

DDoS attack detection in large-scale networks using wavelet transform and machine learning

Bohdan Kotyk^{1,*†}, Denys Bakhtiiarov^{1,2†}, Oleksandr Lavrynenko^{1†}, Andrii Leleko^{1†}, Dmytro Kocherga^{1†} and Yaroslav Tertus^{1†}

¹National University "Kyiv Aviation Institute", Liubomyra Huzara Ave., 1, Kyiv, 03058, Ukraine

²State Scientific and Research Institute of Cybersecurity Technologies and Information Protection, Maksym Zaliznyak Str., 3, Kyiv, 03142, Ukraine

Abstract

The rapid expansion of global network infrastructures has led to a significant increase in the frequency and complexity of Distributed Denial of Service (DDoS) attacks. Detecting these malicious activities in large-scale networks with highly diverse traffic remains a critical cybersecurity challenge. In order to improve computation speed and accuracy, this article proposes a two-stage anomaly detection system utilizing data processing based on artificial intelligence. A procedure has been devised to calculate multiple correlations depending on a more streamlined correlation matrix structure extracted from specific network packet parameters. The data obtained from the correlation analysis then filtered with discrete wavelet transform (DWT) coefficients to provide highly efficient and reliable detection capabilities. Quantitative and qualitative characteristics of a signal necessarily contain fluctuations or changes that occur in the signal. Sudden changes in signal variations produce certain characteristics, that need to be classified as attacks. To effectively classify these anomalies, the K-means machine learning algorithm is utilized to cluster the standardized correlation data, minimizing false positives. This immediate alerting of network system administrators is enabled through the use of specific attributes that help in the precise identification of anomalies within the network's traffic flow, ensuring network security and resilience.

Keywords

data processing, artificial intelligence, DDoS attacks, wavelet transform, statistical methods, machine learning, network traffic anomalies, cybersecurity

1. Introduction

The exponential growth of internet-connected devices and cloud-based services has made large-scale networks increasingly vulnerable to Distributed Denial of Service (DDoS) attacks. These attacks aim to overwhelm network resources, causing severe service disruptions and substantial financial losses. Historically, the effectiveness of anomaly detection methodologies has mainly been established on smaller than average databases, which often fail to reflect the complexity of modern, high-speed backbone networks. Intrusion detection and data mining systems are highly sensitive to the sampling rate and the number of samples collected over time. While other research efforts have developed different DDoS detection methodologies, relying primarily on signature-based detection or simple thresholding, these traditional systems struggle to adapt to novel attack vectors. Nonetheless, none of these existing schemes utilize a machine learning approach in conjunction with wavelet analysis to investigate DDoS traffic at a granular level [1].

Traffic modeling in the literature generally uses a variety of aggregated network statistics, for example, network flow rates and packet types, as the foundation for time series generation. However, relying solely on aggregated data can obscure the subtle, early indicators of an attack. In the identification of

WCH'26: Fifth International Workshop on Cyber Hygiene, June 25–26, 2026, Krakow, Poland

*Corresponding author.

†These authors contributed equally.

✉ 3351920@stud.kai.edu.ua (B. Kotyk); denys.bakhtiiarov@npp.kai.edu.ua (D. Bakhtiiarov); oleksandr.lavrynenko@npp.kai.edu.ua (O. Lavrynenko); 8651481@stud.kai.edu.ua (A. Leleko); 2118143@stud.kai.edu.ua (D. Kocherga); 4142569@stud.kai.edu.ua (Y. Tertus)

ORCID 0009-0005-0821-9108 (B. Kotyk); 0000-0003-3298-4641 (D. Bakhtiiarov); 0000-0002-7738-161X (O. Lavrynenko); 0009-0005-8324-1161 (A. Leleko); 0009-0006-4178-8609 (D. Kocherga); 0009-0004-8861-6092 (Y. Tertus)



© 2026 Copyright for this paper by its authors. Use permitted under Creative Commons License Attribution 4.0 International (CC BY 4.0).

hacker activities on a network, the approach discussed in this article focuses on analyzing the actual data packets in the network [2]. In analysing various network attacks, use of several layers of the OSI model and various specific parameters is needed.

For instance, a UDP flood attack is described in order to illustrate the above point. In order to be able to successfully identify this particular kind of attack, it is essential to monitor a considerable number of packets associated with either specific or randomised remote host port numbers. In this situation, the host must determine the appropriate process for each received packet in order to test for its inactivity. It must then send an ICMP "destination unreachable" message to the source. Thus this attack vector can be detected as a correlation between ICMP and UDP packets, where the UDP packets are the cause and the ICMP packets are the effect. This can be accomplished by inspecting the source and destination UDP port numbers and the code field of ICMP messages. Similarly, the information sources most frequently manipulated during a DDoS attack on the TCP protocol are the sender's port number, the recipient's port number and the control flags. By extracting and analyzing these specific packet-level parameters, the system proposed in this paper aims to provide a robust, scalable, and highly accurate defense mechanism against sophisticated DDoS threats.

2. Related work

In our information-rich society, critical information infrastructures are used on a daily basis for work and private life, making their protection a top priority for national and global security [3, 4, 5]. For monitoring potential risks and preventing damage to networks of high complexity, a variety of cybersecurity risk assessment approaches are being discussed by researchers [6, 7, 8, 9]. However, current systems for DDoS and network intrusion detection mainly rely on message analysis, predefined attack signatures, and threshold values for normal traffic characteristics [10].

New challenges for DDoS and network intrusion detection are raised by the growing complexity of attacks, which are increasingly driven by AI, as well as by the deployment of new generation network systems such as 5G and novel applications like automated aviation systems that require secure data transmission and ultra-low latency [11, 12]. Classical solutions fail to address these current challenges [13, 14, 15]. This necessitates a shift toward adaptive and intelligent detection solutions capable of handling zero-day attacks and identifying complex traffic anomalies.

Recent research demonstrates the significant potential of artificial intelligence (AI) and machine learning (ML) for identifying network intrusions. Artificial neural networks and deep learning solutions can be successfully used for deterministic signal detection and for the real-time classification of network intrusions, even under conditions of a priori parameter uncertainty where models are not fixed in advance [16, 17, 18, 19]. Furthermore, signal processing techniques – particularly the Discrete Wavelet Transform (DWT) – can be successfully employed to extract semantic features from non-stationary signals. The application of empirical wavelet transforms and high-resolution DWT for tasks such as signal compression, signal reconstruction, speech emotion recognition, and acoustic detection of UAVs has been reported in several studies, demonstrating their ability to identify sudden changes and hidden patterns in information [20, 21, 22, 23, 24, 25, 26, 27, 28].

To address the security challenges of 5G networks and automated airspaces, new security architectures are currently being researched, including secure network slicing and quantum key distribution (QKD) protocols in IoT and 5G environments [29, 30, 31, 32, 33, 34]. However, several issues remain open. In particular, there is a gap regarding the possibility of integrating powerful signal processing techniques (like DWT) with unsupervised machine learning (e.g., K-means clustering) to implement a real-time DDoS detection system for large-scale networks featuring highly heterogeneous traffic. This problem can be solved by developing a hybrid framework of robust signal processing and unsupervised machine learning for dynamic and heterogeneous large-scale networks.

3. Wavelet transform for anomaly detection

Many approaches are used for processing input signals to get more detailed information about the characteristics of the signal under study. The most typical approach for the spectral analysis of time-series signals is to use the Fourier transform. However, the Fourier transform has restrictions for processing signals because it only allows us to obtain information about the frequency content of the signal and its amplitude in the time-scale. This approach is not suitable for processing many real-world signals, especially non-stationary signals like network traffic sampled over time.

The Short-Time Fourier Transform (STFT) is a time-localised spectral analysis of a non-stationary signal. However, the uncertainty principle sets certain restrictions on the STFT, making it impossible to obtain an exact frequency-time representation of a signal. The wavelet transform, as opposed to the Fourier transform, is used for frequency-time analysis, acting as a method of frequency domain analysis that is particularly well-suited for non-stationary signals.

The Wavelet Transform (WT) is a mathematical tool for the approximation of physical phenomena. Its primary objective is to analyze and study a signal by extracting the most important information, such as identifying the principal characteristics and structures. Wavelet transforms are divided into two major classes: the Continuous Wavelet Transform (CWT) and the Discrete Wavelet Transform (DWT). While CWT uses a continuous wavelet function to analyze a signal within a continuous time-scale framework, DWT utilizes a set of discrete wavelet functions and is mainly used for the analysis of discrete signals.

For a finite number of decomposition levels L , any sequence of discrete samples of the analysed traffic $D(t_j)$ can be represented as an ordered set of coefficients in a system of scaling functions and wavelet functions:

$$D(t_j) = \sum_{k=1}^{2^{K-L}} c_{L,k} \varphi_{L,k}(t_j) + \sum_{m=1}^L \sum_{k=1}^{2^{K-L}} e_{m,k} \psi_{m,k}(t_j), \quad m, k \in I \quad (1)$$

where $\varphi_{L,k}(t_j)$ is the basis scaling function, $\psi_{m,k}(t_j)$ is the basis wavelet function, $c_{L,k}$ and $e_{m,k}$ are the approximation and detail coefficients respectively, m and k are scale and shift parameters in the integer space I , and K is the maximum decomposition level.

Unlike the CWT, the DWT is computed at scales of 2^j , where j is the decomposition level. This allows the coefficients for the DWT to be computed much faster. The computation complexity of the DWT is equal to $m \log_2(m)$, where m is the length of the time series under analysis.

A DDoS attack fundamentally represents an abnormal behavior of network traffic. Thus, attack detection corresponds to the detection of changes in traffic behavior. Network traffic possesses scale-invariant and burst-like behavior on a variety of time scales. This property can be effectively captured by wavelet transforms through the decomposition of a signal into different time scales. Consequently, wavelet transforms are highly adequate for characterizing network traffic and extracting features for anomaly detection.

4. Methodological framework

To detect anomalies, one might employ an approach that involves partitioning the source traffic into non-overlapping time windows. However, this methodology proves to be suboptimal in instances of highly mixed network traffic – specifically when the traffic itself is represented by a diversity of different protocols, or when a single protocol contains a multiplicity of data within its various fields, thereby exhibiting significant heterogeneity. In such contexts, key values across a number of time intervals for this type of traffic will inevitably be skewed, either overestimated or underestimated. Such situations invariably lead to the occurrence of false positives and false negatives (Type I and Type II errors).

To mitigate these issues, the following approach is proposed: to examine time intervals with a shift relative to one another, such that the interval is dominated by the unchanged portion of the traffic from the preceding window. Since network traffic of a single type within a specific time interval is

inherently heterogeneous, a denial-of-service attack will introduce a certain uniformity across a number of parameters. Consequently, at the junctions between heterogeneous, potentially safe traffic and homogeneous, potentially malicious traffic, spikes in DWT frequencies occur, which this study proposes to monitor.

Tracking these spikes becomes significantly more feasible if the time intervals are calculated in an overlapping manner. Thus, as a result of this preprocessing phase, the researcher obtains a dataset composed of windows structured in the following manner:

$$\text{Window}_{j+y \cdot \text{shift}} = \begin{cases} \text{Time series for parameter 1} \\ \text{Time series for parameter 2} \\ \text{Time series for parameter 3} \end{cases} \quad (2)$$

where j represents the window number, shift denotes the time shift, and y indicates the offset number. Figure 1 provides a clearer visual demonstration of this window overlapping technique.

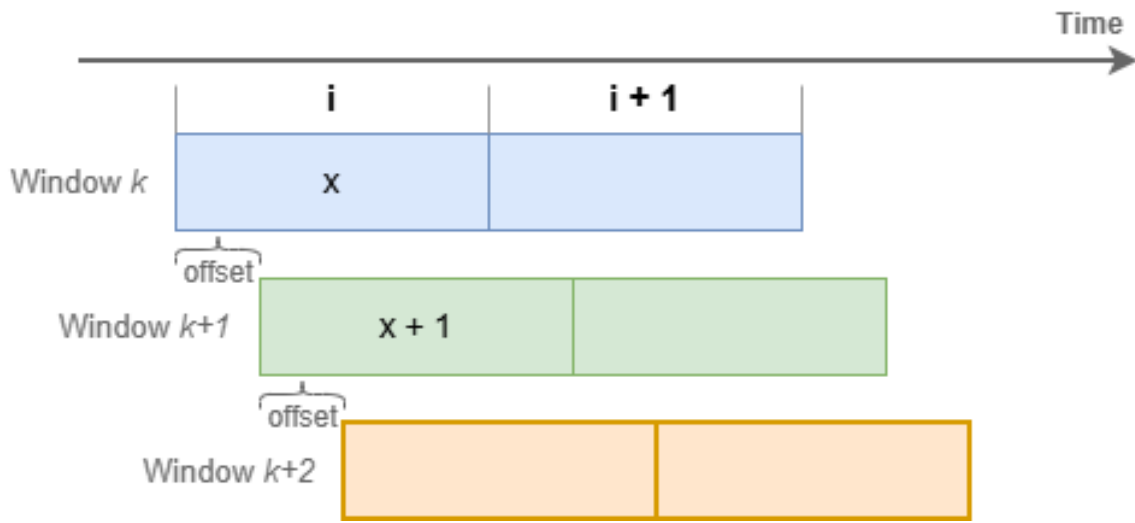


Figure 1: Example of time window overlap.

Thus, if the time interval is established at 10 seconds and the offset is set to 5 seconds, the following windows will be generated:

$$\begin{aligned} & [[0 \text{ seconds} - 10 \text{ seconds}], [5 \text{ seconds} - 15 \text{ seconds}]], \\ & [[10 \text{ seconds} - 20 \text{ seconds}], [15 \text{ seconds} - 25 \text{ seconds}]], \\ & \dots \\ & [[m \times 10 \text{ s.} - (m + 1) \times 10 \text{ s.}], [m \times 10 + 5 \text{ s.} - (m + 1) \times 10 + 5 \text{ s.}]] \end{aligned}$$

In this instance, data grouping must be performed in accordance with the first interval, as it is precisely in relation to this offset that the dynamics of changes in traffic composition are considered. Subsequently, each resulting sequence is fed into a discrete wavelet transform, from which the detail coefficients are of the primary interest.

In order to characterize the behavior of network traffic within a given time window, it is proposed to monitor the degree of dependence among different parameters of the network packet. The multiple correlation coefficient can be utilized as a metric to determine this degree of dependence; for the sequences a, b, c , this is calculated using the standard formula:

$$R_b(a, c) = \sqrt{\frac{r_{ba}^2 + r_{bc}^2 - 2 \cdot r_{ba} \cdot r_{bc} \cdot r_{ac}}{1 - r_{ac}^2}} \quad (3)$$

$$r_{ba} = \frac{\sum(a_j - \bar{a}) \cdot (b_j - \bar{b})}{\sqrt{\sum(a_j - \bar{a})^2 \cdot \sum(b_j - \bar{b})^2}} \quad (4)$$

A deviation of the multiple correlation coefficient $R_b(a, c)$ from the threshold value serves as an indicator of the presence of an anomaly within the network traffic. The more closely connected the network packets are within the interval under study, the higher the multiple correlation coefficient value will be, and conversely, the lower the probability of a DDoS attack within that interval. This choice of metric is substantiated by the high probability of changes in the multiple correlation coefficient values occurring specifically at the junctions between traffic with and without an attack.

Figure 2 presents a comparison chart illustrating the multiple correlation coefficients at the junction of traffic without an attack and traffic containing a TCP SYN attack.

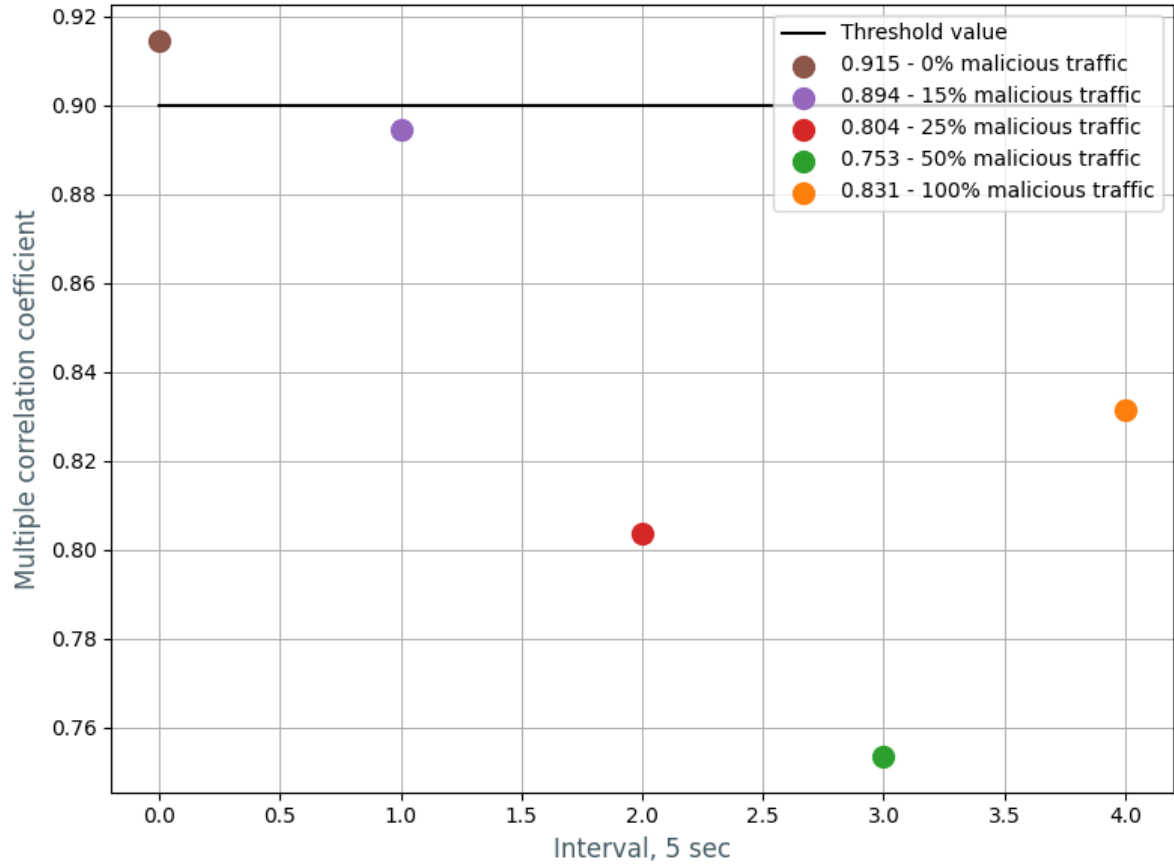


Figure 2: Comparison of multiple correlation coefficients for different percentages of traffic with and without TCP SYN attacks.

The figure displays five distinct time intervals containing varying percentage ratios of malicious network traffic, representing a TCP SYN attack, alongside harmless network traffic. The figure also highlights the threshold value that separates traffic without an attack (above the line) from traffic with an attack (below the line). This threshold value of 0.9 was derived empirically as a result of a series of experiments. The intervals under consideration are detailed below, proceeding from left to right.

First, the interval without an attack represents the traffic associated with downloading a file from a remote server. This specific type of traffic was deliberately selected for comparison purposes, as it is relatively uniform and is situated close to the threshold value. Nevertheless, this traffic remains above the boundary, which characterizes it as traffic free from attacks. Moving below the threshold value, the next point is a time interval containing 15% malicious network traffic, followed subsequently by a point representing a time interval with 25% malicious network traffic. The next point represents a

time interval containing 50% malicious network traffic; assuming that half of the network traffic in the interval under consideration consists of safe traffic and half consists of traffic representing an attack, the indicator is most strongly determined as an interval containing malicious traffic. Finally, the last value represents a time interval containing 100% malicious network traffic. This value is located closer to the threshold value of 0.9, as there are no spikes present within this interval. Nevertheless, it is strictly defined as attack traffic due to the uniformity of the network packets according to the selected parameters.

The discrepancy between the first value of the interval without an attack and the last interval with an attack is attributable to the selection of parameters. In this manner, this study demonstrates the feasibility of detecting DDoS attacks which constitute at least 15% of the analyzed time interval of network traffic.

Based on this conclusion, it is proposed to employ artificial intelligence methods – specifically machine learning algorithms – to create an adaptive model for the detection of DDoS attacks [16]. In order to apply machine learning methods effectively [17], it is necessary to unify the number of parameters (multiple correlation coefficients) within each time interval. These coefficients are grouped by time intervals; however, there may be a differing number of coefficients within a time interval depending on the intensity of the network traffic.

To unify traffic within each time window, it is proposed to use the root mean square (RMS) deviation over the specified intervals. The RMS is determined by equation (5), where $\bar{a}$ is the arithmetic mean of the sample.

$$D = \sqrt{\frac{1}{m} \sum_{j=1}^m (a_j - \bar{a})^2} \quad (5)$$

$$\bar{a} = \frac{1}{m} \sum_{j=1}^m a_j \quad (6)$$

It is proposed that this standardized (unified) data be used for training artificial intelligence using the K-means clustering algorithm. In this algorithm, the centers of clusters with the largest number of elements concentrated in a given area are determined, and subsequently, the algorithm seeks to minimize the total quadratic deviation of cluster points from the centers of these clusters using equation (7).

$$W = \sum_{j=1}^p \sum_{a \in C_j} (a - \mu_j)^2 \quad (7)$$

The proposed approach is comprised of two distinct iterations. The first iteration performs the identification of sections of spikes containing potentially malicious traffic, as determined by the clustering algorithm. This algorithm is implemented as a computer program and is registered with the Federal Service for Intellectual Property under number 2018660604. During this phase, the traffic under investigation is initially divided into overlapping time windows, and the necessary network parameters are extracted from the network packets. Following this, the Discrete Wavelet Transform (DWT) is applied over the time windows containing various lists of extracted network parameters. A multiple correlation coefficient is then calculated over the DWT coefficients to compute the overall coefficient for each set of coefficients within a single window. Subsequently, the standard deviation is calculated for the multiple correlation coefficients to unify the data, and finally, this unified data is clustered using the K-means algorithm.

The second iteration identifies sections of spikes containing malicious traffic tailored to the recipient IP, as determined by the clustering algorithm. In this phase, time windows containing potentially malicious traffic are divided into lists based on the recipient's IP address. The necessary network parameters are extracted from these network packets, and DWT is applied over time windows containing various lists of extracted network parameters. Similar to the first iteration, a multiple correlation coefficient is calculated over the DWT coefficients to compute the overall coefficient for each set of coefficients within

a single window. The standard deviation is then calculated for the multiple correlation coefficients to standardize the data, which is subsequently clustered using the K-means algorithm.

The first iteration allows for the calculation of spikes in network traffic within backbone networks. Since the first iteration facilitates the identification of potentially malicious traffic – and therefore DDoS attacks – the second iteration breaks down suspicious time intervals of network traffic by recipient IP addresses, thereby allowing the sample to be differentiated in relation to the presumed victim. During the execution of the second iteration, traffic in the detected areas is sorted by recipient IP addresses and selected again for parameter extraction, DWT calculation, multiple correlation coefficients, reduction to RMS, and the launch of the K-means algorithm.

This iteration allows for the discarding of the majority of false positive spikes, which may appear mainly in UDP traffic. Figure 3 presents a general diagram of the proposed anomaly detection method.

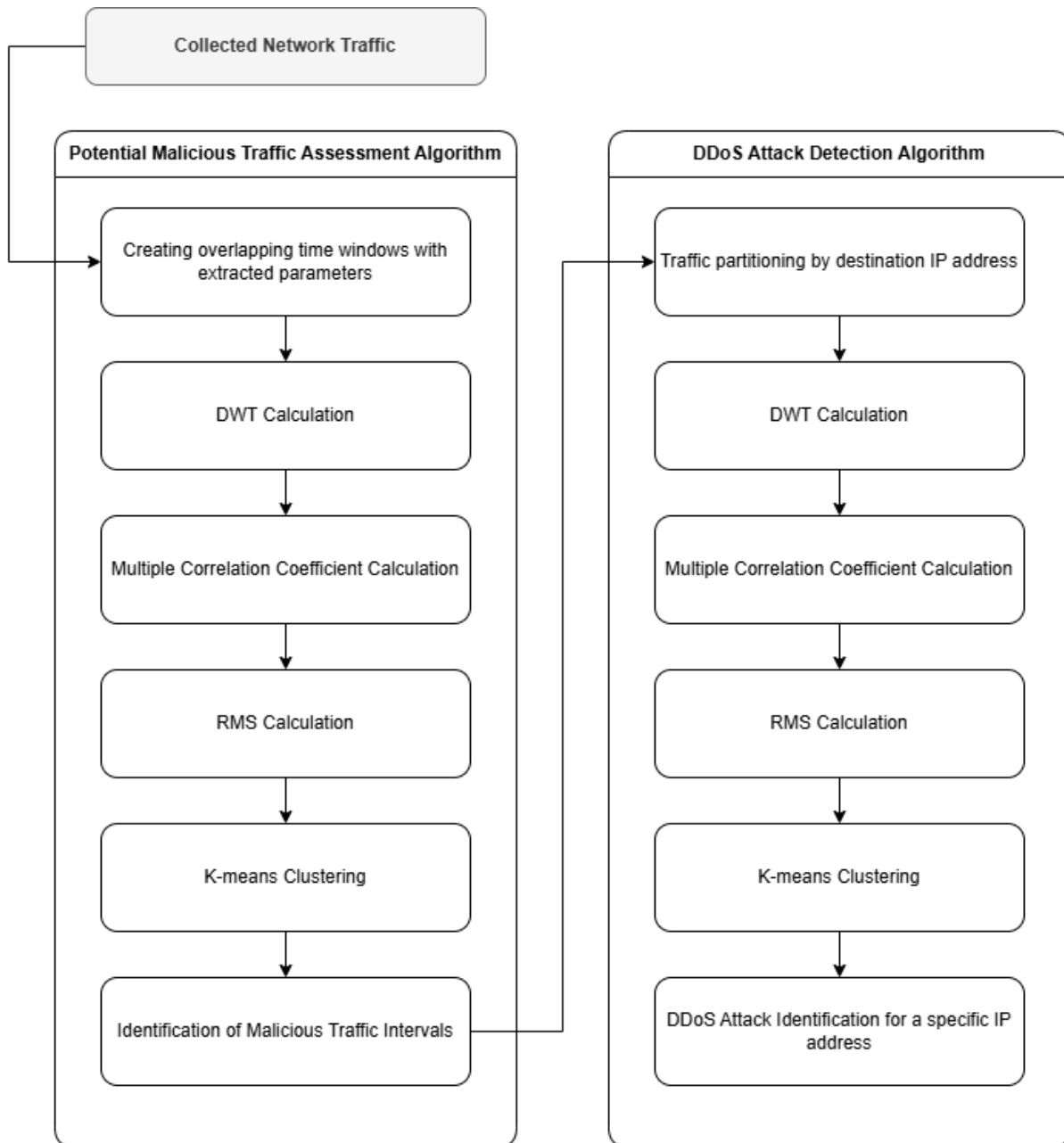


Figure 3: General diagram of the proposed anomaly detection method.

It should be noted that the calculation of the standard deviation is utilized for the unification of parameters for the second iteration, since traffic intensity may vary across different IP addresses. This

results in different numbers of coefficients at different intervals, while clustering must be performed for an equal number of parameters. Nevertheless, the same steps are performed at each iteration to unify the model.

To practically implement the proposed anomaly detection methodology, a prototype system architecture for detecting DDoS attacks in large-scale networks has been developed. The conceptual architecture is illustrated in Figure 4.

Figure 4: Architecture of the prototype DDoS attack detection system in large-scale networks.

1. **Preliminary Traffic Collection:** This initial stage is designed to eliminate real-time processing delays. The captured network traffic is securely stored in a standardized format, making it readily accessible for the subsequent components of the traffic analysis system to extract necessary packet parameters without computational bottlenecks.
2. **Traffic Analysis Execution:** The core processing occurs in this stage, leveraging the detailed methodological framework presented in Section 4. The analysis system systematically divides the incoming traffic into overlapping time windows, performs parameterization, and executes data clustering. It then analyzes the resulting anomaly spikes and automatically triggers the secondary iteration if potential malicious activity is detected.
3. **Target Identification and Mitigation:** The final output generated from the traffic analysis stage contains specific, actionable information, pinpointing the potentially targeted recipient IP addresses under attack. This allows the system to initiate the filtering of the detected attack, ensuring the continuous availability of network resources.

correctly identified by the system, TN (True Negative) the number of correctly identified benign windows, FP (False Positive) the normal traffic incorrectly classified as an attack, and FN (False Negative) the malicious traffic missed by the system.

The primary metric used for evaluation within the system's feedback loop is the Detection Rate (DR). Also referred to as Recall or Sensitivity, the DR is the proportion of all real DDoS attacks that the system is able to successfully detect. It is calculated using the following formula:

$$DR = \frac{TP}{TP + FN} \quad (8)$$

In large-scale backbone networks, minimizing false positives is as critical as detecting the attacks themselves, since frequent false alarms could overwhelm network administrators or even trigger automatic traffic blocking in automated systems. Thus, to measure how much the system misfires, the False Alarm Rate (FAR) is calculated as follows:

$$FAR = \frac{FP}{FP + TN} \quad (9)$$

To obtain a reliable probability that a time window classified as an attack is genuinely malicious, the Precision (PR) metric is utilized by the evaluation module:

$$PR = \frac{TP}{TP + FP} \quad (10)$$

Since network traffic datasets are highly imbalanced (i.e., they contain significantly more benign than malicious traffic on a daily basis), using accuracy as the sole performance measure would be highly misleading. To objectively balance Precision and Detection Rate, the F1-Score is used, which represents their harmonic mean. This provides a single, robust metric for the performance reliability of the given traffic classifier model:

$$F1 = 2 \cdot \frac{PR \cdot DR}{PR + DR} \quad (11)$$

Furthermore, the optimization of the K-means clustering process—conducted during both iterations of the algorithm – relies heavily on selecting the appropriate number of clusters (k). To automate this selection and ensure the model adapts dynamically to varying traffic intensities across different recipient IP addresses, the Elbow Method is employed. This involves calculating the Within-Cluster Sum of Squares (WCSS) for different values of k and searching for the “elbow” point where the rate of decrease sharply shifts. The WCSS optimization function extends equation (7) as follows:

$$WCSS = \sum_{j=1}^k \sum_{a \in C_j} \|a - \mu_j\|^2 \quad (12)$$

By tracking these specific performance metrics across both iterations of the proposed mathematical algorithm, the system architecture guarantees a dynamic thresholding mechanism that actively maintains a high Detection Rate while effectively driving the False Alarm Rate toward zero.

6. Conclusions

This article has described a comprehensive and highly effective approach for the detection of distributed denial-of-service attacks in large-scale networks based on the integration of mathematical statistics, signal processing, and artificial intelligence methods. To improve the efficiency of network traffic security analysis using the proposed approach, several specific methods and algorithms were developed and rigorously evaluated. First, a robust criterion for determining traffic containing at least 15% malicious traffic using Discrete Wavelet Transform (DWT) and multiple correlation coefficients was successfully established, proving that sudden signal variations can be accurately isolated even in heterogeneous traffic.

Additionally, a specific set of TCP and UDP network parameters has been proposed that is sufficient and optimal for further analysis to detect DDoS attacks, significantly reducing the computational overhead required for deep packet inspection.

Furthermore, an algorithm for the preliminary assessment of the potential danger of the analyzed traffic, based on cluster analysis of network traffic in large-scale networks, was proposed. By utilizing the K-means machine learning algorithm across two distinct iterations, the system allows for drastically reducing the number of analyzed network packets while successfully discarding false positive spikes, particularly in UDP traffic. Ultimately, the combined use of these developed methods and algorithms forms a comprehensive, adaptive approach to detecting DDoS attacks in large-scale networks. The proposed system not only allows for the reliable and rapid detection of ongoing distributed denial-of-service attacks but also provides network administrators with a scalable tool to maintain the integrity and availability of critical network infrastructure. Future research will focus on integrating this methodology directly into Software-Defined Networking (SDN) controllers and next-generation 5G architectures, enabling automated, real-time mitigation of sophisticated application-layer anomalies at the network edge [29, 30, 31, 32, 33, 35].

Declaration on Generative AI

The authors have not employed any Generative AI tools.

References

- [1] O. Holubnychyi, O. Lavrynenko, D. Bakhtiiarov, Well-adapted to bounded norms predictive model for aviation sensor systems, in: *Lecture Notes in Networks and Systems*, volume 736, 2023, pp. 179–193. doi:10.1007/978-3-031-38082-2_14.
- [2] D. Bakhtiiarov, B. Chumachenko, O. Lavrynenko, S. Chumachenko, V. Kurushkin, Method of binary detection of small unmanned aerial vehicles, in: *CEUR Workshop Proceedings*, volume 3654, 2024, pp. 312–321.
- [3] S. Mazepa, L. Dostálek, O. Sharmar, S. Banakh, Cybercrime and vulnerability of ukrainian critical information infrastructure, in: *Proceedings of the 10th International Conference on Advanced Computer Information Technologies (ACIT)*, IEEE, Deggendorf, Germany, 2020, pp. 783–786. doi:10.1109/ACIT49673.2020.9208965.
- [4] O. Potii, Y. Tsyplinsky, Methods of classification and assessment of critical information infrastructure objects, in: *Proceedings of the 11th International Conference on Dependable Systems, Services and Technologies (DESSERT)*, IEEE, Kyiv, Ukraine, 2020, pp. 389–393. doi:10.1109/DESSERT50317.2020.9125028.
- [5] L. O. Nweke, S. Wolthusen, Legal issues related to cyber threat information sharing among private entities for critical infrastructure protection, in: *Proceedings of the 12th International Conference on Cyber Conflict (CyCon)*, Estonia, 2020, pp. 63–78. doi:10.23919/CyCon49761.2020.9131721.
- [6] S. B. M. Sabtu, K. M. Mohamad, Critical information infrastructure protection framework development: Preliminary findings from the malaysian public sector, in: *Proceedings of the 8th International Conference on Information Technology and Multimedia (ICIMU)*, IEEE, Selangor, Malaysia, 2020, pp. 1–6. doi:10.1109/ICIMU49871.2020.9263397.
- [7] V. Mokhor, S. Honchar, A. Onyskova, Cybersecurity risk assessment of information systems of critical infrastructure objects, in: *Proceedings of the International Conference on Problems of Infocommunications. Science and Technology (PIC S&T)*, IEEE, Kharkiv, Ukraine, 2020, pp. 19–22. doi:10.1109/PICST51311.2020.9467957.
- [8] O. Illiashenko, V. Kharchenko, O. Odarushchenko, Towards evidence-based cybersecurity assessment of programmable systems to ensure the protection of critical it infrastructure, in: *Proceedings of the 12th International Conference on Intelligent Data Acquisition and Advanced Computing*

Systems: Technology and Applications (IDAACS), IEEE, Dortmund, Germany, 2023, pp. 1178–1183. doi:10.1109/IDAACS58523.2023.10348834.

- [9] O. Shmatko, et al., Synthesis of the optimal algorithm and structure of contactless optical device for estimating the parameters of statistically uneven surfaces, *Radioelectronic and Computer Systems* (2021) 199–213. doi:10.32620/reks.2021.4.16.
- [10] R. Zhang, G. Liu, J. Liu, J. P. Nees, Analysis of message attacks in aviation data-link communication, *IEEE Access* 6 (2018) 455–463. doi:10.1109/ACCESS.2017.2767059.
- [11] G. Wang, G. Xu, Z. Zheng, J. Li, Secure transmission technology based on air-to-ground aviation networks, in: *Proceedings of the 10th Asia Conference on Mechanical Engineering and Aerospace Engineering (MEAE)*, IEEE, 2024, pp. 1580–1583. doi:10.1109/MEAE62008.2024.11026393.
- [12] S. Khan, Y. Wang, G. S. Gaba, A. Gurtov, P. Kumar, A secure framework for controller pilot data link communications in aviation network, in: *Proceedings of the AIAA DATC/IEEE 43rd Digital Avionics Systems Conference (DASC)*, IEEE, 2024, pp. 1–11. doi:10.1109/DASC62030.2024.10749527.
- [13] N. Ahmed, M. E. Hossain, N. Begum, Ai-driven cyber security for safeguarding critical infrastructure and patient data, in: *Proceedings of the International Conference on Machine Learning and Autonomous Systems (ICMLAS)*, IEEE, Prawet, Thailand, 2025, pp. 1485–1492. doi:10.1109/ICMLAS64557.2025.10968807.
- [14] D. Lofù, A. Pazienza, A. Abbatecola, E. Lella, N. Macchiarulo, P. Noviello, Watching against the unseen: Ai-powered approach to detect attacks on critical infrastructure, in: *Proceedings of the 8th International Conference on Smart and Sustainable Technologies (SpliTech)*, IEEE, Split/Bol, Croatia, 2023, pp. 1–6. doi:10.23919/SpliTech58164.2023.10193130.
- [15] O. Solomentsev, et al., Data processing through the lifecycle of aviation radio equipment, in: *2022 IEEE 17th International Conference on Computer Sciences and Information Technologies (CSIT)*, 2022, pp. 146–151. doi:10.1109/CSIT56902.2022.10000844.
- [16] H. A. Al-Mohammed, et al., Detecting attackers during quantum key distribution in iot networks using neural networks, in: *Proceedings of the Globecom Workshops (GC Wkshps)*, IEEE, Madrid, Spain, 2021, pp. 1–6. doi:10.1109/GCWkshps52748.2021.9681988.
- [17] S. Adilzhanova, et al., Improving critical infrastructure protection: Assessment methods, ai, digital twins, in: *Proceedings of the 7th Asia Conference on Cognitive Engineering and Intelligent Interaction (CEII)*, IEEE, Singapore, 2024, pp. 130–134. doi:10.1109/CEII65291.2024.00033.
- [18] V. Volkogon, T. Konrad, O. Kolganova, L. Tereshchenko, Situational synthesis of algorithmic support of regional transport systems based on expert system, in: *Proceedings of the International Workshop on Advances in Civil Aviation Systems Development*, volume 736 of *Lecture Notes in Networks and Systems*, 2023, pp. 321–333. doi:10.1007/978-3-031-38082-2_25.
- [19] O. Holubnychy, et al., Self-organization technique with a norm transformation based filtering for sustainable infocommunications within CNS/ATM systems, in: I. Ostroumov, M. Zaliskyi (Eds.), *Proceedings of the 2nd International Workshop on Advances in Civil Aviation Systems Development*, volume 992 of *Lecture Notes in Networks and Systems*, Springer Nature Switzerland, Cham, 2024, pp. 262–278. doi:10.1007/978-3-031-60196-5_20.
- [20] O. Lavrynenko, D. Bakhtiarov, V. Kurushkin, S. Zavorodnii, V. Antonov, P. Stanko, A method for extracting the semantic features of speech signal recognition based on empirical wavelet transform, *Radioelectronic and Computer Systems* 3 (2023) 101–124. doi:10.32620/reks.2023.3.09.
- [21] B. Kotyk, D. Bakhtiarov, O. Lavrynenko, B. Chumachenko, V. Antonov, V. Fesenko, V. Chupryn, Neural network approach to 5g digital modulation recognition, in: *CEUR Workshop Proceedings*, volume 3925, 2024, pp. 82–92.
- [22] M. Jiménez-Aparicio, M. J. Reno, J. W. Pierre, The high-resolution wavelet transform: A generalization of the discrete wavelet transforms, in: *Proceedings of the IEEE 13th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON)*, IEEE, New York, USA, 2022, pp. 395–401. doi:10.1109/UEMCON54665.2022.9965716.
- [23] N. Mäurer, T. Gräupl, C. Schmitt, Efficient control-channel security for the aeronautical communications system Idacs, in: *Proceedings of the 2023 IEEE 24th International Symposium on*

- a World of Wireless, Mobile and Multimedia Networks (WoWMoM), IEEE, 2023, pp. 407–412. doi:10.1109/WoWMoM57956.2023.00072.
- [24] M. Cutajar, E. Gatt, I. Grech, O. Casha, J. Micallef, Discrete wavelet transforms with multiclass svms for phoneme recognition, in: Proceedings of the Eurocon 2013, IEEE, Zagreb, Croatia, 2013, pp. 1695–1700. doi:10.1109/EUROCON.2013.6625205.
 - [25] S. Ravi, S. Taran, Emotion recognition using rational dilation wavelet transform for speech signal, in: Proceedings of the 7th International Conference on Signal Processing and Communication (ICSC), IEEE, Noida, India, 2021, pp. 156–160. doi:10.1109/ICSC53193.2021.9673412.
 - [26] O. Y. Lavrynenko, D. I. Bakhtiarov, B. S. Chumachenko, O. G. Holubnychyi, G. F. Konakhovych, V. V. Antonov, Application of daubechies wavelet analysis in problems of acoustic detection of uavs, in: CEUR Workshop Proceedings, volume 3662, 2024, pp. 125–143.
 - [27] P. Mehra, S. Kant Verma, Comparing classifiers for recognizing the emotions by extracting the spectral features of speech using machine learning, in: Proceedings of the 2023 International Conference on Device Intelligence, Computing and Communication Technologies (DICCT), IEEE, Dehradun, India, 2023, pp. 387–391. doi:10.1109/DICCT56244.2023.10110282.
 - [28] L. R. S. Olea, E. S. Juan, P. Adasme, L. C. Arratia, A. D. Firoozabadi, Optimization of the signal reconstruction process by multiresolution analysis for a signal with gaussian noise using the sure-shrink algorithm and wavelet daubechies, in: Proceedings of the 2023 South American Conference on Visible Light Communications (SACVLC), IEEE, Santiago, Chile, 2023, pp. 76–81. doi:10.1109/SACVLC59022.2023.10347793.
 - [29] P. Wright, et al., 5g network slicing with qkd and quantum-safe security, Journal of Optical Communications and Networking 13 (2021) 33–40. doi:10.1364/JOCN.413918.
 - [30] M. Mehic, L. Michalek, E. Dervisevic, P. Burdiak, M. Plakalovic, J. Rozhon, N. Mahovac, F. Richter, E. Kaljic, F. Lauterbach, P. Njemcevic, A. Maric, M. Hamza, P. Fazio, M. Voznak, Quantum cryptography in 5g networks: A comprehensive overview, IEEE Communications Surveys & Tutorials 26 (2024) 302–346. doi:10.1109/COMST.2023.3309051.
 - [31] T. A. Pham, N. T. Dang, Quantum key distribution: A security solution for 5g-based iot networks, in: Proceedings of the International Conference on Advanced Technologies for Communications, IEEE, Ha Noi, Vietnam, 2022, pp. 147–152. doi:10.1109/ATC55345.2022.9943041.
 - [32] K. A. Kumar, R. Mohandas, S. Suneel, M. R. Mahalakshmi, A. Kumar, M. Singh, Quantum-driven hybrid network architecture leveraging 5g for high-speed and resilient data transmission, in: Proceedings of the 6th International Conference on Mobile Computing and Sustainable Informatics (ICMCSI), IEEE, Goathgaun, Nepal, 2025, pp. 84–91. doi:10.1109/ICMCSI64620.2025.10883451.
 - [33] P. Burdiak, L. Kapičák, L. Michalek, E. Dervisevic, M. Mehic, M. Vozňák, Demonstration of qkd integration into 5g campus network, in: Proceedings of the International Conference on Software, Telecommunications and Computer Networks (SoftCOM), IEEE, Split, Croatia, 2023, pp. 1–4. doi:10.23919/SoftCOM58365.2023.10271676.
 - [34] O. Solomentsev, M. Zaliskyi, O. Kozhokhina, T. Herasymenko, Efficiency of data processing for uav operation system, in: 2017 IEEE 4th International Conference Actual Problems of Unmanned Aerial Vehicles Developments (APUAVD), 2017, pp. 27–31. doi:10.1109/APUAVD.2017.8308769.
 - [35] B. Kotyk, D. Bakhtiarov, B. Chumachenko, Y. Burmak, S. Chumachenko, O. Lavrynenko, Neural network approach to 5g digital modulation recognition under a priori uncertainty of parameters, in: CEUR Workshop Proceedings, volume 4024, 2025.