Analysis of Deep and Graph Neural Networks for Enhanced DDoS Attack Detection: A Pathway to Hybrid Models

Shayan Athif
Amrita School of AI, Coimbatore
Amrita Vishwa Vidyapeetham
India
shayanathif13@gmail.com

Sharukesh M
Amrita School of AI, Coimbatore
Amrita Vishwa Vidyapeetham
India
sharukesh@gmail.com

Nidish S R
Amrita School of AI, Coimbatore
Amrita Vishwa Vidyapeetham
India
nidishsr@gmail.com

Vignesh V S
Amrita School of AI, Coimbatore
Amrita Vishwa Vidyapeetham
India
vsvignesh6385@gmail.com

Sundaresan Sabapathy *Amrita School of AI, Coimbatore Amrita Vishwa Vidyapeetham* India
s_sundaresan@cb.amrita.edu

Deepika Sasi
Department of ECE
NIT Puducherry
Karaikal, India
deepikajoy2013@gmail.com

Dushantha Nalin K. Jayakody
COPELABS, Lusófona University, 1700-097 Lisboa, Portugal
UNINOVA-CTS (Centro de Tecnologia e Sistemas) & LASI, 2829-516 Costa da Caparica, Portugal
CIET/DEEE, Faculty of Engineering, Sri Lanka Institute of Information Technology
Malabe, Sri Lanka
dushantha.jayakody@ulusofona.pt

2025 7th International Conference on Advancements in Computing (ICAC) | 979-8-3315-6222-9/25/$31.00 ©2025 IEEE | DOI: 10.1109/ICAC69156.2025.11361499

***Abstract*—Distributed denial-of-service (DDoS) attacks pose significant threats to network security, targeting critical infrastructures with increasing complexity. Traditional defense mechanisms that depend on static rules and signatures struggle to address the dynamic nature of these attacks. Software-defined networking (SDN), integrated with machine learning (ML) and deep learning (DL) techniques, has emerged as a promising solution for DDoS detection and mitigation. This paper presents a comparative analysis of deep neural networks (DNNs) and graph neural networks (GNNs) within an SDN framework to detect DDoS attacks. Using real-time network monitoring and traffic anomaly identification, the models are evaluated using metrics such as accuracy, precision, recall, and F1-score against both known and novel attack patterns. Our findings underscore the superiority of GNNs in capturing complex and interconnected relationships within network traffic, offering enhanced detection capabilities. This study contributes to adaptive cybersecurity strategies, advancing the application of ML models in combating evolving cyber threats.**

***Index Terms*—Distributed denial-of-service, network security, DNN, GNN, traffic anomaly detection.**

I. Introduction

Distributed denial-of-service (DDoS) attacks have become one of the recent threats in network security in terms of complexity and magnitude, targeting critical infrastructure. It allows a flood of malicious traffic into the targeted systems to prevent access to services [1]. As DDoS attacks are increasingly complex, classic defenses based on static rules and signatures are seen to be less effective against their dynamics. Due to increasing demand, more sophisticated detection and mitigation methods are needed. One promising technology emerging to overcome these DDoS attacks is the software-defined networking (SDN) in which the control plane is abstracted from the data plane and allows one to centrally manage real-time monitoring of the network. It offers dynamic defense mechanisms to be established [1]. Integration of SDN with machine learning (ML) techniques has already proven to be promising in detecting DDoS attacks more critically and mitigating them by identifying traffic anomalies and malicious patterns [2]. State-of-the-art deep learning (DL) models, including deep neural networks (DNNs) [3] and graph neural networks (GNNs), have shown promise in SDN networks for the classification of network traffic and the detection of DDoS attacks [4], [5].

An approach, detailed in [6], utilizes a spatial-temporal graph convolutional network (GCN) to identify DDoS attacks. Although traditional ML methods have demonstrated reasonable effectiveness, GCNs offer a significant advantage by capturing both spatial and temporal dependencies within network traffic. This capability enables the model to identify complex relationships between nodes and traffic flows, which is particularly relevant for modern SDN architectures. However, in [7] the authors examined the adversarial robustness of GNNs applied to cybersecurity, specifically DDoS detection. It is observed that the model is more robust against adversarial attacks compared to traditional ML models. This quality makes GNN a promising candidate for cybersecurity applications, since adversarial manipulations are a serious concern with

978-8-3315-6222-9/25/$31.00 © 2025 IEEE

Authorized licensed use limited to: SLIIT - Sri Lanka Institute of Information Technology. Downloaded on November 03,2026 at 09:32:09 UTC from IEEE Xplore. Restrictions apply.

these applications. To further enhance accuracy, the flow-to-traffic graph neural network (FTG-Net), a hierarchical network, that utilizes the flow data structure is proposed in [8]. These researches prove that GNNs hold the future of cybersecurity where the focus has been put on attack pattern detection involving dynamic patterns.

Few other studies [9], [10] explored the prospect of DNNs and GNNs, exploring the detection of cyber threats that involve different types of cyber threats based on ML in cybersecurity. For example, in [11] ML models can be tailored for the analysis of DDoS attacks in SDNs, thus consolidating the role of ML in modern network defense. Recently, the application of GNNs to anomaly detection has gained attention in [12] having focused on feature correlation in GNNs for superior performance detection . GNNs can be applied in areas where complex, interconnected data are involved in exact areas where DDoS detection is needed. Once such an element relationship exists, GNN can be the most suitable application area for its employment. Nevertheless, improvements have been made over the years in the area of DDoS detection. Various studies have examined the efficacy of algorithms using techniques such as evolutionary algorithms and the like to improve accuracy, but have not been able to effectively demonstrate the trade-offs or challenges involved in implementing such technology [13]. ML with AI has performed an excellent job in maintaining the explainability of DDoS detection in an SDN environment [14].

On the other side, GNNs have been considered useful for complex data files. However, the use of GNNs has not been very frequent in data traffic analysis, scalability, and real-time challenges in network traffic. This clearly underlines the requirement for studies aimed at the adaptation of GNNs for dynamic network environments [15]. Another important flow is the improvement of DDoS detection performance by applying advanced ML mechanisms to the CICDDoS-2019 data set [16]. However, notwithstanding the extremely high accuracy of this study, it did neglect real-time detection conditions and lack models that can cope with the inevitable changes that might take place in an ever-adapting network.These works illustrate the evolution of DDoS detection methodologies, beginning with traditional ML models and progressively incorporating GNNs to address the increasing complexity of network traffic. Although, ML models remain valuable for real-time anomaly detection, GNNs offer enhanced capabilities in modeling intricate data relationships, making them an ideal choice for dynamic and evolving network environments.

Through this study, our aim is to contribute to ongoing efforts to improve network security and demonstrate that the integration of advanced ML models, particularly GNNs and DNNs, can offer significant advantages over traditional methods in detecting and mitigating DDoS attacks in SDN environments. The performance of the models is checked using accuracy, precision, recall, and F1-score metrics to testing both known and new threats against DDoS attacks. Hence revealing the future of intelligent adaptive cybersecurity models that can dynamically respond to evolving attack strategies.

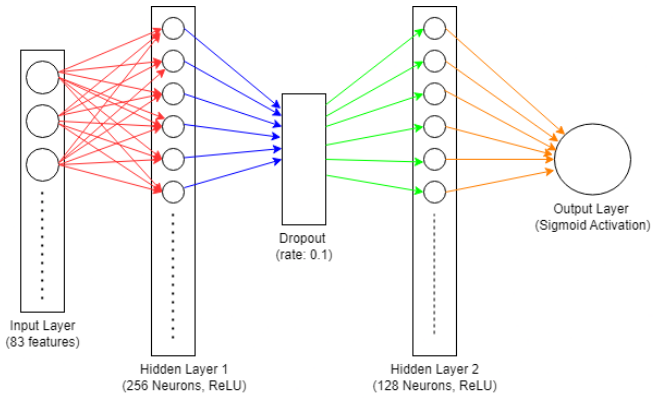


Fig. 1. DNN Architecture Diagram

Section II describes the methodology, detailing the data collection process, preprocessing steps, model architecture, and training procedure. Section III presents the experiments conducted and the results obtained, along with a comparison of the models. In addition, this section includes the feature importance analysis, where the most impactful features for DDoS detection are identified. Finally, Section IV gathers the conclusions and directions for future research.

II. Methodology

A. Data Collection and Preprocessing

To test the performance of our DDoS detection model, we chose several datasets that represent a wide range of network traffic scenarios. To train, we used the InSDN dataset, typically used in research for SDN-based traffic analysis, which provides exhaustive coverage of all standard network traffic patterns. To test our models, we used multiple datasets. We used CICIDS2017, CICIDS2018, CICEV2023, and Kaggle DDoS, ensuring that the models could be generalized over different types of DDoS attack data. The datasets were chosen to represent a diverse class of DDoS attacks, their workloads, and the underlying protocols, thereby enabling a comprehensive assessment of the model's performance. The datasets were consistently partitioned into an 80% training set and a 20% testing set. For DNNs, categorical features were numerically encoded to ensure compatibility and efficient processing, as neural networks require normalized numerical inputs. For GNNs, data was transformed into graph structures with nodes and edges to capture spatial interactions and connectivity patterns. This enabled the GNN to effectively learn complex stealthy DDoS attack behaviors.

B. Model Architecture

The model architectures uses the strengths of both DNN and GNN to enhance DDoS detection accuracy and efficiency. The DNN, illustrated in Fig. 1, processes 83 traffic-related features such as packet size, flow duration, and protocol type enabling fast real-time detection of malicious activity. Each architecture is tailored to effectively distinguish between benign and attack traffic.

Authorized licensed use limited to: SLIIT - Sri Lanka Institute of Information Technology. Downloaded on November 03,2026 at 09:32:09 UTC from IEEE Xplore. Restrictions apply.

Following the input layer, the DNN includes two fully connected hidden layers. The first hidden layer consists of 256 neurons with rectified linear unit (ReLU) activation, a non-linear activation function that introduces sparsity and helps the model learn complex patterns by activating only specific neurons based on the input. Over-fitting is a common challenge in neural networks, especially with high-dimensional data. To mitigate its effect, a dropout layer with a rate of 0.1 follows the first hidden layer, randomly disabling 10% of neurons during training to encourage generalization. The second hidden layer (128 neurons, ReLU) refines feature representations to improve the distinction between benign and malicious traffic. The output layer uses a sigmoid activation to classify each flow probabilistically. The model is trained using the Adam optimizer (learning rate: 0.0001) and binary cross-entropy loss, ensuring stable and efficient convergence for binary classification.

The GNN model, shown in Fig. 2, captures the relational structure of network traffic by representing data as a graph, with nodes connected via k-nearest neighbors. This allows the model to learn spatial dependencies and detect coordinated DDoS patterns across flows by using the distributed nature of such attacks.

The GNN architecture begins with two sample and aggregate (SAGE) convolutional layers, chosen for their effectiveness in processing graph data. The first SAGEConv layer transforms the raw input features into a hidden representation by aggregating information from neighboring nodes. This operation allows each node to learn not only from its features, but also from those of its neighbors, effectively modeling the local structure of the graph. SAGEConv is particularly beneficial in this application because it can capture both the individual node features and the surrounding context, essential to recognize the distributed nature of DDoS attacks. The second SAGEConv layer further reduces the dimensionality of the hidden representation, focusing the model on the most critical features for classification. By applying another layer of SAGE convolution, the GNN enhances its ability to capture deeper relationships within the traffic data, which is useful for detecting subtle patterns that may not be apparent in isolated data points. After the convolutional layers, global mean pooling is applied to aggregate the information from all nodes. This creates a compact, global representation of the entire graph. The pooled representation summarizes the network interactions, enabling the model to make a holistic assessment of the traffic flow. The GNN outputs class probabilities via a fully connected layer with softmax activation, allowing interpretable predictions. It is trained using the Adam optimizer (learning rate: 0.01) and binary cross-entropy loss, aligned with the binary classification task.

III. Experiments and Results

A. Experiments

The performance and robustness of the DNN and GNN models are evaluated by performing experiments on multiple datasets, including CICIDS2017, CICIDS2018, CICEV2023 DDoS, Kaggle DDoS and InSDN. These datasets vary in traffic patterns, attack intensities, and protocols. Models trained on InSDN were tested on the same to assess generalization and resilience to unseen attack scenarios, reflecting real-world deployment conditions. Sequentially, the models are deployed in a controlled SDN environment to simulate diverse DDoS attacks, including high-volume (UDP, TCP SYN floods), low-volume stealth, and application-layer (HTTP GET) attacks. The SDN setup enabled dynamic traffic orchestration, providing a realistic testbed to assess model performance in adaptive, real-time threat scenarios. Each attack was designed to evaluate the models' ability to detect both high-intensity and subtle traffic anomalies. To ensure consistent comparisons and reproducible results, all experiments were conducted with a fixed random seed (42) and a uniform set of hyperparameters, which were not tuned for individual datasets.

B. Results

The experimental results show that DNN and GNN models have marked strengths for two different approaches in terms of training dynamics, accuracy, precision, recall, and F1 score. These metrics were used to measure the ability of each model to classify DDoS attacks while ensuring the least possibility of false negatives and positives. The training process of the DNN model demonstrates strong convergence across epochs, as shown in Fig. 3. The model achieved a final training loss of 0.1500 and a validation loss of 0.0300, indicating its ability to generalize well on structured datasets with well-defined DDoS patterns. These results highlight the DNN model's strength in detecting straightforward and high-volume DDoS attacks efficiently.

The GNN model exhibited strong convergence during training, as shown in Fig. 4. The final training loss of 0.0404 and validation loss of 0.0350 reflect its adaptability to datasets with complex and nuanced attack patterns. This supports the GNN's ability to model interdependencies within network traffic, making it well-suited for detecting subtle and distributed DDoS attacks.

The DNN model's high accuracy on structured datasets with well-defined DDoS patterns, as shown in Table. I, indicates its strong detection capabilities when traffic features align closely with known attack types. In contrast, the GNN model, while slightly lower in overall accuracy compared to the DNN, demonstrated strong performance on datasets with more complex and subtle attack structures. This highlights its adaptability to nuanced network behaviors.

TABLE I. Model Accuracy Comparison

Model	Accuracy (%)
DNN	98.0
GNN	96.0

Precision, recall, and F1 score were used to evaluate model performance. Precision indicates accuracy of positive predictions, recall measures detection of actual positives, and F1

Authorized licensed use limited to: SLIIT - Sri Lanka Institute of Information Technology. Downloaded on November 03,2026 at 09:32:09 UTC from IEEE Xplore. Restrictions apply.

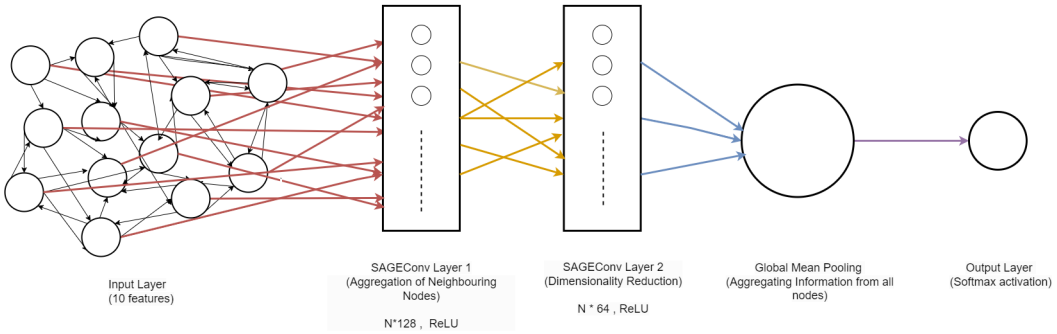


Fig. 2. GNN Architecture Diagram

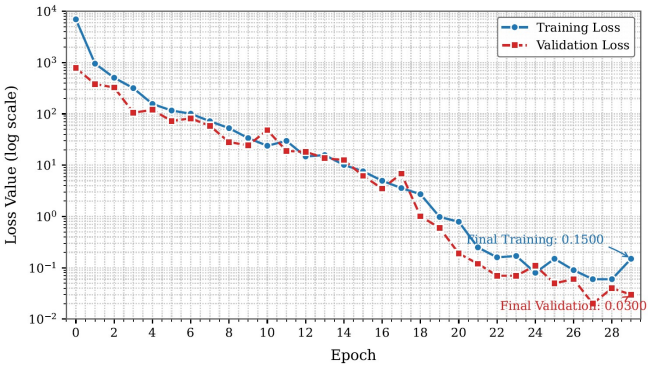


Fig. 3. Training and validation loss graph for the DNN model, demonstrating convergence across epochs.

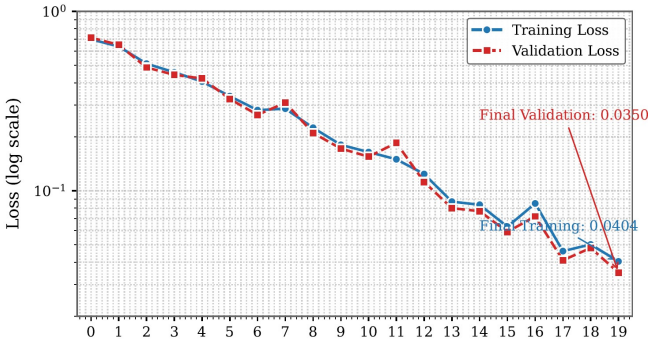


Fig. 4. Training and validation loss graph for the GNN model, indicating convergence across epochs

balances both. As shown in Table. II, the DNN achieved 96.5% precision, 99% recall, and a 97.5% F1 score, demonstrating strong detection capability with minimal false positives.

In contrast, the GNN model achieved precision, recall, and F1 score values of 97%, 86%, and 91%, respectively. The GNN outperformed the DNN in precision, indicating it was more accurate in identifying true positives. However, its recall was lower, suggesting it missed some DDoS attacks compared to the DNN. The F1 score for the GNN reflects t his trade-off between high precision and relatively lower recall, as highlighted in Table. II.

TABLE II. DETAILED PERFORMANCE METRICS COMPARISON

Model	Precision (%)	Recall (%)	F1-score (%)
DNN	96.5	99.0	97.5
GNN	97.0	86.0	91.0

The model discrimination is analyzed using receiver operating characteristic (ROC) (Fig. 5) and Precision-Recal (PR) (Fig. 6) curves. Both models showed strong discrimination via ROC, with AUCs of 0.974 (DNN) and 0.998 (GNN). The PR curves, crucial for imbalanced data, highlight a strategic trade-off: the DNN (AP=0.966) maximizes recall, while the GNN (AP=0.965) favors higher precision at the cost of lower recall (86% per Table II).

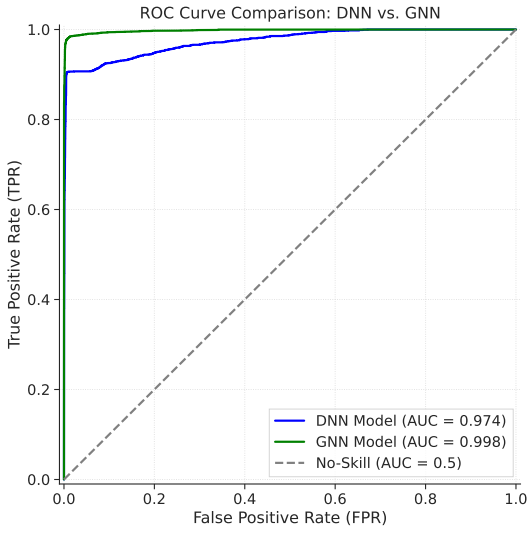


Fig. 5. ROC Curve Comparison. Both models show high AUC scores, indicating strong discrimination capability

1) Performance Against Different DDoS Datasets: The DNN and GNN models were tested on four benchmark DDoS datasets. As shown in Table. III, the DNN achieved accuracies of 99.70%, 99.52%, 99.86%, and 99.69% on CICIDS2017, CICIDS2018, CICEV2023, and Kaggle DDoS, respectively,

Authorized licensed use limited to: SLIIT - Sri Lanka Institute of Information Technology. Downloaded on November 03,2026 at 09:32:09 UTC from IEEE Xplore. Restrictions apply.

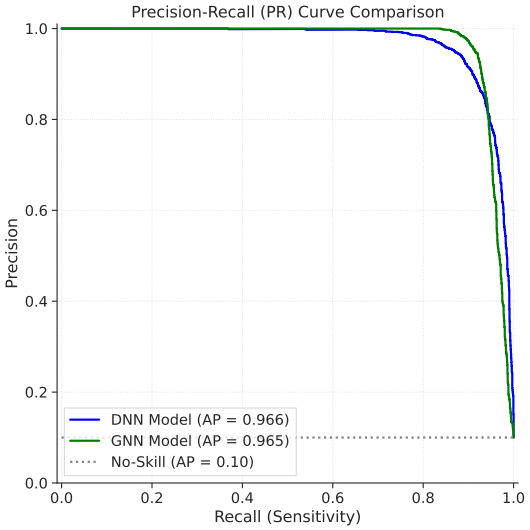


Fig. 6. PR Curve Comparison. The plot highlights the DNN's high recall versus the GNN's high precision on an imbalanced dataset.

highlighting its consistent and high performance across diverse attack scenarios. The GNN achieved accuracies of 96.7%, 95.4%, 92.99%, and 99.56% across the same datasets. While slightly lower than the DNN, the GNN performed well, especially in handling complex attack patterns. As shown in Table. III, these results highlight each model's adaptability to varying attack scenarios. Confusion matrices for both models are presented in Fig. 7 and Fig. 8.

TABLE III. MODEL ACCURACY COMPARISON ACROSS DATASETS

Dataset	DNN Accuracy (%)	GNN Accuracy (%)
CICIDS2017	99.70	96.70
CICIDS2018	99.52	95.40
CICEV2023	99.86	92.99
Kaggle DDoS	99.69	99.56

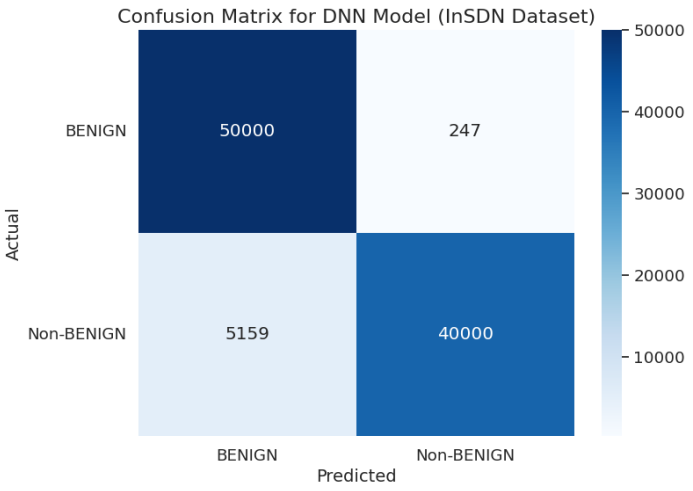


Fig. 7. Confusion matrix for the DNN model performance on the InSDN dataset, showing effective classification of BENIGN and Non-BENIGN traffic

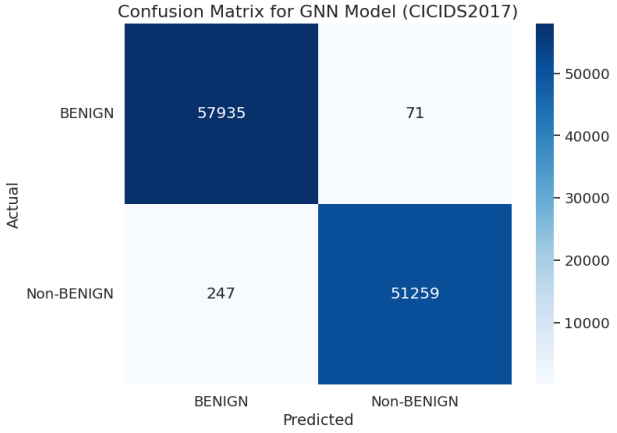


Fig. 8. Confusion matrix for the GNN model evaluated on the CICIDS2017 dataset, demonstrating balanced detection across traffic classes

2) Performance Against Different DDoS Attack Types: In the SDN environment, the DNN model demonstrated strong performance in detecting high-intensity attacks such as TCP and UDP floods. As shown in Table. IV, the DNN achieved accuracies of 99.34% for TCP floods, 98.87% for UDP floods, 98.56% for HTTP floods, and 91.23% for low-volume stealth attacks. These results show that the DNN model excels in detecting well-defined, high-volume attacks, where the attack signatures are more prominent and easier to classify. On the other hand, the GNN model performed better in detecting more complex attack types. The GNN achieved accuracies of 98.76% for TCP floods, 98.45% for UDP floods, 97.89% for HTTP floods, and 97.56% for low-volume stealth attacks. The GNN's strength lies in its ability to model the inter-dependencies within network traffic, enabling it to recognize subtle patterns and detect low-volume, stealthy attacks. This capability makes the GNN a more robust option for environments where attacks are dynamic, distributed, and harder to detect using traditional models like DNN.

TABLE IV. MODEL ACCURACY COMPARISON ACROSS DDOS ATTACK TYPES

Attack Type	DNN Accuracy (%)	GNN Accuracy (%)
TCP Flood	99.34	98.76
UDP Flood	98.87	98.45
HTTP Flood	98.56	97.89
Low-volume Stealth	91.23	97.56

The experimental results indicate that while the DNN is effective for detecting high-volume, straightforward DDoS patterns with high speed and accuracy, the GNN offers enhanced robustness in scenarios where the attack patterns are complex or distributed. These findings reinforce the suitability of combining both models in a hybrid approach, utilizing the DNN's efficiency alongside the GNN's adaptability to achieve a more comprehensive DDoS detection framework.

Authorized licensed use limited to: SLIIT - Sri Lanka Institute of Information Technology. Downloaded on November 03,2026 at 09:32:09 UTC from IEEE Xplore. Restrictions apply.

C. Feature Importance Analysis

To identify the most impactful features for DDoS detection, we conducted a feature importance analysis using a Random Forest model. The top features found to be critical indicators of malicious activity were:

- Total Forwarded Packets (Tot Fwd Pkts): A key metric for identifying volumetric attacks attempting to overwhelm network resources.
- Mean Length of Forwarded Packets (Fwd Pkt Len Mean): Useful for detecting small packet flood attacks.
- Maximum Length of Forwarded Packets (Fwd Pkt Len Max): Helps identify large packet attacks.
- Minimum Inter-Arrival Time (Flow IAT Min): Critical for spotting high-frequency flooding patterns.
- SYN Flag Count (SYN Flag Cnt): A strong indicator of SYN flood attacks.
- Minimum Inter-Arrival Time for Forwarded Packets (Fwd IAT Min): Helpful for detecting rapid, sustained flooding.
- Total Backward Packets (Tot Bwd Pkts): Can assist in identifying attack patterns with few responses from the target.

These findings indicate that characteristics related to packet volumes, sizes, timing, and TCP flags were the strongest predictors of DDoS attacks in the dataset. The model was able to detect distinct patterns in these traffic attributes that distinguished benign from malicious activity. Focusing on these high-impact features allows for optimization of feature engineering and data collection efforts to enhance overall DDoS detection capabilities.

IV. Conclusion

This paper presents a comparative analysis of DNN and GNN for DDoS detection in an SDN environment, highlighting their unique strengths and limitations. The findings indicate that while DNN-based approaches perform well in detecting high-volume, easily distinguishable attacks, their effectiveness decreases against stealthy low-volume intrusions. In contrast, GNNs demonstrate superior capability in identifying such subtle and distributed attack patterns, owing to their ability to capture and exploit relational dependencies among network entities. The analysis carried out suggests that a hybrid approach that combines DNN and GNN models could provide a balanced solution for DDoS detection, offering both rapid response to high-intensity attacks and adaptability to more sophisticated threats. Future work could focus on developing such integrated models that enhance real-time security in dynamic network environments.

Acknowledgement

This work was supported in part by the European Commission through Marie Skłodowska-Curie Actions (MSCA) as part of the REMARKABLE project (No. 101086387), by the Program for the Promotion of Academic Collaboration & Research (SPARC), Government of India, through grant no. SPARC/2024-2025/NXTG/P3524, by the Sri Lanka Institute of Information Technology through the grant PVC(R&I)/RG/2024/12, by the COFAC - Cooperativa de Formação e Animação Cultural, C.R.L. (University of Lusófona University), via the project PortuLight (COFAC/ILIND/COPELABS/2/2023), by the national funds through FCT - Fundação para a Ciência e a Tecnologia - as part of the projects URLLC-UAV (2023.08191.CEECIND), UNINOVA-CTS (UIDB/00066/2020) and COPELABS (no. UIDB/04111/2020).

References

[1] J. Singh and S. Behal, "Detection and mitigation of DDoS attacks in SDN: A comprehensive review, research challenges and future directions," *Computer Science Review*, vol. 37, p. 100279, 2020. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1574013720301647

[2] M. Mittal, K. Kumar, and S. Behal, "Deep learning approaches for detecting DDoS attacks: A systematic review," *Soft computing*, vol. 27, no. 18, pp. 13 039–13 075, 2023.

[3] B. G. HB, P. Poornachandran, S. KP *et al.*, "Deep-net: Deep neural network for cyber security use cases," *arXiv preprint arXiv:1812.03519*, 2018.

[4] T. E. Ali, Y.-W. Chong, and S. Manickam, "Machine learning techniques to detect a DDoS attack in SDN: A systematic review," *Applied Sciences*, vol. 13, no. 5, pp. 31–83, 2023.

[5] V. Hnamte, A. A. Najar, H. Nhung-Nguyen, J. Hussain, and M. N. Sugali, "DDoS attack detection and mitigation using deep neural network in SDN environment," *Computers & Security*, vol. 138, pp. 103–661, 2024.

[6] Y. Cao, H. Jiang, Y. Deng, J. Wu, P. Zhou, and W. Luo, "Detecting and mitigating ddos attacks in sdn using spatial-temporal graph convolutional network," *IEEE Transactions on Dependable and Secure Computing*, vol. 19, no. 6, pp. 3855–3872, 2021.

[7] S. Gunneemann, "Graph neural networks: Adversarial robustness," in *Graph Neural Networks: Foundations, Frontiers, and Applications*. Springer Nature Singapore, 2022, pp. 149–176.

[8] L. Barsellotti, L. De Marinis, F. Cugini, and F. Paolucci, "Ftg-net: Hierarchical flow-to-traffic graph neural network for ddos attack detection," in *2023 IEEE 24th International Conference on High Performance Switching and Routing (HPSR)*. IEEE, 2023, pp. 173–178.

[9] N. Yungaicela-Naula, C. Vargas-Rosales, and J. Perez-Diaz, "Sdn-based architecture for transport and application layer ddos attack detection using machine and deep learning," *IEEE Access*, vol. 9, pp. 108 495–108 512, 2021.

[10] B. Buchanan, "A national security research agenda for cybersecurity and artificial intelligence," *Cent. Secur. Emerg. Technol. Issue Brief*, vol. 7, 2020.

[11] A. Sharma, H. S. Chauhan, H. Kaur, and H. Babbar, "Analysis of *ddos* attacks in software defined networking using machine learning," in *2023 International Conference on Intelligent and Innovative Technologies in Computing, Electrical and Electronics (IITCEE)*. IEEE, 2023, pp. 1190–1195.

[12] H. Ko, I. Praca, and S. G. Choi, "Anomaly detection analysis based on correlation of features in graph neural network," *Multimedia Tools and Applications*, vol. 83, no. 9, pp. 25 487–25 501, 2024.

[13] R. K. Batchu and H. Seetha, "A generalized machine learning model for ddos attacks detection using hybrid feature selection and hyperparameter tuning," *Computer Networks*, vol. 200, p. 108498, 2021.

[14] P. S. Pericherla, S. K. Thangavel, K. Srinivasan, A. Tibrewal, and S. Vajipayajula, "Early detection of ddos attacks in sdn using machine learning techniques," in *2023 14th International Conference on Computing Communication and Networking Technologies (ICCCNT)*. IEEE, 2023, pp. 1–7.

[15] S. Venkatapathy, M. Votinov, L. Wagels, S. Kim, M. Lee, U. Habel, I.-H. Ra, and H.-G. Jo, "Ensemble graph neural network model for classification of major depressive disorder using whole-brain functional connectivity," *Frontiers in psychiatry*, vol. 14, p. 1125339, 2023.

[16] R. K. Batchu and H. Seetha, "On improving the performance of ddos attack detection system," *Microprocessors and Microsystems*, vol. 93, p. 104571, 2022.

Authorized licensed use limited to: SLIIT - Sri Lanka Institute of Information Technology. Downloaded on November 03,2026 at 09:32:09 UTC from IEEE Xplore. Restrictions apply.