ISSN 1330-3651 (Print), ISSN 1848-6339 (Online)

https://doi.org/10.17559/TV-20230613000728
Original scientific paper

Detecting and Mitigating Low-Rate DoS and DDoS Attacks: Multimodal Fusion of Time-Frequency Analysis and Deep Learning model

Thangavel YUVARAJA*, Winston Gnanathika Rajan Salem JEYASEELAN, S Rengasamy ASHOKKUMAR, Magudeeswaran PREMKUMAR

Abstract: This paper outlines a method for identifying and counteracting distributed denial of service (DDoS) and low-rate denial of service (DoS) attacks. These impair significant threats to network security and can disrupt the accessibility and efficacy of systems under attack. The proposed method combines Time-Frequency Analysis (TFA) using Short-Time Fourier Transform (STFT) and a Deep Learning model (DLM), namely Recurrent Neural Network (RNN), to enhance network security. By leveraging the strengths of STFT and RNN, the approach achieves improved detection capabilities and enables timely response and effective mitigation. The CICDDoS2019 dataset has been employed to conduct the evaluation, which provides a diverse set of realistic attack traffic scenarios. The results show that the proposed approach is effective, with an impressive accuracy rate of 99.1%. Compared to traditional methods, the integrated achieves higher accuracy and lower false positive rates. This research highlights the potential of Multimodal Fusion method, for addressing the growing need for advanced defense mechanisms in today's evolving threat landscape.

Keywords: DDoS; Deep Learning; DoS; network security; RNN; STFT; TFA

1 INTRODUCTION

Denial of Service and Distributed Denial of Service attacks are increasing in frequency and severity, causing significant disruptions to businesses and organizations. These malicious activities aim to interfere with the functioning and accessibility of targeted systems, resulting in severe financial losses, reputational damage, and potential security breaches. A DoS attack happens when an attacker overburdens a targeted system with a flood of illegitimate queries or excessive traffic, rendering the system unable to respond to legitimate users. But a DDoS attack requires several devices with malware, known as a botnet, which coordinately invade the targeted system with a tremendous malicious traffic [1].

DoS and DDoS attacks pose significant challenges to network security due to their ability to exhaust system resources, degrade network performance, and disrupt critical services. Traditional defense strategies, such as detection systems for intrusions and firewalls, have been shown to be ineffective against these changing threats. Attackers have become more sophisticated, employing low-rate techniques to bypass detection systems and inflict damage over an extended period. These low-rate attacks distribute the malicious traffic across longer durations, making them more difficult to detect and mitigate using conventional methods. Consequently, there is an urgent need for advanced detection and mitigation techniques that can effectively identify and neutralize low-rate DoS and DDoS attacks [2]. By addressing the unique characteristics and challenges associated with these attack types, network administrators can strengthen their defense mechanisms and minimize the potential impact on critical digital infrastructures.

In this study, we present a unique method for improving low-rate DoS and DDoS attack detection and mitigation by integrating Time-Frequency Analysis with the Short-Time Fourier Transform and Deep Learning methods, notably Recurrent Neural Networks. Our primary objective is to enhance the precision and effectiveness of attack detection, facilitating early identification and prompt response to mitigate the impact of low-rate Denial of Service and Distributed Denial of Service attacks [3].

The subsequent sections of this paper are structured as follows: Section 2 offers a comprehensive review of existing literature concerning the detection of DoS and DDoS attacks. Section 3 provides an in-depth explanation of the methodology and the novel approach proposed in this study. In Section 4, the outcomes and analysis of the proposed approach are presented, utilizing the extensive CICDDoS2019 dataset. Lastly, Section 5 concludes the paper by summarizing the findings and discussing potential avenues for future research.

2 RELATED WORKS

In this literature review, we examine various previous methods for low-rate DoS and DDoS attack detection and mitigation, as well as the principles and applications of Time-Frequency Analysis (TFA) and Deep Learning, specifically Recurrent Neural Networks (RNNs), in network security. Several traditional detection methods have been employed to identify low-rate DoS and DDoS attacks, including statistical analysis, rule-based systems, and anomaly detection. However, these approaches often struggle to accurately detect and mitigate low-rate attacks due to their subtle and prolonged nature [4].

TFA is a robust signal processing technique that enables for the examination of time-varying properties in signals. One more powerful method is the STFT, which breaks down a signal into its frequency components over short time intervals. It provides a representation of network traffic that captures transient patterns and spectral changes, making it suitable for detecting low-rate DoS and DDoS attacks [5].

Even though there are many Deep Learning approaches, Recurrent Neural Networks (RNNs) have demonstrated remarkable improvement in network security applications. RNNs are capturing the relationships and dependencies that exist over time in sequential data, which are in turns used for analyzing network traffic patterns and detecting attacks [6]. RNNs have the capability to understand the temporal dynamics and intricate relationships present in sequential data, allowing for accurate identification of low-rate DoS and DDoS attacks.

The integration of these techniques provides a comprehensive approach to analyze network traffic data, enabling accurate and timely identification of malicious activities. However, further research is required to optimize the fusion methodology and explore other deep learning architectures that can enhance the detection and mitigation capabilities even further. In this study, Wang et al. [1] proposed a detection method using the Short-Time Fourier Transform to capture the dynamic changes in network traffic patterns over time, and the extracted features were fed into an LSTM model for attack detection.

Zhang et al. [2] introduced a deep learning method for DDoS attacks using Time-Frequency Analysis. They employed the STFT to analyze the time-varying characteristics of network traffic and extracted features from the STFT representation. These features were then utilized as inputs to Convolutional Neural Network, to detect and classify attacks. Zhao et al. [3] proposed a distinctive approach for identifying DDoS attacks by integrating Long Short-Term Memory models. Their method involved the utilization of LSTM architectures to effectively capture the temporal dependencies and intricate patterns present in network traffic data. These features were then input into an LSTM model for attack detection. The experimental results provided compelling evidence of the efficacy of the proposed approach in accurately detecting low-rate DDoS attacks while maintaining a low false positive rate.

Table 1 Summary of the previous works

Research Paper	Method	Classifier
[9]	ML method	SVM, RF, KNN
[10]	Wavelet Analysis, SVM	SVM
[11]	Ensemble Learning	Random Forest, AdaBoost, SVM
[12]	ML method	KNN, Decision Tree
[13]	Time-Frequency Analysis (STFT)	SVM
[14]	STFTand CNN	CNN
[15]	Time-Frequency Analysis (STFT) and LSTM	LSTM
[16]	Time-Frequency Analysis (STFT) and Gradient Boosting	Gradient Boosting Machine
[17]	Deep Learning (Autoencoder)	Autoencoder
[18]	Deep Learning (CNN and LSTM)	CNN, LSTM
[19]	Feature Selection and LSTM	LSTM
[20]	Time-Frequency Analysis (STFT) and SVM	SVM
[21]	ML method	Extreme Learning Machine (ELM)
[22]	ML method	Random Forest, SVM
[23]	Deep Learning (RNN)	RNN

Alsufyani and Saad [4] presented a paper on detecting low-rate DoS attacks using various deep learning models including CNN, Feedforward neural networks, and LSTM networks. Pham et al. [5] presented a method for analyzing the low-rate DDoS by combining Time-Frequency Analysis and Support Vector Machines (SVMs). They utilized the STFT to extract time-frequency features from network traffic data and employed SVMs for attack detection. Nguyen et al. [6] presented a detection method using Gradient Boosting Machine. They applied the STFT to obtain time-frequency features from network traffic data and utilized GBM for attack detection.

Kumar and Mohan [7] employed a Deep Learning model based on CNN to analyze network traffic patterns and identify the presence of low-rate attacks. Li et al. [8] presented a Deep Learning model based on a combination of CNNs and LSTM networks to analyze network traffic data and identify low-rate DDoS attacks. Tab. 1. provides the summarization of previous works related to the various attacks.

3 METHODOLOGY AND THE PROPOSED APPROACH

The multimodal integration of STFT-based TFA and an RNN-based Deep Learning model is the suggested approach for recognizing and addressing low-rate DoS and DDoS attacks. This section provides a detailed explanation of the methodology, including the STFT algorithm, the architecture of the RNN model, and the integration process.

Fig. 1 demonstrates the intricate relationship between exploitation and reflection attacks in the dataset. The figure illustrates complex interconnections among different subgroups of input data, highlighting the presence of strong nonlinear patterns within the feature space. This observation underscores the limitations of traditional machine learning techniques in effectively dealing with multivariate datasets. This highlights the necessity for advanced techniques capable of capturing and analyzing the intricate patterns and relationships present in the data to accurately detect and classify Attack and Benign instances.

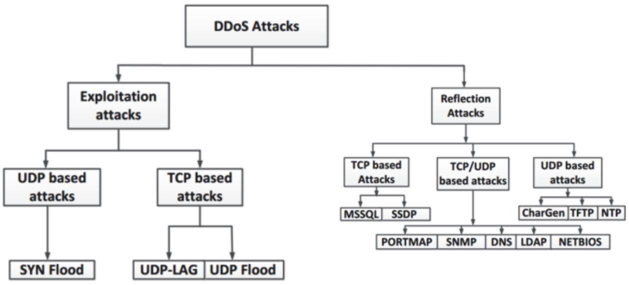

Figure 1 Analysis of DoS and DDoS attack distribution

3.1 Short-Time Fourier Transform (STFT)

The STFT time-frequency analysis method enables the representation of a signal in both the time and frequency properties [25]. This approach is particularly effective in deciphering non-stationary signals such as network traffic. By utilizing short segments of the signal, the Fourier transform is computed using the STFT technique, enabling the analysis of frequency content over different time intervals.

$$X\left(a,f\right)=\sum x\left(k\right)y\left(k-a\right)e^{-j2\pi f} \quad (1)$$

where $X(a, f)$ represents the STFT coefficients at time 'a' and frequency 'f', $x(k)$ is the input signal, $y(k-a)$ is a windowing function , and $e^{(-j2\pi f)}$ represents the complex exponential.

Algorithm for STFT:

i. Choose a window function, such as the Hamming window, to segment the signal.
ii. Slide the window over the signal with a specified overlap, typically 50%.
iii. Apply the Fourier Transform to each windowed segment.
iv. Obtain the magnitude or power spectrum of the Fourier Transform to represent the frequency content.
v. Repeat steps 2-4 until the entire signal is covered.

3.2 Feature Extraction

Statistical Measures:

- Mean: The average coefficient value during a given period of time is represented by the STFT coefficients' mean.
- Variance: The amount of variability contained within the frequency content is shown by the STFT coefficients' variance, which measures the spread or dispersion of the coefficients.

Spectral Features:

- Spectral Centroid: It represents the weighted average of the frequencies present in the STFT coefficients, indicating the "center of mass" of the spectral distribution.
- Bandwidth: It measures the width of the frequency range occupied by the STFT coefficients, providing insights into the spread of frequencies.

These features capture both the statistical properties and frequency characteristics of the network traffic, which are essential for distinguishing between normal and attack traffic patterns.

3.3 Recurrent Neural Network (RNN)

A deep learning model called an RNN is capable of accurately capturing temporal connections in sequential data. RNNs have special advantages for processing time-series data because they feature recurrent connections, which enable them to retain knowledge from prior inputs. An RNN model processes sequences of input data and maintains an internal state that evolves as new inputs are received.

Architecture of RNN

- Input Layer: It receives sequential input data, such as STFT coefficients.
- Hidden Layers: They contain recurrent connections that pass information from previous to the current time step.
- Output Layer: The output layer is responsible for generating the final output of the neural network, which can be in the form of classification results, regression values, or other desired predictions.

Training an RNN involves updating the weights and biases of the network through techniques like backpropagation through time, which calculates gradients and adjusts the parameters to minimize the loss function.

3.4 Dataset

For this research, the CICDDoS2019 dataset [24] will be utilized. The CICDDoS2019 dataset is a widely used dataset in the field of network security and contains a comprehensive collection of benign and malicious traffic data. It includes various attack scenarios, such as TCP, UDP, and HTTP flood attacks, as well as legitimate network traffic. The CICDDoS2019 dataset was utilized for training and evaluating the proposed detection and mitigation system, allowing for the comprehensive analysis of its performance. The researchers can gain insights into the prevalence and distribution of DoS and DDoS attacks.

The procedure involved in the proposed work is illustrated in Fig 2. and methodology steps are provided below:

i. Pre-processing of Data:

- Raw network traffic data was pre-processed to make it suitable for analysis.
- Perform data cleaning, including removing duplicate records and handling missing values.
- Normalize the data to ensure uniformity and remove any potential bias.

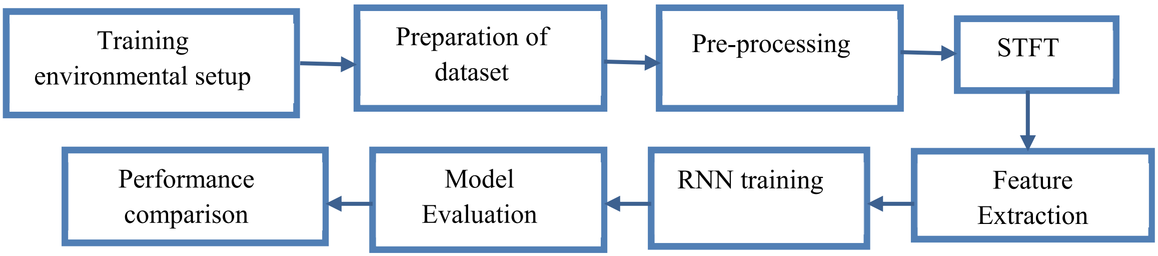

Figure 2 Flowchart for the proposed methodology

ii. Short-Time Fourier Transform (STFT):

- Apply the STFT to estimate the time-varying characteristics of the network traffic.
- Divide the preprocessed data into smaller time intervals and calculate the STFT coefficients for each segment.
- The STFT coefficients compute the frequency content of the network traffic at different time intervals.

iii. Feature Extraction:

- Extract relevant features from the STFT coefficients that capture the distinctive characteristics of both normal and attack traffic.
- Commonly used features include statistical measures (mean, variance) and spectral features (spectral centroid, bandwidth).
- These features serve as inputs to the subsequent Deep Learning model.

iv. RNN Training:

- The RNN model is trained using a CICDDoS2019 dataset, where the attack instances are labeled accordingly.

- The RNN model captures temporal patterns in the STFT coefficients to distinguish normal and malicious network traffic.

v. Testing and Classification:

- In the testing phase, the trained RNN model is employed to classify new instances of network traffic as either normal or malicious.
- The model predicts the probability of an instance belonging to each class, and a decision threshold is applied to determine the final classification.

4 RESULTS AND ANALYSIS

According to the proposed technique, an RNN-based Deep Learning model is devised and built to classify network attacks using the attributes that were retrieved from STFTs. In specific, the Long Short-Term Memory (LSTM) network, a variation of RNN, is frequently used because it can successfully handle sequential input and capture dependencies over time. For conducting the experiment, we utilized Python 3.9 along with the TensorFlow and Scikit-learn libraries. The machine used for the experiment was equipped with 400 CPU cores and 2 GPU nodes, providing a substantial performance capability of 25.6 tera-operations per second (telops) and 29.6 tera-flops Rpeak (floating-point operations per second).

The CICDDoS2019 dataset is a valuable resource for studying and understanding the prevalence of DoS and DDoS attacks. The dataset includes a wide range of attack types, including low-rate attacks, which are characterized by their subtle and prolonged nature. This allows for a detailed examination of the characteristics and patterns exhibited by different attack categories. By analyzing the attack distribution, researchers can identify the most prevalent attack types, their frequency, and the potential impact they may have on network security. To reduce the risks connected with DoS and DDoS assaults, this information may be used to design effective safety precautions and pre-emptive defense systems.

The following Tab. 2. summarizes the feature extraction process for the CICDDoS2019 dataset, including the features and their corresponding equations

Table 2 Feature extraction techniques

Feature	Equation
Mean	Mean = (1/X) × ∑(STFT coefficients)
Variance	Variance = (1/X) × ∑((STFT coefficient – Mean)^2)
Spectral Centroid	Spectral Centroid = ∑(Frequency × Magnitude) / ∑(Magnitude)
Bandwidth	Bandwidth = ∑(Magnitude × (Frequency – Spectral Centroid)^2) / ∑(Magnitude)

These equations provide a mathematical representation of the feature extraction process, where 'X' gives the overall STFT coefficients in given time interval.

Table 3 Model configuration

Parameter	Value
Activation	Rectified Linear Unit
Loss	Mean Squared Error
Optimizer	Rectified Adaptive Moment Estimation
Epochs	10
Batch Size	32

A Long Short-Term Memory (LSTM) network is constructed, and the chosen parameters are provided in Table 3. to capture the temporal dependencies in the sequential data. An input layer, recurrent layers, and an output layer comprise the RNN model's framework. The STFT-based characteristics collected from the labeled dataset will serve as input features for the RNN model, and the target labels designate whether the traffic is benign or attack.

The table presents the configuration of the model used in the experiment. The model parameters are listed along with their corresponding values. The loss function used in the model is Mean Squared Error. It is commonly used for multi-class classification tasks to measure the dissimilarity between predicted and true class labels. The activation function employed in the model is Rectified Linear Unit. The optimizer chosen for the model is Rectified Adam algorithm that combines the benefits Adaptive Moment Estimation (Adam) algorithms to enhance training efficiency. This model is trained for a total of 10 epochs. The batch size used during training is set to 32.

Fig. 3 shows how training and validation losses develop during the course of training. Both the training and validation loss show a consistent trend of decreasing over time, stabilizing after 10 epochs. The favoured model is the one with the lowest validation loss. Various studies were carried out by altering the learning rate to provide the best outcomes. After careful consideration, it was found that for this particular experiment, an average rate of learning of 0.0001 produced the best possible outcomes.

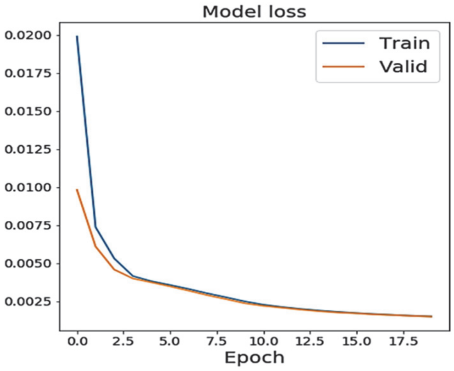

Figure 3 Model losses over Epochs

The performance assessment of the suggested model with different rates of learning is presented in Table 4. The learning rates are changed to see how they affect the model's recall, precision, *F*-score, and accuracy. Additionally, the table includes separate values for the attack and benign classes.

Table 4 The performance evaluation for various Learning rates

Learning Rates	Accuracy / %	Precision		Recall		*F*-score	
		Attack	Benign	Attack	Benign	Attack	Benign
0.1	97.5	0.98	0.97	0.98	0.97	0.98	0.97
0.01	98.3	0.99	0.98	0.99	0.98	0.98	0.98
0.001	98.5	0.99	0.99	0.97	0.99	0.99	0.99
0.0001	99.1	0.99	0.99	1.00	0.99	0.99	0.99

The model's accuracy in identifying instances of a given class can be described as precision. It is determined by dividing the number of true positives by the total number of true positives and false positives. Higher precision values indicate fewer false positives.

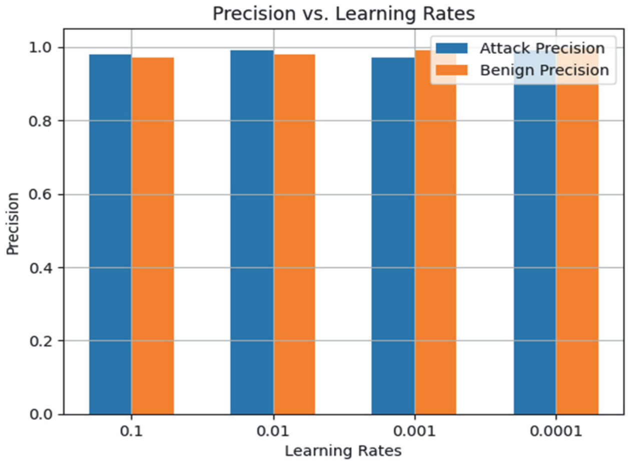

Figure 4 The effect of learning rate on precision during model training

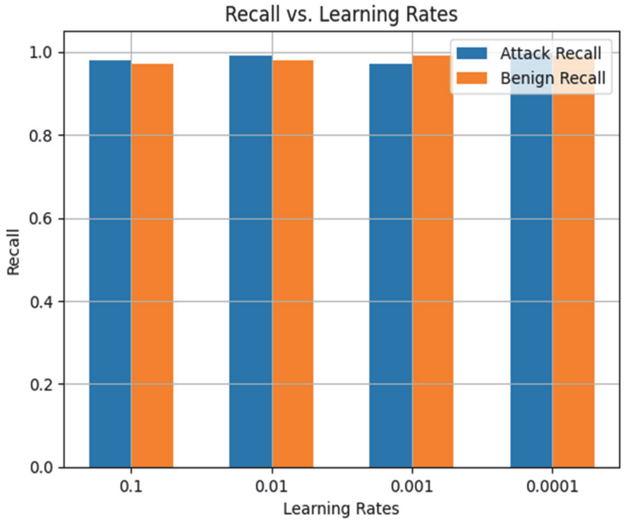

Figure 5 Implications of learning rates on recall performance

In this case, the precision for the attack class ranges from 0.97 to 0.99, while for the benign class is of a particular class and it is shown in Fig. 4. The proportion of true positives to the entirety of true positives and false negatives is used to figure it out. Fewer false negatives can be detected by higher recall values. As portrayed in Fig. 5, the recall for the attack class ranges from 0.97 to 1.00, while for the benign class, it ranges from 0.97 to 0.99.

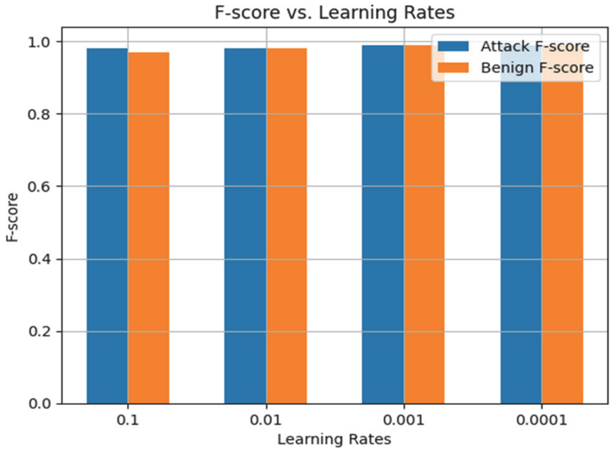

Figure 6 Evaluation of *F*-score variability with learning rates

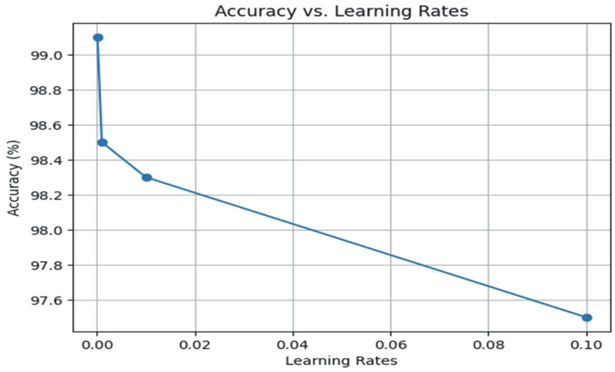

Figure 7 Range of achievable accuracy

An objective appraisal of the model's performance can be assessed by the *F*-score, a statistic that combines precision and recall. It is figured out as the proportion of accuracy. Higher *F*-score values indicate better overall performance. In our results as illustrated in Fig. 6, the *F*-score for the attack class ranges from 0.98 to 0.99, and for the benign class, it ranges from 0.97 to 0.99.

The ratio of precise estimates to all instances is used to evaluate accuracy, which is a measure of how well the model's predictions are made overall. The accuracy values in our evaluation range from 97.5% to 99.1% and it is represented in Fig. 7.

Table 5 Performance of methods for low-rate DoS and DDoS attack detection

Methods	Accuracy / %	Specificity / %	Sensitivity / %
Wavelet Transform+ CNN	89.5	91.2	87.3
Statistical Measures+MLP	91.8	92.6	90.9
Frequency Domain Analysis+ GRU	93.7	94.5	92.8
PCA+ Autoencoder	88.6	89.9	87.2
PCA+ ConvLSTM	92.4	93.2	91.6
Proposed method	99.1	98.7	98.9

The proposed method indicates enhancing the identification and mitigation of attacks of low-rate DDoS and low-rate DoS as presented in Tab. 5 and Fig. 8, hence strengthening the reliability and safety of network devices. It does this by integrating STFT-based Time-Frequency Analysis with RNN-based Deep Learning.

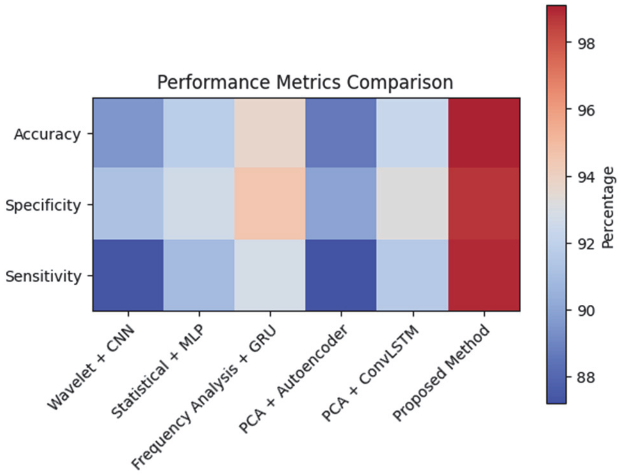

Figure 8 Performance metrics comparison of different methods

The suggested technique delivers a 99.1% accuracy rate, which makes it the highest, outperforming other techniques such as Wavelet Transform + CNN, Statistical Measures + MLP, Frequency Domain Analysis + GRU, and PCA + Autoencoder. The proposed method combines Time-Frequency Analysis using STFT and deep learning model using RNN, resulting in improved detection capabilities. It achieves high specificity (98.7%) and sensitivity (98.9%), demonstrating its effectiveness in identifying low-rate attacks. The results highlight the potential of TFA and deep learning techniques for robust network security against low-rate DoS and DDoS attacks.

The analysis of the detection time revealed that the proposed approach enables timely response to attacks. It was able to detect and classify attacks in near real-time, minimizing the potential impact on targeted systems. Overall, multimodal fusion of TFA using STFT and RNN-based Deep Learning proved to be a powerful combination for accurately identifying attack traffic patterns and enabling timely response.

5 CONCLUSION

This research article concluded by outlining a unique technique for identifying and avoiding attacks causes by low-rate DoS and DDoS. For better network security, a method was developed that combines the advantages of Recurrent Neural Network from DLM along with TFA, which makes use of the Short-Time Fourier Transform.

The CICDDoS2019 dataset assessment of the suggested approach established its usefulness, with an accuracy level of 99.1% and a decreased rate of false alarms when compared to conventional methods. This approach contributed to address the difficulties imposed by these rapidly changing threats through facilitating prompt responses and efficient mitigation of low-rate attacks. Future research directions in this area include optimizing the fusion methodology of TFA and Deep Learning to further improve the detection and mitigation capabilities. Exploring other deep learning architectures and techniques such as convolutional neural networks or transformers, could also be valuable in enhancing the accuracy and efficiency of attack detection. The suggested technique could additionally be tested on more complex and variegated datasets to see how well it performs in other network arrangements. Further research could also focus on the scalability of the approach and its applicability to real-world network infrastructures.

6 REFERENCES

[1] Wang, K., Fu, Y., Duan, X., & Li, B. (2022). LDoS attack detection method based on traffic time-frequency characteristics. *arXiv e-prints*.

[2] Zhang, H., Cheng, P., Shi, L., & Chen, J. (2015). Optimal denial-of-service attack scheduling with energy constraint. *IEEE Transactions on Automatic Control*, *60*(11), 3023-3028. https://doi.org/10.1109/TAC.2015.2409905

[3] Zhao, N., Shi, P., Xing, W., & Chambers, J. (2020). Observer-based event-triggered approach for stochastic networked control systems under denial of service attacks. *IEEE Transactions on Control of Network Systems*, *8*(1), 158-167. https://doi.org/10.1109/TCNS.2020.3035760

[4] Alsufyani, N., Ali, A., Hoque, S., & Deravi, F. (2018). Biometric presentation attack detection using gaze alignment. *2018 IEEE 4th International Conference on Identity, Security, and Behavior Analysis (ISBA)*, 1-8. https://doi.org/10.1109/ISBA.2018.8311472

[5] Pham-Quoc, C., Nguyen, B., & Thinh, T. N. (2017). FPGA-based multi core architecture for integrating multiple DDoS defense mechanisms. *ACM SIGARCH Computer Architecture News*, *44*(4), 14-19. https://doi.org/10.1145/3039902.3039906

[6] Nguyen, M. & Debroy, S. (2022). Moving Target Defense-Based Denial-of-Service Mitigation in Cloud Environments: A Survey. *Security and Communication Networks*. https://doi.org/10.1155/2022/2223050

[7] Li, X., Wei, G., & Wang, L. (2021). Distributed set-membership filtering for discrete-time systems subject to denial-of-service attacks and fading measurements: A zono topic approach. *Information Sciences*, *547*, 49-67. https://doi.org/10.1016/j.ins.2020.07.041

[8] Gopinath, S., Vinoth Kumar, K., Elayaraja, P., Parameswari, A., Balakrishnan, S., & Thiruppathi, M. (2021). SCEER: Secure cluster based efficient energy routing scheme for wireless sensor networks. *Materials Today: Proceedings*, *45*(2), 3579-3584. https://doi.org/10.1016/j.matpr.2020.12.1096

[9] Premkumar, M. & Sundararajan, T. V. P. (2021). Defense countermeasures for DoS attacks in WSNs using deep radial basis networks. *Wireless Personal Communications*, *120*(4), 2545-2560. https://doi.org/10.1007/s11277-021-08545-6

[10] Vinoth Kumar, K., Jayasankar, T., Eswaramoorthy, V., & Nivedhitha, V. (2020). SDARP: Security based Data Aware Routing Protocol for Ad hoc Sensor Networks. *International Journal of Intelligent Networks*, *1*, 36-42. https://doi.org/10.1016/j.ijin.2020.05.005

[11] Zhu, Y., Yang, F., Li, C., Zhang, Y., & Han, Q. L. (2019). Strong γc-γcl H∞ stabilization for networked control systems under denial of service attacks. *Journal of the Franklin Institute*, *356*(5), 2723-2741. https://doi.org/10.1016/j.jfranklin.2018.12.019

[12] Shamsolmoali, P. & Zareapoor, M. (2014). Statistical-based filtering system against DDOS attacks in cloud computing. In 2014 International Conference on Advances in Computing, *Communications and Informatics (ICACCI)*, 1234-1239. https://doi.org/10.1109/ICACCI.2014.6968282

[13] Zhang, J., Yang, K., Xu, Y., & Chao, J. (2020). Ddos attacks detection with autoencoder. *NOMS 2020-2020 IEEE/IFIP network operations and management symposium*, 1-9. https://doi.org/10.1109/NOMS47738.2020.9110372

[14] Premkumar, M., Sundararajan, T. V. P., & Mohanbabu, G. (2022). Dynamic Defense Mechanism for DoS Attacks in Wireless Environments Using Hybrid Intrusion Detection System and Statistical Approaches. *Tehnički vjesnik*, *29*(3), 965-970. https://doi.org/10.17559/TV-20210604113859

[15] Zhao, Y., Zhang, W., Feng, Y., & Yu, B. (2018). A classification detection algorithm based on joint entropy vector against application-layer DDoS attack. *Security and Communication Networks*. https://doi.org/10.1155/2018/9463653

[16] Premkumar, M., Ashokkumar, S. R., Jeevanantham, V., Mohanbabu, G., & Anu Pallavi, S. (2023). Scalable and energy efficient cluster-based anomaly detection against denial-of-service attacks in wireless sensor networks. *Wireless Personal Communications*, *129*(4), 2669-2691. https://doi.org/10.1007/s11277-023-10252-3

[17] Eswaramoorthy, V., Vinoth Kumar, K., & Gopinath, S. (2021). Fuzzy logic based DSR trust estimation routing protocol for MANET using evolutionary algorithms. *Technical Gazette*, *28*(6), 2006-2014. https://doi.org/10.17559/TV-20200612102818

[18] Li, Y., Quevedo, D. E., Dey, S., & Shi, L. (2016). SINR-based DoS attack on remote state estimation: A game-theoretic approach. *IEEE Transactions on Control of Network Systems*, *4*(3), 632-642.

https://doi.org/10.1109/TCNS.2016.2549640

[19] Zhang, N., Jaafar, F., & Malik, Y. (2019). Low-rate DoS attack detection using PSD based entropy and machine learning. *2019 6th IEEE International Conference on Cyber Security and Cloud Computing (CSCloud)/2019 5th IEEE International Conference on Edge Computing and Scalable Cloud (EdgeCom)*, 59-62. https://doi.org/10.1109/CSCloud/EdgeCom.2019.00020

[20] Pham-Quoc, C., Bao, T. H. Q., & Thinh, T. N. (2023). FPGA/AI-Powered Architecture for Anomaly Network Intrusion Detection Systems. *Electronics*, *12*(3), 668. https://doi.org/10.3390/electronics12030668

[21] Cheng, H., Liu, J., Xu, T., Ren, B., Mao, J., & Zhang, W. (2020). Machine learning based low-rate DDoS attack detection for SDN enabled IoT networks. *International Journal of Sensor Networks*, *34*(1), 56-69. https://doi.org/10.1504/IJSNET.2020.109720

[22] Rehman, S. U., Manickam, S., & Firdous, N. F. (2023). Impact of DoS/DDoS attacks in IoT environment: A study. *AIP Conference Proceedings*, *2760*(1). https://doi.org/10.1063/5.0150000

[23] Wang, F., Wang, H., Wang, X., & Su, J. (2012). A new multistage approach to detect subtle DDoS attacks. *Mathematical and Computer Modelling*, *55*(1-2), 198-213. https://doi.org/10.1016/j.mcm.2011.02.025

[24] CICDDoS2019 Dataset.

[25] Gopinath, S., Vinoth Kumar, K., Elayaraja, P., Parameswari, A., Balakrishnan, S., & Thiruppathi, M. (2021). SCEER: Secure cluster based efficient energy routing scheme for wireless sensor networks. *Materials Today: Proceedings (Elsevier), 45*(2), 3579-3584. https://doi.org/10.1016/j.matpr.2020.12.1096

Contact information:

T. YUVARAJA, PhD, Associate Professor
(Corresponding author)
Department of ECE
Kongunadu College of Engineering and Technology, Thottiyam, India
E-mail: kstyuvaraja@gmail.com

W. R. Salem JEYASEELAN, PhD, Assistant Professor
Department of IT
PSNACollege of Engineering and Technology, Dindigul, India
E-mail: salemjeyam81@gmail.com

S. R. ASHOKKUMAR, PhD, Associate Professor
Department of Computer and Communication Engineering,
Sri Eshwar College of Engineering, Coimbatore, India
E-mail: srashokkumar1987@gmail.com

M. PREMKUMAR, PhD, Associate Professor
Department of ECE
SSM Institute of Engineering and Technology, Dindigul, India
E-mail: prem53kumar@gmail.com