Image-Based Frequency-Domain Analysis for Robust DDoS Detection in SDN

1st Ramin Fuladi
Ericsson Research
Istanbul, Turkiye
ramin.fuladi@ericsson.com

2nd Bilal Cicek
Ericsson Research
Istanbul, Turkiye
bilal.cicek@ericsson.com

2025 IEEE 11th International Conference on Network Softwarization (NetSoft) | 979-8-3315-4345-7/25/$31.00 ©2025 IEEE | DOI: 10.1109/NETSOFT64993.2025.11080612

***Abstract*—Software-Defined Networking (SDN) enhances network management by offering greater adaptability, flexibility, and scalability. However, its centralized controller is susceptible to Distributed Denial of Service (DDoS) attacks, which can compromise network availability. This study proposes an innovative real-time DDoS detection mechanism integrated into the SDN controller. The approach employs frequency-domain analysis to examine Packet-In messages. A time series is created by sampling the number of Packet-In messages at specific time intervals. This time series is then transformed into one or more images using frequency-domain analysis, enabling the extraction of hidden patterns indicative of DDoS attack traffic. Converting time series data into images allows for multi-scale frequency analysis by adjusting the window size, which helps capture both short-term fluctuations and long-term trends. Additionally, different images obtained from varying window sizes are rescaled to a uniform size with minimal information loss, enhancing the effectiveness of pattern recognition. These frequency-based images, encapsulating both amplitude and phase information, are then utilized by a Convolutional Neural Network (CNN) to detect DDoS attack traffic with improved accuracy.**

***Index Terms*—Distributed Denial of Service, Frequency domain analysis, SoftwareDefined Networking, PacketIn message.**

I. Introduction

Software-Defined Networking (SDN) is a flexible, dynamic, and cost-effective architecture that separates the control and data planes, and enables centralized, software-based management of the network and its devices [1]. Unlike traditional architectures where all planes are integrated into individual devices, SDN centralizes control in a software-based controller, allowing administrators to quickly configure, secure, and optimize resources [2]. While SDN supports dynamic behaviors required by mobile network technologies like 5G and beyond 5G (B5G), its centralized design makes it vulnerable to threats such as Distributed Denial of Service (DDoS) attacks [3]. In a DDoS attack, a network of compromised devices floods the controller with crafted traffic, depleting resources such as bandwidth and memory and disrupting service for legitimate users. The use of spoofed IP addresses makes it even more difficult to trace the origin of the attack [4].

To detect DDoS attacks, network administrators utilize Intrusion Detection Systems (IDS), which are classified as either signature-based or anomaly-based. Signature-based IDSs identify threats by matching them against known signatures, while anomaly-based IDSs detect deviations from normal network behavior, making them capable of identifying zero-day attacks but more prone to higher number of false positives [5].

Various methods for DDoS detection have been proposed for traditional networks [4], [6]–[9]. However, SDN's unique characteristics enable advanced features and greater flexibility, enhancing the effectiveness of DDoS detection and mitigation strategies.

A. Problem Definition

The centralized and dynamic nature of SDN makes it vulnerable to Distributed Denial of Service (DDoS) attacks, which exploit the controller's role in managing multiple devices by flooding it with malicious traffic [3]. Detecting these attacks is a challenge, as the attackers often use spoofed IP addresses to disguise their activities, therefore; advanced techniques are required to distinguish malicious patterns from normal traffic.

Data analytics, including Machine Learning (ML) and statistical methods, provide effective solutions for detecting DDoS attacks in SDN by analyzing traffic statistics such as Packet-In messages sent to the controller. During an attack, these messages show distinct patterns, with time-domain analysis revealing sharp spikes in message arrival rates that are above normal thresholds. Time-series analysis helps identify these anomalies by tracking deviations from baseline traffic.

In addition, analysis in the frequency domain can be performed using methods such as Fast Fourier Transform (FFT), can detect changes in the spectral components and highlight attack-specific patterns. DDoS attacks can introduce new frequencies or amplify frequencies that are associated with high traffic volumes, altering the normal frequency distribution.

This study introduces a software-based detection system integrated into the SDN controller to analyze the behavior of Packet-In messages and identify anomalies caused by

This work was funded by The Scientific and Technological Research Council of Turkey, under 1515 Frontier R&D Laboratories Support Program with project (Grant number: 5169902), and in part by the ROBUST-6G Project through the Smart Networks and Services Joint Undertaking (SNS JU) under the European Union's Horizon Europe Research and Innovation Program (Grant number: 101139068).

Authorized licensed use limited to: Ericsson. Downloaded on February 20,2026 at 06:46:51 UTC from IEEE Xplore. Restrictions apply.

protocol-based volumetric attacks. These attacks include TCP-SYN floods, NTP amplification, and DNS reflection attacks, which exploit network protocols to overwhelm SDN controllers with excessive traffic. The proposed system builds upon the foundation of the approach presented in [10]. In [10], the detection mechanism relies on analyzing the frequency-domain characteristics of a time-series generated from the number of Packet-In messages received by the SDN controller. However, the existing approach only considers the absolute values of the frequency-domain features and ignore important phase-related information. This limitation reduces the effectiveness of the system in preserving the complete spectral representation of network traffic. To address this gap, this study extends the previous methodology by including phase information in the analysis. It also converts the extracted data into an image representation instead of working directly with raw features in the frequency domain. This transformation preserves the semantic relationships between complex-number elements in the frequency domain and enables more effective feature extraction and classification. Furthermore, the selection of an appropriate window size (w) for frequency-domain analysis is a complex trade-off. If w is too small, lower-energy frequency components may be overlooked, reducing the method's sensitivity. Conversely, the method may suffer from the non-stationarity of network traffic, which can distort frequency resolution and hinder accurate analysis. To solve this problem, several ws can be selected by converting the time series in the frequency domain into a square image representation.. Each transformed time-series is converted into an image, and all images are then rescaled to a uniform size with minimal information loss. In this way, multiple frequency representations can be fed into ML models simultaneously, using different window sizes to capture a wider range of dominant frequency components. As a result, our approach enhances detection performance by incorporating richer frequency-domain information while maintaining computational efficiency. The key contributions of this study are summarized as follows:

- An improved SDN-based anomaly detection approach that integrates phase information from the frequency-domain representation of Packet-In message behavior, enhancing the accuracy of DDoS attack detection.
- A novel method for converting frequency-domain data into image representations, preserving both magnitude and phase information to maintain the structural integrity of network traffic patterns.
- Converts time-series data from the frequency domain to square image representations and allows the integration of multiple window sizes to preserve more phase-related information. This improves the performance of the ML model by capturing a wider range of frequency components, improving the accuracy of DDoS detection.

The rest of this paper is organized as follows: Firstly, a related work on the area is given in Section II. In Section III, the proposed DDoS attack detection method is described. Implementation details and experiments are elaborated in Section IV. The limitation of the proposed system is discussed in Section V. Finally, the study is concluded in Section VI.

II. Literature Overview

DDoS attack detection techniques in SDN generally fall into two categories: statistical-based and machine learning (ML)-based approaches. Statistical methods analyze network traffic features using predefined thresholds, while ML-based techniques extract traffic features for classification using conventional or deep learning models.

Entropy is widely used in statistical approaches to measure randomness within a given time window. Several studies utilize entropy-based methods for DDoS detection. For example, [11] evaluates entropy's effectiveness in identifying both low- and high-rate DDoS attacks, demonstrating improved detection for high-rate attacks. In [12], entropy variations in source IP addresses and packet sizes are used to detect and mitigate shrew attacks, with Access Control Lists (ACLs) and flow tables handling mitigation. [13] introduces a two-level detection approach combining fast entropy analysis with ML classification. Other works, such as [14], [15], and [16], propose various entropy-based detection methods, leveraging statistical measures like Kullback-Leibler divergence, Hurst coefficients, and Rényi entropy for improved accuracy. [17] presents SynFloWatch, which employs Tsallis entropy to detect TCP-SYN-based DDoS attacks in hybrid SDN environments.

Despite their advantages, entropy-based approaches have limitations. They compress all probability distribution characteristics into a single value, potentially leading to information loss and reduced detection accuracy. Furthermore, fixed threshold values used during training may fail to adapt to dynamic network behavior. To overcome these issues, time-series-based methods have been proposed. For instance, [18] utilizes an Auto-Regressive Integrated Moving Average (ARIMA) model with an adaptive threshold to detect DDoS attacks more effectively than entropy-based approaches.

Given the success of artificial intelligence (AI) and ML algorithms in classification, they have also been applied to DDoS detection in SDN. These approaches rely on selecting the most relevant features to differentiate attack traffic from normal traffic, using both time-domain and frequency-domain features. Several studies explore ML-based solutions: [19] introduces FMDADM, an SDN-based framework integrating multiple detection modules, including a deep learning classifier. [20] applies ML models such as KNN, SVM, Decision Tree, and Random Forest, with the latter two demonstrating the best performance. Other works, including [21] and [22], employ ML classifiers for attack detection, with some models integrating SHAP-based feature selection and hybrid deep learning architectures.

Deep learning techniques have also been explored for DDoS detection in SDN. [2] applies Continuous Wavelet Transform

Authorized licensed use limited to: Ericsson. Downloaded on February 20,2026 at 06:46:51 UTC from IEEE Xplore. Restrictions apply.

(CWT) to extract two-dimensional frequency-domain features, classifying traffic samples using a CNN. Similarly, [23] utilizes statistical features from Discrete Wavelet Transform (DWT) in an autoencoder-based neural network. The effectiveness of frequency-domain analysis for DDoS detection in traditional networks [24], [25] has inspired its adaptation for SDN, highlighting its potential for improving detection accuracy. In [10], a DDoS attack detection system based on frequency domain analysis is proposed. This method transforms a time-series generated from the number of PacketIn messages received by the SDN controller into the frequency domain. The absolute values of the resulting complex-number time-series serve as feature inputs for various ML models to distinguish volumetric DDoS traffic from legitimate network traffic.

Compared to statistical-based techniques, ML-based approaches exhibit superior performance in detecting DDoS attacks in SDN environments due to their ability to adapt to intricate and evolving traffic behaviors. However, their success is highly dependent on selecting an optimal feature set—a task that remains a fundamental challenge. The ideal feature set should be generalizable across different attack scenarios and network conditions while being independent of the specific ML model used. Striking a balance between detection accuracy and computational efficiency is critical, as many existing approaches suffer from feature redundancy, information loss, or high processing overhead.

In this study, we tackle this challenge by proposing an enhanced version of the approach introduced in [10]. Unlike the original method, which primarily focuses on the magnitude of frequency-domain characteristics, our approach incorporates both magnitude and phase information to mitigate information loss, leading to more robust attack detection. Additionally, we introduce an innovative image-based representation of the frequency-domain time-series, preserving the spatial and semantic relationships between complex-number elements. By converting the transformed data into a square image format, we enable the integration of multiple window sizes, ensuring that both short- and long-term frequency components are effectively captured. This transformation not only enhances the feature expressiveness but also allows deep learning models to better capture intricate patterns within the data. By leveraging both frequency-phase information and spatial correlations, our approach significantly improves detection accuracy while maintaining computational efficiency, making it a more effective solution for securing SDN networks against DDoS attacks.

III. Proposed Detection and Defense system

In this section, the DDoS attack detection and defense system based on frequency domain analysis is presented. The proposed system relies on Packet-In messages sent to the controller for detecting DDoS attack traffic. Communication between the controller and switches is managed using the OpenFlow [26] protocol.

Figure 1 provides an overview of the proposed system, which comprises two main modules: (i) *Statistic Generation* module and (ii) *DDoS Attack Detection* module.

The *Statistic Generation* module monitors the Packet-In messages arriving at the controller and extracts two statistics: the number of Packet-In messages received during each time interval t, denoted as x_t, and the hash table of unique destination IP addresses (H_D). The time series of x_t, $\mathcal{X}$, is utilized by the *DDoS Attack Detection* module to identify DDoS attack traffic samples.

A. Statistic Generation Module

This module extracts important statistics from the Packet-In messages received at the controller to detect DDoS attack traffic. Attackers typically use random source IP addresses, reducing the likelihood of matching flow entries in the switches' flow tables. Consequently, the number of Packet-In messages sent to the controller increases, altering their patterns in both time and frequency domains during a DDoS attack.

The first statistic, x_t, represents the number of Packet-In messages received during a specific time interval t. This statistic is employed by the *DDoS Attack Detection* module to identify DDoS attack traffic.

Additionally, the module employs statistics obtained from a hash table, H_D, to track destination IP addresses and their occurrence frequencies. Each entry in H_D contains a destination IP address and a counter that records the number of occurrences. During a DDoS attack, the destination IP address with the highest count in H_D typically belongs to the victim, as the number of packets directed to the victim increases significantly. The *DDoS Attack Detection* module utilizes H_D during the countermeasure phase to identify the victim's IP address.

B. DDoS Detection Module

The primary function of the DDoS Detection module is to extract features for identifying DDoS attacks using frequency domain analysis. Initially, the module takes the time-series data of x_t and concatenates w consecutive samples to create a windowed time-series, denoted as $\mathcal{X} = \{x_1, x_2, \ldots, x_w\}$. This time-series is then transformed into the frequency domain by applying the Discrete Fourier Transform (DFT), resulting in the complex frequency-domain time-series, $X(f)$.

The frequency-domain representation can then be expressed as:

$$X(f) = \{r_1 e^{j\phi_1}, r_2 e^{j\phi_2}, \ldots, r_w e^{j\phi_w}\}, \tag{1}$$

where each r_w represents amplitude and each $e^{j\phi_w}$ is a complex exponential, with ϕ_i representing the phase of the corresponding frequency component.

To further process the frequency domain data into a form suitable for machine learning, an approach inspired by the Gramian matrix is utilized to convert the frequency-domain signal into an image. In this approach, each element in $X(f)$ is treated as a vector, and the similarity or semantic distance between these vectors is captured in a square matrix. Specifically,

Authorized licensed use limited to: Ericsson. Downloaded on February 20,2026 at 06:46:51 UTC from IEEE Xplore. Restrictions apply.

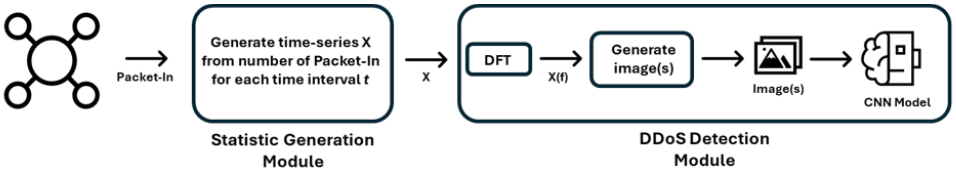

Packet-In
Generate time-series X from number of Packet-In for each time interval t
X
DFT
X(f)
Generate image(s)
Image(s)
CNN Model
Statistic Generation Module
DDoS Detection Module

Fig. 1: Proposed System.

an $w \times w$ matrix is constructed, where each element corresponds to the inner product of pairs of vectors in $X(f)$.

For our case, the phase difference between each pair of elements in $X(f)$ is also considered in the complex plane. The similarity matrix is constructed by multiplying a vector with its Hermitian transpose. Mathematically, this is represented as:

$$Y = X * \frac{1}{X^H} = \begin{bmatrix} e^{j(2\phi_1)} & \dots & \frac{r_1}{r_w} e^{j(\phi_1 - \phi_w)} \\ \vdots & \ddots & \vdots \\ \frac{r_w}{r_1} e^{j(\phi_w - \phi_1)} & \dots & e^{j(2\phi_w)} \end{bmatrix}, \qquad (2)$$

where the matrix elements are the complex exponential of phase differences between each pair of frequency components. This matrix contains both the cosine and sine components, as $e^{j\phi} = \cos\phi + j\sin\phi$. Thus, the matrix consists of both real (cosine) and imaginary (sine) parts.

Then, the maximum amplitude value of each row is calculated and each row is normalized via this maximum value. This normalized matrix represented as Y_N is given to the logarithmic operation. This can be formulated as $\log_{10}(Y_N)$. The cosine and sine components of this matrix define two distinct planes: the cosine plane and the sine plane. These two planes form the basis of the image generated from the frequency similarity matrix. The size of the resulting image is $w \times w$, corresponding to the number of time-series samples used. By selecting either the cosine or sine part of the matrix, we obtain the final image representation of the frequency similarity, which is then used by the CNN model to detect DDoS traffic samples.

IV. Experimental Results

This section presents the evaluation of the proposed system's performance, including the experimental setup, dataset,and detailed results.

A. Simulation Setup

The experimental setup, depicted in Figure 2, follows the network topology used in [23]. Simulations are conducted in the GNS3 environment [27] using the Mininet emulator [28]. The SDN topology consists of a Ryu controller [1] managing three OpenFlow switches ($S1$, $S2$, and $S3$), with communication via OpenFlow 1.3 [29].

To simulate real-world traffic, trace data from the MAWI dataset [30] is used as normal and background traffic, injected into the network via the TcpReplay tool [31]. DDoS attack traffic, including TCP-SYN, NTP, and DNS-based attacks, is generated using a Docker container in the SDN setup, integrated through a virtual router. The network is hosted in VirtualBox and all components run within the GNS3 environment. Attack traffic is generated using Hping3, with spoofed and randomized source IPs, mimicking real-world DDoS attacks.

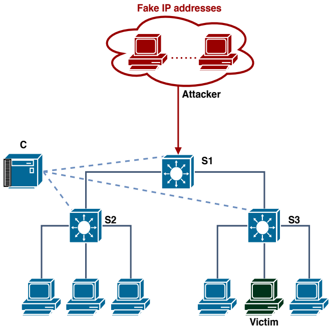
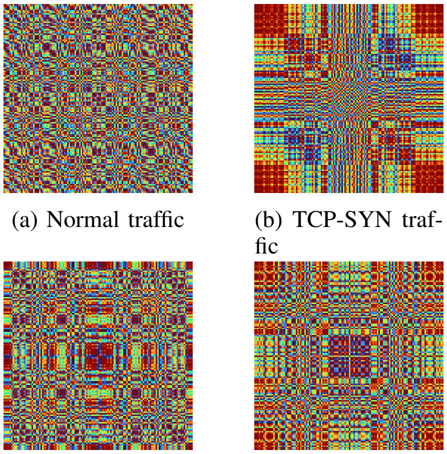


Fig. 2: Proposed Scheme.



(a) Normal traffic

(b) TCP-SYN traffic

(c) NTP traffic

(d) DNS traffic

Fig. 3: Images representing four traffic types: (a) Normal, (b) TCP-SYN, (c) NTP, (d) DNS.

The attack traffic enters through $S1$, traverses $S2$ and $S3$, and reaches the victim. The attacks evaluated are:

- TCP-SYN: TCP-based, Destination port = 80, SYN flag, Packet size = 90 bytes.
- NTP: UDP-based, Destination port = 123, Packet size = 90 bytes.
- DNS: UDP-based, Destination port = 53, Packet size = 60 bytes.

The goal of the TCP-SYN flood is to overwhelm the system with SYN requests, while the NTP and DNS attacks aim to exhaust the bandwidth with a high volume of UDP packets.

[1] https://ryu-sdn.org/

Authorized licensed use limited to: Ericsson. Downloaded on February 20,2026 at 06:46:51 UTC from IEEE Xplore. Restrictions apply.

B. Discussion

In this section, the performance of the proposed system is thoroughly evaluated using the experimental setup depicted in Figure 2. The evaluation follows a structured methodology, starting from data collection and progressing through a series of processing steps, ultimately leading to the transformation of the data into an image representation. The process begins with the *Statistic Generation* module, which is responsible for monitoring and analyzing network activity. This module counts the number of incoming Packet-In messages, denoted as x_t, within fixed time intervals of $t = 10$ ms. By continuously recording these values over consecutive time windows, a time-series representation of network traffic is formed, expressed as $\mathcal{X} = \{x_1, x_2, \ldots, x_w\}$, where the total number of samples within a single observation window is set to $w = 128$. Once the time-series data $\mathcal{X}$ is generated, it is processed by the *DDoS Attack Detection* module, which applies analytical techniques to identify potential attack patterns. To extract meaningful frequency-domain features, the time-series $\mathcal{X}$ undergoes transformation using the Fast Fourier Transform (FFT) algorithm [32], an efficient method for computing the Discrete Fourier Transform (DFT). This transformation converts the original time-domain signal into its corresponding frequency-domain representation. The output is $\mathcal{X}(f)$, a complex-valued time-series with the same length as the original sequence, i.e., $w = 128$. After the frequency-domain transformation, an image representation is generated from the processed data. This step involves reshaping the extracted frequency components into a structured two-dimensional matrix representation with dimensions $R^{128\times128}$. The resulting image serves as a crucial input for further analysis, such as deep learning-based classification or anomaly detection, leveraging both spatial and spectral characteristics to enhance the accuracy of DDoS detection. This approach effectively captures both temporal and frequency-domain features, providing a robust and efficient method for detecting and mitigating DDoS attacks.

Figure 3 presents a set of image examples derived from Packet-IN samples, illustrating distinct patterns associated with different traffic types. As depicted in the figure, each traffic category exhibits a unique visual signature, making these features well-suited for distinguishing between normal and attack traffic.

Following the conversion of frequency-domain features into image representations, these visualized data structures serve as the primary input for the machine learning models employed in the analysis. By transforming raw network traffic information into a structured image format, the system enables more effective feature extraction and pattern recognition, facilitating enhanced detection capabilities. In this study, a Convolutional Neural Network (CNN) is utilized as the core model for identifying and classifying potential DDoS attacks. CNNs are particularly well-suited for this task due to their ability to automatically learn hierarchical spatial features from image data, making them highly effective in distinguishing between normal and anomalous traffic patterns. The model processes the generated images through multiple convolutional layers, capturing both low-level and high-level frequency patterns associated with DDoS attacks. Table I provides a detailed breakdown of the CNN classifier architecture, including the number of layers and the corresponding parameter counts. The selection of layer depth, number of filters, and filter sizes was made empirically to optimize performance. Each convolutional kernel within the network is configured as a 5×5 filter. The overall CNN model consists of 10,871,898 trainable parameters, which are iteratively updated during the training process. With the exception of the final layer, which employs the Softmax activation function for classification, all other layers utilize the ReLU activation function to enhance non-linearity and improve feature extraction.

To assess the effectiveness of our proposed method and compare it with the previous study [10], we train the CNN model using both normal and DDoS traffic. Our dataset consists of a total of 9,000 images, with 4,500 representing normal traffic and 4,500 representing DDoS traffic. For training, we allocate 70% of each traffic type (3,150 samples), while the remaining 30% (1,350 samples) is reserved for testing.

Our evaluation relies on standard performance metrics, including True Positive Rate (TPR) / Recall, False Positive Rate (FPR), Precision (PER), F1-score (F1), and Accuracy (ACC). The results, summarized in Table II, provide a comparative analysis between the method proposed in [10] and our novel image-based approach. The findings demonstrate that our method achieves detection performance, with improvements in precision, recall, F1-score, and overall accuracy. By leveraging frequency-phase information and spatial correlations through image representation, our approach effectively captures complex traffic patterns, reducing misclassification rates and enhancing detection reliability. These results highlight the potential of our method as a robust and efficient solution for frequency-based DDoS attack detection in SDN environments.

TABLE I: The layers and parameters of CNN architecture.

Layer	Output shape	# of Parameters
Conv_1	$60 \times 60 \times 32$	1632
MaxPooling	$30 \times 30 \times 32$	0
Conv_2	$26 \times 26 \times 64$	51264
MaxPooling	$13 \times 13 \times 64$	0
Flatten	10816	0
Fully connected	1000	10817000
Fully connected	2	2002

V. Threats to Validity

It is essential to acknowledge and address potential threats that may affect the validity of our research. Below, we outline key factors that could influence our findings and discuss future directions to mitigate these concerns.

A. Scalability and Granularity

Our experiments were conducted in an isolated emulation environment, which may not fully reflect the complexities of real-world networks. The impact of DDoS attack traffic varies across different network layers, exhibiting distinct characteristics at each level. Additionally, DDoS attack patterns are diverse and continuously evolving, which may limit the generalizability of our approach. To overcome these limitations, future research will focus on evaluating the proposed method in real-world scenarios and practical deployments.

B. DDoS Attack Type Coverage

This study primarily investigates three types of volumetric DDoS attacks. However, numerous other attack types exist, each with unique characteristics and potential impacts. Expanding the scope of our analysis to include a broader range of DDoS attack variants will be a key focus of future research.

By recognizing and addressing these threats to validity, we aim to enhance the robustness and applicability of our proposed method, ensuring its effectiveness in dynamic and diverse network environments.

VI. Conclusion

In this paper, we proposed an enhanced DDoS detection method for SDN environments by leveraging both magnitude and phase information from frequency-domain analysis. Unlike prior approaches that rely solely on magnitude, our method reduces information loss and improves detection accuracy. Furthermore, we introduced an innovative image-based representation of frequency-domain time-series data,

Authorized licensed use limited to: Ericsson. Downloaded on February 20,2026 at 06:46:51 UTC from IEEE Xplore. Restrictions apply.

TABLE II: The comparison of DDoS attack detection between proposed system and the systems in [10]

	TPr (%)	FPr (%)	PEr (%)	ACC (%)	F1_score
Proposed system	99.96	0	100	99.98	0.999
system in [10], 2024	99.88	0.18	99.84	99.85	0.998

allowing deep learning models to capture intricate spatial and semantic relationships. This transformation enhances feature expressiveness and enables more effective detection of evolving attack patterns.

Our experimental results demonstrate that the proposed approach outperforms existing methods in terms of precision, recall, F1-score, and overall accuracy. By incorporating multiple window sizes in the frequency transformation process, our method preserves dominant frequency components, further refining detection performance. Future work will focus on evaluating the approach in real-world network environments, exploring additional DDoS attack variations, and optimizing computational efficiency to enhance scalability. The findings of this study highlight the potential of frequency-domain-based image representations for advancing network security solutions in SDN architectures.

References

[1] C. Jisi, B.-h. Roh, and J. Ali, “Reliable paths prediction with intelligent data plane monitoring enabled reinforcement learning in sd-iot,” *Journal of King Saud University-Computer and Information Sciences*, vol. 36, no. 3, p. 102006, 2024.

[2] R. F. Fouladi, O. Ermiş, and E. Anarim, “A novel approach for distributed denial of service defense using continuous wavelet transform and convolutional neural network for software-defined network,” *Computers & Security*, vol. 112, p. 102524, 2022.

[3] Y. Maleh, Y. Qasmaoui, K. El Gholami, Y. Sadqi, and S. Mounir, “A comprehensive survey on sdn security: threats, mitigations, and future directions,” *Journal of Reliable Intelligent Environments*, pp. 1–39, 2022.

[4] L. Abdelrazek, R. Fuladi, J. Kövér, L. Karaçay, and U. Gülen, “Detecting ip ddos attacks using 3gpp radio protocols,” *IEEE Access*, vol. 12, pp. 24 776–24 790, 2024.

[5] S. Santhosh Kumar, M. Selvi, and A. Kannan, “A comprehensive survey on machine learning-based intrusion detection systems for secure communication in internet of things,” *Computational Intelligence and Neuroscience*, vol. 2023, no. 1, p. 8981988, 2023.

[6] H. Che and J. Wang, “A nonnegative matrix factorization algorithm based on a discrete-time projection neural network,” *Neural Networks*, vol. 103, pp. 63–71, 2018.

[7] H. Che, J. Wang, and A. Cichocki, “Bicriteria sparse nonnegative matrix factorization via two-timescale duplex neurodynamic optimization,” *IEEE Transactions on Neural Networks and Learning Systems*, vol. 34, no. 8, pp. 4881–4891, 2021.

[8] H. Jing and J. Wang, “Ddos detection based on graph structure features and non-negative matrix factorization,” *Concurrency and Computation: Practice and Experience*, vol. 34, no. 9, p. e5783, 2022.

[9] R. Fuladi, T. Baykas, and E. Anarim, “The use of statistical features for low-rate denial-of-service attack detection,” *Annals of Telecommunications*, pp. 1–13, 2024.

[10] R. F. Fouladi, L. Karaçay, U. Gülen, and E. U. Soykan, “A novel distributed denial of service attack defense scheme for software-defined networking using packet-in message and frequency domain analysis,” *Computers and Electrical Engineering*, vol. 120, p. 109827, 2024.

[11] M. A. Aladaileh, M. Anbar, A. J. Hintaw, I. H. Hasbullah, A. A. Bahashwan, T. A. Al-Amiedy, and D. R. Ibrahim, “Effectiveness of an entropy-based approach for detecting low-and high-rate ddos attacks against the sdn controller: Experimental analysis,” *Applied Sciences*, vol. 13, no. 2, p. 775, 2023.

[12] N. Agrawal and S. Tapaswi, “An sdn-assisted defense mechanism for the shrew ddos attack in a cloud computing environment,” *Journal of Network and Systems Management*, vol. 29, no. 2, p. 12, 2021.

[13] K. Puranik, K. Patil, G. Ghaligi, R. Jannu, S. Patil, D. Narayan, and A. Kachavimath, “A two-level ddos attack detection using entropy and machine learning in sdn,” in *2023 3rd International Conference on Intelligent Technologies (CONIT)*. IEEE, 2023, pp. 1–7.

[14] M. Saiyed and I. Al Anbagi, “Entropy and divergence-based ddos attack detection system in iot networks,” in *2023 19th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)*. IEEE, 2023, pp. 224–230.

[15] M. Solanki and S. Chaudhari, “Ddos attack forensics pattern identification using entropy and hurst coefficient based fusion model,” in *2023 IEEE 8th International Conference for Convergence in Technology (I2CT)*. IEEE, 2023, pp. 1–7.

[16] V. A. Shirsath, M. M. Chandane, C. Lal, and M. Conti, “Syntropy: Tcp syn ddos attack detection for software defined network based on rényi entropy,” *Computer Networks*, vol. 244, p. 110327, 2024.

[17] M. Sinha, “Synflowatch: A detection system against tcp-syn based ddos attacks using entropy in hybrid sdn,” in *Proceedings of the 25th International Conference on Distributed Computing and Networking*, 2024, pp. 359–364.

[18] R. F. Fouladi, O. Ermiş, and E. Anarim, “A ddos attack detection and defense scheme using time-series analysis for sdn,” *Journal of Information Security and Applications*, vol. 54, p. 102587, 2020.

[19] W. I. Khedr, A. E. Gouda, and E. R. Mohamed, “Fmdadm: A multi-layer ddos attack detection and mitigation framework using machine learning for stateful sdn-based iot networks,” *IEEE Access*, vol. 11, pp. 28 934–28 954, 2023.

[20] R. Anusuya, M. R. Prabhu, C. Prathima, and J. A. Kumar, “Detection of tcp, udp and icmp ddos attacks in sdn using machine learning approach,” *Journal of Survey in Fisheries Sciences*, vol. 10, no. 4S, pp. 964–971, 2023.

[21] J. Bhayo, S. A. Shah, S. Hameed, A. Ahmed, J. Nasir, and D. Draheim, “Towards a machine learning-based framework for ddos attack detection in software-defined iot (sd-iot) networks,” *Engineering Applications of Artificial Intelligence*, vol. 123, p. 106432, 2023.

[22] M. A. Setitra, M. Fan, B. L. Y. Agbley, and Z. E. A. Bensalem, “Optimized mlp-cnn model to enhance detecting ddos attacks in sdn environment,” *Network*, vol. 3, no. 4, pp. 538–562, 2023.

[23] R. F. Fouladi, O. Ermiş, and E. Anarim, “A ddos attack detection and countermeasure scheme based on dwt and auto-encoder neural network for sdn,” *Computer Networks*, p. 109140, 2022.

[24] R. F. Fouladi, C. E. Kayatas, and E. Anarim, “Frequency based ddos attack detection approach using naive bayes classification,” in *2016 39th International Conference on Telecommunications and Signal Processing (TSP)*. IEEE, 2016, pp. 104–107.

[25] R. F. Fouladi, O. Ermiş, and E. Anarim, “Anomaly-based ddos attack detection by using sparse coding and frequency domain,” in *2019 IEEE 30th Annual International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC)*. IEEE, 2019, pp. 1–6.

[26] N. McKeown, T. E. Anderson, H. Balakrishnan, G. M. Parulkar, L. L. Peterson, J. Rexford, S. Shenker, and J. S. Turner, “Openflow: enabling innovation in campus networks,” *ACM SIGCOMM computer communication review*, vol. 38, no. 2, pp. 69–74, 2008. [Online]. Available: https://doi.org/10.1145/1355734.1355746

[27] “The book of GNS3,” *Network Security*, vol. 2015, no. 8, p. 4, aug 2015.

[28] B. Lantz, B. Heller, and N. McKeown, “A network in a laptop: rapid prototyping for software-defined networks,” in *Proceedings of the 9th ACM SIGCOMM Workshop on Hot Topics in Networks*, 2010, pp. 1–6.

[29] E. L. Fernandes and C. E. Rothenberg, “Openflow 1.3 software switch,” *Salao de Ferramentas do XXXII Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuıdos SBRC*, pp. 1021–1028, 2014.

[30] P. Borgnat, G. Dewaele, K. Fukuda, P. Abry, and K. Cho, “Seven years and one day: Sketching the evolution of internet traffic,” in *INFOCOM 2009, IEEE*, 2009, pp. 711–719.

[31] A. Turner, *Tcpreplay*, 2011, accessed in November 2019. [Online]. Available: http://tcpreplay. synfin. net/trac/

[32] J. Duoandikoetxea, *Fourier analysis*. American Mathematical Society, 2024, vol. 29.

Authorized licensed use limited to: Ericsson. Downloaded on February 20,2026 at 06:46:51 UTC from IEEE Xplore. Restrictions apply.