є раннє виявлення вторгнень, за рахунок швидкого обчислення ентропії із застосуванням методу рухомого вікна. Запропонований алгоритм було програмно реалізовано та проведено експерименти на тестових даних, які було взято з датасетів.*

Ключові слова: *системи виявлення вторгнень, атаки, ентропія, аналіз аномалій, трафік.*

I. Вступ

Постійне збільшення використання мережевої зв'язку в останні роки призвело до збільшення ризику компрометації інформації. Методи вторгнень розвиваються і стають більш витонченими. Отже, класичні системи виявлення вторгнень показують зниження продуктивності при виявленні нових атак. [1]

Системи виявлення вторгнень класифікуються за методиками аналізу на сигнатурні, статистичні (аномальні) і гібридні. Статистичні методи створюють статистичну модель, що описує нормальний мережевий трафік, і ідентифікують будь-яку ненормальну поведінку, що відхиляється від моделі. Основною проблемою аномальних методів є складність в налаштуванні і велика кількість хибнопозитивних тривог в разі некоректно заданих правил [2]. У даній роботі основна увага приділяється системам виявлення вторгнень на основі аномалій, зокрема, щодо виявлення мережевих атак.

Статистичні методи виявлення аномалій створюють статистичну модель, що описує нормальний мережевий трафік та поведінку мережі, і ідентифікують будь-яку ненормальну поведінку, що відхиляється від моделі. На відміну від сигнатурних методів, методи на основі аномалій мають ту перевагу, що вони можуть виявляти атаки з нульовим днем, так як нові атаки можуть бути виявлені, як тільки вони відбудуться. Основною проблемою методів на основі аномалій є складність в налаштуванні і велика кількість хибнопозитивних тривог в разі некоректно заданих правил [2]. У даній роботі основна увага приділяється системам на основі статистичного виявлення аномалій, зокрема, щодо виявлення DDoS атак.

II. Статистичний метод виявлення DDoS атак

У зв'язку з цим запропоновано алгоритм виявлення та захисту від DDoS атак (таких як UDP-flood, потоків TCP SYN, Ping of Death атак та HTTP flood). Запропонований алгоритм зосереджується на трьох важливих частинах, а саме виявленні, захисті і повідомленні про напади. Запропонований алгоритм виявлення буде перевіряти вхідний трафік, будь то трафік DDoS або звичайний трафік. Якщо вхідний трафік є DDoS-трафіком, то запропонований алгоритм виявлення буде визначати типи DDoS-атак, такі як UDP-flood, потоків TCP SYN, Ping of Death та HTTP flood, засновані на поведінці атаки. Наш алгоритм виявлення вторгнень вимірює статистичні властивості конкретних полів в заголовках пакетів. Наприклад, якщо детектор захоплює 1000 послідовних пакетів в точці пірингу і обчислює частоту зустрічі кожної унікальної IP-адреси джерела в цих 1000 пакетах, то детектор буде мати модель розподілу адреси джерела. Подальші обчислення з цим розподілом дозволяють виміряти випадковість або однорідність адрес, а також «добротність» розподілу по відношенню до попередніх вимірювань. Далі застосовується умовна ентропія для виявлення відмінностей між розподілом класів пакетів в поточному трафіку в порівнянні з розподілом, знайденим в результаті методу максимуму. [2]

Ентропія трафіку залежить від ймовірностей p_i появи пакетів і-го типу при їх передачі $H = -\sum_{i=1}^{n} p_i \log_2 p_i$, де p_i – ймовірність появи пакету і-го типу, яка може виступати його частотою $f_i = n_i / N$; n_i – кількість пакетів і-го типу; N – загальна кількість пакетів трафіку. Для збільшення швидкості обчислень ентропії використовувався метод рухомого вікна.

Якщо кількість отриманих пакетів нижче значення ентропії в 0.3, пакет автоматично видаляється за допомогою алгоритму захисту. Алгоритм захисту забезпечить можливість проходження в мережі тільки легітимного трафіку.

Для аналізу роботи запропонованого алгоритму проводився аналіз трафіку з датасету [3]. Датасет містив нормальний трафік та атаки DDoS, UDP-flood, потоків TCP SYN, Ping of Death та HTTP flood.

III. Висновки

Запропонований алгоритм виявлення вторгнень на основі статистичних методів аналізу аномалій показав високі значення точності виявлення атак (близько 94%) та низькі значення помилкового позитивного показника (близько 16%).

Список літератури

[1] Gupta, N., Srivastava, K., Sharma, A.: Reducing False Positive in Intrusion Detection System: A Survey. International Journal of Computer Science and Information Technologies 7 (3), 1600-1603 (2016)

[2] Vytalii Bulakh, Lyudmyla Kirichenko, Tamara Radivilova. Classification of Multifractal Time Series by Decision Tree Methods. 14th International Conference ICTERI 2018 ICT in Education, Research, and Industrial Applications, 2018, p.1-4.

[3] Al-kasassbeh, M.; Al-Naymat, G.; Al-Hawari, E. Towards Generating Realistic SNMP-MIB Dataset for Network Anomaly Detection. Int. J. Comput. Sci. Inf. Secur. 2016, 14, 1162–1185.

Огляд змін та проблеми програмування на Python

Гузей Ольга Іванівна

Харківський національний університет радіоелектроніки, пр. Науки 14, Харків, UA-61166, Україна
olha.huzei@nure.ua

Анотація. *Розглядається Python як мова програмування, її актуальність на даний момент та проблеми, з якими зустрічаються початківці та досвідчені спеціалісти. Розглядаються методи покращення написання та компіляції коду. Визначається дієздатність та актуальність цієї мови в сучасному світі. Плани розробників на подальші оновлення.*

Ключові слова: *Python, програмування, Jupyter, Visual Studio, Just-in-time (JIT).*

I. Вступ. Постановка завдання

Мова програмування Python, розробка якої була закінчена в 1991 році, на думку багатьох спеціалістів являє собою одну з найкращих та популярних мов, стала особливо популярною в останні роки для створення веб-сайтів з використанням їх численних веб-фреймворків.

Python - це 3 речі: мова, стандартна бібліотека і механізм виконання. Python, ймовірно, найпростіший спосіб зробити що-небудь найближчим часом. І в наші дні його популярність також зросла, є кілька тонн бібліотек. як для Big Data, так і для машинного навчання [1]. Останнім часом все більше спірних запитань щодо актуальності цієї мови та чи є подальший розвиток і удосконалення її механізмів. Завданням роботи є огляд найважливіших аспектів роботи з Python, змін, які були впроваджені за останні роки та методів покращення написання та компіляції коду.

II. Вирішення Проблеми Та Результати

Python існує вже 25 років, але найбільш важливою з усіх перетворень була зміна самого процесу розвитку мови і перехід на більш прозорий процес його створення. Python 3.0 була розроблена задля усунення фундаментальних недоліків у мові. Однією з відчутних змін є відсутність у версії 3.x оператора print, проблеми з виконанням старого коду, дійсно, можуть виникнути.

В перших двох версіях (3.0, 3.1) виник ряд серйозних помилок і проблем з безпекою. Python 3.3 був першим випуском серії 3.x, що включає швидкі десяткові типи, virtualenv в якості основної функції і підтримку пакету простору імен [5].

Ефективний план переходу старої бази кодів в Python 3 супроводжує створення надійних інструментів і допоміжних засобів, що полегшують процес переходу. До числа таких інструментів відносяться наступні: конвертор кодів 2 to 3, найостанніший випуск Python 2.x (як мінімум 2.6), а також зовнішній інструмент 3 to 2 і бібліотека six [2].

Зараз, коли CPython знаходиться на GitHub, що може означати лише одне, спільнота сперечається про функції системи відстеження проблем або, що означає, що все більше людей піднімають pull-запити, виправляють помилки і покращують підтримку платформи Python.

Розширення Python для редактора коду Visual Studio отримав деякі нові функції Jupyter в грудневому випуску. У новому випуску розширення Python для коду Visual Studio розробники Python тепер мають нові опції для експорту файлів Python у вигляді блокнотів Jupyter. Нова версія також включає в себе віддалену підтримку Jupyter [4].

Методи покращення написання та компіляції коду:

– впровадження інструментів для полегшення упакування Python та компіляції його в exe;
– використовуючи PyOpenCL і багатопроцесорну бібліотеку в 3.6 (і нижче), можливе використання міці обробки на GPU для високопаралельних обчислень. Для Python, щоб закріпити свою позицію як Data Science, машинного навчання King, вбудована підтримка паралельної обробки на GPU була б чудовою;
– NumbaPro, який використовує окремий JIT-движок для компіляції в паралельні нативні потоки, але він специфічний для NumPy. Поряд з підтримкою PEP523 (JIT) вбудований модуль компіляції може використовувати CPython для паралельного виконання в графічних процесорах;
– Муру прагне об'єднати переваги динамічної (або «качиної») типізації та статичної типізації, які можливо втілити в Python 4.0, оскільки все більше і більше даних, споживаних з служб REST в JSON, такі бібліотеки, як схема, можуть бути надзвичайно корисні при перевірці введення даних [5].

III. Висновки

Перш за все, нічого не змінилося в процесі пропозиції щодо поліпшення Python розробниками - все ще пропонуються зворотньо сумісні зміни з додаванням нових модулів (наприклад asyncio) і мовних функцій (наприклад yield from) для розширення можливостей, доступних для додатків Python. Згодом Python 3 буде продовжувати випереджати Python 2 по можливостям, які він пропонує за замовчуванням, навіть якщо користувачі Python 2 мають доступ до еквівалентних можливостей через сторонні модулі або бекпорти з Python 3 [3]. Конкуруючі реалізації та розширення інтерпретатора також продовжать досліджувати різні способи поліпшення Python, включаючи дослідження PyPy генерації JIT-компіляторів і пам'яті транзакцій програмного забезпечення, а також дослідження співтовариства дослідників і даних в області програмування, орієнтованого на масиви, яке в повній мірі використовує пропоновані можливості векторизації сучасними, графічними процесорами. Очікується, що з часом покращиться інтеграція з іншими середовищами виконання віртуальних машин (такими як JVM і CLR), особливо з урахуванням того, що Python впроваджується в освітній сектор, що може зробити його ще більш популярним в якості вбудованої мови сценаріїв у великих додатках, що працюють в цих середовищах [3].

В Python 4 не повинно бути такої ж величезної кількості критичних змін, як в 3, але ці зміни будуть необхідні для просування Python в майбутнє.

Перелік Посилань

[1] Wes McKinney, “Python for Data Analysis”, O’Reilly Media, Inc., 1005 Gravenstein Highway North, Sebastopol, CA 95472, pp. 453, October 2012.
[2] Wesley J. Chun “Core Python Applications Programming, 3rd Edition”, Pearson Education, Inc., pp. 816, 2012.
[3] Офіційний сайт www.curiousefficiency.org - Інформаційний портал - http://www.curiousefficiency.org/posts/2014/08/python-4000.html
[4] Офіційний сайт www.visualstudiomagazine.com – Інформаційний портал - https://visualstudiomagazine.com/articles/2018/12/14/vs-code-python-december.aspx
[5] Офіційний сайт www.hackernoon.com – Інформаційний портал -

ЗМІСТ

Наукове видання

«КОМП’ЮТЕРНІ ТА ІНФОРМАЦІЙНІ СИСТЕМИ І ТЕХНОЛОГІЇ»

Відповідальні за випуск: Рубан І.В.,
Коваленко А.А.,
Мовсесян Я.С.

Комп'ютерна верстка: Коваленко А.А.
Мартовицький В.О.
Мовсесян Я.С.

Матеріали збірника публікуються у авторському варіанті без редагування

Затверджено Науково-технічною радою Харківського національного університету радіоелектроніки № 3 від 19.04.2019 р.