МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЦЕНТРАЛЬНОУКРАЇНСЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЧЕРКАСЬКИЙ ДЕРЖАВНИЙ ТЕХНОЛОГІЧНИЙ УНІВЕРСИТЕТ

Кваліфікаційна наукова
праця на правах рукопису

Котелянець Віталій Володимирович

УДК 004.716:504.064.36

ДИСЕРТАЦІЯ

ІНФОРМАЦІЙНА ТЕХНОЛОГІЯ МОНІТОРИНГУ НАВКОЛИШНЬОГО СЕРЕДОВИЩА НА БАЗІ КОНЦЕПЦІЇ ІНТЕРНЕТУ РЕЧЕЙ

05.13.06 – «Інформаційні технології»

Подається на здобуття наукового ступеня кандидата технічних наук

Дисертація містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело ___

Науковий керівник:
Смірнов Олексій Анатолійович,
доктор технічних наук, професор
Центральноукраїнський національний технічний університет, завідувач кафедри кібербезпеки та програмного забезпечення

Кропивницький – 2019

АНОТАЦІЯ

Котелянець В.В. Інформаційна технологія моніторингу навколишнього середовища на базі концепції Інтернету речей. – Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття наукового ступеня кандидата технічних наук за спеціальністю 05.13.06 – Інформаційні технології. – Черкаський державний технологічний університет, Черкаси, 2019.

Дисертаційна робота присвячена розв’язанню актуальної й важливої науково-технічної задачі розроблення стохастичної інформаційної технології моніторингу параметрів навколишнього середовища в сучасній концепції Інтернету речей з урахуванням апріорної невизначеності джерел інформації та можливості виникнення кризових ситуацій.

У роботі проведено аналіз принципів побудови, технологічних рішень і напрямів розвитку систем моніторингу в концепції Інтернету речей, у результаті чого виявлено недоліки відомих підходів і доведено необхідність створення математичних моделей, методів, комунікаційних протоколів мереж WSN з випадковим доступом і відповідних інформаційних технологій моніторингу для забезпечення високої продуктивності, якості і живучості їх функціонування.

Встановлено, що концепція Інтернету речей має три взаємопов’язані базові проблеми – це забезпечення інформаційної безпеки (Internet of Things Security), масштабування зростаючого обсягу технічних пристроїв і даних (Internet of Things Scalability), а також урахування вимог до зниження енергоспоживання (Internet of Things Technical Solutions and Low-Power Consumption). Також, проведено аналіз протоколів для вирішення завдань Інтернету речей:

1) MQTT: протокол для збору даних пристроїв і передавань їх серверів (D2S). Легкий і простий протокол обміну повідомленнями, який реалізує так звану модель «публікація / підписка» і призначений для зв'язку

комп'ютеризованих пристроїв, підключнних до локальної або глобальної мережі, між собою і різними громадськими чи приватними веб-сервісами.

2) XMPP: протокол для з'єднання пристроїв з людьми, частковий випадок D2S-схеми, коли люди з'єднуються з серверами. Розширюваний протокол обміну повідомленнями та інформацією про присутність. Він був розроблений для системи миттєвого обміну повідомленнями для зв'язку між людьми за допомогою текстових повідомлень.

3) DDS: швидка шина для інтегрування інтелектуальних пристроїв (D2D);

4) AMQP: система організація черг для з'єднання серверів між собою (S2S). Вдосконалений протокол організації черги повідомлень), який іноді розглядають як протокол Інтернету речей. Як випливає з назви, AMQP обслуговує виключно черги. Він пересилає транзакційні сполучення між серверами. Цей протокол в якості орієнтованого на повідомлення проміжного програмного забезпечення, був створений для банківської галузі і здатний обробляти тисячі організованих в чергу транзакцій.

Удосконалено стохастичні моделі функціонування бездротових сенсорних мереж, які використовують рандомізовані мережеві параметри (зі змінною кількістю вузлів і випадковою участю вузлів в окремих групах мережевих вузлів), що дозволило оцінити ймовірність колізії сигналів і більш ефективно проектувати протоколи комунікації Інтернету речей.

Зазначені моделі дозволили оцінити ймовірність колізії сигналів: максимальна кількість вузлів, які забезпечують якість передавання на рівні ймовірності колізії не вище 10^{-2}, становить 50 шт., причому кількість задіяних в колізії вузлів нехтовно мала в порівнянні з середньою кількістю передавань, зокрема відношення середньої кількості задіяних в колізії вузлів до середньої кількості передавань становить 10^{-7}.

Удосконалено метод моніторингу параметрів навколишнього середовища, який враховує нестаціонарну просторово-часову локалізацію первинних джерел вимірювань та оптимізацію процесу динамічного

моніторингу, що дало можливість забезпечити своєчасне та оперативне надходження інформації від первинних джерел інформації із заданими показниками якості для ефективного прийняття управлінських рішень.

Методологічні засади удосконаленого методу спрямовані на функціонування в умовах кризових ситуацій і охоплюють чотири базових режими: 1. Звичайний (стандартне функціонування, штатний режим роботи); 2. Підвищеної готовності (нестандартне функціонування, активна підготовка та практична імплементація низки превентивних / попереджувальних заходів); 3. Кризовий (дії в умовах виникнення кризової ситуації); 4. Післякризовий (ліквідація довгострокових наслідків кризового режиму).

Отримала подальший розвиток інформаційна технологія моніторингу, яка за рахунок використання стохастичних моделей функціонування бездротових сенсорних мереж та удосконаленого методу моніторингу, дозволила забезпечити ефективне спостереження і контроль параметрів навколишнього середовища. Ця технологія із використанням засобів Arduino, JavaScript, NodeJs, HTML та CSS дала можливість розробити відповідний програмно-технічний комплекс моніторингу реального часу в сучасній концепції Інтернету речей. Зазначений програмно-технічний комплекс може використовуватись як прототип для організації моніторингу в динамічно змінюваних середовищах та при виникненні критичних ситуацій різного характеру. До складу програмно-технічного комплексу включені наступні підсистеми (проте комплекс є гнучким і може змінюватись відповідно до запитів користувачів і наявного обладнання):

1) Акумулювання даних. Ця підсистема поєднує віддалені автоматизовані робочі місця суб’єктів загальної системи моніторингу, які збирають дані і передають за визначеними комунікаційними (мережевими) протоколами до центру системи управління.

2) Інфокомунікацій. Ця підсистема є синтезом сучасної продуктивної і надійної серверної частини, високошвидкісних мереж зв’язку (у тому числі й WSN) та комунікаційних протоколів. У складі програмно-технічного комплексу

вона забезпечує приймання даних від автоматизованих робочих місць, їх обробку і запис до відповідних баз даних, ефективну комунікацію з відокремленим інформаційно-аналітичним центром, а також з особами, що приймають управлінські рішення тощо.

3) Обробки первинного інформаційного трафіку та аналітики. Зазначена підсистема включає в себе автоматизовані робочі місця адміністраторів баз даних і відповідних фахівців, які приймають, обробляють та аналізують первинний інформаційний трафік. Автоматизовані робочі місця адміністраторів розподіляють доступ відповідно до фіксованих повноважень, узгоджують надходження і видачу даних, а також забезпечують захист даних і їх вчасне відновлення у випадку збоїв і аварій різноманітного характеру. Автоматизовані робочі місця фахівців, які є забезпеченими необхідними технічними / програмними засобами і сучасним високошвидкісним зв'язком, здійснюють попередній аналіз первинного інформаційного трафіку, його уніфікацію, занесення до відповідних баз даних, моделюють кризові ситуації і відпрацьовують плани виходу з них.

4) Відображення і аналізу даних. Ця підсистема містить цифрові карти (локальні та глобальні); інформаційно-пошукові засоби; модулі синтезу цифрових карт та баз даних; засоби картографічного аналізу і візуального представлення результатів у зручному для кінцевих користувачів вигляді.

5) Підтримки баз даних. Зазначена підсистема базується на спеціальному програмному забезпеченні і є орієнтованою на створення, збереження і забезпечення доступу користувачів до інформаційних ресурсів. Також, вона виконує певні функції захисту інформації, зокрема, архівування і створення резервних копій на випадок виникнення кризових ситуацій чи інцидентів.

Проведено експериментальне дослідження запропонованих моделей, методу та інформаційної технології моніторингу. Розроблено спеціалізовані UML-діаграми прецидентів моделювання та послідовності моделювання запропонованої інформаційної технології. Результати дисертації використані та

впроваджені в Національному авіаційному університеті, Центрально-українському національному технічному університеті та телекомунікаційній компанії Local Students Networks.

Ключові слова: інформаційна технологія, моніторинг навколишнього середовища, Інтернет речей, стохастичні моделі, метод моніторингу, програмно-технічний комплекс моніторингу, бездротова сенсорна мережа.

ABSTRACT

Kotelianets V. Information Technology for Environmental Monitoring Based on Internet of Things Concept. – Qualifying scientific work as a manuscript.

Thesis for a Candidate of Technical Science (PhD) degree on specialty 05.13.06 – Information Technology. – Cherkasy State Technological University, Cherkasy, 2019.

Thesis is devoted to solving the urgent and important scientific and technical task of developing stochastic information technology for monitoring environmental parameters in the modern Internet of Things concept, taking into account the a priori uncertainty of the sources of information and the possibility of emerging crisis situations.

The analysis of principles of construction, technological decisions and directions of development of monitoring systems in the Internet of Things concept was carried out. As a result of this analysis shortcomings of known approaches were identified and the necessity of creating mathematical models, methods, communication protocols of WSN networks with random access and corresponding information monitoring technologies for ensuring high productivity, quality and the vitality of their functioning was proved.

It has been established that the Internet of Things concept has three interrelated basic issues: providing information security (Internet of Things Security), scaling up the growing volume of technical devices and data (Internet of Things

Scalability), and also Internet of Things Technical Solutions and Low-Power Consumption. Also, the analysis of protocols for solving Internet of Things tasks was carried out:

1) MQTT: protocol for collecting data of devices and transmitting their servers (D2S). Easy and easy messaging protocol, which implements the so-called. model «publication / subscription» and is intended for communication of computerized devices, connected to the local or global network, with each other and various public or private web services.

2) XMPP: protocol for connecting devices to humans, partial case of D2S-schemes when people connect to servers. Extensible messaging protocol and presence information. It was designed for instant messaging for people to communicate with text messages.

3) DDS: fast bus for integrating smart devices (D2D);

4) AMQP: The system organizes queues for connecting servers to each other (S2S). Improved protocol for arranging message queues), which is sometimes viewed as a protocol for the Internet of Things. As the name implies, AMQP serves exclusively queues. It transmits transaction connections between servers. This protocol, as intermediate-oriented messaging, was created for the banking industry and capable of handling thousands of transaction-based transactions.

Stochastic models of the functioning of wireless sensor networks that use randomized network parameters (with variable number of nodes and random participation of nodes in separate groups of network nodes) have been improved. It allowed to estimate the probability of collision of signals and to more effectively design communications protocols of the Internet of Things. These models allowed to estimate the probability of collision of signals: the maximum number of nodes that provide the quality of transmission at the level of the probability of collision no higher than 10^{-2} is 50, with the number of nodes involved in the collision is negligible in comparison with the average number of transmissions, in particular the ratio of the average number involved in the collision of nodes to the average number of transmissions is 10^{-7}.

The method of monitoring environmental parameters has been improved. It takes into account the unsteady spatial and temporal localization of primary sources of measurement and optimization of the dynamic monitoring process, which made it possible to ensure the timely and prompt receipt of information from primary sources of information with specified quality indicators for effective management decision-making.

The development of information monitoring technology, which, due to the use of stochastic models of the operation of wireless sensor networks and the advanced monitoring method, has allowed the software-technical complex (using Arduino, JavaScript, NodeJs, HTML and CSS) to monitor real-time environment parameters in the modern Internet of Things concept. The designated software-technical complex for monitoring of real-time environmental parameters can be used as a prototype for monitoring organization in dynamically changing environments and in case of emergencies of a different nature (in various spheres).

The designated software-technical complex can be used as a prototype for monitoring organization in dynamically changing environments and in case of emergencies of a different nature. The following subsystems are included in the software-technical complex (however, the complex is flexible and may vary according to user requests and available equipment):

1) Data storage. This subsystem combines remote automated workplaces of entities of the general monitoring system, which collect data and pass on defined communication (network) protocols to the control system center.

2) Infocommunications. This subsystem is a synthesis of the modern productive and reliable server part, high-speed communication networks (including WSN) and communication protocols. As part of the software-technical complex, it provides the reception of data from automated workplaces, their processing and recording to the corresponding databases, effective communication with a separate information and analytical center, as well as with those who make managerial decisions etc.

3) Processing of primary information traffic and analytics. This subsystem includes automated workplaces of database administrators and relevant specialists who receive, process and analyze primary informational traffic. Automated workplace administrators allocate access in accordance with the fixed authority, coordinate the receipt and delivery of data, and provide data protection and their timely recovery in the event of a variety of failures and accidents. Automated workplaces of specialists who are provided with the necessary technical / software tools and modern high-speed communication, carry out a preliminary analysis of the primary information traffic, its unification, insertion into the corresponding databases, model crisis situations and work out their exit plans.

4) Data display and analysis. This subsystem contains digital maps (local and global); information retrieval tools; modules for synthesis of digital maps and databases; means of cartographic analysis and visual presentation of results in the form convenient for end users.

5) Database support. The specified subsystem is based on special software and is focused on the creation, storage and provision of users access to information resources. It also performs certain security functions, including archiving and backup in case of emergencies or incidents.

The experimental research of proposed models, method and information technology of monitoring was carried out. It has been found that when transmitting data at short distances (for example, indoors – laboratory, office, home), devices can use the PAN provided by wireless technologies such as BLE (Bluetooth Low Energy), ZigBee, 6LoWPAN and the leading USB interface. When it comes to transmitting data over long distances (for example, in an large office or in a large building), you can use a Local Area Network. Wired LAN in most cases is based on Ethernet and fiber optic technology, and wireless one can be based on Wi-Fi technology. Also can be used WiMAX, LTE, and LPWAN to organize global WAN. Measured parameters are not limited to humidity and air temperature (as it was performed in experimental part of this thesis). Any parameters can be used in view of available sensors, which are part of the software-technical complex.

Besides, specialized UML diagrams of simulation precedents and simulation sequences of the proposed information technology have been developed. The results of the dissertation have been used and implemented at the National Aviation University, the Central Ukrainian National Technical University and the telecommunication company Local Students Networks (special implementation acts are attached to thesis).

Keywords: information technology, environmental monitoring, Internet of things, stochastic models, monitoring method, software and hardware monitoring complex, wireless sensor network.

Список основних публікацій здобувача:

1. Hu Z., Gizun A., Gnatyuk V., Kotelianets V., Zhyrova T., «Method for rules set forming of cyber incidents extrapolation in network-centric monitoring», *Proceedings of 2017 4th International Scientific-Practical Conference Problems of Infocommunications Science and Technology (PIC S&T 2017),* pp. 121-132, 2017 DOI: 10.1109/INFO COMMST.2017.8246435 *(Scopus).*

2. S. Gnatyuk, V. Kinzeryavyy, I. Stepanenko, Ya. Gorbatyuk, V. Kotelianets, «Code obfuscation technique for enhancing software protection against reverse engineering», *Advances in Intelligent Systems and Computing,* Springer, pp. 232-239, 2018 *(Scopus,Web of Science).*

3. V. Gnatyuk, N. Dyka, V. Kotelianets, S. Dakov, «IoT architecture for air pollution monitoring system», *Proceedings of VII Międzynarodowa Konferencja Studentów oraz Doktorantów «Inżynier XXI wieku»,* Bielsko-Biala, pp. 83-97, 2017.

4. Смірнов О.А., Котелянець В.В., «Стійкі до колізій стохастичні моделі функціонування бездротових сенсорних мереж», *Вісник інженерної академії України*, №3, с. 145-152, 2018.

5. Гнатюк С.О., Котелянець В.В., Кищенко В.В., Бауиржан М.Б., «Мережево-центричний моніторинг інцидентів кібербезпеки у секторах

критичної інфраструктури держави», *Кібербезпека: освіта, наука і техніка,* №2, с. 80-89, 2018.

6. Котелянець В.В., Усик П.С., Кищенко В.В., Гнатюк В.О., «Інтелектуалізована система моніторингу параметрів навколишнього середовища на базі технології інтернету речей», *Вісник інженерної академії України,* №4, с. 133-140, 2018.

7. Одарченко Р.С., Ткаліч О.П., Дика Н.В., Котелянець В.В. «Дослідження можливостей комунікаційних протоколів для потреб IoT», *Проблеми інформатизації та управління,* Том 3, № 59, с. 43-55, 2017.

8. Гнатюк В.О., Терентьєва І.Є., Котелянець В.В., «Модель даних для удосконалення кібербезпеки IP-АТС», *Безпека інформації,* Том 24, № 3, с. 175-180, 2018.

9. Gnatyuk S., Sydorenko V., Polishchuk Yu., Kotelianets V., «Analisys of modern aaproaches to security assessment of information resources for critical information infrastructure of the state», *Scientific and Practical Cyber Security Journal*, Vol. 2, №4, p. 81-86, 2018.

10. Odarchenko R., Gnatyuk V., Sydorenko V., Kotelianets V., «Quality of service assessment rules development for mobile operators», *збірник тез доповідей III міжнародної наук.-практ. конференції «Інформаційна безпека та комп'ютерні технології»,* 19-20 квітня 2018 р., м. Кропивницький: ЦНТУ, с. 168-169, 2018.

11. Смірнов О.А., Котелянець В.В., «Застосування концепції Інтернету речей для побудови інтелектуалізованих систем моніторингу параметрів навколишнього середовища», *матеріали VI всеукраїнської наук.-практ. конференції молодих учених і студентів з міжнародною участю «Проблеми та перспективи розвитку авіації та космонавтики»,* 29-30 листопада 2017 р., К. : НАУ, с. 47-48, 2017.

12. Котелянець В.В., «Базові аспекти побудови сучасних систем моніторингу довкілля на основі концепції Інтернету речей», *матеріали X міжнародної наук.-практ. конференції «Інтегровані інтелектуальні*

робототехнічні комплекси (ІІРТК-2017)», 16-17 травня 2017 р., К.: НАУ, с. 184-186, 2017.

13. Котелянець В.В., Ткаліч О.П., Гнатюк С.О., «Метод підвищення кібербезпеки ір-телефонії», *матеріали ІІІ міжнародної наук.-техн. конференції «Інформаційна безпека у сучасному суспільстві»,* 29-30 листопада 2018 р., м. Львів: Видавництво ЛДУБЖД, с. 16-18, 2018.

14. Котелянець В.В., «Розробка і дослідження програмно-технічного комплексу моніторингу параметрів навколишнього середовища реального часу», *збірник матеріалів IV міжнародної наук.-практ. конференції «Актуальні питання забезпечення кібербезпеки та захисту інформації»,* 21-24 лютого 2018 р., с. Верхній Студений: Видавництво Європейського університету, с. 26-28, 2018.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

АРМ – автоматизоване робоче місце;

АС – автоматизована система;

ІКС – інформаційно-комунікаційна система;

ІКТ – інформаційно-комунікаційні технології;

ІТ – інформаційна технологія;

НСД – несанкціонований доступ;

ПЗ – програмне забезпечення;

ПТК – програмно-технічний комплекс;

BLE – протокол bluetooth з режимом економії електроенергії;

CDMA – множинний доступ із кодовим розподілом;

CSS – мова для опису веб-інтерфейсів;

EDCA – удосконалений розподілений доступ до каналу;

ESSID – ідентифікатор розширеного набору послуг;

GPS – система глобального позиціонування;

IoT – Інтернет речей;

IP – Інтернет протокол;

IrDA – асоціація передавання даних в інфрачервоному діапазоні;

ISO – Міжнародна організація по стандартизації;

ITU – Міжнародний союз електрозв’язку;

LAN – локальна мережа;

LTE – стандарт бездротового передавання даних 4G;

MQTT – спрощений мережевий протокол, що працює на TCP / IP;

NIST – Національний інститут стандартизації і технологій США;

OSI – взаємодія відкритих систем;

QoS – якість обслуговування;

TCP – протокол управління передачею даних;

UML – уніфікована мова моделювання;

WLAN – безпроводова локальна мережа;

WSN – бездротова сенсорна мережа.

ВСТУП

Актуальність. Сьогодні існує нагальна необхідність контролю та вимірювання майже всіх фізичних величин у великій кількості і майже в усіх галузях діяльності людини. Застосування сенсорів та пов'язаних з ними комунікаційних вузлів дає уявлення про універсальність проблеми розвитку бездротових сенсорних мереж (Wireless Sensors Network, WSN), зокрема, у будинках та будівлях; на промислових об'єктах; на складах; у природному довкіллі (у лісах, на полях, над річками, в горах, у ґрунті, в повітрі і т.д.); в середовищі, ураженому біологічною та хімічною зброєю; в автомобілях і літаках; на рухомих перехрестях; на дні океану; всередині великих машин, обертових сфер, куль; на поверхні океану під час торнадо; на полі бою за лінією фронту; як індикатор для тварин та товарів; у річках в поєднанні з енергією води тощо.

Розвиток електроніки, інформаційних та комунікаційних технологій (ІКТ) дав підстави для реалізації ідеї вимірювань і контролю будь-яких необхідних фізичних величин середовища, промислових процесів, процесів керування, моніторингу тощо. Такий величезний обсяг застосувань вимірювальної техніки, який також реалізовується у рухомих (мобільних) об'єктах, вимагає рішень, що відносяться до техніки збирання, передавання та обробки інформації для різного типу використовуваних процесів. Розроблено і впроваджено багато мережевих рішень на базі попереднього досвіду з реалізації ІКТ в концепції Інтернету речей (IoT), що являють собою обчислювальні мережі фізичних предметів (тобто власне, речей), які оснащені технологіями для взаємодії один з одним. У цих рішеннях домінують детерміністичні алгоритми доступу функціонування мережі. Кількість рішень є достатньо великою і різноманітною (мережі LAN, MAN, WAN, WLAN, Wi-Fi, мобільна телефонія, Bluetooth, ZeegBee і т.д.).

Серед вчених, які зробили вагомий внесок у розвиток сучасних інформаційних систем моніторингу, варто відмітити таких вітчизняних і

закордонних фахівців, як Бертсекас Д., Болгер Дж., Гандел Р., Девід Е., Комарова Л., Романюк А., Райба С., Шахгільдян В. та ін. Проте, для окремого виду застосувань з багатьох причин попередні рішення, такі як, наприклад, детерміністичні рішення, є мало придатними (витрати на обладнання, складність, високі енергетичні потреби, складність алгоритмів, широка займана радіосмуга) – це значно обмежує можливість їх застосування. У той же час, пошуки стохастичних рішень відкривають широкі можливості доповнення, які до цього були мало придатними мережевими рішеннями у деяких застосуваннях (для неможливої до цього часу реалізації). Вони поширюють категорію рішень для сучасних застосувань, наприклад, моніторинг навколишнього середовища, лікарняний моніторинг тощо. З огляду на це, розроблення інформаційних технологій моніторингу навколишнього середовища в концепції IoT є *актуальною науково-технічною задачею,* що має важливе наукове та практичне значення.

Зв'язок роботи з науковими програмами, планами, темами. Дослідження проводились у відповідності із Законом України «Про Концепцію Національної програми інформатизації» (№ 75/98-ВР від 04.02.1998 р.) та Концепцією розвитку зв'язку України (№ 2238 від 9.12.1999 р.), а отримані здобувачем результати відображені у звітах держбюджетних науково-дослідних робіт Національного авіаційного університету («Організація систем захисту інформації від кібератак», д.р. № 0111U000171, виконавець) та Центрально-українського національного технічного університету («Розробка методів синтезу тестових моделей поведінки програмних об'єктів, підвищення оперативності передачі та захисту інформації у телекомунікаційних системах», д.р. № 0115U003103, виконавець).

Метою дослідження є розроблення стохастичної інформаційної технології моніторингу параметрів навколишнього середовища в сучасній концепції Інтернету речей з урахуванням апріорної невизначеності джерел інформації та можливості виникнення кризових ситуацій.

Для досягнення цієї мети необхідне розв'язання наступних задач:

1. Провести аналіз принципів побудови, технологічних рішень і напрямів розвитку систем моніторингу в концепції IoT та можливого використання для вирішення поставленого завдання.

2. Розробити і дослідити стохастичні моделі функціонування бездротових сенсорних мереж для оцінювання ймовірності колізії сигналів у системі.

3. Удосконалити метод моніторингу параметрів навколишнього середовища з урахуванням нестаціонарної просторово-часової локалізації первинних джерел вимірювань.

4. Розробити інформаційну технологію і відповідний програмно-технічний комплекс моніторингу параметрів навколишнього середовища реального часу в сучасній концепції IoT.

Об'єкт дослідження – процес моніторингу параметрів навколишнього середовища.

Предмет дослідження – математичні моделі, методи, інструментальні засоби та інформаційні технології моніторингу параметрів навколишнього середовища в концепції IoT.

Методи дослідження: методи теорії ймовірностей і випадкових процесів (для розробки стохастичних моделей з випадковим доступом), математичної статистики (для збирання, оброблення та інтерпретації експериментальних даних), методи теорії зв'язку (для розробки і реалізації топологій WSN) і мікропроцесорів (для реалізації запропонованох інформаційної технології на Arduino).

Наукова новизна одержаних результатів:

1. Вперше розроблено стохастичні моделі функціонування бездротових сенсорних мереж, які використовують рандомізовані мережеві параметри (зі змінною кількістю вузлів і випадковою участю вузлів в окремих групах мережевих вузлів), що дозволило оцінити ймовірність колізії сигналів і більш ефективно проектувати протоколи комунікації IoT.

2. *Удосконалено* метод моніторингу параметрів навколишнього середовища, який враховує нестаціонарну просторово-часову локалізацію первинних джерел вимірювань та оптимізацію процесу динамічного моніторингу, що дало можливість забезпечити своєчасне та оперативне надходження інформації від первинних джерел інформації із заданими показниками якості для ефективного прийняття управлінських рішень.

3. *Отримала подальший розвиток* інформаційна технологія моніторингу, яка за рахунок використання стохастичних моделей функціонування бездротових сенсорних мереж та удосконаленого методу моніторингу, дозволила забезпечити ефективне спостереження і контроль параметрів навколишнього середовища реального часу в сучасній концепції IoT із урахуванням апріорної невизначеності джерел інформації та можливості виникнення кризових ситуацій.

Практичне значення отриманих автором результатів:

1. Розроблені стохастичні моделі дозволи оцінити ймовірність колізії сигналів: максимальна кількість вузлів, які забезпечують якість передавання на рівні ймовірності колізії не вище 10^{-2}, становить 50 шт., причому кількість задіяних в колізії вузлів нехтовно мала в порівнянні з середньою кількістю передавань, зокрема відношення середньої кількості задіяних в колізії вузлів до середньої кількості передавань становить 10^{-7}.

2. Створений і апробований програмно-технічний комплекс (ПТК) моніторингу параметрів навколишнього середовища реального часу (із використанням засобів Arduino, JavaScript, NodeJs, HTML та CSS) може використовуватись як прототип для організації моніторингу в динамічно змінюваних середовищах та при виникненні критичних ситуацій різного характеру.

3. Розроблено спеціалізовані UML-діаграми прецидентів моделювання та послідовності моделювання запропонованої інформаційної технології.

4. Результати дисертації використані та впроваджені в Національному авіаційному університеті, Центральноукраїнському національному технічному університеті та телекомунікаційній компанії Local Students Networks.

Особистий внесок здобувача. Усі результати, які формують основний зміст дисертації, автор отримав особисто. У друкованих працях, опублікованих в співавторстві, здобувачеві належать (див. анотацію): [1, 5, 6] – розробка і експериментальне дослідження методу моніторингу параметрів навколишнього середовища з метою забезпечення своєчасного та оперативного надходження інформації від первинних джерел; [2] – аналіз обфускаційних алгоритмів і оцінювання їх придатності в програмно-технічному комплексі моніторингу в системі Інтернету речей; [3, 7] – дослідження ефективної архітектури і топології сенсорної мережі в концепції Інтернету речей; [4, 8] – дослідження моделей функціонування бездротових сенсорних мереж, оцінювання ймовірності колізії сигналів; [9, 10, 13] – визначення показників якості функціонування та рівня кібербезпеки бездротових сенсорних мереж; [11] – аналіз концепції Інтернету речей в контексті можливості побудови інтелектуалізованих систем моніторингу параметрів навколишнього середовища.

З робіт, що опубліковані дисертантом у співавторстві, у дисертаційній роботі використовуються виключно результати, отримані особисто здобувачем.

Апробація результатів дисертації. Основні положення і результати дисертаційної роботи доповідалися та обговорювалися на низці науково-технічних і науково-практичних конференціях в Україні та закордоном, серед яких: International Scientific-Practical Conference Problems of Infocommunications Science and Technology (Харків, 2017 р.), Międzynarodowa Konferencja Studentów oraz Doktorantów «Inżynier XXI wieku» (Бельсько-Бяла, 2017 р.), Всеукраїнська науково-практична конференція молодих учених і студентів з міжнародною участю «Проблеми та перспективи розвитку авіації та космонавтики» (Київ, 2017 р.), Міжнародна науково-практична конференція «Інформаційна безпека та комп'ютерні технології» (Кропивницький, 2018 р.), Міжнародна науково-практична конференція «Актуальні питання забезпечення кібербезпеки та захисту

інформації» (Верхній Студений, 2018 р.), наукові семінари НАН України («Технічні засоби захисту інформації», Київ, 2017-2018 рр.), Національного авіаційного університету та Центральноукраїнського національного технічного університету та ін.

Публікації. Основні результати дисертаційних досліджень опубліковані у 14 наукових роботах, серед яких: 7 наукових статей у вітчизняних і закордонних спеціалізованих виданнях (з яких 5 у фахових виданнях); 1 стаття у збірнику матеріалів міжнародної конференції IEEE; 1 розділ у колективній монографії англійською мовою, що видана закордоном (Польща); 5 публікацій в матеріалах міжнародних і всеукраїнських наукових конференцій. До того ж, 2 публікації індексуються у наукометричній базі Scopus.

Структура та обсяг дисертації. Дисертаційна робота складається з анотації, вступу, чотирьох розділів, висновків, списку джерел із 123 найменувань та додатків. Загальний обсяг дисертації 162 сторінки, з яких основний текст викладений на 127 сторінках, містить 36 рисунків, 14 таблиць.

РОЗДІЛ 1. СУЧАСНІ ПІДХОДИ ДО ПОБУДОВИ СИСТЕМ МОНІТОРИНГУ НА БАЗІ КОНЦЕПЦІЇ ІНТЕРНЕТУ РЕЧЕЙ

1.1. Принципи побудови сучасних бездротових систем передавання даних

Сучасний розвиток радіотехніки та телекомунікацій, а також ІТ відкрив нові можливості в галузі передавання інформації. Особливе значення для цього розвитку становить розроблення стільникового зв’язку та телефонії, а також комп'ютерних мереж, які використовують комунікацію на радіохвилях (WLAN, Wi-Fi, WiMAX). Застосування радіозв'язку в комп'ютерних мережах відкрило нові перспективи в сфері використання радіокомунікації [1-3], а також інфрачервоного спектру для отримання та передавання інформації з різних джерел. Внаслідок цього виникли бездротові сенсорні мережі – WSN. В останні роки дана галузь науки набрала динамічного розвитку та практичних застосувань майже у всіх сферах людської діяльності.

WSN вносять нову якість в сучасних системах отримання, нагромадження, оброблення та передавання інформації. Однак їх реалізація ставить цілком нові завдання в області радіокомунікації і керування телекомунікаційними процесами, які вдається вирішити шляхом щораз інтенсивнішого розвитку інформаційних технологій [4-8]. Для того щоб наблизитися до проблематики питання, насамперед потрібно розуміти, що створення WSN означає, в першу чергу, розвиток та зміну дотеперішнього рівня знань про радіокомунікацію [9].

Широко зрозумілим є звичне використання стандартної радіокомунікації в системах широко трансльованих повідомлень (broadcast), наприклад, радіомовлення, телебачення, а також GPS. Передавач емітує повідомлення, яке може відбирати кожен, хто володіє відповідним приймачем, що знаходиться в зоні покриття електромагнітного поля з досить високою інтенсивністю, щоб отриманий з антени сигнал міг відтворити приймач. Розпоряджаються в даному

випадку однією частотою (гармонічним перебігом), яка використовується в носію інформації та застосовується протягом всього приділеного часу роботи станції, тобто у однонапрямленій (симплексній) трансляції (рис. 1.1). У зоні дії вказаної станції під час її роботи не може з'явитися жодна інша станція з тією самою частотою, бо це призведе до колізії і унеможливить правильний відбір сигналу.

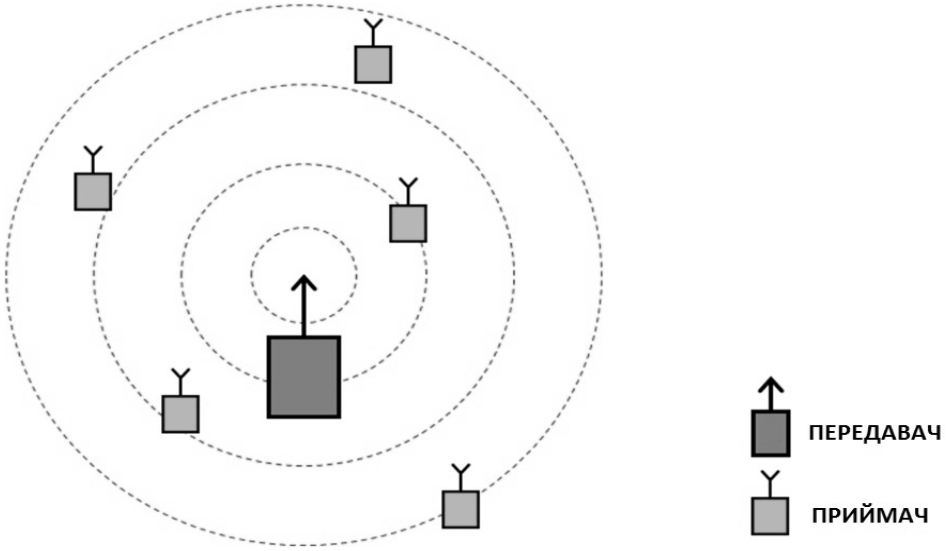


Рис. 1.1. Схема однонапрямленої радіотрансляції (симплекс) в режимі широкотрансльованих повідомлень (broadcast)

Іншим поширеним рішенням з області радіокомунікації є двонапрямлена трансляція (точка-точка). Тоді можлива інтерактивна комунікація двох користувачів. Її можна реалізувати двома способами: шляхом використання обома користувачами тільки одної несучої частоти, але вживаючи її позмінно, тобто так званий дуплекс позмінний, або якщо наявні для розпорядження дві несучі частоти, то можна реалізувати дуплексну різноканальну трансляцію. Тоді кожен з користувачів може водночас надавати і приймати відбирати, наприклад, як це має місце у стільниковій телефонії (рис. 1.2).

Слід зауважити, що різноканальна робота двох користувачів означає, що в зоні покриття їх приймачів ніхто інший не може користуватися тими двома частотами у той же час. Більш того, навіть використання цих частот третім

користувачем поза існуючою зоною покриття їх станцій може зумовити заглушування або припинення зв'язку, якщо розпоряджатиметься, наприклад, більшою потужністю передавача чи або умови поширення радіохвиль будуть для нього некорисні.

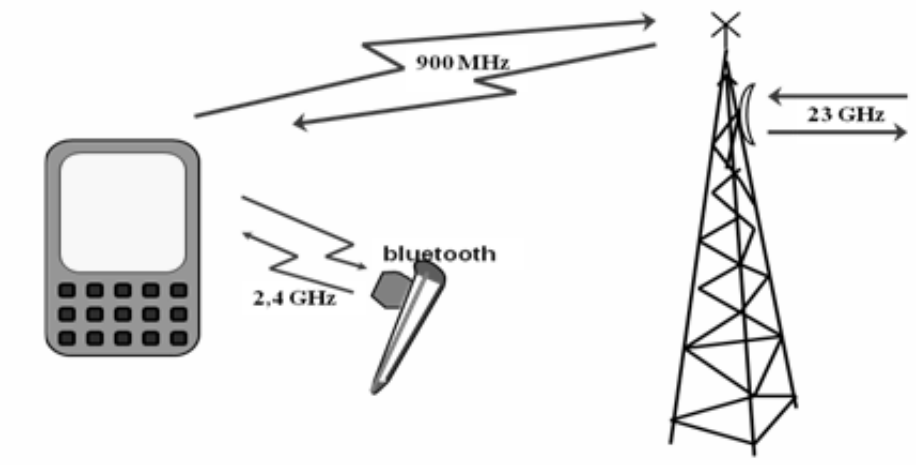


Рис. 1.2. Двонапрямлена (дуплексна) радіотрансляція
в телефонії GSM 900

У цьому контексті з'являється ще інше поле використання радіо-комунікації – WSN. Цей вид комунікації являє згадану вище зміну дотеперішнього підходу, що застосовується в радіокомунікації. Тепер цікавитиме отримання інформації так званими вузлами мережі, які є джерелами інформації та до яких приєднані вимірювальні сенсори (сенсори).

Вузлів є багато, вузол містить передавальний пристрій або зазвичай прийомодавач (transceiver), а також процесор для обслуговування отриманих даних і керування процесами на самому вузлі, включно з керуванням наданням і передаванням даних радіоканалом до спільного входу, тобто базової станції. Це так звані мережі типу «всі до одного», які іменуються також бездротовими збиральними (агрегувальними) мережами типу sink (рис. 1.3). У контексті раніше представленої проблеми щодо обмеженої кількості радіоканалів постало питання керування мережевим доступом.

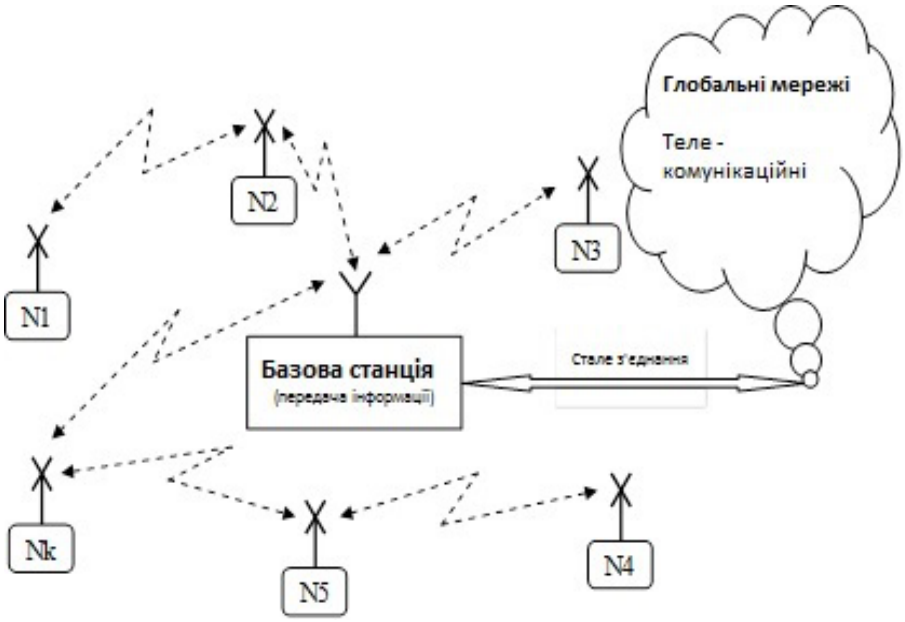


Рис. 1.3. Бездротова збиральна мережа типу sink у поєднанні з телекомунікаційними глобальними мережами

Побудова мережі із використанням радіопередачі означає, що застосовується одне спільне середовище передачі, а саме – простір, у якому можуть поширюватись електромагнітні хвилі. Отже, для того, щоб багато користувачів могли користуватись спільним середовищем, необхідно створити у цьому середовищі багато незалежних передавальних каналів.

1.2. Застосування WSN в задачах моніторингу

Концепція збиральної мережі типу sink [10], якою зокрема може бути WSN [11], полягає в тому, що джерела інформації, які розподілені в просторі, причому як стаціонарні, так і мобільні, та яких може бути дуже багато, передають інформацію безпосередньо до базової станції (центру збирання інформації). Це мережі типу single-hop. Якщо мережа організована так, що має можливість передавати інформацію через інші вузлові точки, в деякій мірі посередньо, тоді це мережі типу multi-hop.

Мережам типу single-hop притаманна топологія зірки, в якій окремі канали можуть реалізуватися симплексно або дуплексно залежно від кількості

потрібних каналів: частотних (наявних в розпорядженні частот) або частотно-часових, в яких на даній частоти здійснюється додатково мультиплексування з поділом за часом (чи часове ущільнення), збільшуючи кількість наданих в розпорядження комунікаційних каналів. Прикладом може бути система DCS 1800 в стільниковій телефонії. Натомість мережам типу multi-hop характерна архітектура найчастіше типу сітка (mesh).

У всіх збиральних мережах, для яких характерна технологія «всі до одного», наявна принципова проблема. В даний момент часу вибраний частотний канал може бути зайнятий тільки одним користувачем мережі. Отже, основне завдання таких мереж полягає в безколізійній організації доступу інформації з окремих вузлів до центру збирання інформації (базової станції).

Отже необхідна розробка спеціальних алгоритмів та протоколів доступу і підготовка комунікаційних вузлів до функціонування в середовищі багатьох сенсорів, які намагаються отримати доступ до одного центру збирання інформації (базової станції). Тобто, постає задача розроблення протоколу керування роботою самої мережі. Розглядаючи це питання, потрібно також згадати про проблему електромагнітної сумісності. Використовуючи простір середовищем передачі, аналізована WSN не є ізольованою структурною одиницею в просторі, а з факту використання радіочастот її робота, як і інших користувачів радіокомунікації є взаємозалежними.

Питання сумісності, охоплене унормуваннями, вказує на обмежені можливості використання довільних частот і застосування довільних потужностей випромінювання (EIRP). Таке питання врегульоване юридично, через системи правосуддя держав з врахуванням міжнародних норм. Більше того, можна сказати, що електромагнітний спектр поділено на смуги, які підлягають спеціальному юридичному захисту, і користування ним в цих діапазонах вимагає отримання ліцензії. Тоді гарантію роботи без завад пристроїв, які працюють на ліцензованих частотах, переймають державні служби, приміром, у Польщі – це Установа електронної комунікації. Також виділено неліцензійні смуги, наприклад, 27 МГц для зв'язку СВ, 35 МГц для

керування в моделізмі, 2,4 ГГц для безпроводових комп'ютерних мереж WLAN і Wi-Fi або 433 МГц для пультів до автомобілів та інших пристроїв автоматики і керування. На практиці користування цими смугами не вимагає ліцензії, хоча і так само повинні бути дотримані принципи щодо максимальної випромінюваної потужності EIRP і ширини використаної смуги. Проте неліцензійні смуги не гарантують роботи пристроїв без завад. Сьогодні на практиці, наприклад, вказані вище частоти досить інтенсивно та широко застосовуються і реалізація на цих частотах нових мережевих рішень обтяжена дуже серйозним ризиком правильної дії, беручи до уваги також використаний простір. У спектрі електромагнітних хвиль є також смуги, які до сьогодні неохоплені нормами. Це головні смуги з області дуже високих частот – вище 100 ГГц, інфрачервоного діапазону, видимої області.

Топологічна та комунікаційна специфіка WSN. Сенсорна мережа складається з багатьох вузлів, які розташовані як всередині вимірювального середовища, так і назовні поблизу досліджуваних фізичних величин. Прийнято, що окремі комунікаційні вузли, пов'язані з сенсорами, можуть переміщатися в полі дослідження фізичних впливів, контрольованих сенсорами. Отже, припускається мобільність вузлів, що в свою чергу часто зумовлює зміни в конфігурації мережі, а особливо призводить до змін в умовах поширення електромагнітних хвиль. Ці вимоги накладаються на дуже істотні і необхідні ознаки та характеристики для розглянутих в [10] вузлів WSN, а саме: алгоритми і протоколи повинні володіти здатністю до самоорганізації. Це означає, що вузол від апаратної сторони повинен бути обладнаний процесором, який дозволить часто реалізовувати дуже складні алгоритми обслуговування в умовах вимірювального середовища, які змінюються.

Застосування з цією метою спонтанної мережі типу ad hoc, незважаючи на багато протоколів і алгоритмів, якими в цих мережах розпоряджаються, не розв'язує унікальних потреб сенсорних мереж, які виникають з відмінностей між, здавалося б, дуже універсальними рішеннями в стандартних мережах ad

hoc і фактичними потребами вимірювальних мереж. Ця специфіка та унікальність вимірювальних WSN зумовлена наступними складовими [12]:

– кількість вузлів в сенсорній мережі зазвичай на декілька порядків вища, ніж в мережі ad hoc,

– вузли в сенсорних мережах, як правило, щільно розміщені,

– сенсори з вузлами, з якими співпрацюють, – часто становлять інтегральний засіб – більш піддаються аваріям,

– мають місце часті зміни в топології мережі,

– сенсор зазвичай користується комунікаційними рішеннями вузла, загалом більш складними, ніж в разі мережі ad hoc, де комунікація в загальному базується на моделі точка-точка,

– вузли в сенсорній мережі, в принципі, розпоряджаються обмеженою потужністю живлення, що становить обмеження для обчислювальних можливостей, наявного обсягу пам'яті, потужності випромінювання антени і частоти активізації надавачів ("пробудження" сенсорів),

– вузли не можуть володіти глобальною ідентифікацією ID з огляду на величезну кількість і приділений простір для реалізації завдань.

Вище згадані вимоги та обмеження для сенсорної мережі можна прокоментувати наступним чином: обмежене розпорядження потужністю живлення зумовлює подальші наслідки в розв’язаннях, а саме спричиняє те, що частішим рішенням є топологія multi-hop (ретрансляція від вузла до вузла аж до центру збирання даних), ніж sigle-hop, в якій потрібно більше енергії для самої радіотрансляції.

Для топології multi-hop притаманні більш складні комунікаційні алгоритми. Низький рівень випромінюваної потужності, що може бути перевагою, але також створює додаткові проблеми із забезпеченням відповідної QoS. Подальшим наслідком обмеження потужності, що приділена для використання, є необхідність вбудовування механізмів trade-off, які дозволяють

користувачеві можливість довшого "життя" мережі за рахунок зменшення пропускної здатності або збільшення затримки передавання.

Аналіз чинників впливу на топологію мережі. Серед багатьох істотних факторів, які впливають на архітектурні та комунікаційні аспекти, також на області використання мережі, можна виділити: призначене до реалізації мережею завдання, вплив середовища (довкілля), стійкість до завад і помилок, мережева архітектура, обмеження щодо апаратних засобів, трансляційні алгоритми, потреба в живлення потужності, чинники, які впливають на кошти виробництва. Згадані чинники є предметом багатьох досліджень для різних просторів застосувань WSN [10-12]. Вище перелічені фактори, що мають вплив на мережеві рішення, становлять важливі настанови для проектування комунікаційних протоколів та алгоритмів дії мережі [13].

Можна скорочено виділити наступні істотні умови в проектуванні WSN: смуги пропускання здатність і комунікаційні частоти; потреба в потужності живлення, наприклад, для цілей зв'язку та обробки даних; зовнішні обмеження, пов’язані з середовищем; апаратні обмеження; масштабованість; діапазон стійкості до помилок.

Діапазон стійкості до помилок. У збиральній WSN з низкою вузлів появляються помилки або перерви в трансляції, що є результатом багатьох причин. У разі радіокомунікації істотний вплив зумовлюють проблеми, пов'язані з поширенням радіосигналів (електромагнітних хвиль), що викликане перш за все фізичними умовами середовища, яке оточує давальні вузли. Отже наявність відбиття сигналів на місцевих перешкодах, кліматичні умови, інтерференції, недостатній рівень потужності сигналу або надмірний рівень сигналу і низка інших. Передача інформації за допомогою радіохвиль є найважчим завданням по відношенню до трансляції з використанням проводових засобів – мідних кабелів, світлопроводів тощо.

Проблематику якості радіотрансляції у збиральних WSN широко висвітлено в літературі [27-30]. При цьому завдання надійності чи теж задачі,

пов’язані з безпекою (fault tolerance), розглянуто з точки зору моделювання з використанням розподілів Пуассона [31]. При цьому надійність як функцію часу виражено формулою (1.1):

$$R_k(t) = \exp(-\lambda_k t), \tag{1.1}$$

де λ_k – коефіцієнт помилок в аналізованому інтервалі часу (0, t), k – номер вузла радіозв'язку.

Проектовані трансляційні протоколи повинні враховувати у своїй структурі віднесення до рівня помилок, чи інтервалу точності для наявності помилок. Змінність умов поширення, яку часто модельовано на підставі на стохастичних моделей, належить до одного з найважчих завдань в комунікації з використанням електромагнітного випромінювання. Задачі поширення, хоча і найістотніші в радіокомунікації, очевидно не вичерпують всіх чинників, які впливають на коефіцієнт бітових помилок комунікаційної системи, що для проведення детального аналізу також вимагає врахування.

Ємність мережі. Ємність мережі – кількість комунікаційних вузлів. Кількість вузлів в WSN залежить від виду досліджуваного явища, кількості контрольованих параметрів технологічного процесу, простору, в якому контролюються параметри і т.д. Це мережі, що налічують від декількох чи кільканадцяти сенсорів до сотень вузлів, які взаємодіють між собою. У екстремальних ситуаціях їх кількість може досягати тисяч та навіть сотень тисяч вузлів. Створюване нове програмне забезпечення повинно бути здатним подолати бар’єр в обслуговуванні такої величезної кількості вузлів. Можна ввести означення поняття густини або щільності вузлів в даному просторі функціонування, наприклад, визначаючи радіус дії вузлів, наприклад, менше 10 м). Густину вузлів обчислено згідно (1.2):

$$\mu(R) = \frac{(N\pi R^2)}{A} \tag{1.2}$$

де N – кількість вузлів, розподілених в просторі дії мережі, R – радіус радіопередачі, причому $\mu(R)$ дає кількість вузлів в кожній з вершин мережі.

Кількість вузлів в просторі дії дозволяє визначити густину вузлів. Густина вузлів в принципі залежить від виду аплікації, застосованої до реалізації завдань мережі. Наприклад, в діагностиці машин густина вузлів становить приблизно 300 шт. на 5 х 5 м^2 простору. Пильнування транспортного засобу, приміром, здійснюється за допомогою близько 10 вузлів в околі дії. Якщо брати загальний коефіцієнт густини, то він може бути і у межах 20 вузлів на м^3. У домашньому господарстві густина вузлів може бути дуже різна залежно від кількості контрольованих величин [22]. Для моніторингу території густина вузлів вагатиметься в межах 25-100 шт. в передбачуваній зоні. Зокрема, густина вузлів може бути дуже велика в ситуації моніторингу різних параметрів тіла людини.

Обмеження пристроїв. Вузол складається з чотирьох базових блоків [3]: засобу вимірювання (з сенсором досліджуваної величини), процесора, трансівера (приймально-передавальний модуль) і системи живлення. У залежності від потреб, вузол може бути ще обладнаний додатковими модулями, такими як: система місцезнаходження (позиціонування), мобілайзер, зовнішнє джерело живлення. У загальному, вузли повинні виконувати ряд вимог, між іншим [32]: споживати мало енергії, бути надзвичайно малогабаритними у конструкції та дуже щільно упакованими, бути дуже дешевими у виробництві, бути автономними модулями і працювати без нагляду, адаптуватись до середовища. Доступність вузлів залежить передусім від впровадженої процедури доступу. У випадку сенсорної мережі WINS, загальний середній струм живлення повинен бути менший від 30 мкА для забезпечення тривалого терміну служби. Вузли WINS живляться типовими літій-іонними акумуляторами (Li). Можливе збільшення терміну експлуатації WSN за допомогою використання відновлюваних джерел, що означає отримання енергії з довкілля. Найбільш відомими у цих застосуваннях є сонячні батареї.

Приймодавачі (трансивери) можуть бути пасивними та активними. Також їх можна виконати оптичними, однак найчастіше ці засоби є радіопристроями [24], які працюють на обраній радіочастоті (RF). Пристрої радіозв'язку вимагають модуляції, працюючи у відповідній радіо-смузі, фільтрування, демодуляції та мультиплексування кіл, що робить їх складними і дорогими. Окрім того, затухання траси для надаваного сигналу між двома вузлами може бути дуже високим (в четвертій степені відстані між ними), між іншим, через близькість до землі антен сенсорів [13, 24]. Незважаючи на це, радіозв'язок використовується у більшості застосувань та продовжуваних досліджень WSN. Пакети, що передаються у WSN, є малими, а швидкості передачі даних – низькими [26], частота передачі може бути різною, але часто досить високою, хоча б з огляду на малі відстані зв'язку і функціонування мережі типу multi-hop (ретрансляції між почерговими вузлами). Вище наведені характеристики зумовлюють доцільність використання для радіопередачі у WSN несучу хвилю з відносно низькою частотою. Однак отримати високу енергетичну ефективність на низьких радіочастотах є надалі складним з технічної точки зору, а наявні безпроводові комерційні технології, до якої належить Bluetooth, не є достатньо ефективними для WSN внаслідок високого споживання енергії.

Незважаючи на щораз кращі пропозиції постійно удосконалюваних процесорів, все вищу обчислювальну потужність зі все меншими габаритними розмірами процесорів, пам'яті та модулів перетворення сигналів сенсорів, необхідні ресурси обробки і надалі обмежені. Більшість завдань, які реалізуються WSN, вимагає знання про положення вузлів. Беручи до уваги, що вузли сенсорів зазвичай розміщені випадково і залишаються без нагляду, повинні бути часто обладнані системою місцезнаходження (позиціонування). Визначення місцезнаходження вимагає також нерідко протоколу маршрутизації. Часто передбачається, що кожен вузол буде обладнаний у приймач глобального позиціонування GPS. Це дозволяє зазвичай визначати положення вузла з точністю до 5 м. У деяких роботах стверджується, що обладнання всіх вузлів у GPS не виправдано. Альтернативний підхід полягає на

обмеженій кількості вузлів, які використовують GPS, та доповнення інформації про місцезнаходження за допомогою інших вузлів завдяки наземному розташуванню.

Зовнішні обмеження. Вимірювальні WSN можуть бути застосовані в найрізноманітніших середовищах роботи. Цей факт накладає додаткові вимоги як на технологічні і виконавчі рішення самих сенсорів, так і на розв’язання, зумовлені застосованими ІКТ [19-22, 26]. Вузли можуть працювати під високим тиском на дні океану, у важкодоступних місцях (зсувні ґрунти, виїмки, на деревах, полігонах), у важких умовах, при екстремальних температурах (тепла і холоду , наприклад, в соплі двигуна літака або в арктичних регіонах), в надзвичайно шумному середовищі, у рамках доцільного звукомаскування і т.д. Представлений нижче список можливих місць застосувань дає уявлення про умови роботи самих сенсорів і вузлів, які їх обслуговують: пожвавлені перехрестя, інтер'єр великих машин, на дні океану, всередині обертових сфер, на поверхні океану під час торнадо, в забрудненому біологічному або хімічному середовищі, на полі бою за лінією фронту, в будинку або у великих будинках, на великих складах, як мітки для тварин, на швидкісних рухомих транспортних засобах, в дренажі, річках при русі вниз за течією.

Слід взяти до уваги додатково ще способи їх встановлення, які, наприклад, можуть бути наступними: традиційне монтування на підприємстві, розміщення один за одним, або з допомогою людини чи робота, приміром, на дні озера чи океану, викид з літака, вистріл в спеціальному артснаряді або ракеті, викид катапультами, наприклад, з палуби судна, і т.д.

Представлені приклади застосувань та способи розміщання вузлів WSN дають уявлення про необхідну різнорідність рішень і використаних ІКТ [23-29]. В цьому випадку важко створити якісь уніфіковані рішення, а стандартні рішення, що стосуються для безпроводового зв’язку комп'ютерів в мережі, виявляються мало придатними.

Комунікаційні смуги та частоти. Вибір відповідного носія інформації належить до одного з ключових завдань в проектуванні WSN. В принципі

можна констатувати, що в кожному випадку це є вибір частоти несучої хвилі та необхідної смуги з точки зору застосованої модуляції і кількості наданої інформації. Однак це питання вимагає певних уточнень. Традиційно приймаються певні термінологічні розрізнення для конкретних частотних діапазонів, що застосовуються в техніці. Вживається означення радіохвилі до частоти близько 300 ГГц, вище послуговуються терміном інфрачервоне випромінювання, визначаючи зазвичай довжину хвилі, яку використовується для передавання інформації, – діапазон від близько 1000 мкм до 0,78 мкм. Діапазон для коротших хвиль між 0,78 мкм до 0,4 мкм належить до видимого світла. Кожен із згаданих діапазонів електромагнітного випромінювання суттєво відрізняється за характеристиками поширення електромагнітного випромінювання в різних матеріальних середовищах і вакуумі. У WSN користуються цією класифікацією. Отже, можна зробити висновок, що пристрої працюють на радіохвилях, в інфрачервоному діапазоні або в діапазоні видимого світла.

У WSN типу multi-hop вузли комунікуються на радіохвилях [31, 33]. Канали можуть бути утворені, як згадано вище, на радіохвилях, інфрачервоному діапазоні або в діапазоні оптичних (видимих) хвиль. Для того щоб WSN могли функціонувати в глобальному масштабі, необхідні узгодження, що зобов'язують у всьому світі щодо використовуваних з цією метою смуг частоти. Одним з основних рішень, що стосується діапазонів радіочастот, які використовуються для комунікації у WSN, є використання неліцензованих діапазонів у більшості країн світу, які мають промислове, наукове і медичне застосування (ISM) (табл. 1.1) [33].

Деякі з цих смуг частоти вже використано для комунікації у безпроводових телефонних системах і безпроводових локальних мережах WLAN. Оскільки очікується, щоб вузли в WSN були малогабаритні, дешеві і споживали ультра малу потужність, з'являється низка взаємно суперечливих умов до побудови цих мереж. Це вимагає компромісу і одним з істотних елементів цього компромісу є вибір частоти роботи. Це пов'язується перш за

все з коефіцієнтом корисної дії щодо випромінювання потужності. Ці умови вдається досить добре забезпечити для досить високих частот – дуже коротких хвиль, які у свою чергу набагато гірше поширюються в середовищі з перешкодами [30].

Таблиця 1.1

Частотний діапазон в застосовуваннях ISM

Діапазон частоти	Основна частота
6765 – 6795 кГц	6780 кГц
13553 – 13567 кГц	13560 кГц
26,957 – 27,283 МГц	27,120 МГц
40,66 – 40,70 МГц	40,68 МГц
433,05 – 434,79 МГц	433,92 МГц
902 – 928 МГц	915 МГц
2400 – 2500 МГц	2450 МГц
5,725 – 5,875 ГГц	5,800 ГГц
24 – 24,25 ГГц	24,125 ГГц
61 – 61,5 ГГц	61,25 ГГц
122-123 ГГц	122,5 ГГц
244-246 ГГц	245 ГГц

Частою пропозицією є застосування частоти 433 МГц ISM в Європі та ISM 915 МГц в Північній Америці. Питання, пов'язані з проектуванням трансиверів в цих двох діапазонах частоти, обговорено в [32]. Головними перевагами використання смуг ISM є: неліцензійна частота, дуже широкий спектр і глобальна доступність. Використання цих частот не підкріплено спеціальними юридичними обмеженнями. В принципі єдині обмеження зумовлені допустимим рівнем випромінюваної потужності, виходячи з допустимого рівня завад, що саме у безпроводових вимірювальних мережах не є суперечливим з умовами їх реалізації та роботи. Зазвичай користуються

набагато меншими рівнями випромінюваної потужності. Подальшим наслідком користування неліцензійних смуг частоти є більша свобода в реалізації способу трансляції і, відповідно видів модуляції, організація алгоритмів трансляції з врахування стратегії економії енергії, тощо. Більшість сьогоднішнього устаткування вимірювальних WSN орієнтуються на Circuit Design RF. Безпроводовий вузол μAMPS використовує технологію Bluetooth 2,4 ГГц [33]. Передавач має вбудований синтезатор частоти. Опис такого вузла з низькою споживаною потужністю представлено в [28]. Трансівер використовує один канал на частоті 916 МГц. В архітектурі WINS для комунікації застосовано радіоканали [124].

Іншим можливим способом комунікації в мережах між вузлами є використання випромінювання в інфрачервоному діапазоні. Комунікація в інфрачервоному діапазоні не вимагає ліцензії і досить стійка до завад. Передавально-приймальні компоненти для інфрачервоного діапазону дешевші і легші в побудові. Однак головною вадою є вимога оптичної видимості, оскільки комунікація відбувається на прямій лінії між давачем і приймачем, і на цій лінії не можуть знаходитися жодні перешкоди. Це наводить на те, що інфрачервоний діапазон неохоче застосовується у вимірювальних WSN.

Іншою проблемою є рішення комунікації в морському середовищі. Тут виникає потреба використання довгих хвиль, які можуть проникати через поверхню води. Загалом, вибір частоти для комунікації вимагає проведення аналізу конкретних умов поширення радіохвиль, особливо врахування ефективності випромінювання потужності антенами, зокрема з врахуванням умов підгонки антен, роботи поблизу землі – низько змонтовані антени і т.д.

Аналіз потреб в енергії живлення. Бездротовий вузол вимірювальної мережі, будучи мікроелектронним пристроєм, може бути зазвичай обладнаний джерелом живлення обмеженої ємності, наприклад, < 0,5 А год, 1,2 В. У деяких випадках доповнення енергетичної ємності джерела може бути неможливе. Отже, час життя вузла перебуває у сильній залежності від живучості батареї. У мережах типу multi-hop та ad hoc кожен вузол виконує подвійну роль:

ініціатора вимірювання і трансляції та маршрутизатора. Помилкова дія декількох вузлів може спричинити значні зміни в топології та вимагати зміни шляху пакетів і реорганізації мережі. У зв'язку з цим керування наявною енергією живлення та її економія набуває особливого значення і належить до одного з найістотніших елементів проектування мережі цього типу. Заощадження енергії живлення породжує цілу низку задач [25-27], пов'язаних з максимальним продовженням часу життя вузла. Крім енергозаощаджувальної електроніки, енергозберігаючих процедур перетворення інформації на вузлі, низько енергетичному збиранню вимірювальних даних і їх обробці, витраті енергії на трансляцію сигналу даних, ключову задачу становлять енергозаощаджувальні алгоритми функціонування вузла. Динамічне керування живленням в мережі WSN розглянуто в [34], де передбачено п'ять режимів заощадження енергії.

Очевидно в різних мережевих рішеннях акцент буде спрямовано на певні пріоритетні функції, які передбачено для реалізації мережею, і необов'язково енергозбереження джерел живлення повинно бути ключовим питанням. Зазвичай енергозбереження стоїть в суперечності з отриманням відповідної якості реалізованої функції (послуги) (QoS). Головним завданням вимірювального вузла в полі впливу сенсора є вимірювання досліджуваної величини, локальне швидке оброблення сигналу, який представляє досліджувану величину, а потім передавання даних (трансляція).

Споживання потужності вузлом пов’язане з живленням трьох основних функціональних блоків вимірювального вузла: вимірювання, оброблення, комунікації.

Таким чином, радіус дії мережі та окремих вузлів, рівень виявлення досліджуваних величин, складність виявлення подій в полі досліджуваних величин, рівень супроводжувальних завад досліджуваним величинам безпосередньо накладатиметься на споживання потужності вузлом і дискусію про джерела і способи живлення.

Вузол мережі повинен володіти необхідною обчислювальною здатністю і, зокрема, бути пов'язаним із зовнішньою комунікацією. Пошуки в напрямі обмеження потреби в живленні енергією призводять до вибору технології CMOS (Complementary Metal Oxide Semiconductor) виконання мікропроцесора. Очевидно в інтегральних мікросхемах, виконаних за цією технологією, так само мають місце певні обмеження щодо енергоспоживання. Споживана потужність в цих інтегральних мікросхемах зростає пропорційно до збільшення частоти перемикання і зменшується при зниженні напруги живлення.

Отже, зниження напруги живлення належить до ефективного способу зменшення енергоспоживання в активному стані. Це один із способів пристосування пропозиції енергії і частоти процесора. Для змінного обчислювального навантаження процесора можна зазвичай зменшити частоту перемикання, що дає змогу заощадити електроенергію пропорційно до зменшення швидкості перемикання (тактової частоти процесора). У свою чергу зменшення напруги живлення забезпечує в енергозаощадження пропорційно до квадрата зменшення напруги. Очевидно, потрібно пам'ятати, що напругу не можна довільно знижувати, оскільки це може призвести до припинення роботи процесора. Крім цього, слід взяти до уваги, що значне зменшення напруги живлення суттєво сповільнить роботу процесора. Отже, існує компроміс між необхідною продуктивністю процесора і напругою живлення. Можна динамічно пристосовувати частоту процесора і напругу живлення до вимог короткочасної обробки. Інші енергоощадні технології живлення модуля CPU розглянуто в [35].

Споживання потужності під час обробки даних (P_p) може бути сформульовано таким чином (1.3):

$$P_p = CV_{dd}^2 f + V_{dd} I_0 e^{V_{dd}/n' \cdot V_T}, \qquad (1.3)$$

де C – загальна перемикана ємність, V_{dd} – напруга живлення, f – частота перемикання.

Друга складова у вищенаведеному виразі вказує на втрати потужності в результаті протікання струму. Зниження напруги живлення здійснюється в залежності від експлуатаційних вимог. У зв'язку з повільнішою обробкою даних мікропроцесором у вимірювальному вузлі та зумовленим цим зменшенням споживаної потужності економія енергії стає досить суттєвою. Крім цього слід зауважити, що існують також певні додаткові компоненти для кодування і декодування даних у вузлах. Застосування спеціалізованих інтегральних мікросхем може також мати місце в деяких випадках. У всіх варіантах схемних рішень вузлів проектування алгоритмів і мережевих протоколів завжди має вплив на споживану енергію.

1.3. Архітектура WSN згідно моделі комунікації відкритих систем

WSN стають як новим важливим рівнем в IT екосистемі, так і об'єктом жвавих досліджень, що включають апаратну і програмну архітектуру, мережеві технології та з'єднання, розподілені алгоритми, програмні моделі, управління даними, безпеку і т.д. В загальному розумінні WSN – це безліч маленьких зчитувальних пристроїв (датчиків), здатних реєструвати зміни різних параметрів навколишнього середовища і транслювати ці параметри іншим подібним пристроям, що знаходяться в зоні досяжності, з певною метою, наприклад: відеоспостереження, моніторинг навколишнього середовища тощо (рис. 1.4).

Серед основних цілей використання WSN можна виділити наступні.

1) Системи безпеки – контроль периметрів, визначення вторгнення, віддалене спостереження; моніторинг персоналу, охорона цінностей та творів мистецтва, домашні системи безпеки, системи пожежної сигналізації.

2) Системи моніторингу і контролю навколишнього середовища (вологість, температура, склад повітря / ґрунту / води, тиск, магнітний фон); моніторинг забруднення навколишнього середовища, міграція тварин, комах.

3) Системи електроенергії – управління енергопостачанням; контроль кондиціонування, вентиляції, опалення, освітлення; ретранслятори для лічильників газу, води, електроенергії.

4) Надзвичайні ситуації – оповіщення про стихійні лиха: лісові пожежі, зсуви і т. п., порятунок людей при надзвичайних ситуаціях.

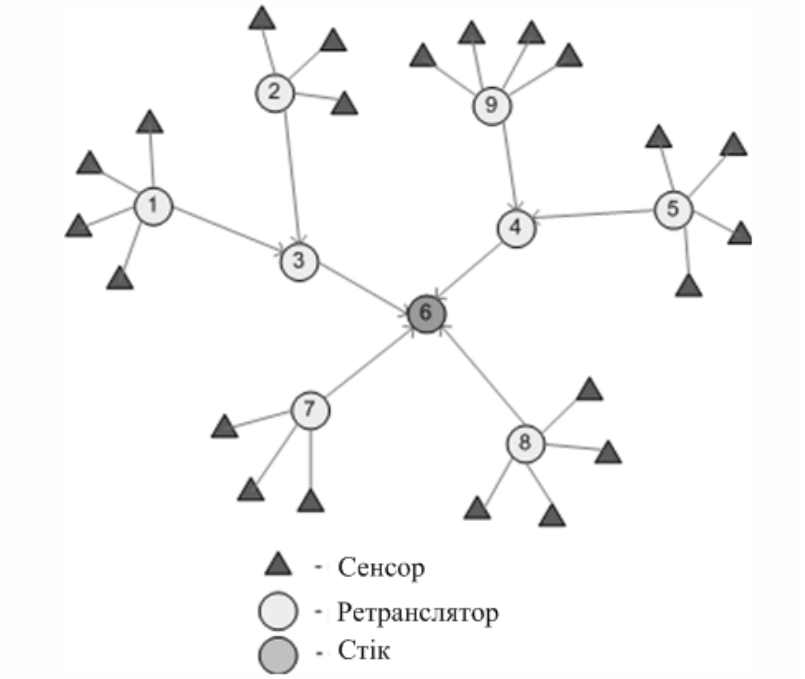


Рис. 1.4. Типова структура WSN

Тому, як бачимо, досить часто WSN можуть розгортатися в агресивних несприятливих середовищах, де можуть бути зроблені навмисні спроби впливу на їх роботу. Яскравим прикладом може служити їх застосування в зоні бойових дій, де таємність переданих даних і розташування, а також стійкість до спроб компрометації даних і знищення мережі мають ключове значення.

Питання функціонування існуючих протоколів в WSN розглядаються багатьма вченими [14-26]. У загальному випадку кожний пристрій оснащений мікроконтролером, прийомопередавачем, елементом живлення і набором датчиків для вимірювання деяких параметрів навколишнього середовища,

наприклад, температури, освітленості, вібрації, тиску, рівня шуму та інших (рис. 1.5) [24].

Інтелектуальні вузли такої мережі здатні ретранслювати повідомлення один від одного по черзі, забезпечуючи значну площу покриття системи при малій потужності передавачів. За рахунок цього досягається висока енергетична ефективність системи.

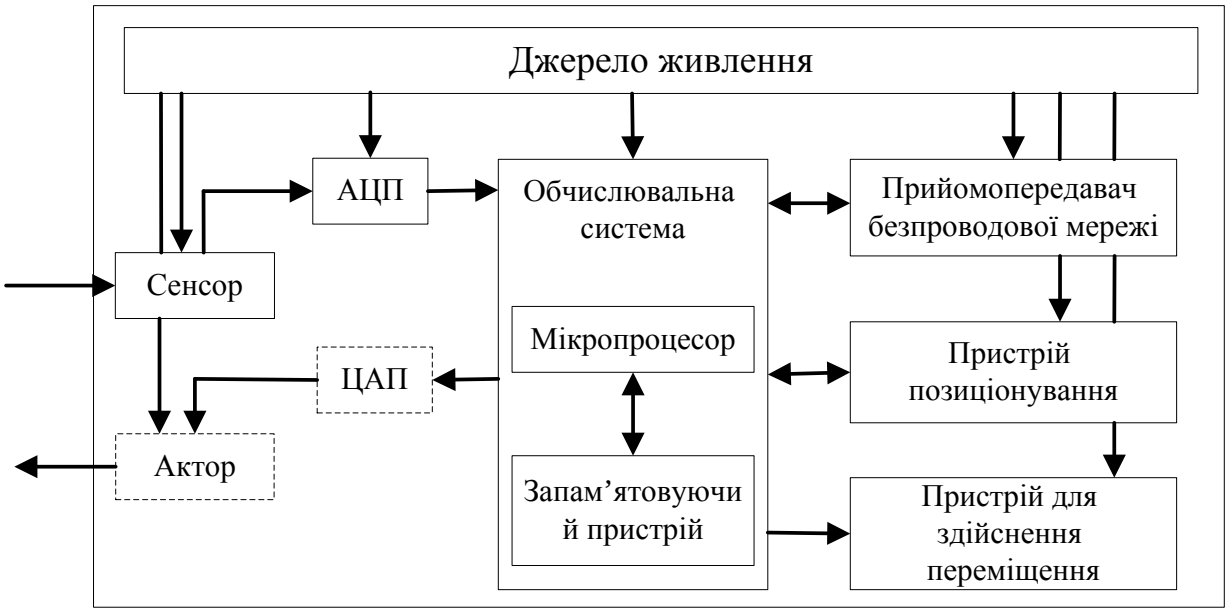


Рис. 1.5. Архітектура сенсорного (сенсорно-акторного) вузла WSN (обов'язкові елементи виділені безперервної лінією, необов'язкові – пунктиром)

Розглянемо протоколи, які використовуються в сучасних WSN:

1) Протоколи фізичного рівня. До протоколів фізичного рівня для WSN застосовуються ті ж обмеження, що і до протоколів інших рівнів, а саме: невеликий запас електроенергії, маленькі габарити і вартість сенсорного вузла. З даних обмежень безпосередньо випливає, що протокол фізичного рівня повинен забезпечувати мінімально ресурсомісткі алгоритми модуляції і демодуляції, а також забезпечувати невелику площу радіопокриття, так як потужність радіопередавача в умовах обмеженого запасу електроенергії безпосередньо впливає на час життя сенсорного вузла WSN: чим більше

потужність передавального пристрою, тим швидше вичерпається автономне джерело електроживлення [17-19].

Серед відкритих протоколів для фізичного рівня загальноприйнятим для побудови WSN є стандарт IEEE 802.15.4, що визначає крім фізичного рівня для низькошвидкісних персональних безпроводових мереж (Wireless Personal Area Networks, WPAN) ще і частину канального рівня – рівеня доступу до середовища (Medium Access Control, MAC) [23].

Остання версія стандарту IEEE 802.15.4 описує шість різних типів організації фізичного рівня (не враховуючи регіональних типів, призначених для Китаю і Японії і описуваних в IEEE 802.15.4c і IEEE 802.15.4d відповідно), які представляють собою поєднання використання зазначених частотних смуг із застосуванням різних типів модуляції сигналу: двійкової фазової маніпуляції, квадратурної фазової маніпуляції, комбінації двійкової фазової маніпуляції і амплітудної маніпуляції, широкосмугової технології UWB і методу лінійної частотної модуляції (Chirp Spread Spectrum, CSS).

Найбільш перспективним для побудови WSN виглядає використання широкосмугових технологій, які входять в стандарт IEEE 802.15.4 останньої редакції, так як вони дозволяють створювати прийомопередавачі з низьким енергоспоживанням. Цю тезу також підтверджує велика кількість досліджень даної технології, виконаних за останні роки [14-18]. Базова відстань передачі сигналу для IEEE 802.15.4 – 10 метрів, що є цілком достатньою для WSN. Максимальна швидкість передачі даних складає 250кбіт/с.

2) Протоколи канального рівня. Канальний рівень, відповідно до концепції IEEE 802, можна розділити на два підрівні, що виконують різні функції. Більш низький підрівень доступу до середовища або MAC-рівень виконує функції розмежування і розпізнавання кадрів, адресації в рамках одного середовища доступу, а також розмежування доступу до середовища передачі, в тому числі уникнення, виявлення та вирішення колізій. Верхній

підрівень управління логічним зв'язком (Logical link control, LLC) займається мультиплексуванням і демультиплексуванням потоків даних, встановленням з'єднань між вузлами в рамках одного середовища передачі, в деяких випадках – контролем коректності переданих кадрів та виправленням помилок. Вимоги до протоколів канального рівня WSN можна сформулювати наступним чином: дані протоколи повинні бути енергетично економічними, повинні давати можливість швидко встановлювати з'єднання між будь-якими двома вузлами, що мають доступ до одного і того ж середовища (так як WSN є ad hoc, а не інфраструктурними мережами), і забезпечувати можливість самоорганізації великого числа вузлів. Також слід зазначити, що реалізація таких протоколів не повинна вимагати великих обчислювальних ресурсів. Для організації MAC-рівня WSN також досить часто використовується стандарт IEEE 802.15.4. Він реалізує всі необхідні функції даного рівня з невеликими витратами електроенергії. Розмежування доступу до середовища передавання реалізується за допомогою методу множинного доступу з контролем несучої і униканням колізій (Carrier Sense Multiple Access With Collision Avoidance, CSMA/CA) [17].

Стандарт IEEE 802.15.1 є набагато більш економічним і з цієї точки зору цілком підходить для організації WSN. Але даний стандарт має ряд інших обмежень. Так, Bluetooth, що розроблявся спочатку для того, щоб обмін інформацією між пристроями проводився не за допомогою проводів, а через бездротовий інтерфейс, має дуже великий (близько 5 секунд) час встановлення з'єднання, що робить його непридатним для WSN, в яких необхідно мати можливість, наприклад, швидкого переконфігурування мережі. До того ж об'єднання в одну мережу більше 8 Bluetooth-пристроїв вимагає з'єднання декількох підмереж, що також створює деякі складності при реалізації WSN з використанням даної технології.

3) Протоколи мережевого рівня і протоколи маршрутизації. Протоколи мережевого рівня WSN, крім стандартних вимог до енергетичної ефективності

та використання невеликих обчислювальних потужностей, також мають ряд додаткових вимог, пов'язаних зі специфікою WSN. Це, в першу чергу, підтримка режиму багатоітеральної (multihop) передачі даних. Також протоколи мережевого рівня повинні забезпечувати підтримку самоорганізації мережі. Крім того, при проектуванні протоколів мережевого рівня WSN зазвичай враховується, що дані в таких мережах передаються здебільшого в напрямку від сенсорних вузлів до шлюзу WSN [20].

4) Протоколи транспортного рівня. Оскільки протоколи транспортного рівня призначені для доставки даних, в тому числі між мережами, для WSN, що представляють собою окрему мережу, в складних і інтелектуальних протоколах даного рівня найчастіше немає необхідності, оскільки будь-який протокол вимагає для своєї роботи додаткових апаратних ресурсів і електроживлення, які в сенсорних вузлах WSN можуть бути дуже обмежені. У той же час, з урахуванням розвитку протоколу 6LoWPAN, а також концепції IP, видається цілком розумним використання в WSN транспортних протоколів, широко застосовуваних у мережі Інтернет, для забезпечення доступу до сенсорних вузлів WSN з глобальної мережі. І якщо використання протоколу контролю передачі (TCP) може бути не зовсім виправдано з урахуванням великого розміру заголовку (від 20 байт) і відносної складності реалізації, які можуть вимагати неприйнятно великих для WSN ресурсів, то протокол призначений для передачі дейтаграм користувача (User Datagram Protocol, UDP), хоч і не забезпечує гарантованої доставки, цілком може застосовуватися в WSN у зв'язку з більшою, ніж для TCP, простотою реалізації і меншим розміром заголовку (8 байт) [21-24]..

5) Протоколи верхніх рівнів. Необхідно зауважити, що протоколи верхніх рівнів, зокрема, прикладного рівня для WSN, значною мірою залежать від того, для яких саме цілей буде використовуватися WSN. Оскільки зараз вже існує достатньо велика кількість додатків для WSN, і ще більша кількість додатків

знаходиться на стадії розробки, зараз складно виділити якісь загальновизнані і широко використовувані відкриті протоколи верхніх рівнів для WSN [22, 23].

У табл. 1.2 відображено виявлені проблеми на різних рівнях моделі OSI:

Таблиця 1.2

Виявлені проблеми згідно моделі комунікації відкритих систем

Рівень OSI	*Порушення і атаки*	*Контрзаходи*
Фізичний	Jamming (глушіння)	Розширення спектру, пріоритизація повідомлень, картування областей.
	Tampering (підробка)	Випробувальні пакети проти підробки, використання нечутливих до відмов протоколів.
Канальний	Колізії	Корегувальне кодування, перебудування (налаштування).
	Виснаження	Обмеження швидкості передавання даних.
	Збір інформації	Захисту проти повторних відправлень, сувора аутентифікація на канальному рівні.
Мережевий	Фальсифікація маршр. інформації	Аутентифікація, використання захисту проти повторних відправлень.
	Селект. просування	Використання різних маршрутів, підтвердж. доставки
	Sinkhole атака	Перевірка надмірності.
	Sybil атака	Аутентифікація, надмірність, моніторинг.
Транспортний	Flood атака	Клієнтські пазли.
	Розсинхронізація	Аутентифікація.
Прикладний	DoS атака на базі маршруту	Аутентифікація, використання захисту проти повторних відправлень.
	Перепрограмування	

З позиції побудови ІТ моніторингу найбільш важливим з табл.. 1.2 буде канальний рівень, зокрема проблеми, пов’язані з колізіями.

1.4. Особливості сучасної концепції IoT

Відповідно до [36] сучасна концепція IoT передбачає комунікацію об’єктів, які використовують технології для взаємодії між собою та з навколишнім середовищем, що дає змогу так званим «речам» (пристроям) без втручання і впливу людини. Отже, усі пристрої в різноманітних системах інфраструктури (у тому числі й критичної [74]) повинні виконувати обробку інформації, її аналіз та здійснювати обмін між собою і залежно від результатів приймати рішення та виконувати певні дії. Фактично IoT може слугувати ефективним інструментом для прийняття управлінських рішень.

Згідно [36] експерти стверджують, що IoT є однією з найперспективніших технологій останніх років, яка вже сьогодні створює низку нових продуктів і приводить до появи нових ІТ компаній на ринку. У багатьох вітчизняних домівках вже встановлені системи «розумного будинку», в які інтегровані десятки сенсорів IoT. Переваги IoT можна продемонструвати на прикладах, тим більше, що галузей використання цієї технології чимало – це і медицина, і охорона навколишнього середовища, сільське господарство, вугільна промисловість, траспорт, енергетика і т.п. [36].

Концепт IoT вперше був сформульований ще у 1999 році, а на сьогодні – це один із головних світових трендів. Будь-які, навіть старі функціонуючі пристрої можуть ставати частиною IoT і виконувати нові функції. Таким чином, галузь IoT вважають рушієм четвертої індустріальної революції [36].

Фактично, кількісний перехід від так званого Інтернету людей до IoT відбувся у 2008-2009 рр. Саме у цей час кількість IoT пристроїв перевищила кількість інтернет-користувачів, а тому світ поступово перейшов у нову фазу розвитку технологій – це фаза IoT.

За прогнозами аналітиків у найближчі роки очікується справжній бум IoT – до 2020 року кількість підключених до Інтернету пристроїв становитиме 26 мільярдів, а дохід від продажу устаткування, ПЗ та послуг становитиме 1,9 трлн доларів. Найбільші світові IT-компанії, зокрема Intel, Google, IBM та ін., вже почали масштабну роботу на ринку IoT і зайняли свою лідерську нішу в цьому напрямку. Для прикладу, компанія Intel у 2014 році створила власний підрозділ під назвою «Internet of Things Solutions Group» для розвитку IoT. Інша відома корпорація Google на початку 2014 року за 3,2 млрд доларів купила невелику фірму Nest Labs, яка займається випуском інтелектуальних термостатів. Спеціалісти компанії Google займаються широким впровадженням на американському ринку технологій IoT різного призначення.

Прикладом впровадження IoT є система «розумний будинок», однією з функцій якого є контроль параметрів навколишнього середовища залежно від температури в контексті економії енергоносіїв (це корелює з тематикою цієї дисертаційної роботи, що вчерговий раз підкреслює її актуальність). Зазначена концепція передбачає використання звичних у побуті приладів, що вже стали інтелектуалізованими [36]: термостати; системи відеоспостереження і сигналізації; холодильники, морозильні камери; телевізори тощо.

Такі технології використовують ситуативні децентралізовані WSN і в сучасних будинках вже можна побачити безліч таких систем, з’являються нові й нові сервіси – віддалене спостереження через смартфон за власним помешканням, автоматичні клімат-системи будівель (для дому, офісу, складу тощо). Основні функції таких систем – це безпека і оптимальне використання енергоресурсів.

Крім того, важливою функцією IoT є полегшення повсякденного життя людей – як приклад, можна відзначити розробку компанії Edyn – універсальний садовий прилад, що надає користувачеві точні відомості про рівень вологості, інтенсивності світла, температури верхніх шарів ґрунту, його насиченості

мінеральними речовинами тощо. На відміну від аналогів, ці сенсори абсолютно автономні з точки зору живлення – електроенергію вони отримують від вбудованої сонячної батареї, а результати вимірювань передають через Wi-Fi на власний хмарний сервіс. Як наслідок, власник має доступ до статистики з будь-якої точки планети, де є доступ до Інтернету.

Також, значний інтерес IoT представляє для моніторингу рухомих об'єктів, в першу чергу, для автомобільного транспорту. Це дозволяє діагностувати роботу авто у процесі експлуатації, попереджати можливі аварійні ситуації, замовляти запчастини, а також здійснювати рекомендації з пошуку необхідної станції і встановлення часу обслуговування транспортного засобу [36].

У результаті аналізу нормативних документів і наукових публікацій [37-44, 53-58, 60, 62-69] встановлено, що концепція IoT (рис. 1.6) має три взаємопов'язані базові проблеми:

1) забезпечення інформаційної безпеки (IoT Security);

2) масштабування зростаючого обсягу технічних пристроїв і даних (IoT Scalability);

3) урахування вимог до зниження енергоспоживання (IoT Technical Solutions and Low-Power Consumption).

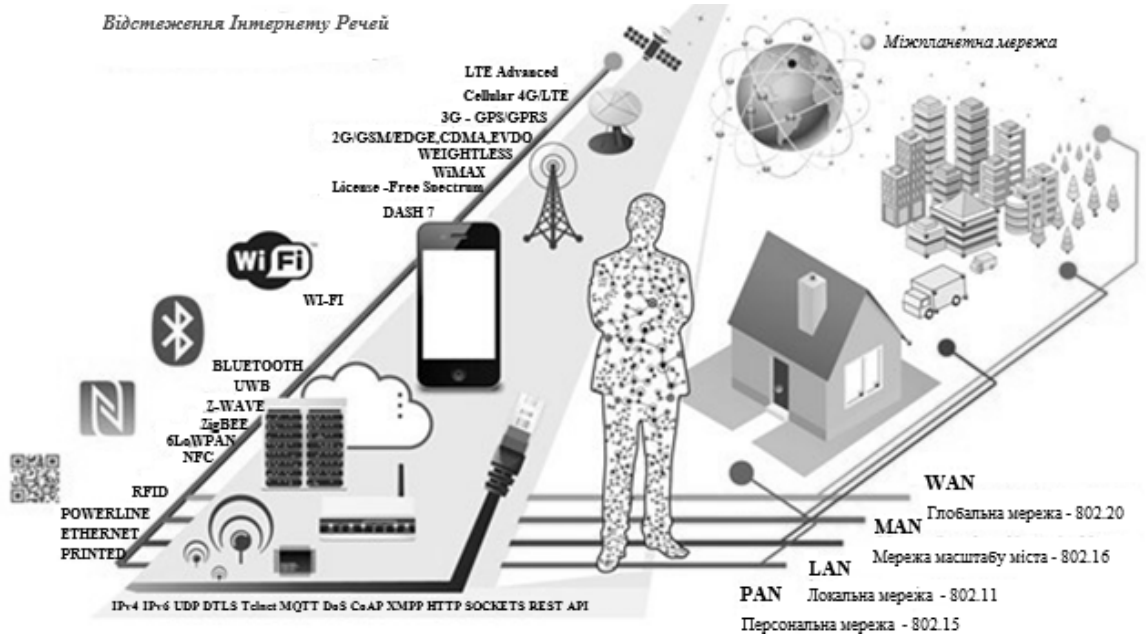


Рис. 1.6. Безпроводові мережеві протоколи для концепції IoT

Також, проведено аналіз протоколів для вирішення завдань IoT [53-58]:

1) MQTT: протокол (рис. 1.7) для збору даних пристроїв і передавань їх серверів (D2S). Легкий і простий протокол обміну повідомленнями, який реалізує т. зв. модель «публікація / підписка» і призначений для зв'язку комп'ютеризованих пристроїв, підключнних до локальної або глобальної мережі, між собою і різними громадськими чи приватними веб- сервісами.

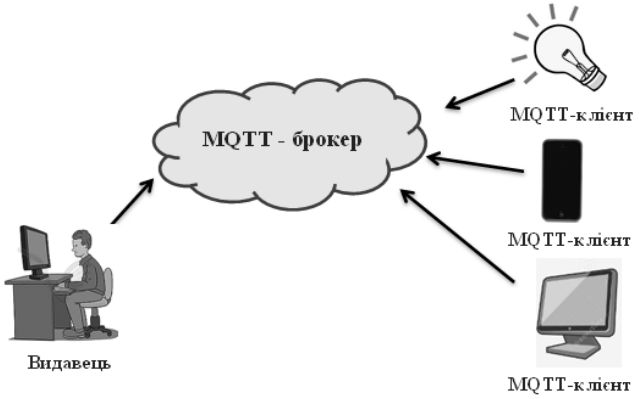


Рис. 1.7. Схема протоколу MQTT

2) XMPP: протокол для з'єднання пристроїв з людьми, частковий випадок D2S-схеми, коли люди з'єднуються з серверами. Розширюваний протокол обміну повідомленнями та інформацією про присутність. Він був розроблений для системи миттєвого обміну повідомленнями для зв'язку між людьми за допомогою текстових повідомлень (рис. 1.8).

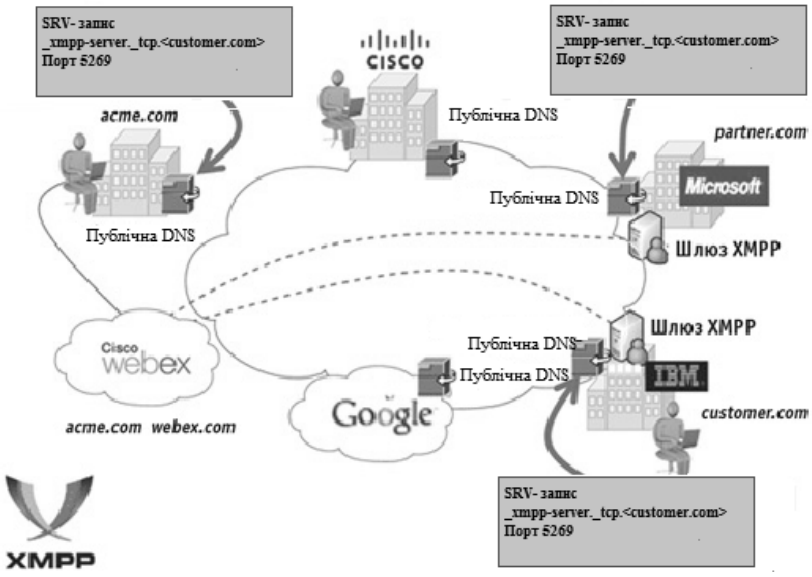


Рис. 1.8. Схема протоколу XMPP

3) DDS (Data Disturbing Service): швидка шина для інтегрування інтелектуальних пристроїв (D2D);

4) AMQP: система організація черг для з'єднання серверів між собою (S2S). Вдосконалений протокол організації черги повідомлень), який іноді розглядають як протокол IoT. Як випливає з назви, AMQP обслуговує виключно черги. Він пересилає транзакційні сполучення між серверами. Цей протокол в якості орієнтованого на повідомлення проміжного ПЗ, був створений для банківської галузі і здатний обробляти тисячі організованих в чергу транзакцій.

На рис. 1.9 наведено екосистему типової мультирівневої архітектури IoT згідно міжнародного стандарту ITU-T Y. 2060 «Overview of the Internet of Things» [43] та інших сучасних наукових публікацій [44-51, 70-73].

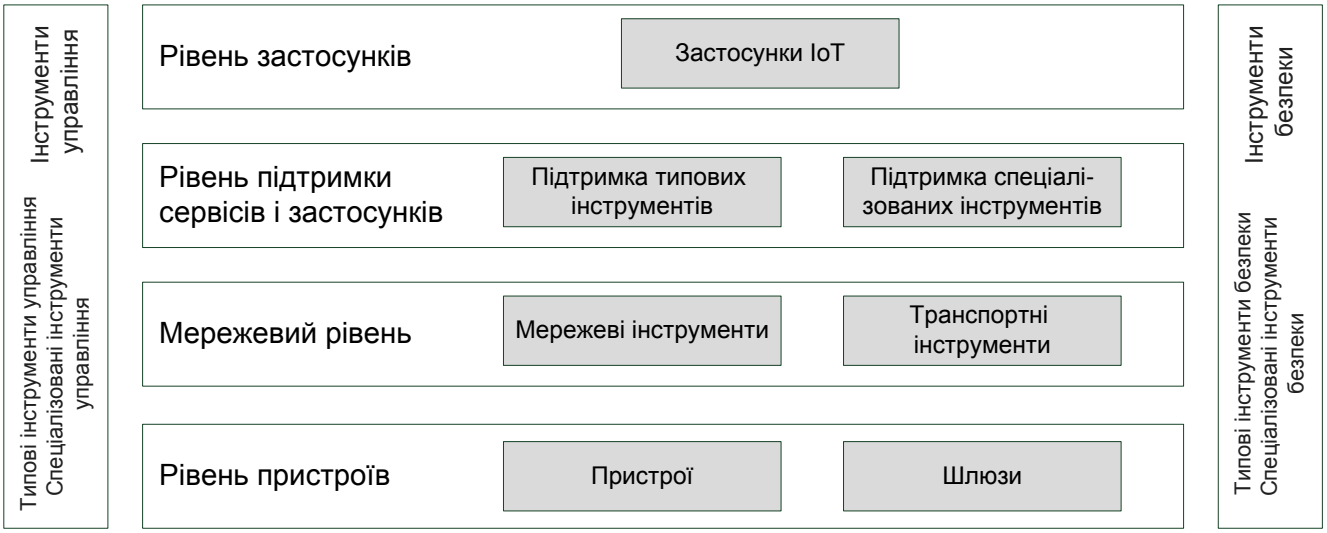


Рис. 1.9. Мультирівнева архітектура IoT відповідно до сучасних міжнародних стандартів [43]

Широкому впровадженню Інтернету речей перешкоджають складні технічні та організаційні проблеми, зокрема, пов'язані зі стандартизацією. Єдиних стандартів для інтернету речей поки немає, що ускладнює можливість інтеграції пропонованих на ринку рішень і багато в чому стримує появу нових. До факторів, що уповільнює розвиток Інтернету речей, слід віднести складності переходу існуючого Інтернету до нової, 6-ї версії мережевого протоколу IP,

перш за все необхідність великих фінансових витрат з боку телекомунікаційних операторів і провайдерів послуг на модернізацію свого мережевого обладнання. Тому метою даної роботи було визначено проведення аналізу комунікаційних протоколів, які можуть бути використані в концепції IoT, визначення їх переваг та недоліків, обґрунтування особливостей їх застосування для конкретних потреб.

Зазначені недоліки IoT негативно впливають на її базові функції, зокрема, її застосування для моніторингу, крім проблем безпеки, стикається з проблемою виникнення колізій під час масштабування, а також високими енергетичними потребами відомих рішень, які у переважній більшості є детерміністичними.

У табл. 1.3 зведено переваги та недоліки бездротових техноголій, які можуть бути використані в концепції IoT, а також їх області потенційного застосування.

Таблиця 1.3

Переваги та недоліки техноголій, які можуть бути використані в концепції IoT

Технічні характеристики	**Wi-Fi**	**Wi-Fi HaLow**	**ZigBee**	**LoRaWAN**	**Z-Wave**	**Bluetooth LE**
Стандарт	IEEE 802.11	IEEE 802.11 ah	IEEE 802.15.4	LoRaWAN	Z-Wave	Bluetooth 4.0
Частота	2,4 ГГц, 5 ГГц	900 МГц	915 МГц / 2,4 Ггц	863-870 МГц	900 МГц	2,4 ГГц
Дальність дії	До 100 м	До 1 км	100 м / Mesh	2-5 км в місті; до 15 км поза	30 м / Mesh	80 м
Швидкість передачі	7 Гбіт/с	50 кбіт/с – 18 Мбіт/с	250 кбіт/с	290 біт/с - 50 Кбіт/с	10-100 кбіт/с	< 1 Мбіт/с

Енерго-споживання	Високе	Понижене	Низьке	Низьке	Низьке	Низьке
Масштабо-ваність	Так	Так	Так	Так	Обмежено	Так
Діапазон ISM	Так	Так	Так	Так	Так	Так
Аутентифікація	Так	Так	Так	Так	Так	Проблема-тично
E2E шифрування	Так	Так	Так	Так	Так	Так
Вартість обладн.	Висока	Висока	Низька	Низька	Висока	Низька
Місцезнаходжен-ня сенсора відомо	Так	Так	-	Так	-	Ні
Повна двоспрямованість	Так	Так	Так	Так, залежно від режиму	Так	Так
Підтримка сенсорів, які рухаються між хабами	Так	Так	Так, mesh	Так	Так, mesh	Так

1.5. Багатокритеріальний аналіз методів моніторингу в концепції IoT

IoT формує тенденції до об'єднання різних телекомунікаційних технологій що відкриє можливості для надання сервісів нового типу. Передбачається інтеграція глобального цифрового мобільного стільникового зв'язку GSM з комунікаціями ближнього радіусу дії (Hear Field Communicationм, NFC) персональними мережами на базі Bluetooth, бездротовими локальними мережами, бездротовими сенсорними мережами стандарту ZigBee, в поєднанні з системою глобального позиціонування і технології ідентифікації абонента (Sim-карти). Кінцеві користувачі будуть платити компаніям, які мають доступ до даних, що надходять від нашого тіла (електронна охорона здоров'я), будинків (ефективність використання енергії), телематику/мобільність (автомобілі, самохідні автомобілі, електромобілі) і за

місто, як набір сервісів (різні держпослуги). Така інтеграція дозволить сервісам проникати через всі адміністративні бар'єри, тоді послуги легко досягнуть кінцевого споживача. Реалізація цих послуг потребує подальшого розвитку хмарних обчислень, будівництва потужних центрів обробки даних (Data Centers), а також створення проміжних вузлів збору та обробки даних, наближених безпосередньо до джерел цих даних.

У табл. 1.4 відображено результати проведеного аналізу відомих підходів до моніторингу параметрів навколишнього середовища в концепції IoT [12-19, 28, 31-36. 38, 40, 45-52, 59, 61, 70-73] за такими критеріями:

1. *Manag.* – врахування аспектів управління (зворотні зв'язки з IoT);
2. *Collis.* – врахування колізій і ефективне їх блокування;
3. *Determ.* – розробки на базі детерміністичних підходів;
4. *Stoch.* – розробки на базі стохастичних підходів;
5. *HSC* – спеціалізовані програмно-апаратні комплекси на базі IoT.

Таблиця 1.4

Багатокритеріальний аналіз підходів до моніторингу в концепції IoT

Підхід	*Критерій*				
	Manag.	*Collis.*	*Determ.*	*Stoch.*	*HSC*
Бертсекас Д.	-	+	+	-	-
Болгер Дж.	+	-	+	-	-
Гандел Р.,	-	+	+	-	+
Девід Е.,	-	-	+	-	-
Комарова Л.	+	-	+	-	+
Романюк А.	-	-	-	+	-
Райба С.	+	+	-	+	-
Шахгільдян В.	-	+	+	-	-

Таким чином, у першому розділі роботи виявлено недоліки відомих підходів і доведено необхідність створення математичних моделей, методів, комунікаційних протоколів мереж WSN з випадковим доступом і відповідних інформаційних технологій моніторингу для забезпечення високої продуктивності, якості і живучості їх функціонування.

Список літератури до першого розділу

1. Fischer K. W. 2004 Atmospheric Laser Communication: New Challenges for Applied Meteorology / K. W. Fischer, M. R. Witiw, J. A. Baars, T. R. Oke, *Bulletin of the American Meteorological Society*, 85, 2004. – P. 725–732.

2. Forin, D. M. Free Space Optical Technologies [Text] / D. M. Forin, G. Incerti, G. M. Tosi Beleffi, A. L. J. Teixeira, L. N. Costa, P. S. De Brito Andre, B. Geiger, E. Leitgeb, F. Nadeem, *Trends in Telecommunications Technologies*, Christos J Bouras (Ed.), ISBN: 978-953-307-072-8, InTech, DOI: 10.5772/8488. Available from: http://www.intechopen.com/books/trends-in-telecommunications-technologies/free-space-optical-technologies

3. Ghassemlooy Z. Free Space Optical Communications [Електр. ресурс], URL: http://www.docstoc.com/docs/22054676/Optical-Wireless-Communication-using-Digital-Pulse-Interval-Modulation.

4. Colwell R. Hearing on Remote Sensing as a Research and Management Tool / R. Colwell, Testimony of Dr., Rita Colwell, Director, *National Science Foundation, Before the Basic Research Subcommitte, House Science Committe*, September 1998, p. 63.

5. Conti M. Wireless Communications and Pervasive Technologies in D. Cook and S.K.Das (eds) *Environments: Technologies, Protocols and Applications* / M. Conti // NY : John Wiley & Sons, 2005, 63–99 p.

6. Cramer R. J. Impulse radio multipath characteristics and diversity reception [Text] / R. Cramer, M. Z. Win, R. A. Scholtz, *Communications : IEEE International Conference*, ICC’98, 1998, Vol. 3, P. 1650–1654.

7. Dechene D. J. A Survey of Clustering Algorithms for Wireless Sensor Networks / D. J. Dechene, A. El Jardali, M. Luccini, A. Sauer, Information and Automation for Sustainability, ICIAFS 2008. *4th International Conference Department of Electrical and Computer Engineering,* P. 295-300.

8. DSN Team / *Multilateration Poster, SensIT Workshop,* St. Petersburg, FL, April 2001, P. 52-59.

9. J. Heidemann, F. Silva, C. Intanagonwiwat, Building efficient wireless sensor networks with low-level naming, *Operating Systems Principles : Proceedings of the Symposium,* Banff, Canada, 2010, P. 146-159.

10. Baccelli, F., The Role of PASTA In Network Measurement [Text] / F. Baccelli, S. Machiraju, D. Veitch, J. Bolot, *Computer Communication Review, Proceedings of ACM Sigcomm,* 2006, Vol. 36, № 4, P. 231-242.

11. A.A.A. Alkhatib, G. S. Baicher, An Overviev of Wireless Sensor Networks, *Computer Networks and Communication System (CNCS 2012): 2012 Inetnational Conference, IPCSIT,* Singapore : IACSIT Press, 2012, V. 35, P. 11-15.

12. Perkins C. *Ad Hoc Networks,* Addison-Wesley, Reading, MA, 2000, 28 p.

13. D. Nadig, S. S. Iyengar, A new architecture for distributed sensor integration, *Proceedings of IEEE Southeastcon'93,* Charlotte, NC, April 1993: thesis, 1993, P. 1-8.

14. W.R. Heinzelman, A. Chandrakasan and H. Balakrishnan, Energy-Efficient Communication Protocol for Wireless Microsensor Networks, IEEE *Proceedings of the 33rd Hawaii International Conference on System Sciences,* 2000, pp. 1-10.

15. A. Akl, T.Gayraud, P.Berthou, An investigation of self-organization in wireless sensor networks, *IEEE International Conference on Networking, Sensing and Control (ICNSC),* 2001, pp. 1-6.

16. K. Sohrabi, J.Gao, V.Ailawadhi and G.J. Pottie, Protocols for Self-Organization of a Wireless Sensor Network, *Personal Communications, IEEE,* October 2000, Vol. 7, N 5, 16-27 pp.

17. IEEE 802.15.4a: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (WPANs), Institute of Electrical and Electronics Engineers, 2007.

18. Баскаков С.С. Исследование способов повышения эффективности маршрутизации по виртуальным координатам в беспроводных сенсорных сетях, *Вестник МГТУ им. Н. Э. Баумана.* 2009. № 2, С. 112–124.

19. ZigBee Alliance [Электр. ресурс] URL: http://www.zigbee.org/

20. Chris Karlof, David Wagner, "Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures", *AdHoc Networks,* p.299-302, 2003.

21. Culpepper B.J., Tseng H.C. Sinkhole intrusion indicators in DSR MANETs, *Proc. 1ST International Conf. on Broad band Networks*. 2004, p. 681-688.

22. Hu Y., C. Perrig, Johnson D.B. Packet leashes: a defense against wormhole attacks in wireless networks, *Twenty-Second Annual Joint Conference of the IEEE Computer and Communications Societies,*Vol. 3, 2003, p. 1976-1986.

23. Blackert W.J., Gregg D.M., Castner A.K., Kyle E.M., Hom R.L., and Jokerst R.M. Analyzing interaction between distributed denial of service attacks and mitigation technologies, *Proc. DARPA Information Survivability Conference and Exposition*, Vol. 1, 2003, p. 26-36.

24. Pathan A.S.K.; Hyung-Woo Lee; Choong Seon Hong, "Security in wireless sensor networks: issues and challenges" *Advanced Communication echnology (ICACT),* p. 6, 2006.

25. Zia T., Zomaya A., "Security Issues in Wireless Sensor Networks", *Systems and Networks Communications (ICSNC)* p.40, 2006.

26. Adrian Perrig, John Stankovic, David Wagner, "Security in Wireles Sensor Networks" *Communications of the ACM*, p. 53-57, 2004.

27. S. Rajba, T. Rajba, The Performance of a Digital FSK System with Actual Discriminator,Time Distortions Effects, *Applicationes Mathematica* – 1990 Vol. 20 (2), p. 261-279.

28. J. Pilarski, S. Rajba, Measurement of light gradient in plant organs with a fiber optic microbe, *Acta Physiologiae Plantarum*, 2004, Vol. 26, No 4, p. 405-410. – ISSN 0137-5881.

29. M. Karpiński, S. Rajba, T. Rajba, Measurement and information system used the mobile phone GSM and Bluetooth, *PAK*, 2007, 53 (12), p.79-81.

30. J. Szczepanik, S. Rajba, I. P. Kurytnik, Temperature measurement using GSM network, *Acta Mechanica Slovaca*, 2008, R.12, No 3, p. 247-252.

31. G. Hoblos, M. Staroswiecki, A. Aitouche, Optimal design of fault tolerant sensor networks, *Control Applications: IEEE International Conference*, Anchorage, AK, September 2000, p. 467-472.

32. J. M. Kahn, R. H. Katz, K. S. J. Pister, Next century challenges: mobile networking for smart dust, *Proceedings of the ACM MobiCom'99*, Washington, USA, 1999, p. 271–278.

33. I. F. Akyildiz, W. Su, Y., Sankarasubramaniam, E. Cayirci Wireless sensor networks: a survey [Text], *Computer networks*, 2002, V. 38, № 4, p. 393-422.

34. Rajba S. Architektura sieci metropolitarnej z szerokopasmową siecią dostępową, Akademia Techniczno-Humanistyczna w Bielsku-Białej, Zeszyty Naukowe Nr 17, *Budowa i Eksploatacja Maszyn*, Seria 6, Publikacje, Bielsko-Biała - 2004, p.104-116.

35. Weiser M. Scheduling for reduced CPU energy, *Operating System Design and Implementation: Proceedings of 1st USENIX Symposium*, November 1994, p. 13–23.

36. А. Й. Наконечний, З. Є. Верес, Інтернет речей і сучасні технології, *Вісник Національного університету «Львівська політехніка». Автоматика, вимірювання та керування,* 2016, № 852, с. 3-9.

37. «Интернет вещей» — реальность или перспектива? [Електронний ресурс], Режим доступу: http://www.mate-expo.ru/ru/article/internet-veshchey-realnost-ili-perspektiva

38. «Умный дом»: 5 технологий будущего [Електронний ресурс], Режим доступу: http://www.lookatme.ru/mag/live/future-research/194385-smart-home

39. Jack Tison, SVP Emerging Business, Panduit-October 2015 3 Steps for Evolving IoT Architectures [Електронний ресурс], Режим доступу: http://www.industrial-ip.org/en/industrial-ip/internet-of-things/3-steps-for-evolving-iot-architectures

40. Интернет вещей открывает киберпреступ-никам новое поле деятельности [Електронний ресурс], Режим доступу: http://www.klaipeda1945.org/sensatsii/34031

41. Эксперты предупредили о растущем количестве киберугроз в сфере «Интернета вещей» [Електронний ресурс], Режим доступу: http://www.securitylab.ru/news/480244.php

42. Интернет вещей ставит под угрозу безопасность пользователей [Електронний ресурс], Режим доступу: http://umvs.kr.ua/internet-veschej-stavit-pod-ugrozu-bezopasnost-polzovatelej

43. ITU-T Y. 2060 *«Overview of the Internet of Things»*, 2012, 22 p.

44. ISO/IEC JTC 1/SC 41, *Internet of Things and related technologies.*

45. Pathan A.S.K.; Hyung-Woo Lee; Choong Seon Hong, Security in wireless sensor networks: issues and challenges, *Advanced Communication echnology (ICACT)*, 2006, p.6.

46. Zia T., Zomaya A., Security Issues in Wireless Sensor Networks, *Systems and Networks Communications (ICSNC)*, 2006, p.40.

47. Adrian Perrig, John Stankovic, David Wagner, *Security in Wireless Sensor Networks Communications of the ACM*, 2004, p.53-57.

48. Chris Karlof, David Wagner, Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures, *AdHoc Networks*, 2003, p. 299-302.

49. Hu Y., C. Perrig, Johnson D.B. Packet leashes: a defense against wormhole attacks in wireless networks, *Twenty-Second Annual Joint Conference of the IEEE Computer and Communications Societies*, Vol. 3, 2003, p. 1976-1986.

50. Постольский С.П. Обзор проблемных областей в безопасности беспроводных сенсорных сетей, атак и механизмов их защиты, *Научное сообщество студентов XXI столетия. техн. науки:* сб. ст. по мат. XXXII междунар. студ. науч.-практ. конф. № 5 (31). [Електронний ресурс], Режим доступу: http://sibac.info/archive/technic/5(31).pdf

51. Blackert W.J., Gregg D.M., Castner A.K., Kyle E.M., Hom R.L. and Jokerst R.M. Analyzing interaction between distributed denial of service attacks and mitigation technologies, *Proc. DARPA Information Survivability Conference and Exposition,* Vol.1, 2003, p. 26-36.

52. А.В. Росляков, С.В. Ваняшин, А.Ю. Гребешков, *Интернет вещей: учебное пособие,* Самара: ПГУТИ, 2015, 200 с.

53. Яка мережа «зловить» речі? [Електронний ресурс], Режим доступу: http://mikrotik.kpi.ua/index.php/courses-list/iot/104-what-network-catch-things

54. Understanding IoT Protocols – Matching your Requirements to the Right Option, [Електронний ресурс], Режим доступу: https://solace.com/blog/use-cases/understanding-iot-protocols-matching-requirements-right-option?utm_source=adroll&utm_medium=cpc&utm_campaign=iot&utm_content=25

55. Recommendation Y.2060 [Електронний ресурс], Режим доступу: https://www.itu.int/rec/T-REC-Y.2060-201206-I

56. Технологія Bluetooth Protocols [Електронний ресурс], Режим доступу: http://wiki.kspu.kr.ua/index.php/Технологія_Bluetooth

57. Сучасні телекомунікації: мережі, технології, безпека, економіка, регулювання, Вид. 2, За загальною ред. Довгого С.О., К.: «Азимут-Україна», 2013, 608 с.

58. Как выбрать стандарт связи для сети IoT [Електронний ресурс], Режим доступу: http://savepearlharbor.com/?m=201602&paged=59

59. Fahier N., Fang W.-C. An Advanced Plug-and-Play Network Architecture for Wireless Body Area Network Using HBC, ZigBee and NFC, *IEEE International Conference on Consumer Electronics (ICCE),* 2014. pp. 165-166.

60. Киричек Р. В., Парамонов А. И., Прокопьев А. В., Кучерявый А. Е. Эволюция исследований в области беспроводных сенсорных сетей, *Информационные технологии и телекоммуникации.* 2014, № 4 (8), с. 29-41. URL: http://www.sut.ru/doci/nauka/review/4-14.pdf

61. Одарченко Р.С. Концепція сенсорної мережі збору метеорологічних даних для системи регулювання випромінюваної потужності радіо-передавальних пристроїв стільникових мереж, *Проблеми створення, випробування, застосування та експлуатації складних інформаційних систем*, Вип. 8, 2013, с. 53-61

62. Архитектура LoRaWAN сетей [Електронний ресурс], електронні Режим доступу: http://lorawan.lace.io/lorawan-networks/

63. Раскрываем тайны 6LoWPAN, *Новости электроники***,** №11, 2015, с. 30-36.

64. Что такое LoRa? [Електронний ресурс], Режим доступу: http://lorawan.lace.io/faqs/lora/

65. Understanding The Protocols Behind The Internet Of Things [Електронний ресурс], Режим доступу: http://www.electronicdesign.com/iot/understanding-protocols-behind-internet-things

66. AMQP Advanced Message Queuing Protocol. Protocol Specification [Електронний ресурс], Режим доступу: https://www.rabbitmq.com/resources/specs/amqp0-8.pdf

67. MQTT, CoAP, IoT Protocols [Електронний ресурс], Режим доступу: https://eclipse.org/community/eclipse_newsletter/2014/february/article2.php

68. IoT современные телекоммуникационные технологии [Електронний ресурс], Режим доступу: http://www.lessons-tva.info/articles/net/013.html

69. И.А. Гепко, В.Ф. Олейник, Ю.Д. Чайка, А.В. Бондаренко. *Современные беспроводные сети: состояние и перспективы развития*, К., 2009, 672 с.

70. R. Odarchenko; A. Abakumova; O. Tkalich; O. Ustinov, LTE and wireless sensor networks integration in the concept of ”Smart Home”, *2016 4th*

International Conference on Methods and Systems of Navigation and Motion Control (MSNMC), pp. 35-38;

71. Одарченко Р.С., Гнатюк С.О., Ткаліч О.П. Архітектура сучасної захищеної інформаційно-комунікаційної мережі аеропорту, *Захист інформації,* 3 (17), с. 240-246.

72. М.Б. Алєксандер, О.Г. Корченко, М.П. Карпінський, Р.С. Одарченко «Дослідження вразливостей сенсорних підмереж архітектури Інтернету речей до різних типів атак», *Безпека інформації*, Том 22, № 1, 2016, с. 12-19.

73. О.Г. Корченко, М.Б. Алєксандер, Р.С. Одарченко, А.А. Наджі, О.Ю. Петренко, «Аналіз загроз та механізмів забезпечення інформаційної безпеки в сенсорних мережах», *Захист інформації,* Том 18, №1, січень-березень 2016, с. 48-56.

74. Gnatyuk S., Sydorenko V., Polishchuk Yu., Kotelianets V., «Analisys of modern aaproaches to security assessment of information resources for critical information infrastructure of the state», *Scientific and Practical Cyber Security Journal*, Vol. 2, №4, p. 81-86, 2018.

РОЗДІЛ 2. РОЗРОБКА МОДЕЛЕЙ ФУНКЦІОНУВАННЯ WSN ДЛЯ ЕФЕКТИВНОГО ПРОЕКТУВАННЯ ПРОТОКОЛІВ КОМУНІКАЦІЇ IoT

2.1. Передавання даних у WSN і ефективне планування протоколів з урахуванням виникнення колізій

Для прийнятих принципів реалізації WSN, істотою правильності дії цієї мережі є передача протоколів від вузлів до базової станції (sink) без колізій. Оскільки ведеться пошук найпростішого рішення для мережі у розумінні простоти реалізації, вартості компонентів (в основному вузлів, припускаючи можливість втрати під час експлуатації), а передусім спрощення всіх процедур (зв'язок типу симплекс, що означає по стороні вузла лише передавальний пристрій), максимальне заощадження енергії живлення вузлів (що у багатьох рішеннях означає час життя вузла), а також обмеження займаної радіо-смуги та зведення дії мережі до роботи на одній несучій частоті.

Цими основними принципами визначено рішення щодо мережі WSN при використанні випадкового доступу вузлів до базової станції на основі моделі PASTA. Це теж означає, що для виконання представлених завдань необхідно проаналізувати подію у радіо-просторі функціонування вузлів і його оточенні (з огляду на можливі зовнішні завади). Найістотнішим елементом цього аналізу є те, що немає колізій під час радіопередачі окремих вузлів в області дії мережі. Через те, що радіотрансляція, тобто передавання протоколу у просторі відбувається у випадкових періодах часу, існує можливість виникнення принаймні двох передач у часі таким способом, що протоколи в якийсь проміжок часу накладуться. Цю подію називаємо колізією і фізично означає вона повну втрату інформації від вузлів, які знаходяться у колізії. Отже, суттю розробки цього методу та визначення галузей його застосування зводиться до аналізу колізійних подій, їх мінімізації та встановлення ймовірності появи колізій у контексті належної роботи мережі. Одним із важливих складових компонентів цього рішення є час тривання протоколу t_p.

У роботах [1, 3, 6, 7] прийнято, що це час $t_p = 3{,}2 \cdot 10^{-5}$ с. Прийняття цього часу є ефектом перших досліджень у цій галузі та застосованих давачів, надалі для отримання порівняльних результатів використано цей час. Це не означає, що цей арбітрально прийнятий час є незмінною величиною. У цьому місці роботи необхідно піддати цей час аналізу з огляду на будову комунікаційного протоколу, його інформаційного вмісту, а також радіо-смуги, яка необхідна під час його передачі (спектр радіо-сигналу, який супроводжує передачу протоколу) [4].

Критерії вибору часу тривання протоколу передачі

З огляду на технологію доступу запропонованого рішення на базі моделі PASTA час тривання протоколу (t_p) повинен бути якнайкоротшим. Чим він коротший, тим ймовірність колізії менша, а тому і менша ймовірність втрати інформації, яка надходить, наприклад, від вимірювальних сенсорів. У свою чергу протокол повинен містити всю необхідну інформацію, пов'язану з ідентифікацією вузла, ідентифікацією сенсора у вузлі та потрібною роздільною здатністю сенсорів, під'єднаних до вузла. До цього додаються певні необхідні елементи протоколу, так як ідентифікація в мережі (прапор) чи контрольна сума (або циклічний надлишковий код), що дозволяє контролювати правильність передавання (не обов'язково пов'язаною із колізією; це може бути пов'язано з зовнішніми втручаннями). У будь якому випадку протокол потрібно максимально обмежувати від непотрібної надлишкової інформації, щоб тривав якнайкоротше [1, 2, 4].

Обмеження протоколу у часі є корисним і через економію енергії, яка витрачається вузлом на радіо-передачу. Це дуже важливо для випадку, коли час життєздатності вузла зумовлений ємністю джерела електроживлення. З іншої сторони, на протокол потрібно дивитись зі сторони переданого радіо-сигналу. Тоді час тривання буде пов'язаний із видом використаної модуляції (кількість значущих станів, які припадають на біт інформації), генерованого спектру сигналу для прийнятого способу модуляції та прийняття параметрів модуляції у

контексті наявного радіо-каналу. Це важливі технічні параметри роботи WSN, які повинні бути усталені для кожного виду рішення цього типу мережі [7, 17].

Критеріїв остаточного встановлення часу тривання комунікаційного протоколу є багато та кожного разу потрібно обирати пріоритетні величини, для яких будуть прийняті остаточні рішення. Аналіз цього типу необхідний для кожного рішення запропонованої мережі WSN, однак немає змоги у цій роботі подати навіть більшість з можливих рішень. Тому нижче на прикладі показано проблему побудови комунікаційного протоколу, а надалі – реалізацію форми сигналу (вибір модуляції, аналіз спектру), який передається вузлом.

Протокол передачі

Беручи до уваги вищенаведені обґрунтування та передумови, пов’язані із запропонованою моделлю випадкового доступу на основі PASTA, та знання про конструкцію протоколів, які використовуються у мережах зв’язку, нижче представлено розроблені автором два протоколи, які можуть бути використані у обговорюваній мережі WSN. Конструкції протоколів представлено на рис. 2.1.

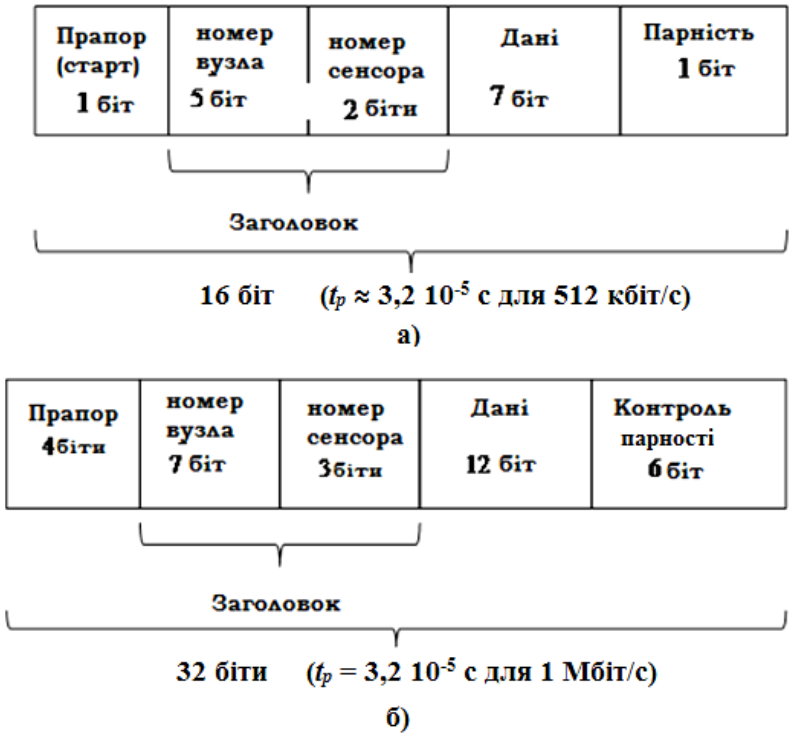


Рис. 2.1. Приклади комунікаційних протоколів в мережі WSN з випадковим доступом (PASTA) з часом тривання t_p = 32 мкс: а) 16-бітний, б) 32-бітний

На рис. 2.1 а показано протокол, який складається із 16 бітів. Протокол містить наступні поля: Старт (1 біт), ідентифікатор вузла (номер вузла) – 5-ти бітне поле, а отже дозволяє реалізувати мережу, що містить 32 вузли, ідентифікатор сенсора у вузлі (номер сенсора) – 2-о бітне поле, отже можемо ідентифікувати 4 сенсори, під'єднані до вузла, 7-ми бітне поле дані, що дає змогу записати 128 рівнів величин стану даного сенсора. Останнє поле – це 16-тий біт парності, який дозволяє контролювати правильність передачі.

На рис. 2.3 б представлено протокол, складений з 32 бітів. Протокол має такі поля: Прапор (4 біти), ідентифікатор вузла (номер вузла) – 7-ми бітне поле, а отже дозволяє реалізувати мережу, що містить 128 вузлів, ідентифікатор сенсора у вузлі (номер сенсора) – 3-бітне поле, завдяки чому можемо ідентифікувати 8 сенсорів, під'єднаних до вузла, 12-бітне поле дані, що дає змогу записати 4096 рівнів величин стану даного сенсора, дозволяючи отримати високу роздільну здатність переданих даних, наприклад, результату вимірювання. Останнє 6-ти бітне поле дозволяє контролювати правильність передачі.

Використовуючи для передачі протоколу 16-ти бітний передавальний пристрій з модуляцією FSK та пропускною бінарною здатністю 512 кбіт/с, отримується, що час передачі t_p протоколу триває близько 32 мкс. Аналогічним чином, використовуючи 32-бітний протокол та надаваючий пристрій зі швидкістю 1 Мбіт/с, отримано тривалість передавання також 32 мкс. У подальшому аналізі, що відноситься до ймовірності колізій, яка становить основну частину цієї роботи, такий власне час t_p прийнято. Звичайно, це не означає у жодному разі, що це є якесь особливе значення часу. Кожне інше значення часу тривання протоколу є теж можливим і при цьому не буде порушена суть питання.

Однак варто пам'ятати, що принципово цей вид випадкового мережевого доступу, який базується на PASTA, вимагає найкоротших в часі протоколів для отримання добрих результатів функціонування мережі WSN.

Спектральні властивості

Теоретичні узагальнення та міркування на тему часу тривання комунікаційного протоколу мають ще один дуже важливий сенс. Очікуючи якнайкоротшого часу передачі для заданої кількості бітів, які накладаються на протокол, слід застосувати пристрої надавання з великою бінарною пропускною здатністю. Однак, чим більша пропускна здатність, тим ширша смуга радіо-каналу передачі. Нижче представлено певне спрощене рішення щодо необхідної смуги для правильної роботи мережі. Таке обґрунтування дозволяє по-суті розв'язати проблему щодо виділення смуги під час використання різних видів модуляції та пристроїв надавання серійного виробництва (рис. 2.2).

Рис. 2.2. Модуль надавача радіо-сигналу у смугах ISM

Для прикладу розглянуто рішення, яке полягає на використанні пристрою надавання, що працює з модуляцією FSK. Тоді сигнал передачі з давача буде мати вигляд, представлений на рис. 2.3, складатись з синусоїдних хвиль з двома різними наближеними частотами f_1 та f_2, які відповідають відповідно f_1 логічному **0** та f_2 логічній **1**. Зміни значущих станів з **1→0** та **0→1** відбуваються з дотриманням неперервності фази синусоїдних хвиль з

частотами f_1 та f_2. Час тривання послідовностей перебігів f_1 та f_2 відповідає довжині протоколу та становить t_p.

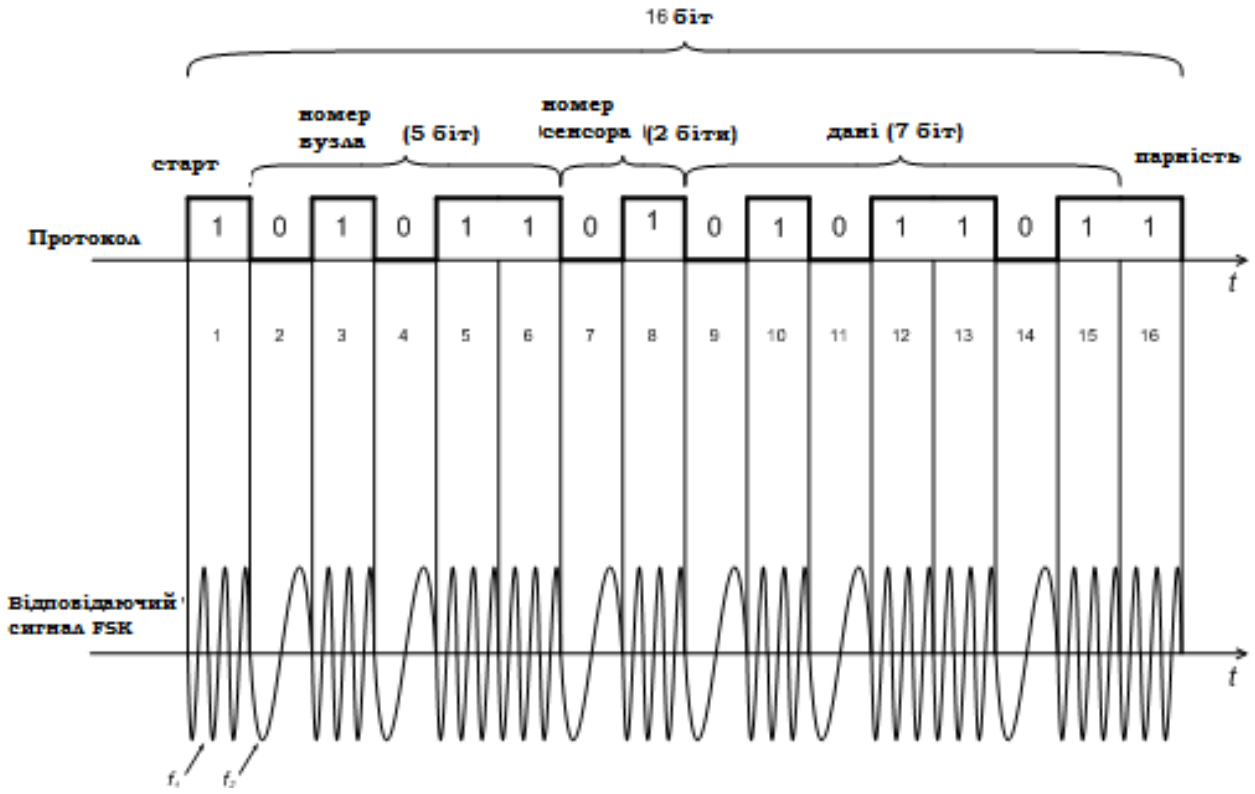


Рис. 2.3. Змодульований сигнал FSK для передачі протоколу WSN

На спектральну ширину сигналу вирішальний вплив має факт завершеного часу тривання синусоїдальних хвиль f_1 та f_2 . Отже встановлення необхідної ширини смуги радіо-каналу вимагає визначення спектру змодульованого сигналу для вибраної модуляції FSK.

Детальне визначення спектру такого сигналу є досить складним. З метою оцінки необхідної смуги радіо-каналу можна використати наступне обґрунтування: припускається, що мінімальна необхідна ширина смуги каналу відповідає ширині головного «листка» функції *Sa(x),* яка становить спектр синусоїдного сигналу зі скінченним часом тривання (t_p) (рис. 2.4). Окрім цього, прийнято (спрощення), що сигналу притаманна частота f_0, яка є середньою з частот f_1 та f_2. Забезпечення неперервності фази між змінами станів в FSK, тобто при переходах з f_1 на f_2 і навпаки, не призведе у цьому випадку до

більшого поширення спектру сигналу, ніж це передбачено скінченним (досить коротким) часом тривання t_p.

Нехай ω_1, ω_2 будуть пульсаціями, які відповідають f_1 та f_2, тобто $\omega_1 = 2\pi f_1$, $\omega_2 = 2\pi f_2$, та нехай

$$\omega_0 = \frac{\omega_1 + \omega_2}{2}. \tag{2.1}$$

Розглядається функція *f(t)*, представлена формулою:

$$f(t) = \begin{cases} \sin \omega_0 t & -\frac{t_p}{2} \le t \le \frac{t_p}{2} \\ 0 & |t| > \frac{t_p}{2} \end{cases} \tag{2.2}$$

Перетворення Фур'є (спектр) F*(ω)*, функції заданої формулою (2.2) є наступним:

$$\mathrm{F}(\omega)=\mathrm{F}(f(t))=$$

$$= -j\frac{t_p}{2}\left\{\frac{\sin[(\omega-\omega_0)\frac{t_p}{2}]}{(\omega-\omega_0)\frac{t_p}{2}} - \frac{\sin[(\omega+\omega_0)\frac{t_p}{2}]}{(\omega+\omega_0)\frac{t_p}{2}}\right\} = \tag{2.3}$$

$$= -j\frac{t_p}{2}\left\{Sa[(\omega-\omega_0)\frac{t_p}{2}] - Sa[(\omega+\omega_0)\frac{t_p}{2}]\right\}$$

де $Sa(x) = \frac{\sin x}{x}$, $\quad (x \in \Re)$

Як закладено вище, ширина смуги В каналу передачі приймається за ширину головного „листка" функції спектральної густини Sa(x).

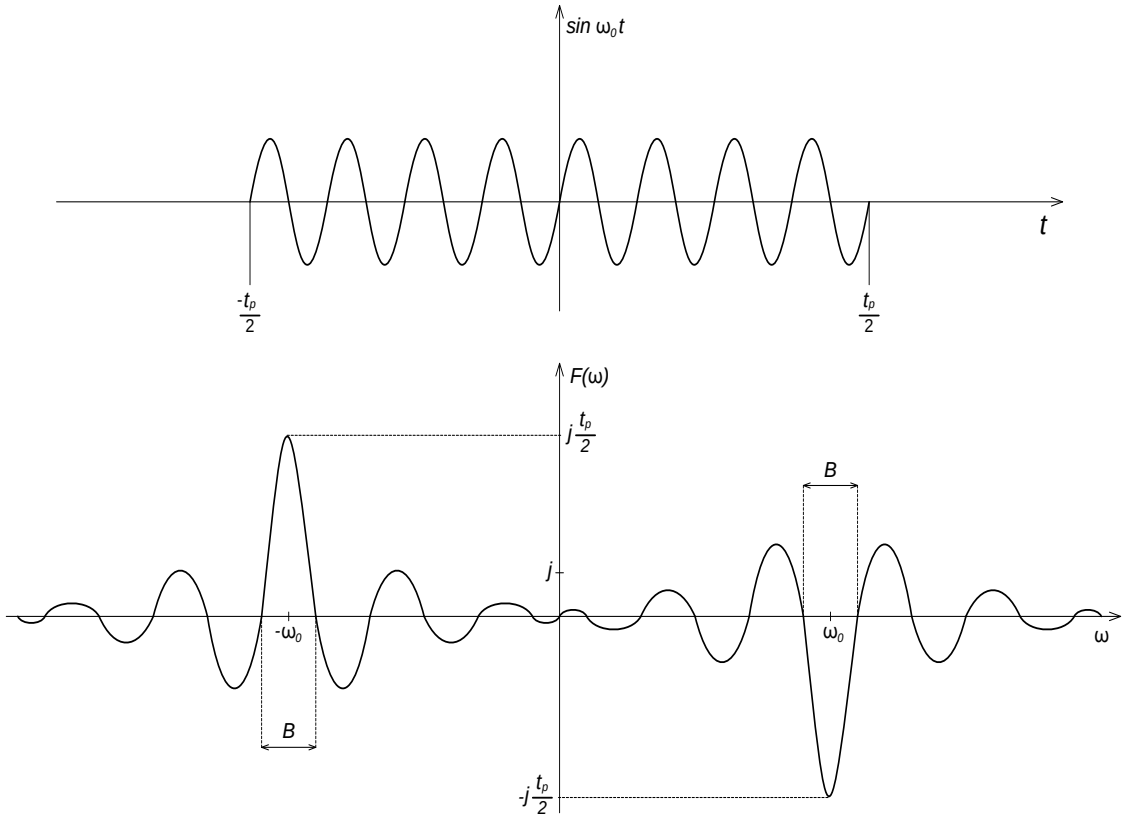


Рис. 2.4. Спектр синусоїдального перебігу з часом тривання t_p

Щоб обчислити довжину відрізка B, як представлено на рис. 2.5, достатньо дослідити функцію $Sa(\frac{t_p}{2}\omega)$, тобто функцію $Sa(b\omega)$, де $b = \frac{t_p}{2}$

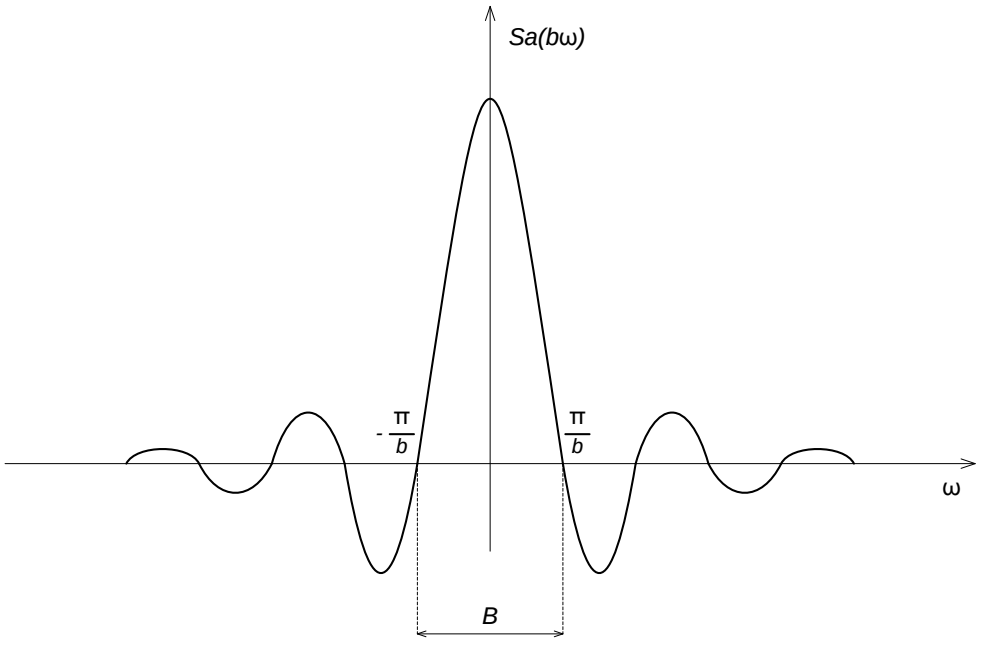


Рис. 2.5. Визначення мінімальної ширини смуги B у спектрі сигналу

Використовуючи властивості функції $Sa(b\omega)$, отримуємо:

$$B = \frac{2\pi}{b} = \frac{2\pi}{\frac{t_p}{2}} = \frac{4\pi}{t_p} \qquad \text{[рад]} \tag{2.4}$$

або еквівалентно

$$B = \frac{2}{t_p} \text{ [Гц]}, \tag{2.5}$$

тому що $\omega_0 = 2\pi f_0$, $T_0 = \frac{1}{f_0}$.

Прийнято, що

$$t_p = kT_0 = \frac{k}{f_0} \text{[s]} \tag{2.6}$$

де $k \in N$ і означає кількість повних періодів синусоїдних несучих хвиль.

На базі (2.5) отримано (2.7) – (2.8)

$$B = \frac{2}{t_p} = \frac{2}{\frac{k}{f_0}} = \frac{2f_0}{k} \text{ [Гц]}, \tag{2.7}$$

$$k = \frac{2f_0}{B} \tag{2.8}$$

Оцінюючи ширину смуги, яка потрібна для реалізації передачі з відповідною пропускною здатністю, а отже визначаючи істотний для дії мережі час t_p на базі моделі PASTA, в подальшому на кількох прикладах проілюстровано відповідні залежності.

Необхідна бінарна пропускна здатність надавача для 16-ти бітних протоколів знаходиться в межах від 400 кбіт/с до 800 кбіт/с, а для 32-ох бітних протоколів вдвічі вища. Необхідна смуга для розглянутої модуляції FSK становить близько 100 кГц. Для таких параметрів сенсори серійного випуску є доступними та дешевими (рис. 2.2), головне у смугах ISM. Звичайно скорочення часу t_p є досить вагоме з точки зору використання методів випадкового доступу у мережах WSN.

Це покращує якість передачі (менша кількість колізій). Тут вибір дуже великий, проте завжди треба взяти до уваги те, що обираючи коротший час тривання протоколу потрібно мати у наявності значно ширшу смугу. Рішення щодо мереж та застосунків WSN є дуже різними і не завжди в змозі мати для використання достатньо широку смугу. Сам факт, що передача у цілій мережі використовує тільки один канал (simplex), а це є основним принципом цієї розробки, дозволяє на роботу мережі WSN у різних, навіть вузьких, смугах з більш дефіцитними частотами, які залишаються ще у розпорядженні користувачів. Використання каналів у смугах ISM є однією з можливостей, яку часто застосовують та яка не є найкращою. Неліцензовані смуги у будь-який спосіб дозволяють безпроблемно реалізовувати мережу (до обмежень, накладених нормами, відносяться лише рівні потужності сенсорів), проте однак робота у цих смугах піддається вагомим зовнішнім завадам, які походять від інших користувачів цих смуг і немає способу уникнути цього типу проблем.

Безумовно кращим рішенням є застосування ліцензійних частот, однак це є складнішим через юридичні процедури та строго визначене використання смуги. Представлені у вищенаведеній таблиці оцінки для різних смуг мають теж практичне значення. Окрім цього, слід пам’ятати, що це оцінювання виконано лише для найпростішого типу модуляції FSK. На даний час появилися на ринку мікронадавачі, які доцільно запропонувати для застосування в мережі WSN та які працюють зі складними типами модуляцій FSK, PSK та ASK, що дає змогу значно (багаторазово) збільшити бінарну пропускну здатність надавача для тієї самої наявної ширини смуги B,

наприклад, визначеної діапазоном ліцензійної частоти. Для кожного випадку, розглядаючи вибір t_p, потрібно мати на увазі відношення між наявною смугою (часто накладеною) та можливою швидкістю передачі (пропускною бінарною здатністю надавача), що, у свою чергу, можна достосувати відповідним добором використаної модуляції.

Кожна з використовуваних мереж WSN працює у відповідних просторових умовах, що обтяжені багатьма зовнішніми факторами, які кожного разу необхідно брати до уваги. Умови поширення радіохвиль та зумовлений ними вибір несучої частоти пов’язані з безпосереднім впливом на конструкцію та габаритні розміри вузлів (йдеться в основному про розміри антен та засобів узгодження), що часто не залишається без значення для побудови відповідної мережі.

Спектральні обмеження

Простір, в якому розходяться електромагнітні хвилі в телетрансляційному сенсі, становить телетрансляційний трек імпедансу 377 Ом (у вакуумі), до якого всі мають доступ. Для забезпечення ефективного способу із врахуванням інтересів різних сторін щодо використання простору для радіотрансляції слід було привести в порядок розпоряджання технічно доступного спектру між багатьма користувачами в загальносвітовому масштабі.

Для радіохвиль кордони країн не мають значення. Отже, виникла міжнародна організація під назвою ITU-R (International Telecommunication Union - Radiocommunication Sector), метою якої є:

– забезпечення раціонального, справедливого, ефективного та економічного використання радіочастотного спектру для служб радіозв'язку,

– прийняття рекомендацій по радіозв'язку.

Рекомендації ITU-R розроблено експертами з адміністрації, операторами, фахівцями з телекомунікаційної промисловості та іншими спеціалістами, які займаються радіокомунікаційними справами зі всього світу. Рекомендації затверджено державами-членами ITU-R. Їх впровадження хоча і не обов'язкове,

однак характеризується великим реноме і приймаються до реалізації у всьому світі.

Таким чином, одним з основних положень даного дослідження було прийняття принципу максимального обмеження смуги частот для функціонування мережі WSN. Прийняття цього принципу тому призвело до розробки симплексної передачі на одній частоті для всієї мережі і засади випадкового доступу вузлів, зокрема на основі PASTA, до базової станції (sink).

2.2. Моделі функціонування WSN з визначенням ймовірності колізій

Нехай A_s' буде подією, яка означатиме відсутність колізії в інтервалі $[0,s]$ $(s>0)$. Приймемо за $P(A_s')$ ймовірність відсутності колізії на проміжку $[0,s]$. Розглянемо інтервал $[0,s]$, де $s > t_p$.

Припустимо, що $N(s)=j$, тобто кількість передач в інтервалі $[0,s]$ дорівнює j $(j \geq 1)$. Випадковий вектор $(U_1,\ldots,U_j)$ часів між передачами є рівномірно розподілений на множині

$$\Omega_t^* = \{(u_1,\ldots,u_j) : u_1 + \ldots + u_j \leq s\} \tag{2.9}$$

з умовною густиною

$$f(u_1,\ldots,u_j \mid N(s)=j) = j!/s^j \tag{2.10}$$

для $(u_1,\ldots,u_j) \in \Omega_t^*$, а також 0 поза тим.

Тоді умовна густина відсутності колізії в інтервалі $[0,s]$, припускаючи $N(s)=j$, дорівнює

$$P(A_s' / N(s)=j) = P(U_1 > t_p,\ldots,U_j > t_p) = \left(1-\frac{jt_p}{s}\right)_+^j ,$$

де вираз x_+ визначається наступним чином: $x_+ = x$ для $x \geq 0$ та $x_+ = 0$ для $x < 0$.

У цей спосіб доведено наступну теорему.

Твердження 2.1. Умовна ймовірність колізії в інтервалі довжини s, де $s > t_p$, за умови $N(s) = j$, задається виразом

$$P(A_s / N(s) = j) = 1 - \left(1 - \frac{jt_p}{s}\right)_+^j . \qquad (2.11)$$

Слід зауважити, що очікувана кількість передач вузлів в інтервалі $[0,T]$ дорівнює n. На підставі (10) з $s = T$ і $j = n$ отримується, що умовна ймовірність відсутності колізії на інтервалі $[0,T]$, припускаючи $N(T) = n$, дорівнює

$$P(A_T' / N(T) = n) = \left(1 - \frac{nt_p}{T}\right)_+^n . \qquad (2.12)$$

Безумовна ймовірність колізії протоколів передачі у визначеному часі

Властивості безумовної ймовірності колізії на інтервалі довжини s, для $s \geq t_p$, досліджено в працях [8-13]. Приступимо до обчислення ймовірності колізії на інтервалі довжиною t_p. Беручи до уваги, що колізія настає на інтервалі довжини t_p, якщо принаймні два вузли розпочнуть передачу (надавання) в цьому інтервалі. На базі формули (2.1) отримано наступний вираз для визначення ймовірності колізії:

$$P(A_{t_p}) = \sum_{j=2}^{\infty} p(j; t_p) = 1 - p(0; t_p) - p(1; t_p) = 1 - e^{-n\frac{t_p}{T}} - n\frac{t_p}{T} e^{-n\frac{t_p}{T}} .$$

Слід зауважити, що кількість передач вузлів, які здійснено в інтервалі $[0, t_p]$, тобто N_{t_p}, має розподіл Пуассона з інтенсивністю $\lambda t_p = n\frac{t_p}{T}$.

Отже

$$EN_{t_p} = n\frac{t_p}{T} = \sum_{j=0}^{\infty} jp(j;t_p) = \sum_{j=1}^{\infty} j\,p(j;t_p).$$

Нехай Y_{t_p} буде кількістю передач, які перебувають в колізії на інтервалі $[0, t_p]$. Тоді маємо

$$P(Y_{t_p} = 0) = p(0; t_p) + p(1; t_p) = e^{-n\frac{t_p}{T}} + e^{-n\frac{t_p}{T}}[n\frac{t_p}{T}],$$

$$P(Y_{t_p} = j) = p(j; t_p) = e^{-n\frac{t_p}{T}}\frac{(n\frac{t_p}{T})^j}{j!}, \qquad j = 2, 3, \ldots.$$

Звідси, отримано:

$$E(Y_{t_p}) = \sum_{k=0}^{\infty} jP(Y_{t_k} = j) = \sum_{k=2}^{\infty} jp(j;t_p) = \sum_{k=1}^{\infty} j\,p(j;t_p) - p(1; t_p) =$$

$$= n\frac{t_p}{T} - e^{-n\frac{t_p}{T}} n\frac{t_p}{T} = (1 - e^{-n\frac{t_p}{T}})n\frac{t_p}{T}.$$

Підсумком вищезгаданих розв'язків є наступне твердження про ймовірність колізії для $s = t_p$.

Твердження 3.2

а) ймовірність колізії в інтервалі довжини t_p подається виразом:

$$P(A_{t_p}) = 1 - e^{n\frac{t_p}{T}} - n\frac{t_p}{T}e^{-n\frac{t_p}{T}}. \qquad (2.13)$$

б) середня кількість передач, які перебувають в колізії на інтервалі довжини t_p, представляється виразом:

$$E(Y_{t_p}) = (1 - e^{n\frac{t_p}{T}}) \cdot n\frac{t_p}{T}, \qquad (2.14)$$

де n – кількість вузлів, T – середній час між передаваннями вузла, t_p – час передавання протоколу.

Наступне твердження подає формулу для ймовірності колізії для $s > t_p$.

Твердження 3.3. Ймовірність колізії в інтервалі довжини s, де $s > t_p$, визначається (2.15):

$$P(A_s) = \sum_{j=2}^{\infty} e^{-n\frac{s}{T}} \frac{(n\frac{s}{T})^j}{j!}[1 - (1 - j\frac{t_p}{s})_+^j], \qquad (2.15)$$

де n – кількість вузлів, T – середній час між передаваннями вузла, t_p – час передавання протоколу.

Розглянемо інтервал $[0, s]$, де $s > t_p$. Припустимо, що $N(s) = j$, кількість передавання протоколів є рівною j $(j \geq 1)$.

З пп.2.1 випливає, що випадковий вектор $(U_1, \ldots, U_j)$ часів між передачами рівномірно розподілений на множині

$$\Omega_t^* = \{(u_1, \ldots, u_j) : u_1, \ldots, u_j \geq 0, u_1 + \ldots + u_j \leq s\}$$

з умовною густиною $f(u_1,\ldots,u_j / N(s)=j) = j!/s^j$, для $(u_1,\ldots,u_j)\in\Omega_s^*$, отже 0 в інших випадках. Тоді умовна ймовірність браку колізії в інтервалі $[0,s]$, приаускаючи, що $N(s)=j$, описується виразом

$$P(A_s'/N(s)=j) = P(U_1 > t_p,...U_j > t_p) = (1-j\frac{t_p}{s})_+^j .$$

Звідси

$$P(A_s / N(s)=j) = 1-(1-j\frac{t_p}{s})_+^j \qquad j=2,3,\ldots \tag{2.16}$$

враховуючи, що $P(A_s / N(s)=0) = P(A_s / N(s)=1) = 0$.

Беручи до уваги, що на підставі формули (2.1) маємо рівняння

$$P(N(s)=j) = p(j,s) = e^{-n\frac{s}{T}}\frac{(n\frac{s}{T})^j}{j!}, \qquad j=0,1,2,\ldots, \tag{2.17}$$

то з виразу повної ймовірності отримано

$$P(A_s) = \sum_{j=0}^{\infty} P(N(s)=j)\cdot P(A_s / N(s)=j) .$$

Аналізуючи (2.16) і (2.17) та застосовуючи відповідні перетворення, отримуємо (2.15). Цим самим закінчується доведення останнього твердження.

Використовуючи відому формулу Баєса:

$$P(A/B) = P(B/A) \cdot P(A/P(B),$$

$$\text{z} \quad A := \{N(s) = j\} \text{ i } B := A_s,$$

отримаємо наступне твердження.

Твердження 3.4. Умовна ймовірність j передавання вузлів в часі $s > t_p$, при припущенні, що настала колізія, задається виразом

$$P(N(s) = j / A_s) = e^{-n\frac{s}{T}} \frac{(n\frac{s}{T})^j}{j!}[1-(1-j\frac{t_p}{s})_+^j] / P(A_s).$$

Зазначені твердження графічно відображені на рис. 2.6 – 2.10.

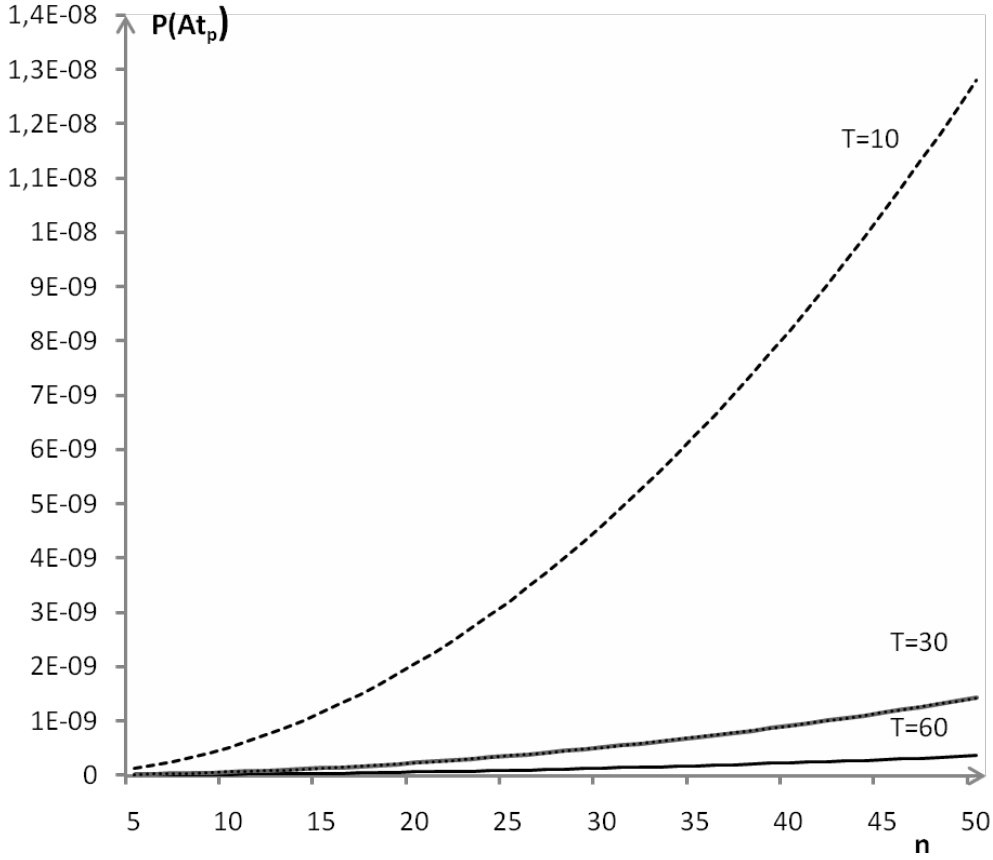


Рис. 2.6. Ймовірність колізії в інтервалі t_p в залежності від кількості вузлів для $T = 10$ с, 30 с, 60 с

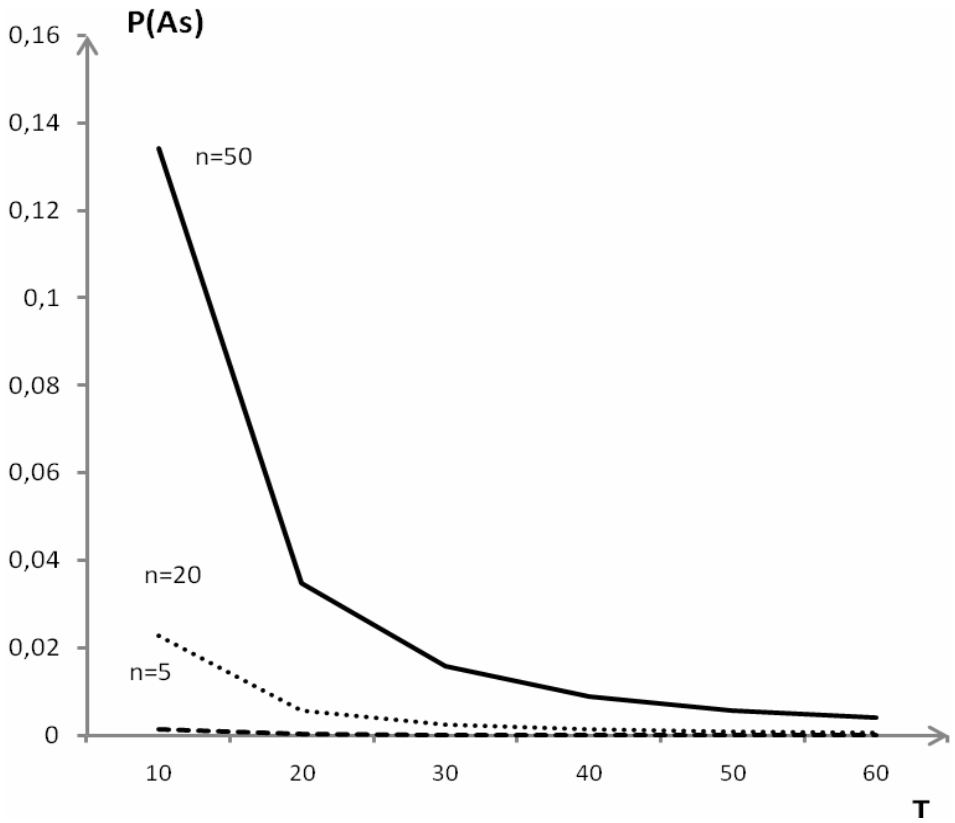


Рис. 2.7. Ймовірність колізії в інтервалі s, де $s > t_p$, в залежності від середнього часу між передаваннями вузла, для $n = 5, 20, 50$ та часу спостереж. $s = 180$ с

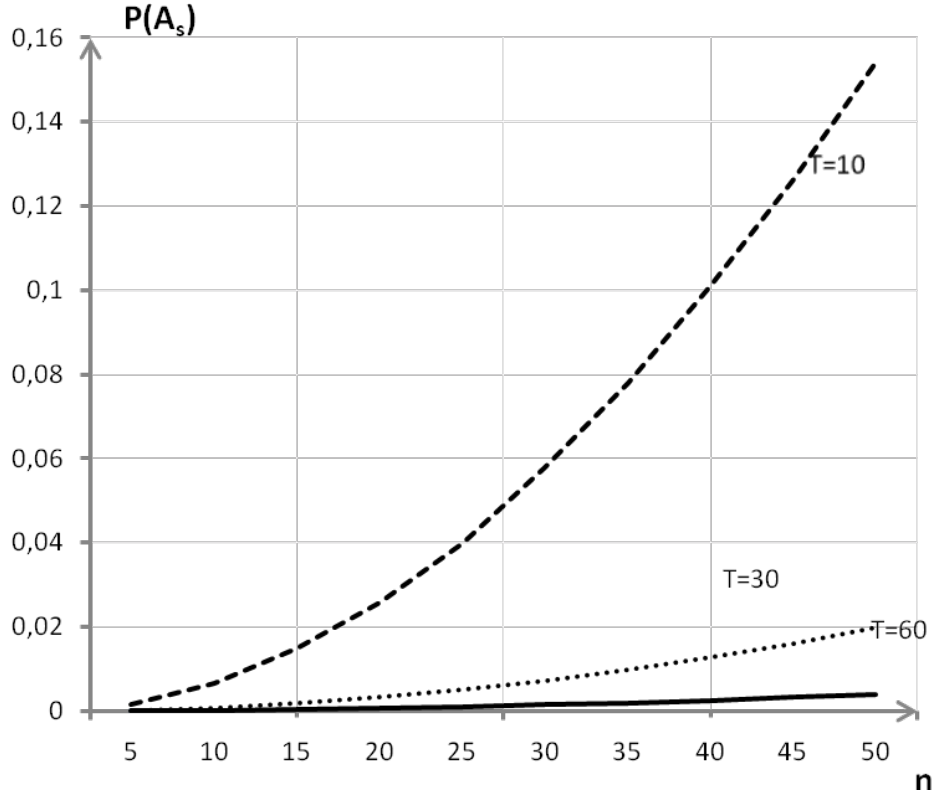


Рис. 2.8. Ймовірність колізії в інтервалі s, де $s > t_p$, в залежності від кількості вузлів, де $T = 10$ с, 30 с, 60 с та часу спостереження $s = 180$ с

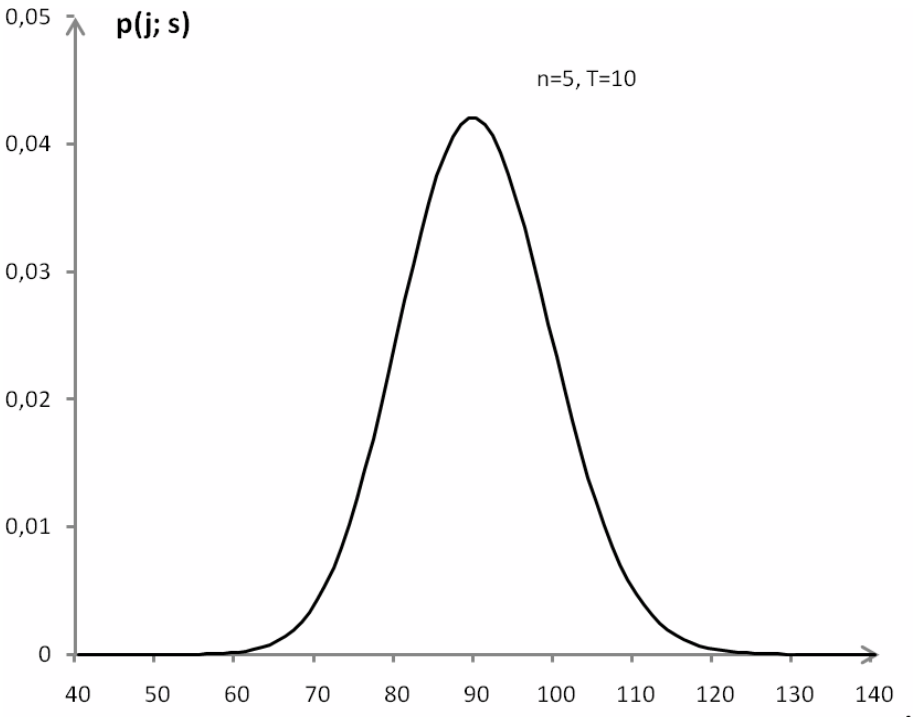


Рис. 2.9. Ймовірність j передавання в інтервалі довжини s, де $s > t_p$, для $n = 5, T = 10$ с та часу спостереження $s = 180$ с

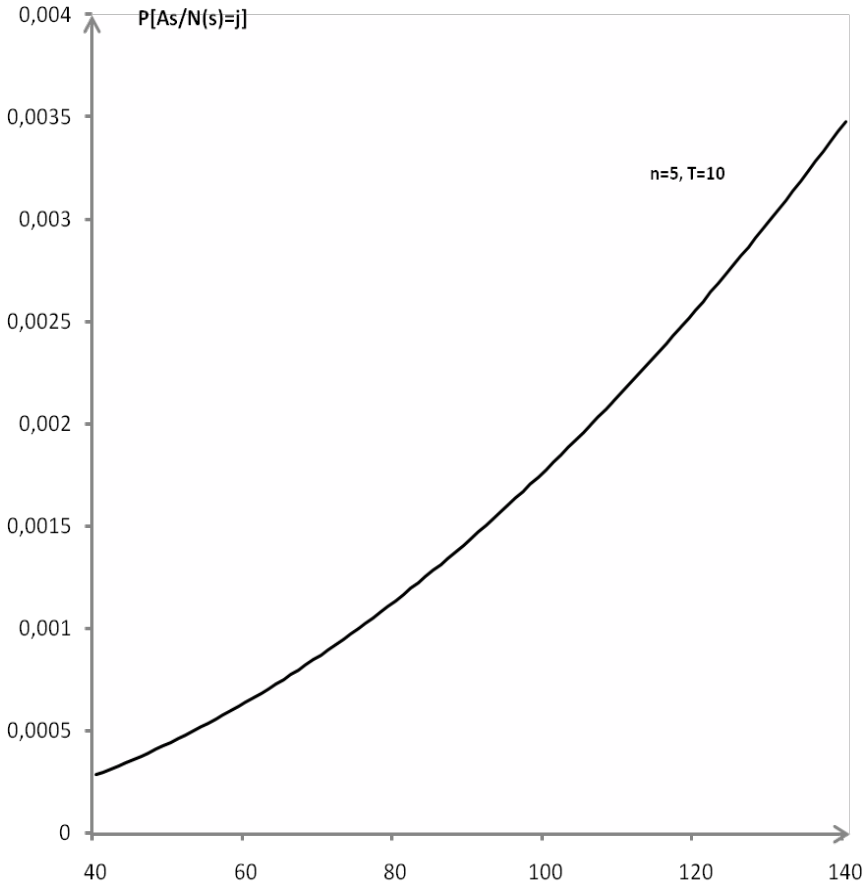


Рис. 2.10. Умовна ймовірність колізії, за умови, що кількість передач дорівнює j, для $n = 5, T = 10$ с та часу спостереження $s = 180$ с

Таким чином, у цій частині дисертації подано дві залежності для ймовірності колізії:

1. Перший вираз описує ймовірність колізії в короткому часі тривання t_p надавання протоколу, визначаючи ймовірність непорушеного надання протоколу (рис. 9).

2. Другий вираз виведено, використовуючи інші власності процесу Пуассона щодо ймовірності колізії в досить довгому часі тривання передачі.

На графіках проілюстровано ймовірність колізії в залежності від кількості вузлів (сенсорів-надавачів) для встановленого середнього часу між передаваннями повідомлень, а також представлено залежність від середнього часу передачі протоколу, якщо усталено кількість вузлів.

Для середнього часу між передачами вузла, що дорівнює 10 с, максимальна кількість вузлів, яка гарантує якість передачі на рівні ймовірності не більше 10^{-2}, становить 10, а для середнього часу між передачами вузла, що дорівнює 30 с, максимальна кількість вузлів дорівнює 50. Подальше зростання середнього часу між передачами вузла дає змогу збільшити максимальну кількість вузлів. Для заданої кількості вузлів збільшення середнього часу між колізіями зумовлює зменшення ймовірності колізії.

Користуючись наведеними графіками (рис. 2.6 – 2.10), можна знайти оптимальні значення параметрів, які впливають на правильність передачі (n, T, t_p). Графіки дають змогу встановити, в якому діапазоні забезпечується якість передавання на заданому рівні, або для яких величин (n, T, t_p) ймовірність колізії різко зростає. Можна визначити порядок значень ймовірності колізії для довільно обраних параметрів: наприклад, для $t_p = 3{,}2 \times 10^{-5}$, кількості сенсорів-надавачів, яка дорівнює 10, і надавання кожним сенсором із середнім часом передачі кожні $T = 60$ с ймовірність колізії становить $1{,}65 \times 10^{-4}$. Отримання таких несподівано добрих умов роботи мережі для досить великої кількості вузлів можливе, якщо відносний час тривання протоколу t_p є на декілька порядків коротший, ніж середній час між передачами. Це класифікує

пропоновану мережу до певного класу застосувань, для якої прийнятними є вище зазначені параметри передачі.

З іншого боку, у свою чергу можна зауважити, що прийняті такі припущення як однонапрямлена передача (Simplex), максимально короткий протокол передачі – бо не вимагає жодної синхронізації, ані додаткового подовження фрейма протоколу додатковими бітами, пов'язаними з процедурами доступу, синхронізації, керування рухом і т.д. дає таку вигідну ситуацію, що протокол передачі може бути короткий. Це є також надзвичайно вигідним з точки зору економії енергії батарей живлення вузлів (максимальна енергоощадність батарей живлення). Очевидно, це можливо тільки там, де кількість інформації, яка передається поодинокими сенсорами, приєднаними до вузлів, є мала. У проведеному аналізі в цій роботі прийнято час тривання протоколу $t_p = 3{,}2 \times 10^{-5}$с

На підставі виведених в роботі залежностей можна, для кожних вимог конфігурованої мережі цього типу *(n, T, t_p)*, визначити умови її правильної роботи (ймовірність колізії). Такий несподівано добрий результат якості передавання в запропонованому мережевому рішенні можливий тільки для випадкових часів передавання. Є тут певна схожість до випадкового керування доступом методом CSMA в комп'ютерній мережі Ethernet.

2.3. Дослідження виникнення колізій на визначеному інтервалі часу і кількості вузлів, які перебувають у колізії

Проведено дослідження ймовірності появи колізії в інтервалі часу *s*, якщо $s < t_p$ та ймовірність спотворення сигналу, що надається .

Розглянемо $0 < s < t_p$. Нехай $p(j;s)$ для $j = 0,1,2,\ldots$ буде ймовірністю, для якої кількість передач в інтервалі $[0,s]$ дорівнює j. З формули (1) для $j = 0,1,2,\ldots$ отримується,

$$p(j;s) = e^{-\lambda s}\frac{[\lambda s]^j}{j!} = e^{-n\frac{s}{T}}[n\frac{s}{T}]^j \;/\; j!, \qquad (2.18)$$

В особливих випадках, $p(j;s)$ для $j = 0,1,2,\ldots$ можна вважати ймовірністю j колізії в інтервалі $[0,s]$, і в результаті, на базі стаціонарного процесу Пуассона, у кожному інтервалі $[t, t+s]$ для $t > 0$.

Приступимо до обчислення ймовірності колізії на інтервалі довжини s.

Твердження 3.4

а) ймовірність колізії в інтервалі довжиною s, де $0 < s < t_p$, визначається формулою

$$P(A_s) = 1 - e^{n\frac{s}{T}} - n\frac{s}{T}e^{-n\frac{s}{T}}. \qquad (2.19)$$

б) середня кількість вузлів у колізії в інтервалі довжиною s, де $0 < s < t_p$ описується виразом

$$E(Y_s) = (1 - e^{n\frac{s}{T}}) \cdot n\frac{s}{T}, \qquad (2.20)$$

де n – це кількість вузлів, T – середній час між передачами вузла, t_p – час тривання передачі протоколу.

Беручи до уваги, що колізія відбувається у інтервалі довжиною s, для $0 < s < t_p$, коли принаймні два вузли почнуть передачу (надавання) у цьому інтервалі, на базі (3.2) одержано:

$$P(A_s) = \sum_{j=2}^{\infty} p(j;s) = 1 - p(0;s) - p(1;s) =$$

$$1 - e^{-n\frac{s}{T}} - n\frac{s}{T}e^{-n\frac{s}{T}}. \qquad (2.21)$$

Слід зауважити, що кількість передач в інтервалі $[0,s]$, тобто N_s, має розподіл Пуассона з інтенсивністю $\lambda s = n\frac{s}{T}$.

Отримуємо

$$EN_s = n\frac{s}{T} = \sum_{j=0}^{\infty} jp(j;s) = \sum_{j=1}^{\infty} jp(j;s). \tag{2.22}$$

Нехай Y_s означає кількість вузлів, які перебувають у колізії на інтервалі $[0,s]$. Тоді маємо

$$P(Y_s = 0) = p(0;\ s) + p(1;\ s) = e^{-n\frac{s}{T}} + e^{-n\frac{s}{T}}[n\frac{s}{T}],$$

$$P(_s = j) = p(j;\ s) = e^{-n\frac{s}{T}}\frac{(n\frac{s}{T})^j}{j!}, \quad j = 2,3,.... \tag{2.23}$$

Звідси, ґрунтуючись на (2.12), одержуємо:

$$E(Y_s) = \sum_{j=0}^{\infty} jP(Y_s = j) = \sum_{j=2}^{\infty} jp(j;s) = \sum_{j=1}^{\infty} j\,p(j;s) - p(1;\ s) =$$

$$= n\frac{s}{T} - e^{-n\frac{s}{T}} n\frac{s}{T} = (1 - e^{-n\frac{s}{T}})n\frac{s}{T}. \tag{2.24}$$

На рис. 2.11-2-13 представлено результати обчислень ймовірності колізії відповідно для інтервалу часу спостерігання *s* (часового вікна аналізу ймовірності), що відповідно дорівнює $s = t_p$, $s = \frac{1}{2}t_p$, $s = \frac{1}{4}t_p$.

Ці обчислення виконані для $t_p = 3{,}2 \cdot 10^{-5}$ с.

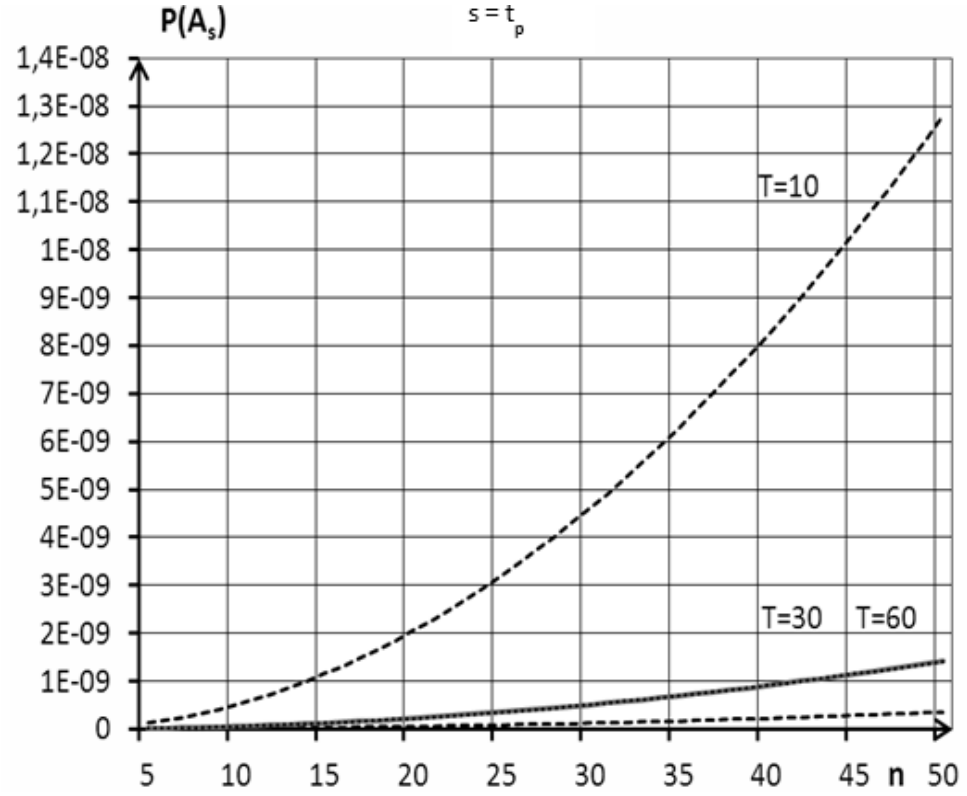


Рис. 2.11. Ймовірність колізії в інтервалі довжиною $s = t_p$ в залежності від кількості вузлів n для T= 10 с, 30 с, 60 с

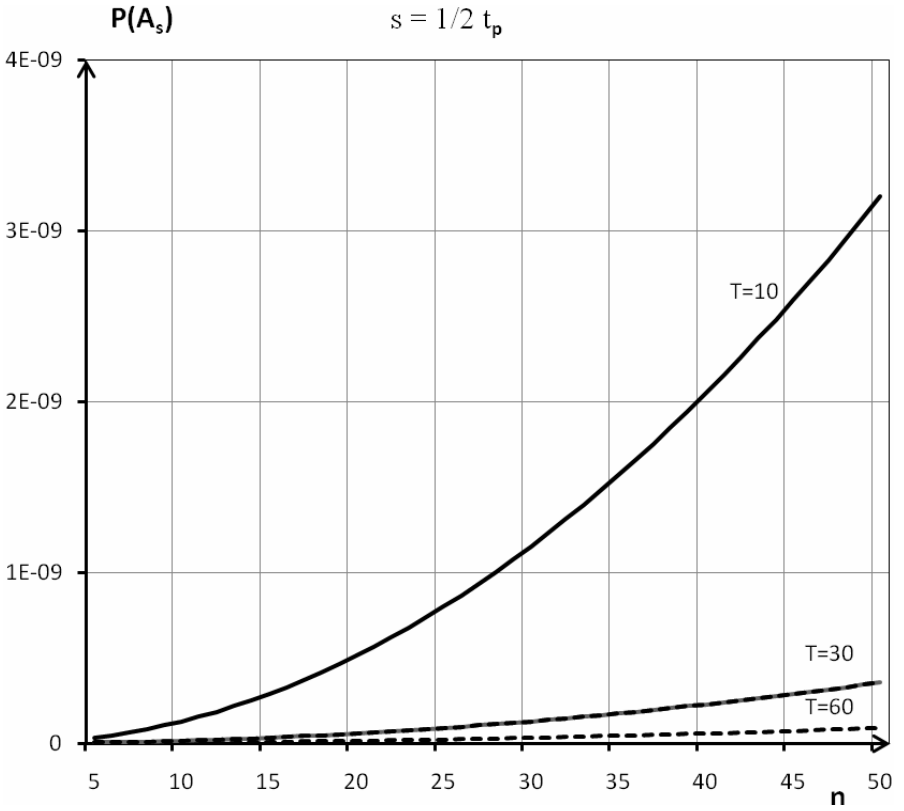


Рис. 2.12. Ймовірність колізії в інтервалі довжиною $s = \frac{1}{2} t_p$ в залежності від кількості вузлів n для T= 10 с, 30 с, 60 с

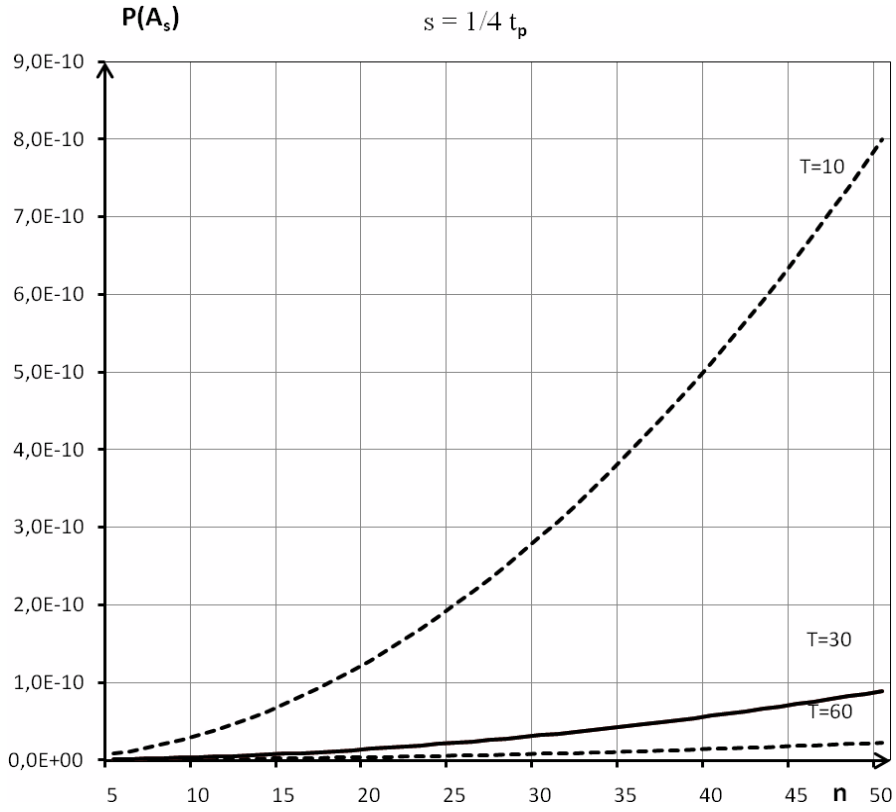


Рис. 2.13. Ймовірність колізії в інтервалі довжиною $s = \frac{1}{4} t_p$ в залежності від кількості вузлів n для T= 10 с, 30 с, 60 с

Цей аналіз представляє ймовірність колізії, тобто такої події, під час якої у вікні спостереження за часом аналізу з'являється протокол передачі з будь-якого вузла мережі та власне у цьому інтервалі спостереження розпочинається передача з іншого вузла чи вузлів.

Такі обчислення дозволяють виконати точне оцінювання якості передачі для випадкового, базованого на апараті PASTA способу керування мережевим доступом. Ці залежності наведено від функції кількості активних вузлів в WSN для трьох різних середніх часів між передачами, *T*, відповідно для *T* = 10 с, 30 с, 60 с. Для цих прийнятих параметрів часу роботи WSN вбачається, що ймовірність колізії є достатньо малою, що у наслідку становитиме добрий результат роботи мережі. Звичайно при тому, як час спостереження зменшується (часове вікно аналізу ймовірності зменшується), то також

зменшується ймовірність колізії. Це підтверджує очікування, пов'язане з роботою мережі.

У роботах [9-11] проаналізовано питання кількості вузлів, які перебувають у колізії в інтервалі довжини s, для випадку $s > t_p$. У цих роботах досліджено ймовірність колізії в інтервалі довжиною s для $s > t_p$.

Досліджено ймовірність колізії в інтервалі довжиною s для випадку $s > t_p$. У нижченаведеному твердженні подано нижні та верхні оцінки умовної ймовірності кількості передач, які залишаються у колізії, в інтервалі довжиною s, припускаючи, що кількість передач в інтервалі передачі в інтервалі довжиною s $(s > t_p)$ дорівнює j. Нехай Y_s буде кількістю передач, які залишаються у колізії в інтервалі довжиною s.

Твердження 2.6. Нехай $s > t_p$. Тоді

$$(j\frac{t_p}{s})^{\kappa-1}(1-j\frac{t_p}{s})^{j-\kappa} \le P(Y_s = \kappa / N(s) = j) \le$$

$$\le (j\frac{t_p}{s})^{\left[\frac{\kappa+1}{2}\right]}(1-\frac{t_p}{s})^{j-\left[\frac{\kappa+1}{2}\right]}. \qquad (2.25)$$

Нехай $2 \le i_2, i_3, ..., i_j \le j$ будуть такі, що $U_{i_2} \le U_{i_3} \le ... \le U_{i_j}$. Приймаючи $Y_s = \kappa$, тоді існує натуральне число k таке, що $\left[\frac{\kappa+1}{2}\right] \le k \le \kappa - 1$ та $U_{i_{k+1}} < t_p \le U_{i_{k+2}}$. Звідси отримується, що

$$P(U_2 < t_p, U_3 < t_p, ..., U_\kappa < t_p, U_{\kappa+1} \ge t_p, ..., U_j \ge t_p) \le P(Y_s = \kappa / N(s) = j) \le$$

$$\le P(U_2 < t_p, ..., U_{\left[\frac{\kappa+1}{2}\right]+1} < t_p, U_{\left[\frac{\kappa+1}{2}\right]+2} \ge t_p, ..., U_j \ge t_p), \qquad (2.26)$$

що й припускає оцінювання, подане у твердженні.

У наступному твердженні наведено нижні та верхні оцінки безумовної ймовірності кількості передач, які перебувають у колізії в інтервалі довжиною s.

Твердження 2.7. Нехай $s > t_p$. Тоді

$$\sum_{j=2}^{\infty} e^{-n\frac{s}{T}} \cdot \frac{\left(n\frac{s}{T}\right)^j}{j!} \left(j\frac{t_p}{s}\right)^{\kappa-1} \left(1-j\frac{t_p}{s}\right)_+^{j-\kappa} \le P(Y_s=\kappa) \le$$

$$\le \sum_{j=2}^{\infty} e^{-n\frac{s}{T}} \cdot \frac{\left(n\frac{s}{T}\right)^j}{j!} \left(j\frac{t_p}{s}\right)^{\left[\frac{\kappa+1}{2}\right]} \left(1-\frac{t_p}{s}\right)_+^{j-\left[\frac{\kappa+1}{2}\right]}. \qquad (2.27)$$

Далі визначено нижні та верхні оцінки очікуваної кількості передач, які перебувають у колізії, та дисперсії кількості передач, які перебувають у колізії в інтервалі довжиною s [14].

Твердження 2.8. Нехай $s > t_p$. Тоді

$$\sum_{\kappa=2}^{\infty}\kappa\sum_{j=2}^{\infty} e^{-n\frac{s}{T}} \cdot \frac{\left(n\frac{s}{T}\right)^j}{j!} \left(j\frac{t_p}{s}\right)^{\kappa-1} \left(1-j\frac{t_p}{s}\right)_+^{j-\kappa} \le EY_s \le \sum_{\kappa=2}^{\infty}\kappa\sum_{j=2}^{\infty} e^{-n\frac{s}{T}} \cdot \frac{\left(n\frac{s}{T}\right)^j}{j!} \left(j\frac{t_p}{s}\right)^{\left[\frac{\kappa+1}{2}\right]} \left(1-j\frac{t_p}{s}\right)_+^{j-\left[\frac{\kappa+1}{2}\right]},$$

(2.28)

$$\sum_{\kappa=2}^{\infty}\kappa^2\sum_{j=2}^{\infty} e^{-n\frac{s}{T}} \cdot \frac{\left(n\frac{s}{T}\right)^j}{j!} \left(j\frac{t_p}{s}\right)^{\kappa-1} \left(1-j\frac{t_p}{s}\right)_+^{j-\kappa} +$$

$$+ - \left[\sum_{\kappa=2}^{\infty}\kappa\sum_{j=2}^{\infty} e^{-n\frac{s}{T}} \cdot \frac{\left(n\frac{s}{T}\right)^j}{j!} \left(j\frac{t_p}{s}\right)^{\left[\frac{\kappa+1}{2}\right]} \left(1-j\frac{t_p}{s}\right)_+^{j-\left[\frac{\kappa+1}{2}\right]}\right]^2 \le \quad D^2(Y_s) \le$$

$$\leq \sum_{\kappa=2}^{\infty} \kappa^2 \sum_{j=2}^{\infty} e^{-n\frac{s}{T}} \cdot \frac{\left(n\frac{s}{T}\right)^j}{j!} \left(j\frac{t_p}{s}\right)^{\left[\frac{\kappa+1}{2}\right]} \left(1 - j\frac{t_p}{s}\right)_+^{j-\left[\frac{\kappa+1}{2}\right]} + \left[\sum_{\kappa=2}^{\infty} \kappa \sum_{j=2}^{\infty} e^{-n\frac{s}{T}} \cdot \frac{\left(n\frac{s}{T}\right)^j}{j!} \left(j\frac{t_p}{s}\right)^{\kappa-1} \left(1 - j\frac{t_p}{s}\right)_+^{j-\kappa}\right]^2 \cdot (2.29)$$

Як приклад розглянемо обчислення оцінок математичного сподівання (нижньої та верхньої) для певної WSN з випадковим доступом, у якій середній час між передачами становить $T = 10\ c$, кількість вузлів становить $n = 5$ та час спостереження становить s =180 с.

$$EN_s = ns/T = 5 \text{ x } 180/10 = 90,$$

$$3{,}1985376 \cdot 10^{-5} \leq EY_s \leq 3{,}1986410 \cdot 10^{-5},$$

де EN_s – середня кількість передач в діапазоні від s = 180 с.

Отримуємо

$$3{,}5539307 \cdot 10^{-7} \leq EY_s / EN_s \leq 3{,}5540456 \cdot 10^{-7}.$$

Під час застосування розроблених моделей, можна скоротити час t_p в 16…300 разів, залежно від передбачуваної смуги частот і виду модуляції. Приймаючи в середньому скорочення часу t_p до $32 \cdot 10^{-8}$, отримуємо $EY_s \approx 1{,}56 \cdot 10^{-7}$, а відповідно коефіцієнт бітових помилок BER $EY_s / EN \approx 1{,}73 \cdot 10^{-9}$. Це означає істотне, приблизно на два порядки, покращення якості передачі в WSN [15].

Таким чином, середня кількість вузлів, що залишаються в колізії (в середньому $3{,}198 \cdot 10^{-5}$) дуже мала в порівнянні з кількістю передач (90) . Відношення середньої кількості вузлів в колізії до кількості передач дорівнює приблизно $3{,}554 \cdot 10^{-7}$, що забезпечує безпечне передавання інформації. З

обчислень бачимо, що буде близько 3,1986 колізій на 10^5 інтервалів довжиною *s*, у яких проведено дослідження. Можна зробити також висновок, що у цих умовах WSN буде працювати ефективно.

Для цих самих параметрів мережі обчислено оцінки нижнього та верхнього значення дисперсії [16]

$$6{,}39705 \cdot 10^{-5} \le \; D^2(Y_s) \le 6{,}39746 \cdot 10^{-5}.$$

Не важко помітити, що як для випадку оцінювання математичного сподівання, так і дисперсії, різниця між нижньою та верхньою оцінками є невеликою, відрізняються вони лише на п'ятому місці значущих цифр. Отже, можна ствердити, що похибка оцінювання у поданих прикладах є невеликою (порядку 10^{-9}) [14-16].

Визначаючи з дисперсії стандартне відхилення $D(Y_s)$ як

$$D(Y_s) = \sqrt{D^2(Y_s)} \tag{2.30}$$

а в подальшому обчислюючи коефіцієнт варіації як

$$DMR(Y_s) = \frac{D(Y_s)}{EY_s} \tag{2.31}$$

(dyspersion–to-mean ratio), отримуємо відповідно

$$\frac{D_L}{E_U} \le \frac{D(Y_s)}{EY_s} \le \frac{D_U}{E_L}, \tag{2.32}$$

де D_L – нижня оцінка стандартного відхилення, D_U – верхня оцінка стандартного відхилення, E_L – нижня оцінка математичного сподівання, E_U – верхня оцінка математичного сподівання.

Есі вищенаведені нижні та верхні оцінки, математичні сподівання та дисперсії подано у твердженнях 2.7 та 2.8.

Для поданого прикладу отримано такі значення оцінки $DMR(Y_s)$:

$$1{,}99993 \le DMR(Y_s) \le 2{,}00012.$$

Коефіцієнт варіації знаходиться в межах 2, тобто стандартне відхилення наявних радіо-колізій є дуже малим, приблизно в 2 рази більше від математичного сподівання, яке є дуже малим (близько $3{,}198 \cdot 10^{-5}$). Цей результат повністю підтверджує принципи випадкового алгоритму управління WSN.

Список літератури до другого розділу

1. Baccelli, F., The Role of PASTA In Network Measurement [Text] / F. Baccelli, S. Machiraju, D. Veitch, J. Bolot, *Computer Communication Review, Proceedings of ACM Sigcomm,* 2006, Vol. 36, № 4, P. 231-242.

2. Adrian Perrig, John Stankovic, David Wagner, “Security in Wireles Sensor Networks” *Communications of the ACM,* p. 53-57, 2004.

3. S. Rajba, T. Rajba, The Performance of a Digital FSK System with Actual Discriminator,Time Distortions Effects, *Applicationes Mathematica* – 1990 Vol. 20 (2), p. 261-279.

4. J. Pilarski, S. Rajba, Measurement of light gradient in plant organs with a fiber optic microbe, *Acta Physiologiae Plantarum*, 2004, Vol. 26, No 4, p. 405-410. – ISSN 0137-5881.

5. M. Karpiński, S. Rajba, T. Rajba, Measurement and information system used the mobile phone GSM and Bluetooth, *PAK*, 2007, 53 (12), p.79-81.

6. J. Szczepanik, S. Rajba, I. P. Kurytnik, Temperature measurement using GSM network, *Acta Mechanica Slovaca*, 2008, R.12, No 3, p. 247-252.

7. G. Hoblos, M. Staroswiecki, A. Aitouche, Optimal design of fault tolerant sensor networks, *Control Applications: IEEE International Conference*, Anchorage, AK, September 2000, p. 467-472.

8. Hu Z., Gizun A., Gnatyuk V., Kotelianets V., Zhyrova T., «Method for rules set forming of cyber incidents extrapolation in network-centric monitoring», *Proceedings of 2017 4th International Scientific-Practical Conference Problems of Infocommunications Science and Technology (PIC S&T 2017),* pp. 121-132, 2017 DOI: 10.1109/INFO COMMST.2017.8246435 *(Scopus).*

9. V. Gnatyuk, N. Dyka, V. Kotelianets, S. Dakov, «IoT architecture for air pollution monitoring system», *Proceedings of VII Międzynarodowa Konferencja Studentów oraz Doktorantów «Inżynier XXI wieku»,* Bielsko-Biala, pp. 83-97, 2017.

10. Смірнов О.А., Котелянець В.В., «Стійкі до колізій стохастичні моделі функціонування бездротових сенсорних мереж», *Вісник інженерної академії України*, №3, с. 145-152, 2018.

11. Котелянець В.В., Усик П.С., Кищенко В.В., Гнатюк В.О., «Інтелектуалізована система моніторингу параметрів навколишнього середовища на базі технології інтернету речей», *Вісник інженерної академії України,* №4, с. 133-140, 2018.

12. Одарченко Р.С., Ткаліч О.П., Дика Н.В., Котелянець В.В. «Дослідження можливостей комунікаційних протоколів для потреб IoT», *Проблеми інформатизації та управління*, Том 3, № 59, с. 43-55, 2017.

13. Гнатюк В.О., Терентьєва І.Є., Котелянець В.В., «Модель даних для удосконалення кібербезпеки IP-АТС», *Безпека інформації,* Том 24, № 3, с. 175-180, 2018.

14. G. Hoblos, M. Staroswiecki, A. Aitouche, Optimal design of fault tolerant sensor networks, *Control Applications: IEEE International Conference*, Anchorage, AK, September 2000, p. 467-472.

15. I. F. Akyildiz, W. Su, Y., Sankarasubramaniam, E. Cayirci Wireless sensor networks: a survey [Text], *Computer networks*, 2002, V. 38, № 4, p. 393-422.

16. J. M. Kahn, R. H. Katz, K. S. J. Pister, Next century challenges: mobile networking for smart dust, *Proceedings of the ACM MobiCom'99*, Washington, USA, 1999, p. 271-278.

17. Gnatyuk S., Sydorenko V., Polishchuk Yu., Kotelianets V., «Analisys of modern aaproaches to security assessment of information resources for critical information infrastructure of the state», *Scientific and Practical Cyber Security Journal*, Vol. 2, №4, p. 81-86, 2018.

РОЗДІЛ 3. УДОСКОНАЛЕНИЙ МЕТОД МОНІТОРИНГУ ПАРАМЕТРІВ НАВКОЛИШНЬОГО СЕРЕДОВИЩА

3.1. Методологічні засади удосконаленого методу моніторингу параметрів навколишнього середовища на базі Інтернету речей

Методологічні засади удосконаленого методу, схема реалізації якого представлена на рис. 3.1, спрямовані на функціонування в умовах кризових ситуацій і охоплюють чотири базових режими [4-6]:

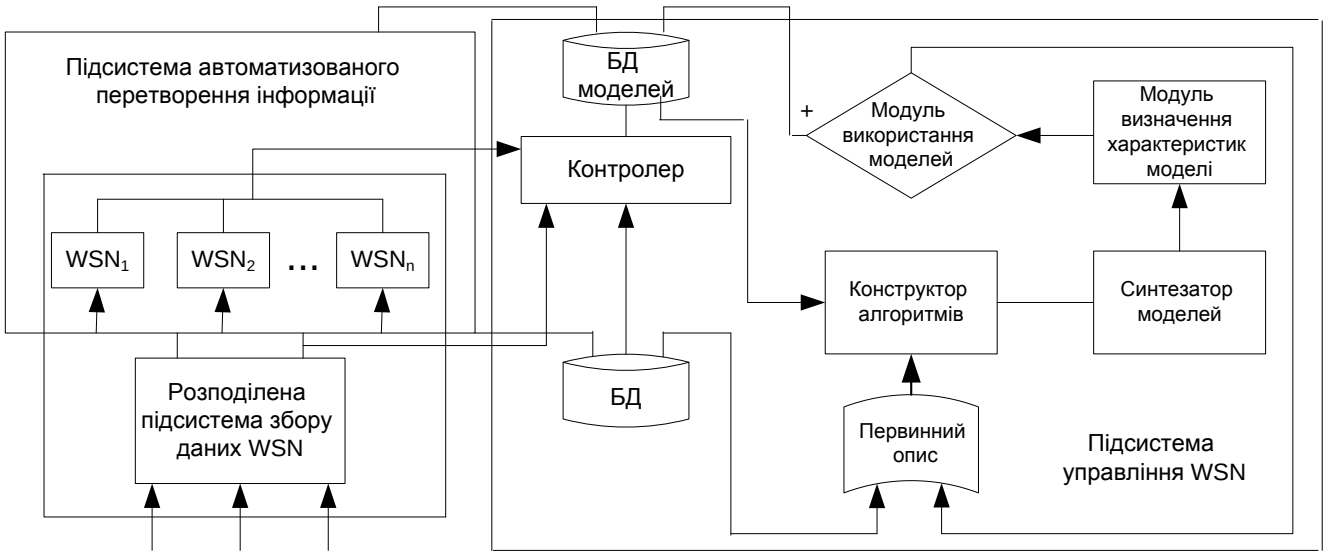


Рис. 3.1. Схема реалізації удосконаленого методу моніторингу

1. Звичайний (стандартне функціонування, штатний режим роботи)

Завдання звичайного режиму функціонування складаються з протиаварійного випереджуючого планування, основною метою якого є збирання інформації для прогнозування можливого виникнення і розвитку кризового режиму і контролю її наслідків, визначення ресурсів телекомунікаційних мереж і засобів, необхідних для ліквідації КС, розробка спеціальних прогнозів, що дозволяють ефективно реагувати на очікування проблеми, обліку всіх сил і засобів для реалізації цільових завдань. У даному режимі визначаються і створюються нормативні, законодавчі й інші механізми, спрямовані на мінімізацію ризику і збитку від КС [2, 5].

2. Підвищеної готовності (нестандартне функціонування, активна підготовка та практична імплементація низки превентивних / попереджувальних заходів);

Система моніторингу у режимі підвищеної готовності повинна базуватись на застосовуванні методів, що виявляють можливість виникнення та розвитку КС і дозволяють швидко реагувати на всі зміни. Для цього слід накопичувати і використовувати в СМ дані про стан елементів внутрішньої і зовнішньої структури, дані для поточного і ретроспективного аналізу з можливістю превентивного планування тенденцій розвитку поточної ситуації, а також планування ресурсів, сил та засобів, необхідних для її нейтралізації, стабілізації і зниження важкості наслідків розвитку КС. Відсутність необхідної інформації часто стає основною перешкодою для функціонування СМ з метою раннього попередження можливих наслідків. У багатьох випадках, це обумовлено несвоєчасним наданням даних, виявленням і використанням необхідних ресурсів взаємопов'язаних, сенсорних засобів та телекомунікаційних мереж різних операторів [2, 6].

3. Кризовий (дії в умовах виникнення кризової ситуації);

У кризовому режимі СМ повинна забезпечувати оперативний режим функціонування реального часу. Завдання повинні реалізовуватись на обмеженому інтервалі часу оперативно і безупинно. При виникненні кризових ситуацій в СМ можуть виникати проблеми пікового навантаження на усі елементи, у зв'язку з чим їх можуть істотно перевищувати функціональні обмеження на їх застосування [2, 7].

4. Післякризовий (ліквідація довгострокових наслідків кризового режиму).

Післякризовий режим є перехідним до звичайного і включає аналіз КС особливостей для її ліквідації, модифікацію вмісту баз даних і баз знань, відновлення нормальних режимів функціонування складових СМ [2, 8].

Зазначений метод моніторингу (рис. 3.1) реалізується за допомогою ієрархічної структури вертикально і горизонтально інформаційно поєднаних компонентів та може слугувати базисом відповідної ІТ моніторингу (рис. 3.2):

– розподілена система збору даних (від локального до глобального рівнів);

– база даних, з розподіленою технологією побудови (для реалізації завдань аналізу даних і прогнозування розвитку контрольованої ситуації);

– складову обробки (перетворення) та візуалізації інформації моніторингу;

– підсистема реагування на зміни кризи, що відображатиме управління діями осіб, які перебувають на об’єкті моніторингу [7-10].

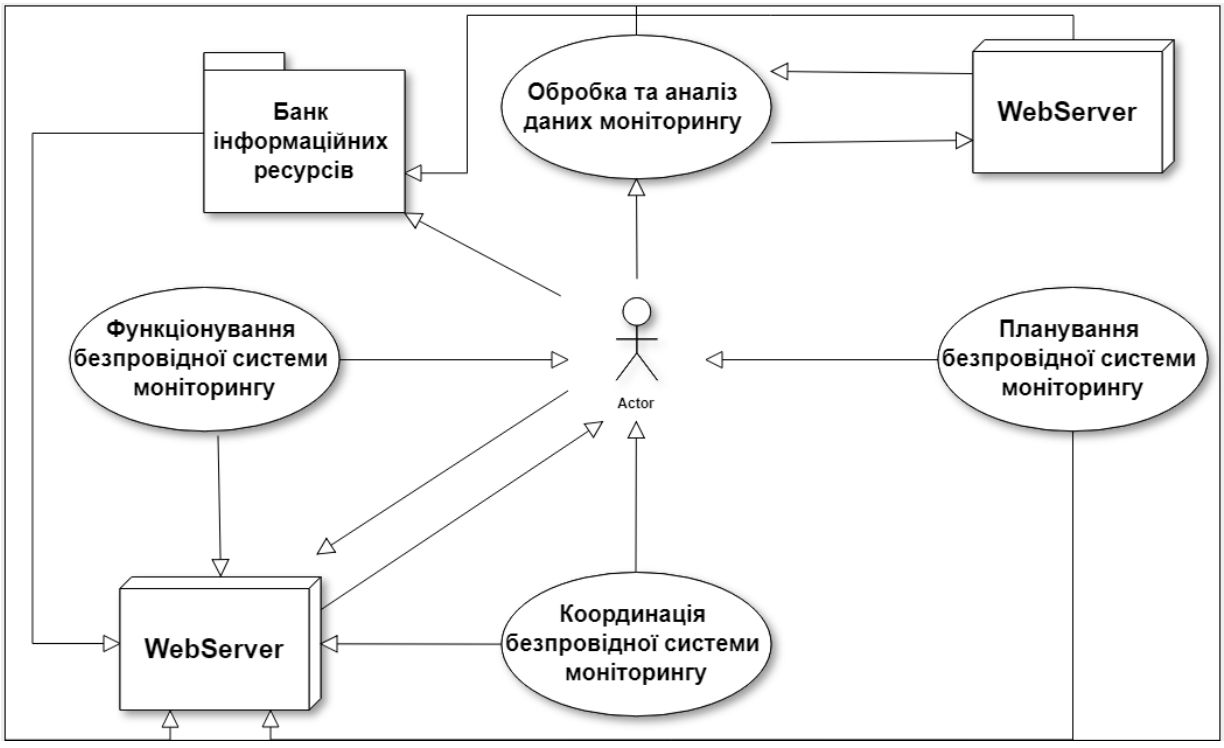


Рис. 3.2. Діаграма прецидентів моделювання запропонованої ІТ

Алгоритм роботи методу об’єднує завдання його функціонування логікою активізації роботи складових методу з N рівнів і P полюсів: $P = \sum_{i=1}^{N} n_i$.

Структурна схема алгоритму (в контексті прийняття управлінських рішень) подана на рис. 3.2 [6].

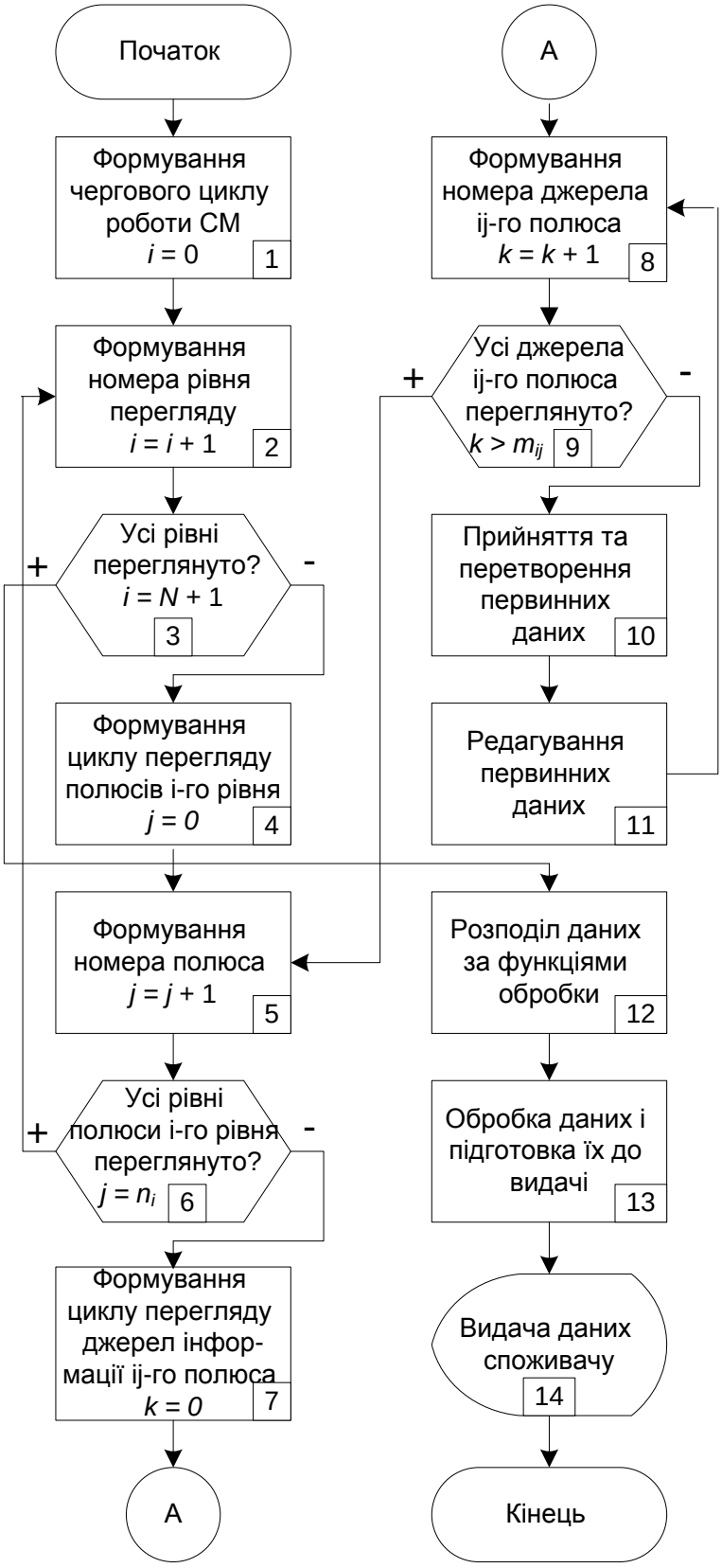


Рис. 3.2. Алгоритм роботи методу моніторингу в контексті прийняття управлінських рішень

Зазначений алгоритм реалізується у 14 основних кроків. Після того як формується запит (крок 1), реалізується активізація функціонування вузлів і полюсів як локального, так і глобального рівня WSN (кроки 2-9). Далі, джерела отримують запити про стан навколишнього середовища, компоненти систем обробки інформації зазначених рівнів WSN – фактично за допомогою кроків 10-14 первинний інформаційний трафік (крок 10) перетворюється в дані, які надаються у зручному вигляді споживачеві (крок 14) відповідно до його запиту (крок 1) [2, 6, 10].

3.2. Прогнозування контрольованих параметрів стосовно зміни параметрів навколишнього середовища

Властивістю фрактальних структур є самоподібність (так звана масштабна інваріантість). Одним з таких самоподібних (фрактальних) процесів є збір інформації від первинних джерел вимірювання параметрів кризової зони в системі моніторингу [1].

Для опису первинного інформаційного трафіку від джерел вимірювання в системах моніторингу, що має фрактальні властивості, вводиться узагальнений броунівський рух, який характеризується залежністю:

$$B_H(t) = \frac{1}{\Gamma\left(H + \frac{1}{2}\right)} \int_{-\infty}^{e} h(t-\tau) dB(\tau), \tag{3.1}$$

де: $dB(\tau)$ – приріст вінерівського процесу; $\Gamma(...)$ – гамма-функція; H – параметр Херста [1-3].

Імпульсна перехідна функція дорівнює:

$$h(t-\tau) = \begin{cases} (t-\tau)^{H-1/2}, & 0 \le \tau \le t \\ (t-\tau)^{H-1/2} - (-\tau)^{H-1/2}, & \tau < 0 \end{cases}. \tag{3.2}$$

На основі $h(bt-b\tau)=b^{H-1/2}h(t-\tau)$, а також залежності для вінерівского процесу $dB(b\tau)=b^{1/2}dB(\tau)$ з виразу (3.2) отримуємо $B_H(bt)=b^H B_H(t)$ або $b^{-H}B_H(bt)=B_H(t)$.

Це підтверджує самоподібний характер фрактального броунівського руху [2]. Для приростів вінеровського процесу математичне очікування і дисперсія на основі (3.2) з урахуванням

$$M\{dB(T)\}=0,\ M\{dB(\tau_1)dB(\tau_2)\}=M\{n(\tau_1)n(\tau_2)\}d\tau_1 d\tau_2=N_0\delta(\tau_2-\tau_1)d\tau_1 d\tau_2.$$

відповідно можна представити таким чином::

$$M\{B_H(t)-B_H(t_0)\}=0, \tag{3.3}$$

$$M\{[B_H(t)-B_H(t_0)]^2\}\approx(t-t_0)^{2H}. \tag{3.4}$$

Нормована кореляційна функція стаціонарних приростів фрактального броунівського руху для двох сусідніх інтервалів часу (t_0,t_1) і (t_1,t_2), які не перекриваються становить:

$$r_H(t)=\frac{M\{[B_H(t_1)-B_H(t_0)][B_H(t_2)-B_H(t_1)]\}}{M\{[B_H(t_1)-B_H(t_0)]^2\}},$$

або при $B_H(t_0)=0$:

$$r_H=\frac{M\{\{B_H(t)B_H(2t)\}-M\{B_H^2(t)\}\}}{M\{B_H^2(t)\}}. \tag{3.5}$$

Після відповідних підстановок та перетворень в (3.5), отримуємо

$$r_H = \frac{M\{[B_H(t) - B_H(2t) + B_H(2t)][B_H(2t) - B_H(t) + B_H(t)]\}}{M\{B_H^2(t)\}} - 1 =$$
$$= \frac{M\{B_H^2(2t)\}}{M\{B_H^2(t)\}} - \left[\frac{M\{B_H(t)B_H(2t)\}}{M\{B_H^2(t)\}} - 1\right] - 2 \quad . \qquad (3.6)$$

Враховуючи співвідношення (3.4) – (3.6) можна представити таким чином:

$$r_H(t) = 2^{2H-1} - 1. \qquad (3.7)$$

Помноживши (3.7) на $M\{B_H^2(t)\} \sim t^{2H}$, отримуємо кореляційну функцію приростів вінеровського процесу на інтервалах $(0, t)$ і $(t, 2t)$, яку можна представити таким чином:

$$K_{2H}(t) \approx \left(2^{2H-1} - 1\right)t^{2H}.$$

Останнє співвідношення вказує на кореляційну залежність приростів, що збільшується із зростанням параметра t.

При $H = 1/2$ процес (3.2) стає вінерівським і можливий перехід вінерівського процесу до фрактального броунівського руху [1]. Тоді кореляційну функцію фрактального броунівського руху можна представити таким чином:

$$K_{2H}(t_1, t_2) \sim 1/2\left[t_1^{2H} + t_2^{2H} - |t_1 - t_2|^{2H}\right]. \qquad (3.8)$$

Коефіцієнт кореляції для стаціонарних приростів фрактального броунівського руху на інтервалах $(t_n, t_n - T)$ і $(t_{n+k}, t_{n+k} - T)$ заданої тривалості T, можна представити, для розрахункових характеристик, співвідношенням

$$r_H(\kappa,T)\sim\frac{1}{2}\left[(\kappa+1)^{\alpha+1}-2\kappa^{\alpha+1}+(\kappa-1)^{\alpha+1}\right].$$

При великих значеннях κ коефіцієнт кореляції можливо апроксимувати і представити таким чином::

$$\begin{aligned} r(\kappa,T)&\sim\frac{1}{2}\alpha(\alpha+1)\kappa^{\alpha-1},\\ r_H(\kappa,T)&\sim\frac{1}{2}\alpha(\alpha+1)\kappa^{\alpha-1}=H(2H-1)\kappa^{2H-2}. \end{aligned} \tag{3.9}$$

Зауважимо, що із збільшенням параметру H, збільшується протяжність залежності $r_H(\kappa,T)$.

Однією з головних особливостей первинного інформаційного трафіку систем динамічного моніторингу реального часу є його чутливість до часових параметрів. Прогнозування часових параметрів первинного інформаційного трафіку дозволяє одержати додаткові відомості для керування системою моніторингу та формування рішень щодо запобігання поширення наслідків надзвичайної ситуації.

Проведемо фрактальні дослідження часових характеристик первинного інформаційного трафіку систем динамічного моніторингу в реальному масштабі часу. Виразимо коефіцієнт кореляції таким чином:

$$\begin{aligned} r(t_1,t_2)&=\frac{k_2(t_1,t_2)}{D_{t_1}},\\ r(t_1,t_2)&=\int_{-\infty}^{\infty}\int_{-\infty}^{\infty}x_1^0x_2^0\,p(x_1,t_1;x_2,t_2)dx_1dx_2,\\ D_{t_1}&=\int_{-\infty}^{\infty}x_1^{0^2}\,p(x_1,t_1)dx_1, \end{aligned} \tag{3.10}$$

де: D_{t_1} – дисперсія випадкового процесу, $k_2(t_1,t_2)$ – кореляційна функція; $x_1^0 = x_1 - \mu_1$, $x_2^0 = x_2 - \mu_2$ – центрована складова; μ_1, μ_2 – математичне очікування випадкового процесу для t_1, t_2 моментів часу, відповідно; $p(x_1,t_1;x_2,t_2)$ і $p(x_1,t_1)$ – двовимірна й одновимірна густина ймовірностей.

Нехай x_1 є відомий, тоді густину імовірності можна представити таким чином:

$$p(x_1,t_1) = \delta(x - x_1).$$

Використовуючи фільтруючі властивості дельта-функції, кореляційну функцію і дисперсію можна представити таким чином::

$$k_2(t_1,t_2) = x_1^0 \int_{-\infty}^{\infty} x_2^0 p(x_{2,}t_2 | x_1,t_1) dx_2 , \qquad D_{t_1} = x_1^{0^2}.$$

де $p(x_{2,}t_2 | x_1,t_1)$ – умовна густина імовірності.

На підставі властивостей фрактального броунівського руху одержимо прогнозовану оцінку інтервалів до моменту часу t_2 за відомим значенням характеристик у момент часу t_1, $t_2 > t_1 > 0$. У якості вихідної для одержання прогнозу розглядається співвідношення

$$x_2^0 = r(t_2,t_1)x_1^0,$$

де x_2^0 – оцінка прогнозу процесу в момент часу t_2.

Для фрактального броунівського руху коефіцієнт кореляції (3.10) можна представити таким чином:

$$r(t_1,t_2)=\frac{k_2(t_1,t_2)}{D_H(t_1)}=\frac{1}{2}\frac{t_1^{2H}+t_2^{2H}-|t_2-t_1|^{2H}}{t_1^{2H}}=\frac{1}{2}\left[1+S_{1,2}^{2H}-|S_{1,2}-1|^{2H}\right],\quad S_{1,2}=\frac{t_2}{t_1}.$$

Прогноз фрактального броунівського руху $B_H(t_2)$ згідно значення $B_H(t_1)$ можна представити таким чином::

$$B_H(t_2)=M\{B_H(t_2)|B_H(t_1)\}=\frac{1}{2}\left[1+S_{1,2}^{2H}-|S_{1,2}-1|^{2H}\right]B_H(t_1).$$

Розглядаючи випадкову зміну затримки як приріст фрактального броунівського руху $B_H(t_{n+1})-B_H(t_n)$, коефіцієнт кореляції приросту можна представити таким чином::

$$r_H(1,\Delta)=\frac{M\{T_nT_{n+1}\}-(T_0+\Delta T_{cp})^2}{M\{T_n^2\}0(T_0\Delta T_{cp})^2}=\frac{M\{[B_H(t_n)-B_H(t_{n-1})][B_H(t_{n+1})-B_H(t_n)]\}}{M\{[B_H(t_n)-B_H(t_{n-1})]^2\}},$$

де: $\Delta=T_0+\Delta T_{cp}$ – прогнозований час доставки пакету; T_0 – середній час доставки пакету; ΔT_{cp} – приріст середнього часу доставки.

Для стаціонарного процесу при $n=1$ можна представити таким чином:

$$r_H(1,\Delta)=\frac{M\{[B_H(t_1)B_H(t_2)]\}-M\{B_H^2(t_1)\}}{M\{B_H^2(t_1)\}},\ t_2-t_1=\Delta.$$

Для загального випадку вираз для $r_H(1,\Delta)$ приймає вигляд (3.9).

Оцінка прогнозу затримки приймає вигляд

$$T_{n+1}=r_H(1,\Delta)[T_n-(T_0+\Delta T_{cp})]+T_0+\Delta T_{cp},$$

тобто прогнозування прогнозу стану доставки відбувається з врахування попередніх часових параметрів [2, 4].

3.3. Модель WSN як базовий компонент удосконаленого методу моніторингу параметрів навколишнього середовища

На практиці цікавим є випадок, коли кількість вузлів WSN при побудові систем моніторингу [9-11] не приймає одного усталеного значення, а є випадковою змінною, тобто дорівнює n з певною ймовірністю p_n $(n = 1, 2, ...)$, причому так, що $\sum_{n=1}^{\infty} p_n = 1.$

Нехай U – випадкова змінна, причому така, що $P(U = n) = p_n$, де $p_n \geq 0, (n = 1, 2, ...)$ та $\sum_{n=1}^{\infty} p_n = 1.$

Приймемо $Y_1(t), Y_2(t), ...$ процесами Пауссона з інтенсивністю, заданою формулою (3.11)

$$A = A(x_1, ..., x_k; T_1, ..., T_k) = \sum_{j=1}^{k} \frac{x_j}{T_j}., \tag{3.11}$$

та такими, що для кожного $t \geq 0,$ випадкові змінні U, $Y_1(t), Y_2(t), ...$ є незалежними. Тоді на базі (3.11) $N(t)$ можна представити у вигляді

$$N(t) = \sum_{j=1}^{U} N_j(t).$$

Користуючись формулою повної ймовірності, ймовірність колізії описуватиметься так

$$P(A_s) = \sum_{n=1}^{\infty} Q(s, n, A)\, p_n , \qquad (3.12)$$

де $Q(s, n, A)$ задається $Q(s, n, A) = \sum_{j=2}^{\infty} e^{-nAs} \frac{(nAs)^j}{j!} [1 - (1 - j\frac{t_p}{s})_+^j]$. та

$p_n = P(U = n)$.

Особливі випадки:

1. Розглядаємо випадкові змінні U з двоточковим розподілом

$$P(U = n_0) = 1 - \varepsilon ,$$
$$P(U = n_1) = \varepsilon ,$$

де $n_0 , n_1 \in N$, $0 < \varepsilon < 1$, (ε є малим числом).

Тоді отримуємо наступне:

$$P(A_s) = (1 - \varepsilon) Q(s, n_0 , A) + \varepsilon Q(s, n_1 , A) =$$
$$= (1 - \varepsilon) \sum_{j=2}^{\infty} e^{-n_0 As} \frac{(n_0 As)^j}{j!} [1 - (1 - j\frac{t_p}{s})_+^j] +$$
$$+ \varepsilon \sum_{j=2}^{\infty} e^{-n_1 As} \frac{(n_1 As)^j}{j!} [1 - (1 - j\frac{t_p}{s})_+^j].$$

2. Розглядаємо випадкову змінну U з геометричним розподілом

$$P(U = n) = p(1 - p)^{n-1}$$
$$(n = 1, 2, ...) , \quad 0 < p \le 1,$$

для якого $E(U)=\frac{1}{p}$.

Тоді

$$P(A_s)=\sum_{n=1}^{\infty}\sum_{j=2}^{\infty}e^{-nAs}\frac{(nAs)^j}{j!}[1-(1-j\frac{t_p}{s})_+^j]p(1-p)^{n-1}.$$

Зокрема, якщо позначити $m=E(U)=\frac{1}{p}$, отримуємо наступне:

$$P(A_s)=\sum_{n=1}^{\infty}\sum_{j=2}^{\infty}e^{-nAs}\frac{(nAs)^j}{j!}[1-(1-j\frac{t_p}{s})_+^j]\frac{1}{m}\left(1-\frac{1}{m}\right)^{n-1}.$$

3. Нехай випадкова змінна U має розподіл Пуассона

$$P(U=n)=e^{-a}\frac{a^n}{n!},$$

$$n=0,1,2,\ldots,a>0,\ E(U)=a\ .$$

Тоді, беручи до уваги $Q(t,0,s)=0,$ отримуємо наступне:

$$P(A_s)=\sum_{n=1}^{\infty}\sum_{j=2}^{\infty}e^{-nAs}\frac{(nAs)^j}{j!}[1-(1-j\frac{t_p}{s})_+^j]e^{-a}\frac{a^n}{n!}.$$

4. Рівномірний розподіл на точках

$$\{n\}_{n=m-k}^{n=m+k},$$

такий, що $P(n) = \frac{1}{2k+1}$, для $n = m-k,\ ...,\ m+k$, де $m \in N$, $k < m$.

Тоді отримуємо наступне:

$$P(A_s) = \frac{1}{2k+1} \sum_{n=m-k}^{m+k} \sum_{j=2}^{\infty} e^{-nAs} \frac{(nAs)^j}{j!} [1-(1-j\frac{t_p}{s})_+^j] .$$

Кожен з наведених випадків можна вважати свого роду «розмиттям» кількості вузлів навколо середньої кількості вузлів m до детерміністичної версії, коли припускалася стала кількість вузлів n. Можна було б дослідити задачу, як вид розподілу та його параметри впливають на ймовірність колізії в мережі. Геометричному розподілу притаманна цікава та варта уваги властивість відсутності пам'яті, що може бути придатним у різних застосуваннях, наприклад, у медицині [11].

У теоретичних дослідженнях, для спрощення розглянутої моделі можна також розглянути випадок випадкової змінної U з необов'язково натуральними значеннями. Розглянуто випадкову змінну U з нормальним розподілом

$$U \sim N(m, \sigma) ,$$

де $m = E(U), \qquad \sigma^2 = D^2(U)$.

Тоді

$$P(A_s) = \int_{-\infty}^{\infty} \frac{1}{\sqrt{2\pi}\,\sigma} e^{-\frac{(x-m)^2}{2\sigma^2}} Q(t,\, x,\, A)\, dx =$$

.

$$= \int_{-\infty}^{\infty} \frac{1}{\sqrt{2\pi}\,\sigma} e^{-\frac{(x-m)^2}{2\sigma^2}} \sum_{j=2}^{\infty} e^{-Asx} \frac{(Asx)^j}{j!} [1-(1- j\frac{t_p}{s})_+^j]\, dx =$$

$$= \sum_{j=2}^{\infty} [1-(1- j\frac{t_p}{s})_+^j] \cdot \frac{(As)^j}{j!} \int_{-\infty}^{\infty} e^{-Asx} x^j \frac{1}{\sqrt{2\pi}\boldsymbol{\sigma}} e^{-\frac{(x-m)^2}{2\boldsymbol{\sigma}^2}} dx \ .$$

Для випадкової змінної U з експоненціальним розподілом густини

$$f(x) = \begin{cases} \frac{1}{a} e^{-\frac{x}{a}} & , \quad x \geq 0 \\ 0 & , \quad x < 0, \end{cases} \qquad E(U) = a,$$

отримано

$$P(A_s) = \int_0^{\infty} \frac{1}{a} e^{-\frac{x}{a}} Q(s,\, x,\, A)\, dx =$$

$$= \int_0^{\infty} \frac{1}{a} e^{-\frac{x}{a}} \sum_{j=2}^{\infty} e^{-Asx} \frac{(Asx)^j}{j!} [1-(1- j\frac{t_p}{s})_+^j]\, dx\,.$$

Використовуючи формулу $\int_0^{\infty} x^n e^{-px} = n!\, p^{-n-1}$ отримуємо наступне:

$$P(A_s) = \sum_{j=2}^{\infty} \frac{1}{a} (As)^j [1-(1- j\frac{t_p}{s})_+^j] \int_0^{\infty} \frac{x^j}{j!} e^{-\left(\frac{1}{a}+As\right)x} dx =$$

$$= \sum_{j=2}^{\infty} \frac{1}{a} (As)^j [1 - (1 - j\frac{t_p}{s})_+^j] \left(\frac{1}{\frac{1}{a} + As} \right)^{j+1} =$$

$$= \frac{1}{\frac{1}{a} + As} \sum_{j=2}^{\infty} \left(\frac{As}{\frac{1}{a} + As} \right)^j [1 - (1 - j\frac{t_p}{s})_+^j] =$$

$$= \frac{\frac{1}{a}}{\frac{1}{a} + As} \left[\sum_{j=2}^{\infty} \left(\frac{As}{\frac{1}{a} + As} \right)^j - \sum_{j=2}^{\infty} \left(\frac{(As)^j (1 - j\frac{t_p}{s})_+^j}{\left(\frac{1}{a} + As \right)^j} \right) \right] =$$

$$= \frac{\frac{1}{a}}{\frac{1}{a} + As} \left[(1 + aAs) - \left(1 + \frac{As}{\frac{1}{a} + As} \right) - \sum_{j=2}^{\infty} \frac{(As)^j (1 - j\frac{t_p}{s})_+^j}{\left(\frac{1}{a} + As \right)^j} \right] =$$

$$= \frac{\frac{1}{a}}{\frac{1}{a} + As} \left[aAs - \frac{As}{\frac{1}{a} + As} - \sum_{j=2}^{\infty} \frac{(As)^j (1 - j\frac{t_p}{s})_+^j}{\left(\frac{1}{a} + As \right)^j} \right] =$$

$$= \frac{As}{\frac{1}{a} + As} - \frac{\frac{1}{a} As}{\left(\frac{1}{a} + As \right)^2} - \sum_{j=2}^{\infty} \frac{(As)^j}{\left(\frac{1}{a} + As \right)^{j+1}} \left[1 - j\frac{t_p}{s} \right]_+^j .$$

Базові аспекти практичного застосування результатів

WSN базується на радіоканалах і залежно від застосованої частотності, матиме різний промінь, тобто займає різний простір. Зважуючи питання вибору частотності роботи мережі в представленому варіанті рішення частота може збільшуватись щоразу. Очевидно, беручи до уваги всі бмеження, які з цього

факту виникають. Проте, коли ми увійдемо в простір смуг, лежачих в сфері інфрачервоного кольору, чи навіть видимого світла, то можна констатувати, що вона зводиться до дуже вузької випромінюваної в'язки наприклад через лазер. Цей факт веде до подальших пропозицій, що стосуються розвитку WSN [12-16].

Як стаціонарна мережа наприклад у багатьох промислових застосуваннях, побудована спираючись на представлений в роботі принцип доступу, дозволить розв'язати ряд проблем, що виступають, цього типу мережах але працюючих на відносно низьких радіочастотах. Головні проблеми з якими тоді ми маємо справу при роботі з області чвстоти радіохвиль, чи смуг комп'ютерних мереж то ємкість мережі (питання числа вузлів), спосіб непересічного доступу вузлів до базової станції і порушення. У разі, коли вузли залишаються мобільними для смуг в інфрачервоному кольорі, ситуація набагато більш складна, хоча і також є предметом зацікавленості.

Використання смуг в сфері інфрачервоного кольору є загальновідомим питанням в різних застосуваннях напр. в дистанційному керуванні устаткування RTV, як комунікаційні канали комп'ютерного устаткування, принтерів, мобільних телефонів і т.д. (IrDA). Зазвичай, це канали дуже малої дальності, придатність яких в мережах WSN має маргінальне значення.

Використання смуг інфрачервоного кольору в мережах (не тільки WSN) стає необхідністю, виникаючою також з дефіциту доступного радіоспектру. Реалізація мережі в смугах інфрачервоного кольору пов'язується з багатьма питаннями і такими проблемами як: направляння в'язки світла, моніторингу, охорона здоров’я людей і тварин, нові алгоритми роутинг і т.д.

Приводом зацікавленості військ технологією мережі WSN з використанням FSOC є дуже висока безпека передавання і дуже велика пропускна здатність. Найбільшим викликом для комунікації, використовуючої смуги в іефрачервоному кольорі на полі бою, є мобільність одиниць, негативно впливаюча на стабільність сполучень [7, 14, 16]..

Список літератури до третього розділу

1. Ю.Г. Даник, В.С. Стогній, М. М. Климаш, Л.О.Комарова, «Системи динамічного моніторингу параметрів навколишнього середовища», *Проблеми створення, випробування, застосування та експлуатації складних інформаційних систем*, Житомир: ЖВІ НАУ, 2012, вип. 6, с. 5-12.

2. Бобало Ю.Я., Даник Ю. Г., Комарова Л.О., та ін., *Моніторинг об'єктів в умовах апріорної невизначеності джерел інформації:* монографія, Львів: Видавництво Української академії друкарства, 2015, 360 с.

3. S. Gnatyuk, V. Kinzeryavyy, I. Stepanenko, Ya. Gorbatyuk, V. Kotelianets, «Code obfuscation technique for enhancing software protection against reverse engineering», *Advances in Intelligent Systems and Computing*, Springer, pp. 232-239, 2018 *(Scopus,Web of Science).*

4. V. Gnatyuk, N. Dyka, V. Kotelianets, S. Dakov, «IoT architecture for air pollution monitoring system», *Proceedings of VII Międzynarodowa Konferencja Studentów oraz Doktorantów «Inżynier XXI wieku»,* Bielsko-Biala, pp. 83-97, 2017.

5. Гнатюк С.О., Котелянець В.В., Кищенко В.В., Бауиржан М.Б., «Мережево-центричний моніторинг інцидентів кібербезпеки у секторах критичної інфраструктури держави», *Кібербезпека: освіта, наука і техніка,* №2, с. 80-89, 2018.

6. Одарченко Р.С., Ткаліч О.П., Дика Н.В., Котелянець В.В. «Дослідження можливостей комунікаційних протоколів для потреб IoT», *Проблеми інформатизації та управління,* Том 3, № 59, с. 43-55, 2017.

7. Odarchenko R., Gnatyuk V., Sydorenko V., Kotelianets V., «Quality of service assessment rules development for mobile operators», *збірник тез доповідей III міжнародної наук.-практ. конференції «Інформаційна безпека та комп'ютерні технології»,* 19-20 квітня 2018 р., м. Кропивницький: ЦНТУ, с. 168-169, 2018.

8. Смірнов О.А., Котелянець В.В., «Застосування концепції Інтернету речей для побудови інтелектуалізованих систем моніторингу параметрів навколишнього середовища», *матеріали VI всеукраїнської наук.-практ.*

конференції молодих учених і студентів з міжнародною участю «Проблеми та перспективи розвитку авіації та космонавтики», 29-30 листопада 2017 р., К. : НАУ, с. 47-48, 2017.

9. Котелянець В.В., «Базові аспекти побудови сучасних систем моніторингу довкілля на основі концепції Інтернету речей», *матеріали X міжнародної наук.-практ. конференції «Інтегровані інтелектуальні робототехнічні комплекси (ІІРТК-2017)»,* 16-17 травня 2017 р., К.: НАУ, с. 184-186, 2017.

10. Котелянець В.В., «Розробка і дослідження програмно-технічного комплексу моніторингу параметрів навколишнього середовища реального часу», *збірник матеріалів IV міжнародної наук.-практ. конференції «Актуальні питання забезпечення кібербезпеки та захисту інформації»,* 21-24 лютого 2018 р., с. Верхній Студений: Видавництво Європейського університету, с. 26-28, 2018.

11. J. Pilarski, S. Rajba, Measurement of light gradient in plant organs with a fiber optic microbe, *Acta Physiologiae Plantarum*, 2004, Vol. 26, No 4, p. 405-410. – ISSN 0137-5881.

12. I. Ahmed, S. Obermeier, M. Naedele, G. G. Richard, SCADA Systems: Challenges for Forensic Investigators, *Computer,* 2012, Vol. 45, No 12, P. 73-78 ISSN 0018-9162.

13. Aleksander M., Litawa G., Karpinskyi V. Distributed computing system which solve an elliptic curve discrete logarithm problem, *The Experience of Designing and Application of CAD Systems in Microelectronics : Xth International Conference CADSM 2009,* 24-28 February 2009: Proceedings. – Lviv-Polyana, Ukraine: Publishing House Vezha&Co, 2009, p. 378-380.

14. Annie Jenniefer1, John Raybin Jose Techniques for Identifying Denial of Service Attack in Wireless Sensor Network: a Survey International Journal of *Advanced Research in Computer and Communication Engineering*, Vol. 3, Issue 6, June 2014.

15. A. Akl, T.Gayraud and P. Berthou, An investigation of self-organization in wireless sensor networks, *IEEE International Conference on Networking, Sensing and Control,* 2001, p. 1-6.

16. J. J. Quisquater, J. P. Delescaille, How easy is collision search? *Advances in cryptology, EUROCRYPT*. LNCS, 1990, Vol. 434, p. 429-434.

РОЗДІЛ 4. ІНФОРМАЦІЙНА ТЕХНОЛОГІЯ МОНІТОРИНГУ ПАРАМЕТРІВ, ЩО ХАРАКТЕРИЗУЮТЬ СТАН НАВКОЛИШНЬОГО СЕРЕДОВИЩА РЕАЛЬНОГО ЧАСУ В СУЧАСНІЙ КОНЦЕПЦІЇ IoT

4.1. Обгрунтування архітектури ІТ моніторингу навколишнього середовища та відповідного ПТК

На базі запропонованих моделей (розділ 2) і методу (розділ 3) розроблено спеціалізовану ІТ моніторингу параметрів, що характеризують стан навколишнього середовища реального часу в сучасній концепції IoT (рис. 4.1).

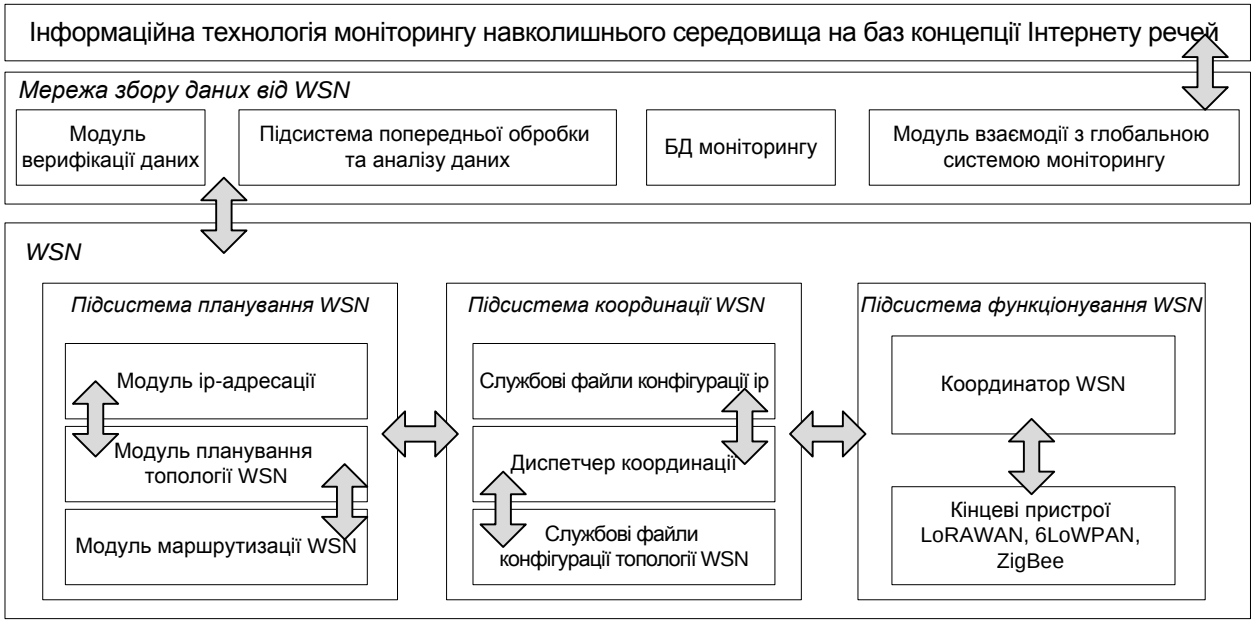


Рис. 4.1. Інформаційна технологія моніторингу навколишнього середовища на базі IoT

На основі зазначеної ІТ із використанням засобів Arduino, JavaScript, NodeJs, HTML та CSS було розроблено спеціалізований ПТК моніторингу необхідних параметрів, що характеризують стан навколишнього середовища.

До складу зазначеного ПТК включені наступні підсистеми (проте комплекс є гнучким і може змінюватись відповідно до запитів користувачів і наявного обладнання):

1) Акумулювання даних. Ця підсистема поєднує віддалені автоматизовані робочі місця (АРМ) суб'єктів загальної системи моніторингу, які збирають дані і передають за визначеними комунікаційними (мережевими) протоколами до центру системи управління.

2) Інфокомунікацій. Ця підсистема є синтезом сучасної продуктивної і надійної серверної частини, високошвидкісних мереж зв'язку (у тому числі й WSN) та комунікаційних протоколів. У складі ПТК вона забезпечує приймання даних від АРМ, їх обробку і запис до відповідних баз даних, ефективну комунікацію з відокремленим інформаційно-аналітичним центром, а також з особами, що приймають управлінські рішення тощо.

3) Обробки первинного інформаційного трафіку та аналітики. Зазначена підсистема включає в себе АРМ адміністраторів баз даних і відповідних фахівців, які приймають, обробляють та аналізують первинний інформаційний трафік. АРМ адміністраторів розподіляють доступ відповідно до фіксованих повноважень, узгоджують надходження і видачу даних, а також забезпечують захист даних і їх вчасне відновлення у випадку збоїв і аварій різноманітного характеру. АРМ фахівців, які є забезпеченими необхідними технічними / програмними засобами і сучасним високошвидкісним зв'язком, здійснюють попередній аналіз первинного інформаційного трафіку, його уніфікацію, занесення до відповідних баз даних, моделюють кризові ситуації і відпрацьовують плани виходу з них.

4) Відображення і аналізу даних. Ця підсистема містить цифрові карти (локальні та глобальні); інформаційно-пошукові засоби; модулі синтезу цифрових карт та баз даних; засоби картографічного аналізу і візуального представлення результатів у зручному для кінцевих користувачів вигляді.

5) Підтримки баз даних. Зазначена підсистема базується на спеціальному програмному забезпеченні і є орієнтованою на створення, збереження і забезпечення доступу користувачів до інформаційних ресурсів. Також, вона виконує певні функції захисту інформації, зокрема, архівування і

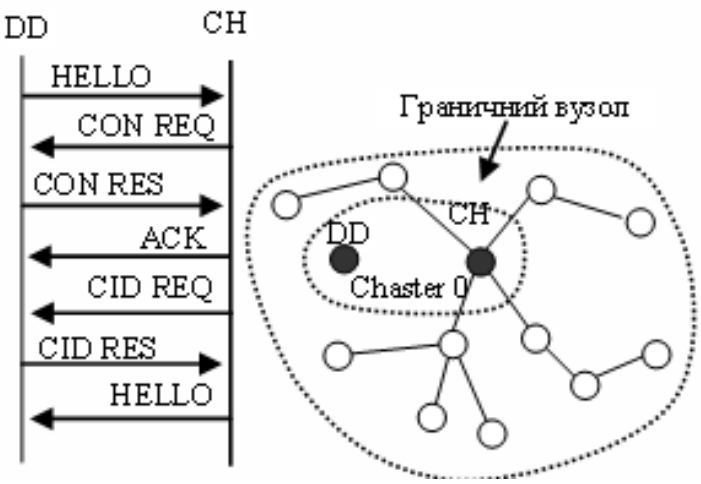
створення резервних копій на випадок виникнення кризових ситуацій чи інцидентів.

При багатокластерному підході, необхідно встановити спеціальний помічений вузол (DD). За його допомогою призначається унікальний кластерний ідентифікатор (CID) для мережевого сенсора, що комбінується з вузловим ідентифікатором CH. Іншою функцією DD є обчислення найкоротшого шляху до кожного кластера та інформування про це інших вузлів у мережі.

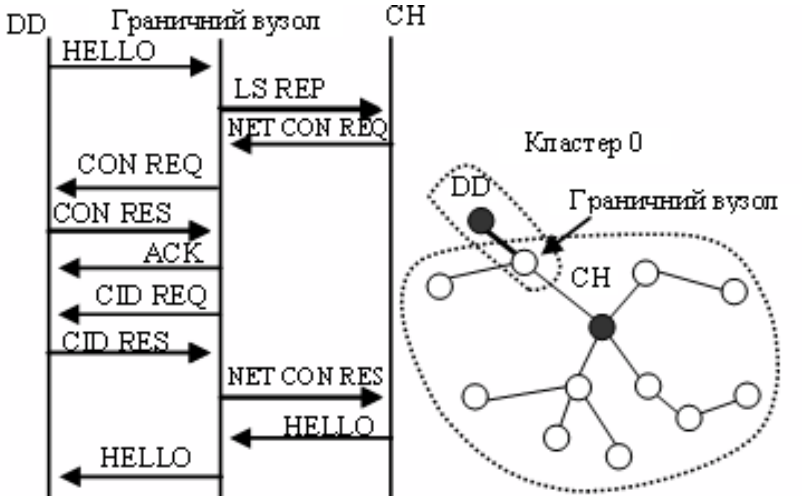
Коли DD приєднується до мережі, він розсилає повідомлення HELLO усім сусідам, під час отримання цього повідомлення сусідній сенсор відправляє у відповідь запит «CONNECTION REQUEST» для приєднання до нульового кластера. Після цього вузол очікуватиме ідентифікатор кластера CID від DD. У цьому випадку CH стане граничним вузлом з двома логічними адресами, одна для ідентифікації його як учасника кластера, інша – вершини кластера. Коли CH отримає кластерний ідентифікатор CID, він проінформує учасників свого кластера про це за допомогою повідомлення HELLO. Якщо учасник кластера отримає повідомлення HELLO, то вони додадуть до таблиці сусідів кластерний ідентифікатор та відрапортують про це CH. Вершина кластера вибирає серед членів кластера вузол для того, щоб зробити його граничним вузлом до центрального кластера, та висилає NETWORK CONNECTION REQUEST-повідомлення до граничного вузла про початок встановлення процедури з'єднання з DD.

Граничний вузол вишле запит про з'єднання та вступ у нульовий кластер. Надалі він вишле CID REQUEST-повідомлення до DD. Після отримання CID RESPONSE-повідомлення граничний вузол вишле NETWORK CONNECTION RESPONSE-повідомлення, що міститиме новий кластерний ідентифікатор до свого заголовка кластера. Коли CH отримає новий CID, він повідомить про нього членів свого кластера за допомогою повідомлення HELLO. Кластери, що безпосередньо не межують з нульовим кластером,

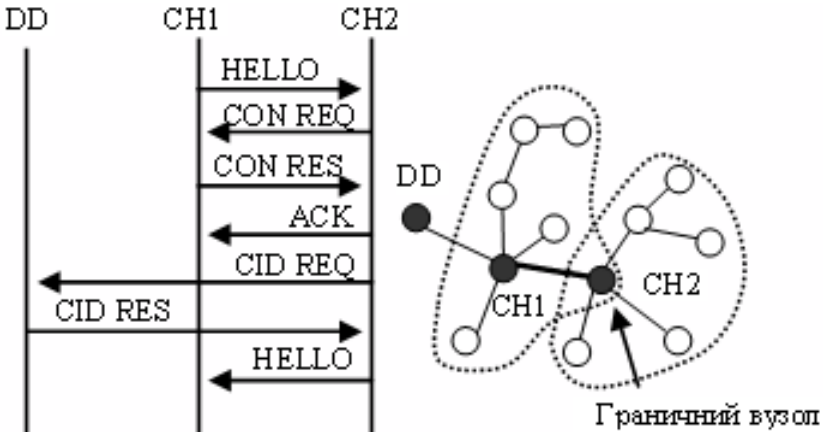
використовують проміжні ланки для отримання кластерного ідентифікатора (процедури описані на рис. 4.2).



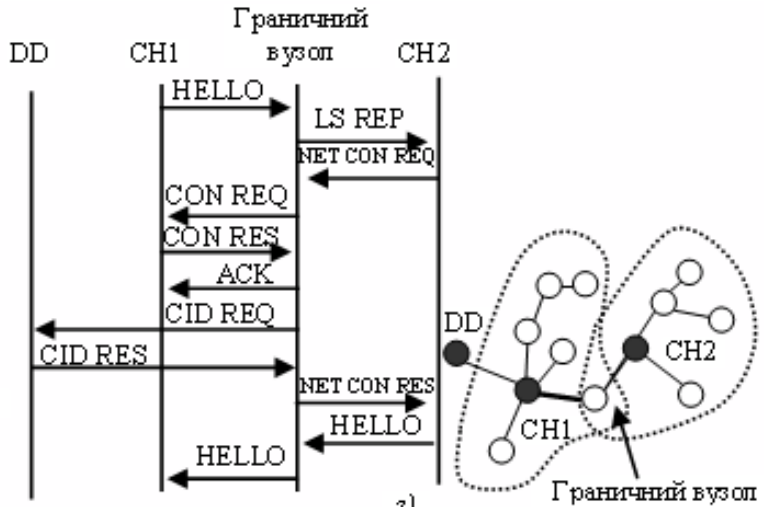
а)



б)



в)



г)

Рис. 4.2. Схеми отримання кластерного ідентифікатора

Вузли в кластері та CH відсилають інформацію про свої безпосередні зв'язки до DD. Згодом ця інформація може бути використана для розрахунку оптимізації топології мережі. Також DD може розсилати «TOPOLOGY UPDATE» повідомлення для інформування про сучасні маршрути від DD до інших кластерів. Можливе існування резервного DD для підтримки мережі.

Міжкластерна комунікація реалізується за допомогою маршрутизації. Граничні вузли відіграють роль роутерів між двома кластерами. Лише DD може вислати повідомлення до усіх вузлів в мережі. Повідомлення буде розіслане деревоподібною структурою кластерів. Граничні вузли відішлють це повідомлення від батьківських до дочірних кластерів. Якщо відбулося об'єднання кластерів згідно з правилами вже існуючої мережі, координатор локальної мережі, що підключається переводиться в ранг маршрутизатора і передає усю інформацію про локальну мережу координаторові існуючої мережі. Отже, для практичної реалізації сенсорної мережі на основі стандарту ZigBee найбільш прийнятною є кластерна топологія, оскільки вона дає змогу створити ієрархічну структуру вузлів (координатор – маршрутизатор – кінцевий пристрій) з динамічною зміною топології мережі здавачів, що однією

із вимог до створюваної динамічної системи локального та глобального моніторингу параметрів навколишнього середовища реального часу.

4.2. Експериментальне дослідження запропонованої IT моніторингу

Також, у цьому розділі було проведено експериментальне дослідження отриманих результатів на прикладі ПТК моніторингу параметрів повітря на основі IoT, архітектура якого відображена на рис. 4.3.

Зокрема, рис. 4.3 відображає архітектуру з використанням різних бездротових технологій таких як LoRAWAN, 6LoWPAN, Z-хвилі, ZigBee тощо. При передаванні даних на короткі відстані (наприклад, в приміщенні) пристрої можуть використовувати PAN, що може надаватися такими технологіями бездротової передавання даних, як BLE (Bluetooth Low Energy), ZigBee, 6LoWPAN і провідний інтерфейс USB.

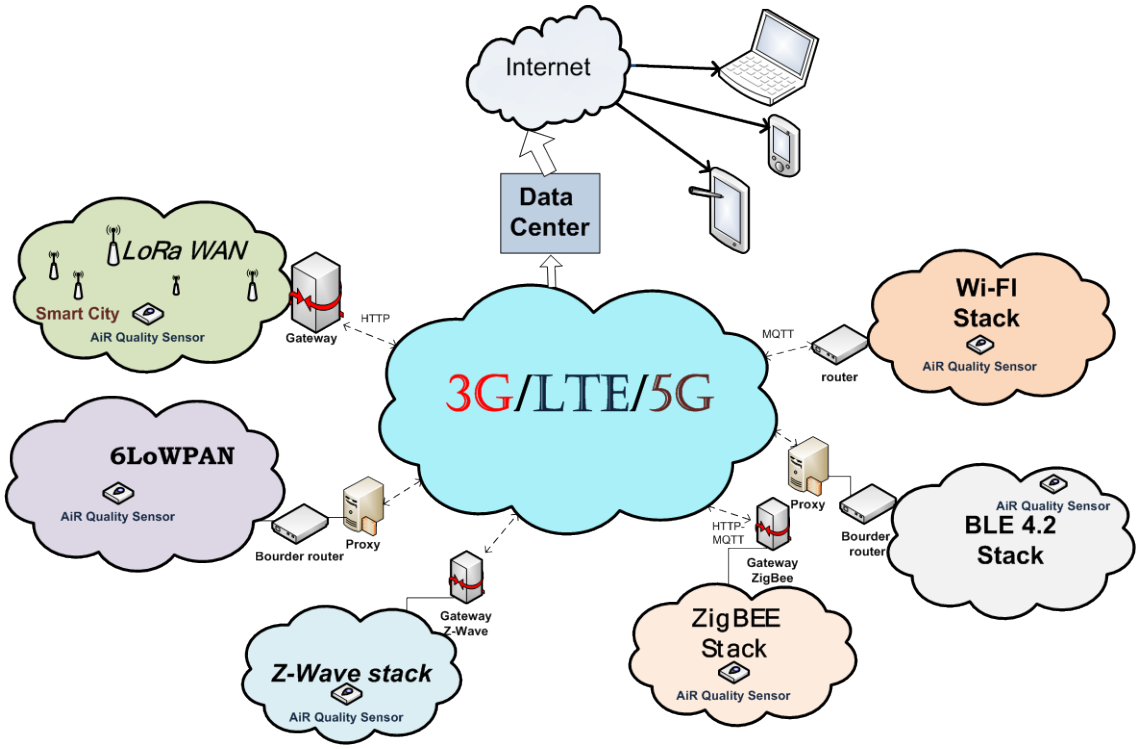


Рис. 4.3. Мережева архітектура IoT системи моніторингу параметрів повітря

Якщо йдеться про передавання даних на досить великі відстані (наприклад, в офісі чи у великій будівлі), то можна задіяти локальну мережу

LAN. Дротові локальні мережі у більшості випадків будуються на базі технології Ethernet і оптоволокна, а бездротові – на базі технології Wi-Fi.

Для організації глобальної обчислювальної мережі WAN в цілях моніторингу можна використати технології LTE, LPWAN та WiMAX, хоча остання на сьогодні не довела свою придатність для практичного застосування і поступається іншим технологіям телекомунікаційних стандартів наступного покоління.

Відповідно до запропонованої методики експерименту усі дослідження проводились у приміщенні (рис. 4.4), дані фіксувались для подальшої статистичної обробки.

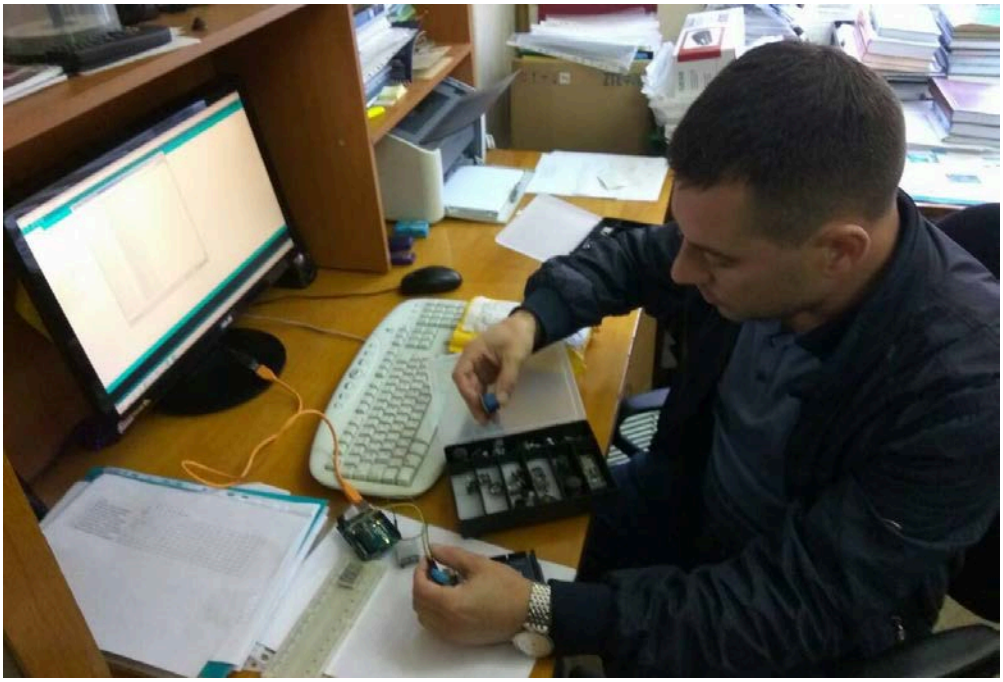
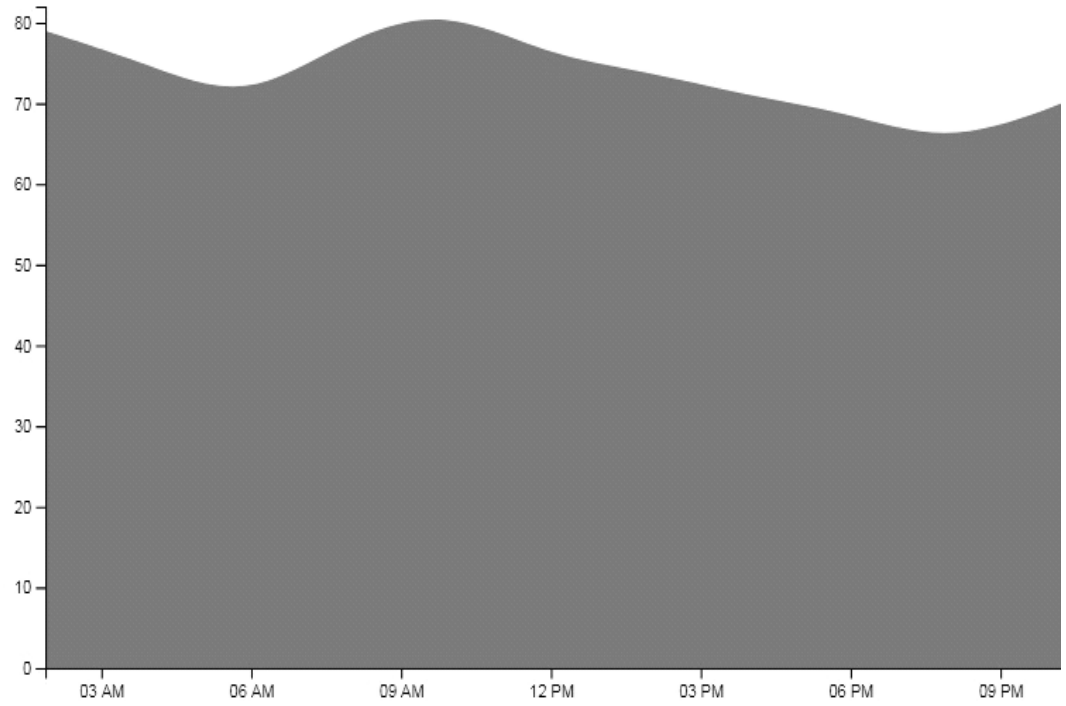


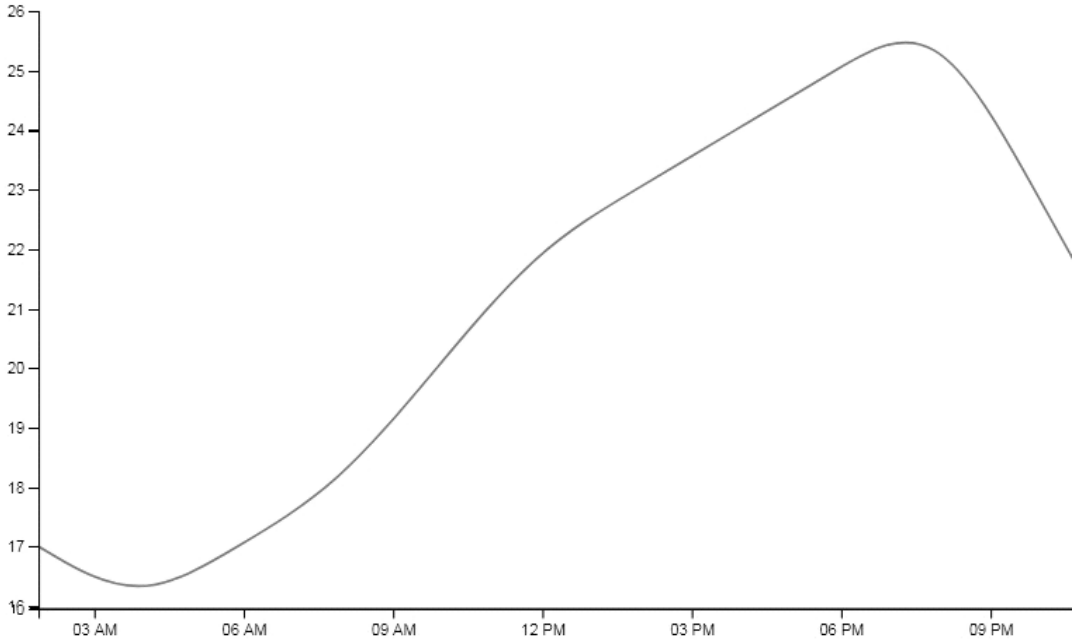
Рис. 4.4. Налаштування здобувачем експериментальної установки моніторингу параметрів повітря

На рис. 4.5 показано зміну вологості (рис. 4.5 а) і температури (рис. 4.5 б) повітря протягом доби (як приклад) у окремій кімнаті. Ці графіки побудовані запропонованим у роботі програмним забезпеченням, яке входить до складу ПТК, у режимі реального часу.

Вимірювані параметри не обмежуються вологістю і температурою повітря, можуть бути використані будь-які параметри з огляду на доступні (наявні) сенсори, що входять до складу ПТК.



а)



б)

Рис. 4.5. Графік зміни вологості (а) та температури (б)

Як показали експериментальні дослідження, запропонований у роботі ПТК моніторингу параметрів навколишнього середовища реального часу є працездатним, може використовуватись як прототип для організації моніторингу в динамічно змінюваних середовищах та при виникненні критичних ситуацій різного характеру.

Розроблено *методику побудови WSN з випадковим доступом.* Її базовано на створених моделях, пристосованих до завдань, які виконує мережа. При цьому враховано набір властивостей і параметрів, що характеризують WSN з випадковим доступом та які можна вибрати для її реалізації:

1. T – середній час між передачами, який вибирається згідно з необхідною частотою проведення вимірювань за допомогою сенсорів, під'єднаних до вузла WSN.

2. t_p – час тривання передачі пакету вузлом, що обумовлений кількістю сенсорів, під'єднаних до вузла, та обраним протоколом з необхідною довжиною двійкового слова для запису інформації з потрібною роздільною здатністю, а також наявною у розпорядженні смугою пропускання радіоканалу.

3. n – кількість вузлів, необхідних для виконання завдання.

4. Мобільність вузлів WSN.

5. Прогнозована якість передачі WSN, враховуючи вимогу щодо ймовірності колізії.

6. Необхідність поділу вузлів на групи відповідно до критерію середнього часу між передачами WSN.

7. Необхідна кількість сенсорів, під'єднаних до вузла, що пов'язано з вибором протоколу та зумовлено наявною в розпорядженні смугою пропускання радіоканалу WSN.

8. Вибір комунікаційного протоколу WSN, відповідно до викладених вище умов.

9. Доступна або необхідна смуга пропускання радіоканалу.

10. Необхідна стала інтенсивність (частота) спостереження явищ, які досліджуються із застосуванням WSN.

11. Необхідна змінна інтенсивність (частота) спостереження явищ, що вивчаються з використанням WSN.

12. Необхідність врахування деяких або всіх мережевих параметрів WSN відповідно до запропонованих моделей.

4.3. Оптимізація процесу моніторингу параметрів навколишнього середовища

Вимірювання параметрів спеціального трафіку локального інфо-комунікаційного кластеру з використанням мобільних пристроїв є багато-критеріальною оптимізаційною задачею. Крім того, складно розробити універсальний алгоритм управління потужністю для мережі в цілому з метою визначення координат вимірювальних пристроїв. Для ефективного вирішення даної задачі враховується не лише вимірювання відстані до мобільної станції на основі метрики BER, але і параметр просторово-часової локалізації абонентського навантаження. Для забезпечення ефективного функціонування механізму управління потужністю в мережі застосовано модель просторово-часової локалізації абонентського навантаження в (рис. 4.6).

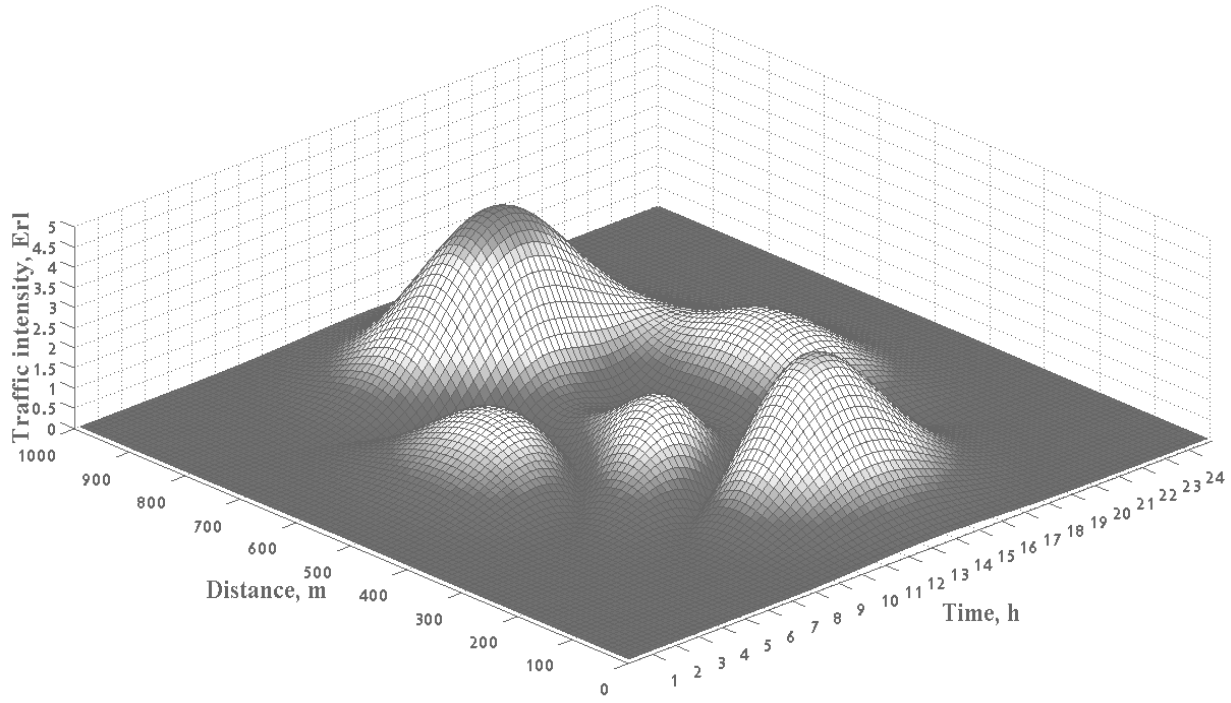


Рис. 4.6. Просторово-часова локалізація джерел протягом доби

Просторово-часова локалізація (рис. 4.6) забезпечує оптимізацію процесу моніторингу шляхом декомпозиції ІКС – кризової області (зони, регіону) на елементарні об’єми. Аналіз просторово-часової локалізації первинних джерел в просторі дозволяє визначити оптимальні статистичні параметри для досягнення заданої точності результатів моніторингу контрольованих параметрів.

Список літератури до четвертого розділу

1. Смірнов О.А., Котелянець В.В., «Застосування концепції Інтернету речей для побудови інтелектуалізованих систем моніторингу параметрів навколишнього середовища», *матеріали VI всеукраїнської наук.-практ. конференції молодих учених і студентів з міжнародною участю «Проблеми та перспективи розвитку авіації та космонавтики»,* 29-30 листопада 2017 р., К. : НАУ, с. 47-48, 2017.

2. V. Gnatyuk, N. Dyka, V. Kotelianets, S. Dakov, «IoT architecture for air pollution monitoring system», *Proceedings of VII Międzynarodowa Konferencja Studentów oraz Doktorantów «Inżynier XXI wieku»,* Bielsko-Biala, pp. 83-97, 2017.

3. Котелянець В.В., «Базові аспекти побудови сучасних систем моніторингу довкілля на основі концепції Інтернету речей», *матеріали X міжнародної наук.-практ. конференції «Інтегровані інтелектуальні робототехнічні комплекси (ІІРТК-2017)»,* 16-17 травня 2017 р., К.: НАУ, с. 184-186, 2017.

4. Смірнов О.А., Котелянець В.В., «Стійкі до колізій стохастичні моделі функціонування бездротових сенсорних мереж», *Вісник інженерної академії України*, №3, с. 145-152, 2018.

5. Котелянець В.В., Усик П.С., Кищенко В.В., Гнатюк В.О., «Інтелектуалізована система моніторингу параметрів навколишнього середовища на базі технології інтернету речей», *Вісник інженерної академії України,* №4, с. 133-140, 2018.

6. Одарченко Р.С., Ткаліч О.П., Дика Н.В., Котелянець В.В. «Дослідження можливостей комунікаційних протоколів для потреб IoT», *Проблеми інформатизації та управління,* Том 3, № 59, с. 43-55, 2017.

7. Котелянець В.В., «Розробка і дослідження програмно-технічного комплексу моніторингу параметрів навколишнього середовища реального часу», *збірник матеріалів IV міжнародної наук.-практ. конференції «Актуальні питання забезпечення кібербезпеки та захисту інформації»,* 21-24 лютого 2018 р., с. Верхній Студений: Видавництво Європейського університету, с. 26-28, 2018.

ВИСНОВКИ

Результатом виконаної роботи є розв'язання актуальної й важливої науково-технічної задачі розроблення стохастичної інформаційної технології моніторингу параметрів навколишнього середовища в сучасній концепції Інтернету речей з урахуванням апріорної невизначеності джерел інформації та можливості виникнення кризових ситуацій.

У процесі виконання дисертаційної роботи було отримано такі вагомі наукові і практичні результати:

1. Проведено аналіз принципів побудови, технологічних рішень і напрямів розвитку систем моніторингу в концепції IoT, у результаті чого виявлено недоліки відомих підходів і доведено необхідність створення математичних моделей, методів, комунікаційних протоколів мереж WSN з випадковим доступом і відповідних інформаційних технологій моніторингу для забезпечення високої продуктивності, якості і живучості їх функціонування.

2. Удосконалено стохастичні моделі функціонування бездротових сенсорних мереж, які використовують рандомізовані мережеві параметри (зі змінною кількістю вузлів і випадковою участю вузлів в окремих групах мережевих вузлів), що дозволило оцінити ймовірність колізії сигналів і більш ефективно проектувати протоколи комунікації IoT. Зазначені моделі дозволили оцінити ймовірність колізії сигналів: максимальна кількість вузлів, які забезпечують якість передавання на рівні ймовірності колізії не вище 10^{-2}, становить 50 шт., причому кількість задіяних в колізії вузлів нехтовно мала в порівнянні з середньою кількістю передавань, зокрема відношення середньої кількості задіяних в колізії вузлів до середньої кількості передавань становить 10^{-7}.

3. Удосконалено метод моніторингу параметрів навколишнього середовища, який враховує нестаціонарну просторово-часову локалізацію первинних джерел вимірювань та оптимізацію процесу динамічного моніторингу, що дало можливість забезпечити своєчасне та оперативне

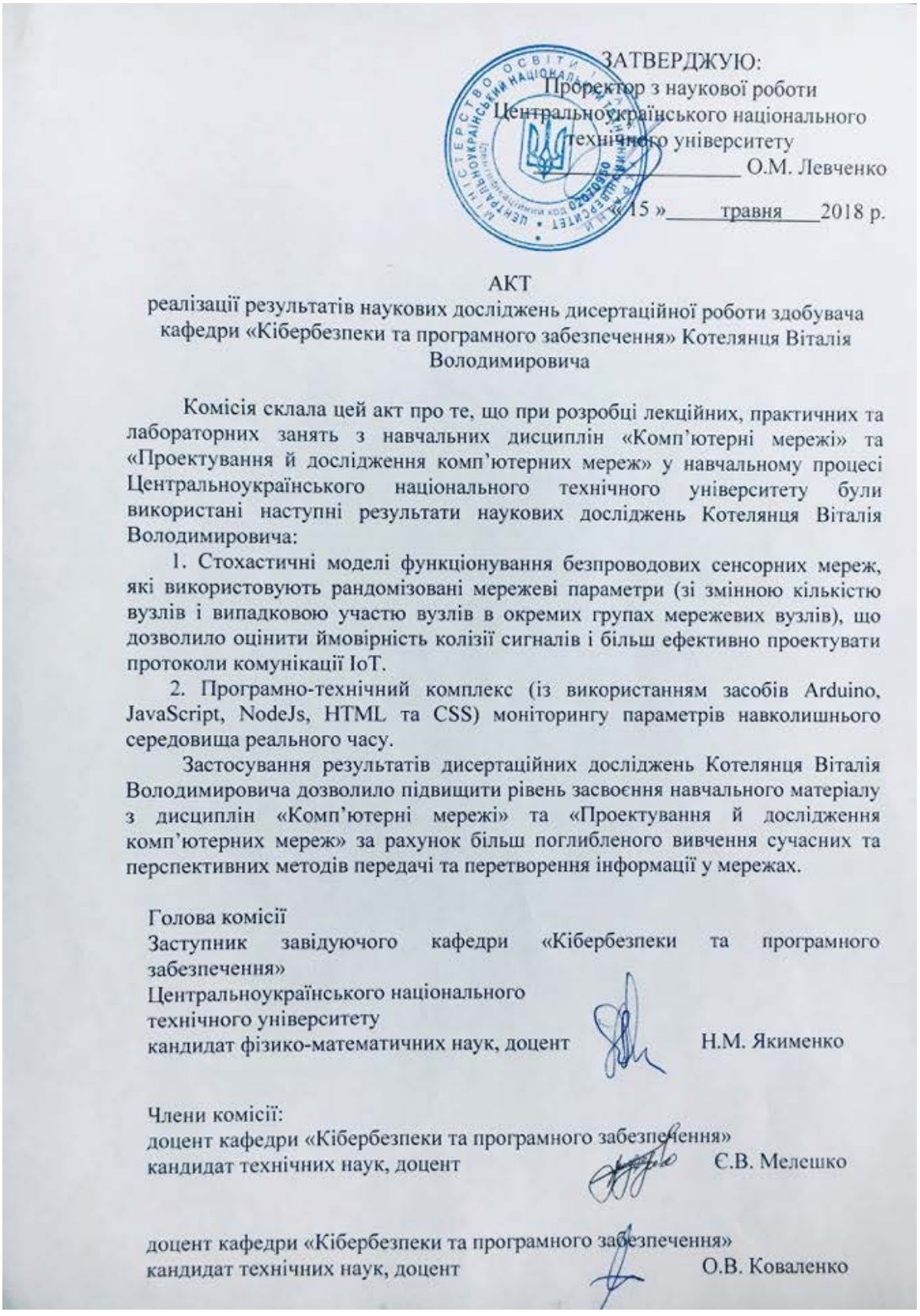
надходження інформації від первинних джерел інформації із заданими показниками якості для ефективного прийняття управлінських рішень.

4. Отримала подальший розвиток інформаційна технологія моніторингу, яка за рахунок використання стохастичних моделей функціонування бездротових сенсорних мереж та удосконаленого методу моніторингу, дозволила забезпечити ефективне спостереження і контроль параметрів навколишнього середовища. Ця технологія із використанням засобів Arduino, JavaScript, NodeJs, HTML та CSS дала можливість розробити відповідний ПТК моніторингу реального часу в сучасній концепції IoT. Зазначений ПТК може використовуватись як прототип для організації моніторингу в динамічно змінюваних середовищах та при виникненні критичних ситуацій різного характеру.

5. Проведено експериментальне дослідження запропонованих моделей, методу та інформаційної технології моніторингу. Розроблено спеціалізовані UML-діаграми прецидентів моделювання та послідовності моделювання запропонованої інформаційної технології. Результати дисертації використані та впроваджені в Національному авіаційному університеті, Центрально-українському національному технічному університеті та телекомунікаційній компанії Local Students Networks.

Додаток А

Відомості щодо впровадження результатів дисертації (1)



ЗАТВЕРДЖУЮ:
Проректор з наукової роботи
Центральноукраїнського національного
технічного університету
_____ О.М. Левченко
«15 » травня 2018 р.

АКТ
реалізації результатів наукових досліджень дисертаційної роботи здобувача кафедри «Кібербезпеки та програмного забезпечення» Котелянця Віталія Володимировича

Комісія склала цей акт про те, що при розробці лекційних, практичних та лабораторних занять з навчальних дисциплін «Комп'ютерні мережі» та «Проектування й дослідження комп'ютерних мереж» у навчальному процесі Центральноукраїнського національного технічного університету були використані наступні результати наукових досліджень Котелянця Віталія Володимировича:

1. Стохастичні моделі функціонування безпроводових сенсорних мереж, які використовують рандомізовані мережеві параметри (зі змінною кількістю вузлів і випадковою участю вузлів в окремих групах мережевих вузлів), що дозволило оцінити ймовірність колізії сигналів і більш ефективно проектувати протоколи комунікації IoT.
2. Програмно-технічний комплекс (із використанням засобів Arduino, JavaScript, NodeJs, HTML та CSS) моніторингу параметрів навколишнього середовища реального часу.

Застосування результатів дисертаційних досліджень Котелянця Віталія Володимировича дозволило підвищити рівень засвоєння навчального матеріалу з дисциплін «Комп'ютерні мережі» та «Проектування й дослідження комп'ютерних мереж» за рахунок більш поглибленого вивчення сучасних та перспективних методів передачі та перетворення інформації у мережах.

Голова комісії
Заступник завідуючого кафедри «Кібербезпеки та програмного забезпечення»
Центральноукраїнського національного
технічного університету
кандидат фізико-математичних наук, доцент Н.М. Якименко

Члени комісії:
доцент кафедри «Кібербезпеки та програмного забезпечення»
кандидат технічних наук, доцент Є.В. Мелешко

доцент кафедри «Кібербезпеки та програмного забезпечення»
кандидат технічних наук, доцент О.В. Коваленко

Додаток А (продовження)

Відомості щодо впровадження результатів дисертації (2)

ПАВУТИНА
ІНТЕРНЕТ ОПЕРАТОР
www.pautina.ua

LOCAL STUDENT NETWORKS
www.lsn.net.ua

ТОВ " Павутина.NET"
02068, Україна, м.Київ
вул. О. Кошиця, 9Б
03058,Україна, м. Київ,
вул. Лебедєва-Кумача, 7в
тел./факс +38 (044) 206-36-37

АКТ ВПРОВАДЖЕННЯ
результатів дисертаційного дослідження
Котелянця Віталія Володимировича

У діяльності мережі «Local Student Networks» ТОВ «ПАВУТИНА. НЕТ» впроваджено і використовуються такі наукові і практичні результати здобувача В. Котелянця:

1. Удосконалений метод моніторингу параметрів навколишнього середовища, який враховує нестаціонарну просторово-часову локалізацію первинних джерел вимірювань та оптимізацію процесу динамічного моніторингу. Цей метод дав можливість забезпечити своєчасне та оперативне надходження інформації від первинних джерел інформації із заданими показниками якості для ефективного прийняття управлінських рішень.

2. Інформаційна технологія моніторингу, яка за рахунок використання стохастичних моделей функціонування бездротових сенсорних мереж та удосконаленого методу моніторингу, дозволила забезпечити ефективне спостереження і контроль параметрів навколишнього середовища. Ця технологія із використанням засобів Arduino, JavaScript, NodeJs, HTML та CSS дала можливість розробити відповідний комплекс моніторингу реального часу в сучасній концепції IoT.

29 вересня 2018 року

Директор
ТОВ «ПАВУТИНА. НЕТ» Арутюнян О. В.

Відомості щодо впровадження результатів дисертації (3)

ЗАТВЕРДЖУЮ
Проректор з наукової роботи
Національного авіаційного університету
_____ В. Харченко
«07» листопада 2018 р.

АКТ
впровадження результатів дисертаційної роботи
Котелянця Віталія Володимировича за темою «Інформаційна технологія моніторингу навколишнього середовища на базі концепції Інтернету речей» у навчальний процес Національного авіаційного університету

Комісія у складі: голова – завідувач кафедри безпеки інформаційних технологій (БІТ) Олександр Григорович Корченко, професор кафедри БІТ Сергій Олександрович Гнатюк та доцент кафедри БІТ Василь Миколайович Кінзерявий склали цей акт про те, що результати дисертаційної роботи Котелянця В.В. за темою «Інформаційна технологія моніторингу навколишнього середовища на базі концепції Інтернету речей» впроваджені у навчальний процес та використовувались на кафедрі БІТ у 2017-2018 н.р. при викладанні дисципліни «Безпека інформації в інформаційно-комунікаційних системах».

№ з/п	Назва роботи, що впроваджується	Форма впровадження	Ефективність від впровадження
	1	2	3
1.	Побудова бездротових комунікацій на базі IoT	Лекція	Ознайомлення студентів з принципами побудови, технологічними рішеннями і протоколами концепції IoT
2.	Інструментарій для забезпечення роботи бездротових систем IoT	Лекція	Ознайомлення студентів з можливістю використання в IoT сучасних засобів Arduino, Java Script, NodeJs, HTML та CSS

Голова комісії
завідувач кафедрою безпеки
інформаційних технологій, д.т.н., професор О. Корченко

Члени комісії:
професор кафедри безпеки
інформаційних технологій, д.т.н., доцент С. Гнатюк

доцент кафедри безпеки
інформаційних технологій, к.т.н. В. Кінзерявий

Додаток Б

Результати вимірювань, отримані в процесі верифікації запропонованого ПТК

У четвертому розділі дисертації проведені дослідження розробленого ПТК моніторингу реального часу в сучасній концепції IoT із використанням засобів Arduino, JavaScript, NodeJs, HTML та CSS. Результати дослідження (табл. Б.1) підтвердили можливість застосування ПТК як прототипу для організації моніторингу в динамічно змінюваних середовищах та при виникненні критичних ситуацій різного характеру.

Таблиця Б.1

Зведені дані моніторингу параметрів навколишнього середовища протягом 21.08-23.08.2018 року

Час *год.*	Температура *°C*	Вологість *%*	Примітки
21 серпня 2018 року			
02:00 AM	17,1	78	
	16,8	78	
	16,8	78	
	16,7	78	
	16,6	77	
	16,5	77	
03:00 AM	16,3	77	
	16,2	77	
	16,2	77	
	16,1	76	*добовий мінімум*
	16,1	76	
	16,2	76	
	16,2	76	
	16,2	76	
	16,2	76	
04:00 AM	16,3	76	

	16,3	75	
	16,3	75	
	16,3	75	
	16,3	75	
	16,3	75	
	16,4	75	
	16,4	75	
	16,4	74	
	16,4	74	
05:00 AM	16,4	74	
	16,5	74	
	16,5	74	
	16,6	74	
	16,6	74	
	16,7	73	
	16,7	73	
	16,8	73	
	16,8	73	
	16,8	73	
	16,8	73	
	16,8	73	
06:00 AM	16,9	72	
	16,9	72	
	16,9	72	
	16,9	72	
	16,9	72	
	16,9	72	
	17,0	72	
	17,0	72	
	17,1	72	
	17,1	72	
	17,2	72	
	17,2	72	
07:00 AM	17,3	72	
	17,4	72	
	17,4	72	
	17,5	72	
	17,5	72	
	17,5	72	
	17,5	72	
	17,6	72	
	17,6	72	

	17,6	73	
	17,6	73	
	17,7	73	
	17,7	73	
	17,7	73	
	17,7	73	
	17,7	73	
	17,8	73	
	17,8	73	
	17,8	73	
	17,8	73	
	17,9	73	
	17,9	73	
08:00 AM	17,9	73	
	17,9	74	
	18,0	74	
	18,0	74	
	18,0	74	
	18,1	74	
	18,1	74	
	18,2	74	
	18,3	74	
	18,3	74	
	18,4	74	
	18,4	74	
	18,5	74	
	18,5	74	
	18,5	74	
	18,5	74	
	18,6	75	
	18,6	75	
	18,6	75	
09:00 AM	18,6	75	
	18,6	75	
	18,7	75	
	18,7	75	
	18,7	76	
	18,8	76	
	18,8	76	
	18,8	76	
	18,8	76	
	18,8	76	

	18,9	76	
	18,9	76	
	18,9	76	
	18,9	76	
	18,9	76	
	19,0	76	
10:00 AM	19,0	77	
	19,1	77	
	19,1	77	
	19,1	77	
	19,2	77	
	19,2	77	
	19,2	77	
	19,2	77	
	19,3	77	
	19,3	77	
	19,3	77	
	19,4	77	
	19,4	77	
	19,4	77	
	19,4	76	
	19,4	76	
	19,5	76	
	19,5	76	
	19,5	76	
	19,5	76	
	19,6	76	
	19,6	76	
	19,6	76	
	19,6	76	
	19,6	76	
	19,6	76	
	19,7	76	
	19,7	76	
	19,7	76	
	19,7	76	
	19,8	76	
	19,8	76	
	19,8	76	
	19,8	75	
	19,8	75	
	19,9	75	

	19,9	75	
	19,9	75	
	19,9	75	
11:00 AM	19,9	75	
	20,0	75	
	20,1	75	
	20,1	75	
	20,2	75	
	20,2	75	
	20,2	75	
	20,2	75	
	20,2	75	
	20,2	75	
	20,2	75	
	20,2	75	
	20,3	75	
	20,3	75	
	20,3	75	
	20,3	75	
	20,4	75	
	20,4	75	
	20,4	75	
	20,4	75	
	20,4	75	
	20,4	75	
	20,4	75	
	20,5	75	
	20,5	75	
	20,5	75	
	20,6	75	
	20,6	75	
	20,7	75	
	20,7	75	
	20,7	75	
	20,8	75	
	20,8	75	
	20,8	75	
	20,8	75	
	20,9	75	
	20,9	75	
	20,9	75	
	21,0	75	
	21,1	75	

12:00 PM	21,1	75	
	21,1	75	
	21,2	75	
	21,2	75	
	21,3	75	
	21,3	74	
	21,4	74	
	21,4	74	
	21,4	74	
	21,5	74	
	21,5	74	
	21,5	74	
	21,5	74	
	21,6	74	
	21,6	74	
	21,6	74	
01:00 PM	21,6	74	
	21,7	74	
	21,7	74	
	21,7	74	
	21,8	74	
	21,8	74	
	21,8	74	
	21,8	74	
	21,8	74	
	21,9	73	
	21,9	73	
	21,9	73	
	21,9	73	
	22,1	73	
	22,2	73	
	22,3	73	
	22,3	73	
	22,4	73	
	22,4	73	
	22,5	73	
	22,5	73	
	22,6	73	
	22,6	73	
02:00 PM	22,6	73	
	22,6	73	
	22,7	72	

	22,7	72	
	22,7	72	
	22,7	72	
	22,7	72	
	22,8	72	
	22,8	72	
	22,8	72	
	22,8	72	
	22,8	72	
	22,8	72	
	22,9	72	
	22,9	72	
	22,9	72	
	22,9	72	
	22,9	71	
	22,9	71	
	23,1	71	
	23,2	71	
	23,3	71	
03:00 PM	23,3	71	
	23,4	71	
	23,4	71	
	23,4	71	
	23,5	71	
	23,5	71	
	23,5	71	
	23,5	71	
	23,6	71	
	23,6	71	
	23,6	71	
	23,6	71	
04:00 PM	23,7	71	
	23,7	71	
	23,7	70	
	23,7	70	
	23,7	70	
	23,7	70	
	23,7	70	
	23,8	70	
	23,8	70	
	23,8	70	
	23,8	70	

	23,9	70	
	23,9	70	
	24,0	70	
	24,1	70	
	24,2	70	
	24,2	70	
	24,2	70	
05:00 PM	24,3	70	
	24,3	70	
	24,3	70	
	24,4	70	
	24,4	70	
	24,4	70	
	24,4	70	
	24,4	70	
	24,4	70	
	24,4	70	
	24,4	70	
	24,4	70	
	24,4	70	
	24,4	70	
	24,4	70	
	24,4	70	
	24,4	70	
	24,4	70	
	24,4	70	
	24,4	70	
	24,4	70	
	24,4	70	
06:00 PM	24,5	70	
	24,5	70	
	24,5	70	
	24,5	70	
	24,5	70	
	24,5	70	
	24,5	70	
	24,6	70	
	24,6	70	
	24,6	70	
	24,6	70	
	24,7	70	
	24,7	70	
	24,7	70	
	24,7	70	
	24,7	70	

	24,7	69	
	24,7	69	
	24,8	69	
	24,8	69	
	24,8	69	
	24,8	69	
	24,8	69	
	24,8	69	
	24,8	69	
	24,8	69	
	24,8	69	
	24,9	69	
	24,9	69	
	24,9	69	
	24,9	69	
	24,9	69	
	25,0	69	
	25,0	68	
	25,1	68	
	25,1	68	
	25,1	68	
	25,2	68	
	25,2	68	
	25,2	68	
	25,3	68	
	25,3	68	
	25,4	68	
	25,4	68	
	25,4	68	
	25,4	68	
	25,4	68	
	25,5	68	
	25,5	68	
	25,5	68	
	25,5	68	
	25,5	68	
	25,5	68	
	25,6	68	
	25,6	68	
	25,6	68	
	25,6	68	
	25,6	68	
	25,6	68	

07:00 PM	25,7	68	
	25,7	68	
	25,7	68	
	25,7	68	
	25,7	68	
	25,8	68	
	25,8	67	
	25,8	67	
	25,8	67	
	25,8	67	
	25,8	67	
	25,9	67	*добовий максимум*
	25,9	67	
	25,9	67	
	25,8	67	
	25,8	67	
	25,7	67	
	25,7	67	
	25,7	67	
	25,6	67	
	25,6	67	
	25,6	67	
	25,6	67	
	25,6	67	
	25,6	67	
	25,5	67	
	25,5	67	
	25,5	67	
	25,5	67	
	25,5	67	
	25,5	67	
	25,4	67	
	25,4	67	
	25,4	67	
	25,4	67	
	25,4	67	
	25,3	66	
	25,2	66	
	25,2	66	
	25,1	66	
	25,1	66	
08:00 PM	25,1	66	

	25,0	66	
	25,0	66	
	24,9	66	
	24,9	67	
	24,8	67	
	24,8	67	
	24,8	67	
	24,8	67	
	24,7	67	
	24,7	67	
	24,7	67	
	24,7	67	
	24,6	67	
	24,5	68	
	24,5	68	
	24,4	68	
	24,4	68	
	24,4	68	
	24,4	68	
	24,4	68	
	24,3	68	
	24,3	68	
	24,3	68	
	24,2	68	
	24,2	68	
	24,2	68	
	23,9	68	
	23,9	69	
09:00 PM	23,8	69	
	23,8	69	
	23,7	69	
	23,7	69	
	23,6	69	
	23,6	69	
	23,5	69	
	23,5	69	
	23,4	69	
	23,4	69	
	23,3	69	
	22,8	69	
	22,7	69	
	22,7	69	

	22,7	69	
	22,7	69	
	22,6	69	
	22,6	69	
	22,4	69	
	22,1	69	
	21,9	69	
10:00 PM	21,9	70	
	21,9	70	
	21,9	70	
	21,8	70	
	21,8	70	
	21,8	70	
	21,7	70	
	21,6	70	
	21,6	70	
	21,6	70	
	21,5	71	
	21,4	71	
	21,4	71	
11:00 PM	21,4	71	
	21,3	71	
	21,3	71	
	21,2	71	
	21,2	71	
	21,1	71	
	20,9	71	
	20,9	71	
	20,9	71	
	20,8	71	
	20,8	71	
	20,8	71	
	20,8	71	
	20,7	71	
	20,5	71	
	20,5	71	
	20,4	71	
	20,3	71	
	20,3	71	
	20,2	71	
	20,2	72	
	20,2	72	

	20,1	72	
	20,1	72	
	20,0	72	
	19,9	72	
	19,9	72	
22 серпня 2018 року			
12:00 AM	19,9	73	
	19,8	73	
	19,8	73	
	19,8	73	
	19,7	73	
	19,6	73	
	19,6	73	
	19,5	73	
	19,4	73	
	19,4	73	
	19,3	74	
	19,3	74	
	19,2	74	
	19,2	74	
	19,1	74	
	19,1	74	
	19,0	74	
	19,0	74	
	18,9	74	
	18,8	74	
01:00 AM	18,8	74	
	18,7	74	
	18,7	74	
	18,6	74	
	18,6	74	
	18,6	74	
	18,6	74	
	18,5	74	
	18,5	74	
	18,5	74	
	18,4	75	
	18,4	75	
	18,3	75	
	18,3	75	

	18,2	75	
	18,0	75	
	18,0	75	
	17,9	75	
	17,9	75	
	17,9	75	
	17,9	75	
	17,8	75	
	17,8	75	
	17,7	76	
	17,7	76	
	17,6	76	
	17,6	76	
	17,5	76	
	17,5	76	
	17,5	76	
	17,4	76	
	17,4	76	
02:00 AM	17,3	76	
	17,2	76	
	17,2	76	
	17,1	76	
	17,1	76	
	17,0	76	
	16,5	77	
	16,5	77	
	16,4	77	
	16,3	76	
	16,3	76	
03:00 AM	16,2	76	
	16,2	76	
	16,1	76	
	16,0	76	*добовий мінімум*
	16,1	76	
	16,1	75	
	16,1	75	
04:00 AM	16,2	75	
	16,2	75	
	16,3	75	
	16,3	75	
	16,3	75	
	16,4	74	

	16,4	74	
	16,4	74	
	16,5	74	
	16,5	74	
	16,6	74	
05:00 AM	16,6	74	
	16,7	73	
	16,7	73	
	16,8	73	
	16,8	73	
	16,8	73	
	16,8	73	
	16,8	73	
	16,9	72	
	16,9	72	
	16,9	72	
	16,9	72	
	16,9	72	
	16,9	72	
	17,0	72	
06:00 AM	17,0	72	
	17,1	72	
	17,1	72	
	17,2	72	
	17,2	72	
	17,3	72	
	17,4	72	
	17,4	72	
	17,5	72	
	17,5	72	
	17,5	72	
	17,5	72	
	17,6	72	
	17,6	72	
	17,6	73	
	17,6	73	
	17,7	73	
07:00 AM	17,7	73	
	17,7	73	
	17,7	73	
	17,7	73	
	17,8	73	

	17,8	73	
	17,8	73	
	17,8	73	
	17,9	73	
	17,9	73	
	17,9	73	
	17,9	74	
	18,0	74	
	18,0	74	
	18,0	74	
	18,1	74	
	18,1	74	
	18,2	74	
	18,3	74	
	18,3	74	
08:00 AM	18,4	74	
	18,4	74	
	18,5	74	
	18,5	74	
	18,5	74	
	18,5	74	
	18,6	75	
	18,6	75	
	18,6	75	
	18,6	75	
	18,6	75	
	18,7	75	
	18,7	75	
	18,7	76	
	18,8	76	
	18,8	76	
	18,8	76	
09:00 AM	18,8	76	
	18,8	76	
	18,9	76	
	18,9	76	
	18,9	76	
	18,9	76	
	18,9	76	
	19,0	76	
	19,0	77	
	19,1	77	

	19,1	77	
	19,1	77	
	19,2	77	
	19,2	77	
	19,2	77	
	19,2	77	
	19,3	77	
	19,3	77	
	19,3	77	
10:00 AM	19,4	77	
	19,4	77	
	19,4	77	
	19,4	76	
	19,4	76	
	19,5	76	
	19,5	76	
	19,5	76	
	19,5	76	
	19,6	76	
	19,6	76	
	19,6	76	
	19,6	76	
	19,6	76	
	19,6	76	
	19,6	76	
	19,7	76	
	19,7	76	
	19,7	76	
	19,7	76	
	19,8	76	
	19,8	76	
	19,8	76	
	19,8	75	
	19,8	75	
11:00 AM	19,9	75	
	19,9	75	
	19,9	75	
	19,9	75	
	19,9	75	
	20,0	75	
	20,1	75	
	20,1	75	
	20,2	75	

	20,2	75	
	20,2	75	
	20,2	75	
	20,2	75	
	20,2	75	
	20,2	75	
	20,3	75	
	20,3	75	
	20,3	75	
	20,3	75	
	20,4	75	
	20,4	75	
	20,4	75	
	20,4	75	
	20,4	75	
	20,4	75	
	20,4	75	
	20,4	75	
	20,5	75	
	20,5	75	
	20,5	75	
	20,6	75	
	20,6	75	
	20,7	75	
	20,7	75	
	20,7	75	
	20,8	75	
	20,8	75	
	20,8	75	
	20,8	75	
12:00 PM	20,9	75	
	20,9	75	
	20,9	75	
	21,0	75	
	21,1	75	
	21,1	75	
	21,1	75	
	21,2	75	
	21,2	75	
	21,3	75	
	21,3	74	
	21,4	74	
	21,4	74	

	21,4	74	
	21,5	74	
	21,5	74	
	21,5	74	
	21,5	74	
	21,6	74	
	21,6	74	
	21,6	74	
	21,6	74	
	21,7	74	
	21,7	74	
	21,7	74	
	21,8	74	
01:00 PM	21,8	74	
	21,8	74	
	21,8	74	
	21,8	74	
	21,9	73	
	21,9	73	
	21,9	73	
	21,9	73	
	22,1	73	
	22,2	73	
	22,3	73	
	22,3	73	
02:00 PM	22,4	73	
	22,4	73	
	22,5	73	
	22,5	73	
	22,6	73	
	22,6	73	
	22,6	73	
	22,6	73	
	22,7	72	
	22,7	72	
	22,7	72	
	22,7	72	
	22,7	72	
	22,8	72	
	22,8	72	
	22,8	72	
	22,8	72	

	22,8	72	
	22,8	72	
	22,9	72	
	22,9	72	
03:00 PM	22,9	72	
	22,9	72	
	22,9	71	
	22,9	71	
	23,1	71	
	23,2	71	
	23,3	71	
	23,3	71	
	23,4	71	
	23,4	71	
	23,4	71	
	23,5	71	
	23,5	71	
04:00 PM	23,5	71	
	23,5	71	
	23,6	71	
	23,6	71	
	23,6	71	
	23,6	71	
	23,7	71	
	23,7	71	
	23,7	70	
	23,7	70	
	23,7	70	
	23,7	70	
	23,7	70	
	23,8	70	
	23,8	70	
	23,8	70	
	23,8	70	
	23,9	70	
	23,9	70	
	24,0	70	
05:00 PM	24,1	70	
	24,2	70	
	24,2	70	
	24,2	70	
	24,3	70	

	24,3	70	
	24,3	70	
	24,4	70	
	24,4	70	
	24,4	70	
	24,4	70	
	24,4	70	
	24,4	70	
	24,4	70	
	24,4	70	
	24,4	70	
	24,4	70	
	24,4	70	
	24,4	70	
	24,4	70	
	24,4	70	
	24,4	70	
	24,4	70	
	24,4	70	
	24,4	70	
	24,5	70	
	24,5	70	
	24,5	70	
	24,5	70	
	24,5	70	
	24,5	70	
	24,5	70	
	24,6	70	
	24,6	70	
	24,6	70	
	24,6	70	
	24,7	70	
	24,7	70	
	24,7	70	
	24,7	70	
	24,7	70	
	24,7	69	
	24,7	69	
	24,8	69	
	24,8	69	
	24,8	69	
	24,8	69	
	24,8	69	
	24,8	69	

	24,8	69	
	24,8	69	
	24,9	69	
	24,9	69	
	24,9	69	
	24,9	69	
	24,9	69	
	25,0	69	
	25,0	68	
	25,1	68	
	25,1	68	
	25,1	68	
	25,2	68	
	25,2	68	
	25,2	68	
	25,3	68	
	25,3	68	
	25,4	68	
	25,4	68	
	25,4	68	
	25,4	68	
	25,4	68	
	25,5	68	
	25,5	68	
	25,5	68	
	25,5	68	
06:00 PM	25,5	68	
	25,5	68	
	25,6	68	
	25,6	68	
	25,6	68	
	25,6	68	
	25,6	68	
	25,6	68	
	25,7	68	
	25,7	68	
	25,7	68	
	25,7	68	
	25,7	68	
	25,8	68	
	25,8	67	
	25,8	67	

	25,8	67	
	25,8	67	
	25,8	67	
	25,9	67	
	26,1	67	*добовий максимум*
	26,1	67	
	26,1	67	
	25,8	67	
	25,7	67	
	25,7	67	
	25,7	67	
	25,6	67	
	25,6	67	
	25,6	67	
	25,6	67	
	25,6	67	
	25,6	67	
	25,5	67	
	25,5	67	
	25,5	67	
	25,5	67	
	25,5	67	
	25,5	67	
07:00 PM	25,4	67	
	25,4	67	
	25,4	67	
	25,4	67	
	25,4	67	
	25,3	66	
	25,2	66	
	25,2	66	
	25,1	66	
	25,1	66	
	25,1	66	
	25,0	66	
	25,0	66	
	24,9	66	
	24,9	67	
	24,8	67	
	24,8	67	
	24,8	67	
	24,8	67	

	24,7	67	
	24,7	67	
08:00 PM	24,7	67	
	24,7	67	
	24,6	67	
	24,5	68	
	24,5	68	
	24,4	68	
	24,4	68	
	24,4	68	
	24,4	68	
	24,4	68	
	24,3	68	
	24,3	68	
	24,3	68	
	24,2	68	
	24,2	68	
	24,2	68	
	23,9	68	
	23,9	69	
09:00 PM	23,8	69	
	23,8	69	
	23,7	69	
	23,7	69	
	23,6	69	
	23,6	69	
	23,5	69	
	23,5	69	
	23,4	69	
	23,4	69	
	23,3	69	
	22,8	69	
	22,7	69	
	22,7	69	
	22,7	69	
10:00 PM	22,7	69	
	22,6	69	
	22,6	69	
	22,4	69	
	22,1	69	
	21,9	69	
	21,9	70	

	21,9	70	
	21,9	70	
	21,8	70	
	21,8	70	
	21,8	70	
	21,7	70	
	21,6	70	
11:00 PM	21,6	70	
	21,6	70	
	21,5	71	
	21,4	71	
	21,4	71	
	21,4	71	
	21,3	71	
	21,3	71	
	21,2	71	
	21,2	71	
	21,1	71	
	20,9	71	
	20,9	71	
	20,9	71	
	20,8	71	
	20,8	71	
	20,8	71	
	20,8	71	
	20,7	71	
	20,5	71	
	20,5	71	
	20,4	71	
	20,3	71	
	20,3	71	
	20,2	71	
	20,2	72	
	20,2	72	
	20,1	72	
	20,1	72	
	20,0	72	
	20,0	72	
	20,0	72	
23 серпня 2018 року			

12:00 AM	20,0	73	
	20,0	73	
	19,9	73	
	19,9	73	
	19,7	73	
	19,6	73	
	19,6	73	
	19,5	73	
	19,4	73	
	19,4	73	
	19,3	74	
	19,3	74	
	19,2	74	
	19,2	74	
	19,1	74	
	19,1	74	
	19,0	74	
	19,0	74	
	18,9	74	
	18,8	74	
01:00 AM	18,8	74	
	18,7	74	
	18,7	74	
	18,6	74	
	18,6	74	
	18,6	74	
	18,6	74	
	18,5	74	
	18,5	74	
	18,5	74	
	18,4	75	
	18,4	75	
	18,3	75	
	18,3	75	
	18,2	75	
	18,0	75	
	18,0	75	
	17,9	75	
	17,9	75	
	17,9	75	
	17,9	75	
	17,8	75	

	17,8	75	
	17,7	76	
	17,7	76	
	17,6	76	
	17,6	76	
	17,5	76	
	17,5	76	
	17,5	76	
	17,4	76	
	17,4	76	
02:00 AM	17,3	76	
	17,2	76	
	17,2	76	
	17,1	76	
	17,1	76	
	17,0	76	
03:00 AM	17,0	77	
	17,0	77	
	17,0	77	
	17,0	76	
	16,8	76	
	16,8	76	
	16,8	76	
	16,7	76	
	16,6	76	
04:00 AM	16,6	76	
	16,6	75	
	16,6	75	
	16,5	75	
	16,5	75	
	16,5	75	
	16,5	75	
	16,4	75	*добовий мінімум*
	16,4	74	
	16,4	74	
05:00 AM	16,4	74	
	16,5	74	
	16,5	74	
	16,6	74	
	16,6	74	
	16,7	73	
	16,7	73	

	16,8	73	
	16,8	73	
	16,8	73	
	16,8	73	
	16,8	73	
06:00 AM	16,9	72	
	16,9	72	
	16,9	72	
	16,9	72	
	16,9	72	
	16,9	72	
	17,0	72	
	17,0	72	
	17,1	72	
	17,1	72	
	17,2	72	
	17,2	72	
07:00 AM	17,3	72	
	17,4	72	
	17,4	72	
	17,5	72	
	17,5	72	
	17,5	72	
	17,5	72	
	17,6	72	
	17,6	72	
	17,6	73	
	17,6	73	
	17,7	73	
	17,7	73	
	17,7	73	
	17,7	73	
	17,7	73	
	17,8	73	
	17,8	73	
	17,8	73	
	17,8	73	
	17,9	73	
	17,9	73	
08:00 AM	17,9	73	
	17,9	74	
	18,0	74	

	18,0	74	
	18,0	74	
	18,1	74	
	18,1	74	
	18,2	74	
	18,3	74	
	18,3	74	
	18,4	74	
	18,4	74	
	18,5	74	
	18,5	74	
	18,5	74	
	18,5	74	
	18,6	75	
	18,6	75	
	18,6	75	
09:00 AM	18,6	75	
	18,6	75	
	18,7	75	
	18,7	75	
	18,7	76	
	18,8	76	
	18,8	76	
	18,8	76	
	18,8	76	
	18,8	76	
	18,9	76	
	18,9	76	
	18,9	76	
	18,9	76	
	18,9	76	
	19,0	76	
10:00 AM	19,0	77	
	19,1	77	
	19,1	77	
	19,1	77	
	19,2	77	
	19,2	77	
	19,2	77	
	19,2	77	
	19,3	77	
	19,3	77	

	19,3	77	
	19,4	77	
	19,4	77	
	19,4	77	
	19,4	76	
	19,4	76	
	19,5	76	
	19,5	76	
	19,5	76	
	19,5	76	
	19,6	76	
	19,6	76	
	19,6	76	
	19,6	76	
	19,6	76	
	19,6	76	
	19,7	76	
	19,7	76	
	19,7	76	
	19,7	76	
	19,8	76	
	19,8	76	
	19,8	76	
	19,8	75	
	19,8	75	
	19,9	75	
	19,9	75	
	19,9	75	
	19,9	75	
11:00 AM	19,9	75	
	20,0	75	
	20,1	75	
	20,1	75	
	20,2	75	
	20,2	75	
	20,2	75	
	20,2	75	
	20,2	75	
	20,2	75	
	20,2	75	
	20,3	75	
	20,3	75	

	20,3	75	
	20,3	75	
	20,4	75	
	20,4	75	
	20,4	75	
	20,4	75	
	20,4	75	
	20,4	75	
	20,4	75	
	20,4	75	
	20,5	75	
	20,5	75	
	20,5	75	
	20,6	75	
	20,6	75	
	20,7	75	
	20,7	75	
	20,7	75	
	20,8	75	
	20,8	75	
	20,8	75	
	20,8	75	
	20,9	75	
	20,9	75	
	20,9	75	
	21,0	75	
	21,1	75	
12:00 PM	21,1	75	
	21,1	75	
	21,2	75	
	21,2	75	
	21,3	75	
	21,3	74	
	21,4	74	
	21,4	74	
	21,4	74	
	21,5	74	
	21,5	74	
	21,5	74	
	21,5	74	
	21,6	74	
	21,6	74	
	21,6	74	

01:00 PM	21,6	74	
	21,7	74	
	21,7	73	
	21,8	73	
	21,8	73	
	21,9	73	