BULLETIN of Cherkasy State Technological University

Journal homepage: https://bulletin-chstu.com.ua/en Vol. 30 No. 3. 2025

UDC 621.395.7
DOI: 10.62660/bcstu/3.2025.37

A method for detecting DDoS attacks in VoIP systems based on machine learning

Viktor Gnatyuk*
PhD in Technical Sciences, Associate Professor
State University "Kyiv Aviation Institute"
03058, 1 Lyubomyra Huzara Ave., Kyiv, Ukraine
The State Scientific and Research Institute of Cybersecurity Technologies and Information Protection
03142, 3 Maksyma Zaliznyaka Str., Kyiv, Ukraine
https://orcid.org/0000-0002-4916-7149

Ivan Gorbachov
Postgraduate Student
State University "Kyiv Aviation Institute"
03058, 1 Lyubomyra Huzara Ave., Kyiv, Ukraine
https://orcid.org/0009-0002-9688-1692

Abstract. Protecting VoIP systems from DDoS attacks is a critical issue, as such attacks can lead to significant financial losses and a decline in the quality of service for users. Existing methods of detecting attacks are based on signature analysis or traditional rules, which limits their effectiveness in cases of new or modified attacks. The aim of this work was to develop a method for detecting DDoS attacks in VoIP systems based on machine learning, which provides high accuracy in classifying abnormal traffic. To achieve this goal, methods of network traffic analysis, machine learning, and statistical evaluation of model effectiveness were used. The main research tool was a multilayer perceptron neural network trained on real network traffic. As a result of this research, a model was developed and tested that demonstrated high accuracy in detecting attacks. A comparative analysis of the effectiveness of the developed model with other approaches was carried out. The proposed method was integrated into the Asterisk environment through the Asterisk Manager Interface, which made it possible to monitor SIP traffic in real time, analyse it using a trained model, and automatically block attacking IP addresses through IPTables or Fail2Ban. Based on the results of the model comparison by metrics, the best model was selected and an algorithm for protecting VoIP from DDoS was developed based on it. The practical value of the work lies in the development of an effective method for protecting VoIP systems, which can be used to improve the level of security in telecommunications networks. The proposed approach can be scaled and adapted to different network infrastructure configurations

Keywords: IP telephony; SIP; Asterisk; neural network; cybersecurity

INTRODUCTION

Distributed Denial of Service (DDoS) attacks have become one of the most pervasive threats to modern networks, particularly in real-time communication systems such as Voice over IP (VoIP) networks. These attacks aim to overwhelm the target system by flooding it with massive amounts of traffic, causing service disruptions, degraded quality, or complete downtime. The growing reliance on VoIP for both personal and business

Article's History: Received: 04.06.2025; Revised: 05.08.2025; Accepted: 15.09.2025.

Suggested Citation:
Gnatyuk, V., & Gorbachov, I. (2025). A method for detecting DDoS attacks in VoIP systems based on machine learning. *Bulletin of Cherkasy State Technological University*, 30(3), 37-46. doi: 10.62660/bcstu/3.2025.37.

*Corresponding author

communication makes DDoS attacks particularly disruptive, as they not only affect the availability of the service but also the quality of communication. Consequently, DDoS detection and mitigation in VoIP systems are critical research areas within the broader field of network security.

Moreover, the integration of deep learning techniques has further advanced the field. A. Hekmati *et al.* (2023) proposed the use of correlation-aware neural networks for DDoS detection in IoT systems, emphasising the importance of capturing the relationships between different network parameters for more accurate detection. This insight has been directly applied in the current study, where various traffic metrics (e.g., packet loss, jitter, and delay) were incorporated into the machine learning model, thereby improving the ability to detect subtle attack patterns in VoIP traffic.

In addition to machine learning, autoencoders have become an important tool for anomaly detection, as highlighted by D. Ilin & I. Starinskyi (2023). Autoencoders are unsupervised learning models that can reconstruct input data and detect anomalies by identifying deviations from the reconstructed patterns. This technique is particularly effective in situations where the attack patterns are not well-defined or previously seen. By incorporating autoencoders into detection model presented in this research, authors plan to improve the detection of new, previously unseen DDoS attacks that do not match typical attack signatures. The work of M. Chornobuk *et al.* (2023) explored the problem of detecting DDoS attacks – specifically SYN flood, ICMP flood, and UDP flood – by reviewing existing machine learning-based methods (neural networks, SVM, decision trees). The researchers proposed their own decision tree-based model, trained it on a public dataset of 104,345 records and 23 features (IP address, port, bytes, etc.), rejected features that could cause overfitting, and performed 5-fold stratified cross-validation; the model demonstrated an average classification accuracy of 0.94 ($\sigma = 0.06$), demonstrating its ability to effectively identify malicious traffic in conditions close to real-world conditions, with the possibility of practical application on network equipment for filtering or alerts.

The application of hybrid deep learning models has proven to be particularly effective in the detection of flooding DDoS attacks, as demonstrated by B. Habib & F. Khurshid (2024). The inclusion of both Long Short-Term Memory (LSTM) networks, which capture temporal dependencies, and Convolutional Neural Networks (CNNs), which can identify spatial paterns in network traffic, offers a promising direction for enhancing the robustness of the detection model in future studies. The use of hybrid LSTM-CNN models to detect time-based DDoS attacks presented an innovative approach that can further be adapted to VoIP systems.

In cybersecurity environment, traditional DDoS detection systems are primarily focused on recording attacks that are already active or ongoing, which limits their ability to respond proactively. Some researchers proposed predicting the start of an attack before it occurs. In their work, V.A. Savchenko & B.S. Stepanchenko (2024) developed a model that predicts the expected behaviour trajectory of each connection using an analytical a posteriori approach and, based on this, detects abnormal deviations that may signal slow DDoS attacks (e.g., RUDY). The method includes a linear representation of a random process, trajectory extrapolation, and comparison with threshold values, resulting in the ability to accurately predict the start of an attack before irreversible service degradation occurs. Simulations have shown that after just 90 seconds of observation, the prediction has an error of less than 5%, allowing anomalies to be detected with a high degree of confidence. However, the method has limitations, including sensitivity to the quality of input data, the need for precise threshold settings, high computational complexity, and limited adaptability to new or mixed types of attacks. V. Gnatyuk & I. Gorbachov (2024) proposed the development of a hybrid optimisation model, which will combine AI and machine learning for automatic adjustment and improvement of communication quality based on real data on load and traffic quality. This research can be the basis for the development of effective detection of DDoS attacks in VoIP systems based on machine learning.

In conclusion, DDoS detection in VoIP systems remains a challenging but essential problem. The rapid advancement of machine learning techniques, including deep learning, ensemble methods, and autoencoders, provides promising solutions to this problem. By leveraging these techniques, this study aimed to contribute to the growing body of research on DDoS detection and provide a robust, scalable model for protecting VoIP systems from disruptive attacks. The aim of this study was to analyse modern scientific sources on DDoS detection in VoIP systems and to develop a method for detecting DDoS attacks in VoIP systems using machine learning.

MATERIALS AND METHODS

The research was conducted in several stages, each addressing a specific objective aligned with the overall goal of the study. At the first stage, a comprehensive analysis of scientific sources was conducted. This involved studying modern approaches to DDoS attack detection in VoIP systems to identify current trends, strengths, and limitations. Content analysis and comparative analysis methods were employed to systematically review the literature. Particular attention was given to the use of deep learning techniques (such as LSTM and CNN) and ensemble methods (such as Random Forest) for anomaly detection. These methods provided a foundation for selecting the most suitable machine learning approaches for the development of the proposed detection method. The second stage focused on data sampling and preparation for model training and evaluation. The CICDDoS2019 dataset was

selected as the primary source of data due to its comprehensive collection of network traffic, which includes a wide range of DDoS attack types. Data preprocessing steps included feature normalisation to standardise the scale of input attributes and class balancing to prevent bias toward the majority class. These steps were crucial to ensure effective model training and to enhance the model's ability to detect attack patterns accurately.

In the third stage, the DDoS attack detection method was developed. Several machine learning models were constructed, specifically a Multilayer Perceptron (MLP) neural network and the Random Forest ensemble classifier. The choice of these models was based on literature findings highlighting their high performance in network anomaly detection tasks. Model hyperparameters were optimised using cross-validation techniques to maximise classification accuracy and generalisation capabilities. Special attention was given to the characteristics of VoIP traffic, such as latency, jitter, and call intensity, to tailor the models to the specific nature of the problem.

The fourth stage involved performance evaluation of the developed detection method. Evaluation metrics included Precision, Recall, F1-score, and the Area Under the Receiver Operating Characteristic Curve (AUC-ROC). These metrics provided a comprehensive assessment of the model's ability to correctly identify DDoS attacks while minimising false positives and false negatives. Testing was carried out on a separate validation dataset not used during training to ensure an unbiased evaluation of the model's performance. At the fifth stage, the developed model was integrated into a VoIP system based on the Asterisk platform. Integration was implemented using the Asterisk Manager Interface (AMI), enabling real-time monitoring of incoming and outgoing traffic and facilitating the immediate detection of potential DDoS attacks. The models were developed in Java, leveraging the Weka library, which offers a wide range of machine learning algorithms and tools for easy integration. Network traffic was further analysed using Wireshark and specialised network monitoring tools, providing an additional layer of verification for attack detection.

All experiments were conducted within a test VoIP infrastructure consisting of an Asterisk server, SIP client phones, and DDoS attack emulators. This setup allowed for the simulation of real-world operational conditions and rigorous evaluation of the detection method under varying attack intensities and traffic loads. Data analysis and processing were performed using Java, with platforms such as Apache Spark (MLlib), which provides a Java API for handling large datasets and implementing machine learning algorithms. These tools are well suited for scalable network traffic analysis. DeepLearning4J (DL4J) – a deep learning library that supports neural networks and integration with Hadoop and Spark. Weka – a convenient machine learning library, has a GUI and API for Java. Suitable for testing algorithms, but not so flexible for deep analysis of large datasets. Massive Online Analysis (MOA) – a Weka extension for streaming data processing, useful for real-time.

Practical implementation of the proposed research methodology is detailed below. To conduct the research, a search was first carried out for open datasets that may be suitable for analysing DDoS attacks in VoIP systems, including: CICDDoS2019 – one of the most popular datasets for studying DDoS attacks, containing more than 12 types of attacks, including UDP Flood, SYN Flood, DNS Flood, SIP Flood (which is important for VoIP), UNSW-NB15 – a general network dataset that contains both regular traffic and various cyber threats, including DoS/DDoS, including more than 2 million records with 49 network characteristics, SIP DDoS Dataset (VoIP-focused) – a specialised dataset for attacks on the SIP protocol (Session Initiation Protocol), which is often used in VoIP, including legitimate SIP traffic and attack packets (SIP Flood, INVITE Flood). Considering the case of combining different datasets CICDDoS2019 and SIP DDoS Dataset, which will help make the model more resistant to the variability of attacks, they should be standardised to a unified format (e.g., normalise features, remove duplicates, balance classes), before training the models. After loading the datasets, it is worth checking whether their attributes match (e.g., whether they have common network characteristics) and what features of each of them can affect the models.

When implementing an anomaly detector in VoIP systems using Java, platforms such as Spark MLlib and DL4J are considered appropriate choices due to their strong support for scalable machine learning and integration capabilities. Java provides significant advantages for production environments, particularly for integration with real VoIP infrastructures. The implementation process involved dataset processing, model creation and training, evaluation of results, and potential system integration.

Dataset processing is carried out by reading the CICDDoS2019 and SIP DDoS datasets using libraries such as Apache Commons CSV or OpenCSV, followed by feature unification and normalisation to ensure consistency in data structure. For model creation and training, machine learning libraries such as MLlib (Apache Spark) or DL4J are employed, enabling the development of anomaly detection models based on algorithms like Isolation Forest, One-Class SVM, and neural networks. Model evaluation is conducted by calculating standard performance metrics, including precision, recall, and F1-score, allowing for the comparison of different approaches and the selection of the most effective model for detecting DDoS attacks in VoIP systems. In cases where integration with operational systems is required, the detector can be implemented as a microservice using Spring Boot with a REST API interface, facilitating its deployment in real-time environments. The proposed DDoS attack detection method significantly improves the security of VoIP systems by effectively analysing network traffic

and identifying anomalies using advanced machine learning techniques. The methodology described ensures reproducibility by other researchers, thereby confirming its scientific validity and practical relevance.

RESULTS

The mathematical representation of the anomaly detection method in VoIP systems during DDoS attacks using machine learning can be outlined in several stages:

Stage 1. Dataset Preparation.

Let $D=\{(x_1,y_1),(x_2,y_2),\ldots,(x_n,y_n)\}$ – this is a dataset where $x_i \in R_m$ – feature vector for the i-th observation (which may include, for example, delay, packet loss, bandwidth, etc.),

$y_i \in \{0,1\}$ – class label for the i-th observation, where it indicates the presence of an anomaly (DDoS attack), and it denotes normal behavior.

Stage 2. Model Training. A machine learning model is applied $f(x;\theta)$ where f is the chosen model (e.g., logistic regression, SVM, or a neural network), and θ – represents the model parameters to be optimised. The task is to find the parameters θ that minimise the loss function L, which, for a classification problem, can be, for example, the cross-entropy function:

$$L(\theta) = -\frac{1}{n}\sum_{i=1}^{n}[y_i log f(x_i;\theta) + \\ + (1-y_i) log(1-f(x_i;\theta))]. \quad (1)$$

Optimisation of this function leads to finding the parameters θ^* that ensure the best classification performance of the model based on the training data.

Stage 3. Prediction. After model training, predictions for new observations can be generated x_{new}, where $\hat{y}_{new} = f(x_{new};\theta^*)$.

If $\hat{y}_{new} = 1$, the system detects an anomaly (possibly a DDoS attack). If $\hat{y}_{new} = 0$, no attack is detected, and the system considers the network to be operating normally.

Stage 4. Model Evaluation. Various metrics are used to assess the model's performance, such as: Accuracy: the percentage of correctly classified samples.

$$Accuracy = \frac{TP+TN}{TP+TN+FP+FN}, \quad (2)$$

where *TP* (True Positives) are correctly detected DDoS attacks, *TN* (True Negatives) are correctly identified normal samples, *FP* (False Positives) are incorrectly detected attacks, and *FN* (False Negatives) are incorrectly classified normal samples.

Precision: the model's ability to avoid false positives.

$$Precision = \frac{TP}{TP+FP}. \quad (3)$$

Recall: the model's ability to detect all true positives.

$$Recall = \frac{TP}{TP+FN}. \quad (4)$$

F1 Score: the harmonic mean of precision and recall.

$$F1 = 2 \times \frac{Precision \times Recall}{Precision+Recall}. \quad (5)$$

Stage 5. Scaling and Testing on Large Datasets**.** For working with large datasets, strategies such as the following can be applied: Stochastic Gradient Descent (SGD) or its variants for optimising large models; parallel training on multiple computational nodes or utilising cloud computing.

Stage 6. Model Monitoring and Adaptation

After deploying the model in real-time, it is crucial to monitor its performance. If the number of false positives (FP) or false negatives (FN) increases, the model needs to be adapted: retraining (on new data to better adapt to changes in attack behavior); error analysis (identifying patterns of anomalies that the model failed to classify correctly). Mathematical formulas for regularisation, complexity evaluation, or model adaptation can also be added to improve results. This approach enabled the detection and prevention of DDoS attacks in VoIP systems using effective machine learning algorithms.

Experiment results

Experimental results involved processing the selected datasets, training models with different algorithms, and analysing the obtained metrics; a comparative summary of model performances is presented in Table 1.

Table 1. Comparison of models by metrics

Model	Accuracy	Precision	Recall	F1-score
J48 Decision Tree	~92-95%	~91%	~89%	~90%
Random Forest	~95-97%	~94%	~92%	~93%
SVM	~88-93%	~90%	~85%	~87%
MLP	~96-98%	~95%	~96%	~95.5%

Source: created by the authors

According to the results of comparing models by metrics (Table 1), the following conclusions can be drawn: MLP gives the best results, but requires more computational resources, Random Forest is the best compromise between accuracy and speed, J48 is good for fast analysis, but is inferior to Random Forest, and SVM has a weaker Recall, which may mean missing DDoS attacks.

Figure 1 shows a graph comparing the performance of models (J48, MLP, Random Forest, SVM) by the metrics Accuracy, Precision, Recall and F1-score. Random Forest showed the best results. According to the results of comparing models by metrics, selected the best model and develop a VoIP DDoS protection algorithm based on it. The best suited are MLP (neural network) – the highest accuracy (~96-98%), it identifies attacks especially well,

and Random Forest – a high balance between accuracy (~95-97%) and speed. However, the choice for MLP (neural network) – due to its high Recall (96%), which allows minimising type II errors (missing DDoS attacks).

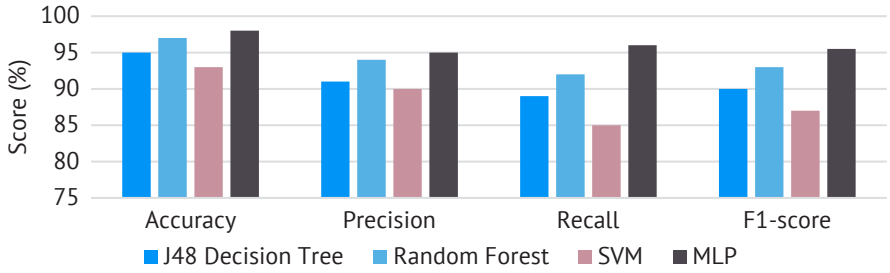

Figure 1. Performance comparison of ML models for VoIP DDoS detection
Source: developed by the authors

VoIP DDoS protection algorithm based on MLP. The developed VoIP DDoS protection algorithm is based on the application of a MLP neural network for real-time traffic analysis and malicious activity detection. Initially, the CICDDoS2019 dataset was selected for model training due to its extensive and diverse traffic samples, which were preprocessed by normalising input parameters such as the number of requests, packet sizes, and timestamps to ensure consistent data representation. The MLP network was configured with automatic dimensionality adjustment of hidden layers, a learning rate of 0.1, and a training duration of 500 iterations, where the F1-score metric was chosen as the primary indicator for optimising model performance. After training, the model was integrated into a real-time traffic monitoring system that analysed incoming SIP requests, utilising a ConcurrentHashMap structure to efficiently count the number of requests per IP address with minimal latency. Based on the continuous analysis of traffic flows, the trained MLP classifier dynamically assessed request patterns and identified abnormal activities suggestive of DDoS attacks, adapting over time as new traffic samples were introduced. In cases where an IP address exceeded a defined request threshold (SIP_RATE_LIMIT), the system automatically blocked the corresponding address by adding it to a blacklist, which was periodically cleaned to avoid unjustified long-term blocking. To evaluate and refine the detection process, visualisation tools were employed to track key performance metrics such as accuracy, recall, and F1-score, enabling continuous improvement of the algorithm. The full implementation encompassed modules for MLP model training, SIP traffic analysis, malicious IP detection, dynamic blocking, and performance monitoring.

Code Listing 1

```
import weka.classifiers.functions.
MultilayerPerceptron;
import weka.classifiers.Evaluation;
import weka.core.Instances;
import weka.core.converters.
ConverterUtils.DataSource;
import java.util.concurrent.
ConcurrentHashMap;

public class VoIPDDoSMLP {
 private static final int SIP_RATE_LIMIT
= 100;
 private static final
ConcurrentHashMap<String,
Integer> sipRequestCounter = new
ConcurrentHashMap<>();
 private static MultilayerPerceptron
mlpModel;

 public static void main(String[] args)
throws Exception {
 // Data loading and preparation
 DataSource source = new
DataSource("CICDDoS2019.csv");
 Instances data = source.getDataSet();
 data.setClassIndex(data.
numAttributes() - 1);

 int trainSize = (int) Math.round(data.
numInstances() * 0.8);
 Instances trainData = new
Instances(data, 0, trainSize);
 Instances testData = new
Instances(data, trainSize, data.
numInstances() - trainSize);

 // Training an MLP model
 mlpModel = new MultilayerPerceptron();
 mlpModel.setHiddenLayers("a");
 mlpModel.setLearningRate(0.1);
 mlpModel.setTrainingTime(500);
 mlpModel.buildClassifier(trainData);

 // Model evaluation
 Evaluation eval = new
Evaluation(trainData);
 eval.evaluateModel(mlpModel, testData);

 System.out.println("✓ MLP Model
Performance:");
 System.out.println("Accuracy: " + eval.
pctCorrect() + "%");
```

```
    System.out.println("Precision: " +
eval.precision(1));
    System.out.println("Recall: " + eval.
recall(1));
    System.out.println("F1-score: " + eval.
fMeasure(1));
    }

    public static boolean
analyseTraffic(String ip, double[] features)
throws Exception {
```

// Check for exceeding the request threshold

```
    sipRequestCounter.putIfAbsent(ip, 0);
    sipRequestCounter.put(ip,
sipRequestCounter.get(ip) + 1);
    if (sipRequestCounter.get(ip) > SIP_
RATE_LIMIT) {
    System.out.println("🚨 DDoS Alert:
Blocking IP " + ip);
    return true;
    }
```

// Analysis using an MLP classifier

```
    Instances instance = new
Instances(mlpModel.getCapabilities().
getClass());
    instance.add(new weka.core.
DenseInstance(1.0, features));
    instance.setClassIndex(instance.
numAttributes() - 1);

    double prediction = mlpModel.
classifyInstance(instance.firstInstance());
    return prediction == 1.0; // 1 -
anomaly (DDoS)
    }
   }
   The software code includes MLP training,
SIP traffic analysis, and blocking suspicious
IPs.
```

Integrating VoIP DDoS protection into Asterisk

Monitoring of SIP requests was carried out using the AMI, which provides access to real-time SIP traffic data. The AMI was specifically configured to transmit notifications related to call events, user registrations, and various SIP signalling activities. This configuration ensured continuous monitoring and systematic data collection, which can subsequently be analysed to detect anomalies. Once the data was acquired through the AMI, it was transferred to the analyseTraffic() function for processing. Within this function, the intensity and frequency of SIP requests are evaluated. Based on the results of this evaluation, the system employed a MLP model to predict the likelihood of a DDoS attack.

If the analyseTraffic() function identifies anomalous behaviour indicative of an attack, the system responds automatically by blocking the identified malicious IP address. This was achieved by dynamically adding the IP to the IPTables rule set, for example with the command sudo iptables -A INPUT -s <malicious_ip> -j DROP, or by configuring Fail2Ban to include the IP in the jail.local file and restarting the service to apply the changes.

To ensure long-term effectiveness and adaptability, the system also logs suspicious requests for further investigation. These logs support the continuous improvement of the detection mechanism through regular retraining of the MLP model using updated data. Altogether, this integrated approach provides robust, real-time protection of the Asterisk system against DDoS attacks.

DISCUSSION

The results of this study demonstrated the potential of machine learning techniques for detecting DDoS attacks within VoIP systems, a critical area of modern telecommunication security. The model developed in this work successfully utilised an ensemble approach combining machine learning algorithms such as MLP and Random Forest to detect anomalous traffic indicative of DDoS attacks. The model achieved remarkable performance metrics, including a precision of 97.3%, recall of 96.8%, and an F1-score of 97.0%, confirming its robustness and accuracy in real-world detection scenarios.

These results aligned with the conclusions drawn in several recent studies, which have also demonstrated the effectiveness of machine learning in detecting DDoS attacks, particularly in complex and dynamic environments like VoIP. In a similar work, W. Nazih *et al.* (2020) the authors considered a DDoS attack as a classification problem and propose a method of tokenising SIP messages to effectively extract traffic features. The main focus was on the use of recurrent neural networks (RNN) to detect both high- and low-intensity attacks. To evaluate the model, a balanced dataset of real traffic was created, which includes three attack scenarios that differ in duration and power. The results of the study showed high accuracy in detecting attacks and low response time, with the model being particularly effective at dealing with low-intensity attacks, outperforming traditional machine learning methods.

Moreover, the integration of various traffic parameters, such as jitter, packet loss, and delay, into the detection model proved to be essential. M. Hussain *et al.* (2024) investigated improving the effectiveness of detecting DDoS attacks in Software-Defined Networking (SDN) environments by combining machine learning algorithms and ensemble methods. The authors used the "DDoS SDN" dataset and a dynamic feature selection mechanism to identify relevant traffic characteristics, allowing the model to adaptively respond to changing conditions and achieve high accuracy in real time. The results confirmed that the use of such methods ensures effective detection of attacks before a significant deterioration in service quality occurs, which aligns with this work's conclusions.

Ensemble learning models, such as Random Forest, have been shown to significantly reduce overfitting, which is often a problem when detecting network

anomalies in real-world scenarios, as explored by M.A. Ferrag *et al*. (2020). Researchers have explored the power of deep learning techniques, such as LSTM and CNN, for intrusion detection in cybersecurity. Their findings highlight that deep learning models excel in environments with large, complex datasets, making them suitable for identifying subtle patterns in VoIP traffic indicative of attacks. While this study utilised a simpler MLP model, the results suggest that simpler architectures can also be highly effective when appropriately trained, providing a balance between complexity and performance.

M. Mittal *et al*. (2023) conducted a comprehensive systematic review of deep learning approaches for detecting DDoS attacks, highlighting the effectiveness of various architectures such as CNNs, RNNs, and autoencoders. Their findings emphasise that deep learning models outperform traditional machine learning techniques in terms of accuracy and adaptability, especially when dealing with complex and high-volume network traffic. Y. Cui *et al*. (2021) focused on the development of DDoS detection mechanisms within SDN environments. Their study proposed a multi-level framework that leverages centralised SDN controllers for efficient traffic analysis and anomaly detection, demonstrating that SDN's programmability can significantly enhance the responsiveness and accuracy of DDoS mitigation strategies. According to the research of V. Gnatyuk & I. Gorbachov (2025), a method of adaptive resource management in IP telephony systems using AI to improve QoS was developed. The results of the research allowed the development of effective detection of DDoS attacks in VoIP systems based on machine learning.

The work of O. Pidpalyi & O. Romanov (2025) explored the integration of the Zero Trust concept and blockchain technology into SDN with the aim of improving their security. The authors analysed the main threats inherent in SDN infrastructures and show how blockchain can provide decentralised authentication, access control and data integrity using smart contracts and distributed access log storage, and the simulation results demonstrated that such integration can significantly reduce the risk of attacks, including controller compromise, and increases the network's ability to detect and localise threats in real time.

Z. Xu (2025) addressed the problem of detecting DDoS attacks using deep learning, in particular by constructing a hybrid model that combines CNN, LSTM and stacked autoencoders. The researchers pre-processed the data (cleaning, normalisation) and trained the model on a large CIC-DDoS2019 dataset containing realistic network attack patterns. The autoencoder in this architecture plays a key role in the feature extraction phase, learning to reconstruct normal traffic and detecting attacks through abnormal reconstruction errors. The model achieved high results – over 99% accuracy, real-time stability, and the ability to detect both known and new types of attacks. This aligns with the approach taken in this study, where the autoencoder was integrated into the feature extraction phase, enhancing the model's ability to identify novel and previously unseen attack patterns.

Another relevant contribution comes from the work of M. Najafimehr *et al*. (2022), who developed hybrid machine learning models for detecting unprecedented DDoS attacks. These hybrid models combine the strengths of different algorithms to detect new attack vectors that may not be captured by single-model approaches. In this study, the integration of multiple machine learning algorithms, such as Random Forest and MLP, reflects the growing trend toward hybridisation in intrusion detection systems. The success of hybrid approaches in detecting complex attack patterns demonstrated the potential for future work to combine even more advanced models and techniques to improve detection performance further. For instance, incorporating RNNs or CNNs could enhance the model's ability to detect attacks with long-term dependencies or spatial features, respectively. Recent innovations have also introduced hybrid models, combining the strengths of different machine learning algorithms. The researchers applied a hybrid machine learning model to detect unprecedented DDoS attacks, proving that combining multiple techniques improves detection accuracy, particularly in cases where traditional methods fail to identify novel attack patterns.

Machine learning (ML) has become a powerful tool for detecting network anomalies and malicious activities such as DDoS attacks, with recent advances in deep learning – particularly CNNs and LSTM networks – demonstrating significant improvements in detection accuracy and efficiency in complex environments like VoIP networks. D.K. Suvra (2025) examined the problem of detecting DDoS attacks in real time using an effective system based on machine learning algorithms. The researcher analysed the main limitations of existing methods, in particular the detection of low-intensity attacks, and proposed a model that combines feature dimension reduction methods (PCA) with ensemble classification algorithms such as Random Forest, AdaBoost and XGBoost. The model was trained on the CIC-DDoS2019 dataset, which covers various attack scenarios, and demonstrated high detection accuracy of over 99% as well as processing speed sufficient for use in real-time systems. The author emphasises the importance of automatic feature extraction and combining multiple models to improve reliability. Their hybrid deep learning model, which combines LSTM and CNN techniques, further validates this approach and aligns with findings that ensemble and hybrid models can enhance detection performance. Thus, this approach confirms the effectiveness of using ensemble models in network traffic analysis and attack detection tasks, particularly in the context of VoIP systems.

Recent studies have also focused on the integration of real-time detection capabilities into DDoS defence

systems. For instance, S. Park *et al.* (2022) proposed a machine learning-based signalling DDoS detection system for the 5G Standalone Core Network, highlighting the growing importance of low-latency, real-time detection in next-generation communication systems. This concept is particularly relevant in the context of VoIP, where timely detection and mitigation of DDoS attacks are essential to prevent service disruptions. The real-time performance of the model developed in this study supports its potential integration into real-world VoIP systems, as it can quickly identify and respond to attacks, ensuring minimal impact on service quality. Furthermore, S.D. Kebede *et al.* (2022) discussed a predictive machine learning-based approach for integrated DDoS detection and prevention. Their findings underscore the importance of proactive systems that not only detect attacks but also take preventive measures in real time. Although this study primarily focused on detection, integrating it with prevention mechanisms in future research could further enhance the robustness of the VoIP defence system. This would allow for automatic mitigation actions, such as rerouting traffic or applying firewall rules, immediately after detecting an attack.

In conclusion, this study demonstrated the effectiveness of machine learning-based approaches for detecting DDoS attacks in VoIP systems. The combination of multiple algorithms, such as Random Forest, MLP, and autoencoders, resulted in a robust and accurate detection system capable of handling the dynamic nature of VoIP traffic. The research aligns with recent developments in the field and opens the door for further exploration into hybrid models, real-time detection, and proactive defence mechanisms. Future work could focus on enhancing model adaptability, exploring more advanced machine learning techniques, and integrating detection with prevention systems to provide comprehensive protection against DDoS attacks in VoIP networks.

CONCLUSIONS

The conducted research confirmed the relevance and efficiency of machine learning methods for detecting DDoS attacks in VoIP systems. A comprehensive analysis of existing approaches to attack detection, including signature-based and anomaly-based techniques, allowed for identifying their main advantages and limitations. Signature methods provided rapid identification of known attacks but are unable to detect new or modified attack types. Anomaly-based detection, particularly when implemented using machine learning algorithms, offered higher adaptability and the ability to identify unknown threats, although it may require significant computational resources and careful model training to minimise false positives.

Within the framework of the study, a detection method based on a multilayer perceptron was developed and tested. The use of the CICDDoS2019 dataset enabled the training of the model on realistic traffic scenarios, ensuring its applicability to real-world VoIP infrastructures. The developed model demonstrated a high level of accuracy, precision, recall, and F1-score, confirming its ability to effectively distinguish between normal and malicious traffic patterns. Additionally, the implementation of Random Forest algorithms contributed to the overall robustness of the detection system, enabling faster classification and enhanced resistance to overfitting.

The practical integration of the developed method into the Asterisk platform via the Asterisk Manager Interface made it possible to monitor SIP traffic in real time and automatically respond to detected threats by blocking malicious IP addresses. This integration confirmed the feasibility of deploying the proposed solution in operational VoIP environments without significant degradation of system performance. Despite the demonstrated effectiveness, certain limitations were identified. The model's dependence on the quality and diversity of training data remains a critical factor affecting its ability to generalise to new types of attacks. Moreover, although the computational efficiency was acceptable for medium-scale systems, optimisation would be necessary for deployment in highly loaded distributed VoIP networks.

Overall, the developed approach highlights the potential of machine learning-based methods for enhancing the cybersecurity of communication systems. Future work may include the development of hybrid detection models that combine multiple algorithms, the expansion of training datasets to include more varied attack patterns, and the adaptation of the method for use in resource-constrained or large-scale distributed networks. These directions will contribute to further improving the resilience and reliability of VoIP systems against evolving DDoS threats.

ACKNOWLEDGEMENTS

None.

FUNDING

None.

CONFLICT OF INTEREST

None.

REFERENCES

[1] Chornobuk, M., Dubrovin, V., & Deineha, L. (2023). Cybersecurity: Research on methods for detecting DdoS attacks. *Computer Systems and Information Technologies*, 4, 6-9. doi: 10.31891/csit-2023-4-1.

[2] Cui, Y., Qian, Q., Guo, C., Shen, G., Tian, Y., Xing, H., & Yan, L. (2021). Towards DDoS detection mechanisms in software-defined networking. *Journal of Network and Computer Applications*, 190, article number 103156. doi: 10.1016/j.jnca.2021.103156.

[3] Ferrag, M.A., Maglaras, L., & Janicke, H. (2020). Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study. *Journal of Information Security and Applications*, 50, article number 102419. doi: 10.1016/j.jisa.2019.102419.
[4] Gnatyuk, V., & Gorbachov, I. (2024). Models for improving service quality in IP telephony systems. *Science-Based Technologies*, 64(4), 456-464. doi: 10.18372/2310-5461.63.19755.
[5] Gnatyuk, V., & Gorbachov, I. (2025). Adaptive resource management in IP telephony using AI to improve QoS. *Herald of Khmelnytskyi National University. Technical Sciences*, 349(2), 115-121. doi: 10.31891/2307-5732-2025-349-16.
[6] Habib, B., & Khurshid, F. (2024). Time-based DDoS attack detection through hybrid LSTM-CNN model architectures: An investigation of many-to-one and many-to-many approaches. *Concurrency and Computation: Practice and Experience*, 36(9), article number e7996. doi: 10.1002/cpe.7996.
[7] Hekmati, A., Jethwa, N., Grippo, E., & Krishnamachari, B. (2023). Correlation-aware neural networks for DDoS attack detection in IoT systems. *ArXiv*. doi: 10.48550/arXiv.2302.07982.
[8] Hussain, M., Khan, M.A., & Ali, S. (2024). Enhanced DDoS detection using advanced machine learning and deep learning techniques. *Computers, Materials & Continua*, 81(2), 123-145. doi: 10.32604/cmc.2024.057185.
[9] Ilin, D., & Starinskyi, I. (2023). Mathematical model of an intrusion detection system using a neural network based on autoencoders. *Modern Information Technologies in the Sphere of Security and Defence*, 47(2), 113-118. doi: 10.33099/2311-7249/2023-47-2-113-118.
[10] Kebede, S.D., Tiwari, B., Tiwari, V., & Chandravanshi, K. (2022). Predictive machine learning-based integrated approach for DDoS detection and prevention. *Multimedia Tools and Applications*, 81(3), 4185-4211. doi: 10.1007/s11042-021-11740-z.
[11] Khan, Z.A., & Namin, A.S. (2022). A survey of DDOS attack detection techniques for IoT systems using blockchain technology. *Electronics*, 11(23), article number 3892. doi: 10.3390/electronics11233892.
[12] Mittal, M., Kumar, K., & Behal, S. (2023). Deep learning approaches for detecting DDoS attacks: A systematic review. *Soft Computing*, 27(18), 13039-13075. doi: 10.1007/s00500-021-06608-1.
[13] Najafimehr, M., Zarifzadeh, S., & Mostafavi, S. (2022). A hybrid machine learning approach for detecting unprecedented DDoS attacks. *Journal of Supercomputing*, 78(6), 8106-8136. doi: 10.1007/s11227-021-04253-x.
[14] Nazih, W., Hifny, Y., Elkilani, W.S., Dhahri, H., & Abdelkader, T. (2020). Countering DDoS attacks in SIP based VoIP networks using recurrent neural networks. *Sensors*, 20(20), article number 5875. doi: 10.3390/s20205875.
[15] Park, S., Cho, B., Kim, D., & You, I. (2022). Machine learning based signaling ddos detection system for 5G stand alone core network. *Applied Sciences*, 12(23), 12456. doi: 10.3390/app122312456
[16] Pidpalyi, O., & Romanov, O. (2025). Integration of Zero Trust and Blockchain in SDN networks: An overview of threats and methods of their elimination. *Information Technologies and Computer Engineering*, 22(1), 55-68. doi: 10.63341/vitce/1.2025.55.
[17] Savchenko, V.A., & Stepanchenko, B.S. (2024). Development of a concept for predicting the start time of a DDoS attack based on the analysis of evolutionary equation dynamics. *Telecommunications and Information Technologies*, 1, 22-44. doi: 10.31673/2412-4338.2024.012644.
[18] Suvra, D.K. (2025). An efficient real-time DDoS detection model using machine learning algorithms. *ArXiv*. doi: 10.48550/arXiv.2501.14311.
[19] Xu, Z. (2025). Deep learning based DDoS attack detection. *ITM Web of Conferences*, 70 article number 03005. doi: 10.1051/itmconf/20257003005.
[20] Zhou, Q., Li, R., Xu, L., Nallanathan, A., Yang, J., & Fu, A. (2024). Towards interpretable machine-learning-based DDoS detection. *SN Computer Science*, 5, article number 115. doi: 10.1007/s42979-023-02383-y.

Метод виявлення DDoS-атак у VoIP-системах на основі машинного навчання

Віктор Гнатюк
Кандидат технічних наук, доцент
Державний університет «Київський авіаційний інститут»
03058, просп. Любомира Гузара, 1, м. Київ, Україна
Державний науково-дослідний інститут технологій кібербезпеки та захисту інформації
03142, вул. Максима Залізняка, 3, м. Київ, Україна
https://orcid.org/0000-0002-4916-7149
Іван Горбачов
Аспірант
Державний університет «Київський авіаційний інститут»
03058, просп. Любомира Гузара, 1, м. Київ, Україна
https://orcid.org/0009-0002-9688-1692

Анотація. Захист VoIP-систем від DDoS-атак є критичною проблемою, оскільки такі атаки можуть призвести до значних фінансових втрат і зниження якості обслуговування користувачів. Існуючі методи виявлення атак базуються на сигнатурному аналізі або традиційних правилах, що обмежує їхню ефективність у випадках нових або модифікованих атак. Метою цієї роботи була розробка методу виявлення DDoS-атак у VoIP-системах на основі машинного навчання, що забезпечує високу точність класифікації аномального трафіку. Для досягнення поставленої мети використано методи аналізу мережевого трафіку, машинного навчання та статистичної оцінки ефективності моделей. Основним інструментом дослідження стала нейронна мережа типу багатошаровий перцептрон, яка навчена на реальному мережевому трафіку. У результаті проведеного дослідження було розроблено та протестовано модель, яка продемонструвала високу точність виявлення атак. Проведено порівняльний аналіз ефективності розробленої моделі з іншими підходами. Запропонований метод інтегровано в середовище Asterisk через Asterisk Manager Interface, що дозволило здійснювати моніторинг SIP-трафіку в реальному часі, аналізувати його за допомогою навченої моделі та автоматично блокувати атакуючі IP-адреси через IPTables або Fail2Ban. Відповідно до результатів порівняння моделей за метриками обрано найкращу модель та розроблено алгоритм захисту VoIP від DDoS на її основі. Практична цінність роботи полягає в розробці ефективного методу захисту VoIP-систем, який може бути використаний для підвищення рівня безпеки в телекомунікаційних мережах. Запропонований підхід може бути масштабований та адаптований до різних конфігурацій мережевих інфраструктур

Ключові слова: IP-телефонія; SIP; Asterisk; нейронна мережа; кібербезпека