Indonesian Journal of Electrical Engineering and Computer Science
Vol. 38, No. 2, May 2025, pp. 1245∼1255
ISSN: 2502-4752, DOI: 10.11591/ijeecs.v38.i2.pp1245-1255

A deep learning approach to detect DDoS flooding attacks on SDN controller

Abdullah Ahmed Bahashwan, Mohammed Anbar, Selvakumar Manickam, Taief Alaa Al-Amiedy, Iznan H. Hasbullah
National Advanced IPv6 (NAv6) Centre, Universiti Sains Malaysia (USM), Penang, Malaysia

Article Info

Article history:

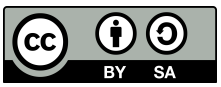
Received May 26, 2024
Revised Oct 22, 2024
Accepted Oct 30, 2024

Keywords:

DDoS
Deep learning
Intrusion detection system
Multi-layer perceptron
Software-defined networking

ABSTRACT

Software-defined networking (SDN), integrated into technologies like internet of things (IoT), cloud computing, and big data, is a key component of the fourth industrial revolution. However, its deployment introduces security challenges that can undermine its effectiveness. This highlights the urgent need for security-focused SDN solutions, driving advancements in SDN technology. The absence of inherent security countermeasures in the SDN controller makes it vulnerable to distributed denial of service (DDoS) attacks, which pose a significant and pervasive threat. These attacks specifically target the controller, disrupting services for legitimate users and depleting its resources, including bandwidth, memory, and processing power. This research aims to develop an effective deep learning (DL) approach to detect such attacks, ensuring the availability, integrity, and consistency of SDN network functions. The proposed DL detection approach achieves 98.068% accuracy, 98.085% precision, 98.067% recall, 98.057% F1-score, 1.34% false positive rate (FPR), and 1.713% detection time.



Corresponding Author:

Mohammed Anbar
National Advanced IPv6 Centre (NAv6), Universiti Sains Malaysia (USM)
Gelugor 11800, Penang, Malaysia
Email: anbar@usm.my

1. INTRODUCTION

The proliferation of network devices has exposed the limitations of traditional networks, complicating internet development and hindering progress in areas such as cloud computing, internet of things (IoT), and big data over the past decade [1]. In response, software-defined networking (SDN) has emerged as a solution by decoupling the control plane from the data plane, enabling centralized control and more efficient management of network elements [2]. SDN offers several advantages, including a holistic network view, centralized control, improved switch protocol magnet, vitalized network construction, and programmability, making it applicable to various network natures [3]. With the OpenFlow protocol, the application, control, and data planes are pivotal in achieving central control in SDN architecture [4]. Nonetheless, the widespread adoption of SDN has introduced security vulnerabilities, including susceptibility to denial of service (DDoS) attacks that can degrade performance by targeting the controller and depleting network resources [5], [6].

Furthermore, DDoS flooding attacks, while often simple in execution, pose significant challenges in detection and mitigation [7], [8]. These attacks are launched through compromised devices within a botnet and utilized various techniques to evade detection systems, increasing their chance of success. Specifically, when targeting SDN networks or controllers, these attacks flood the network with spoofed transmission control

protocol (TCP), internet control message protocol (ICMP), and user datagram protocol (UDP) traffic, consuming network bandwidth and overwhelming system resources, ultimately disrupting legitimate services and causing widespread outages. Figure 1 illustrates the impact of a DDoS attack on an SDN controller and its effects on the entire SDN network. Attackers further complicate defense by spoofing source IP, which prevents Openflow switches from finding matching rules, forcing them to forward packets to the SDN controller. This exhausts controller resources and can lead to a cascading failure. Protection against such attacks is critical, as they pose significant threats to both switches and the southbound application programming interface (API), and due to their broad scope, these attacks are classified as global threats within SDN networks [9], [10].

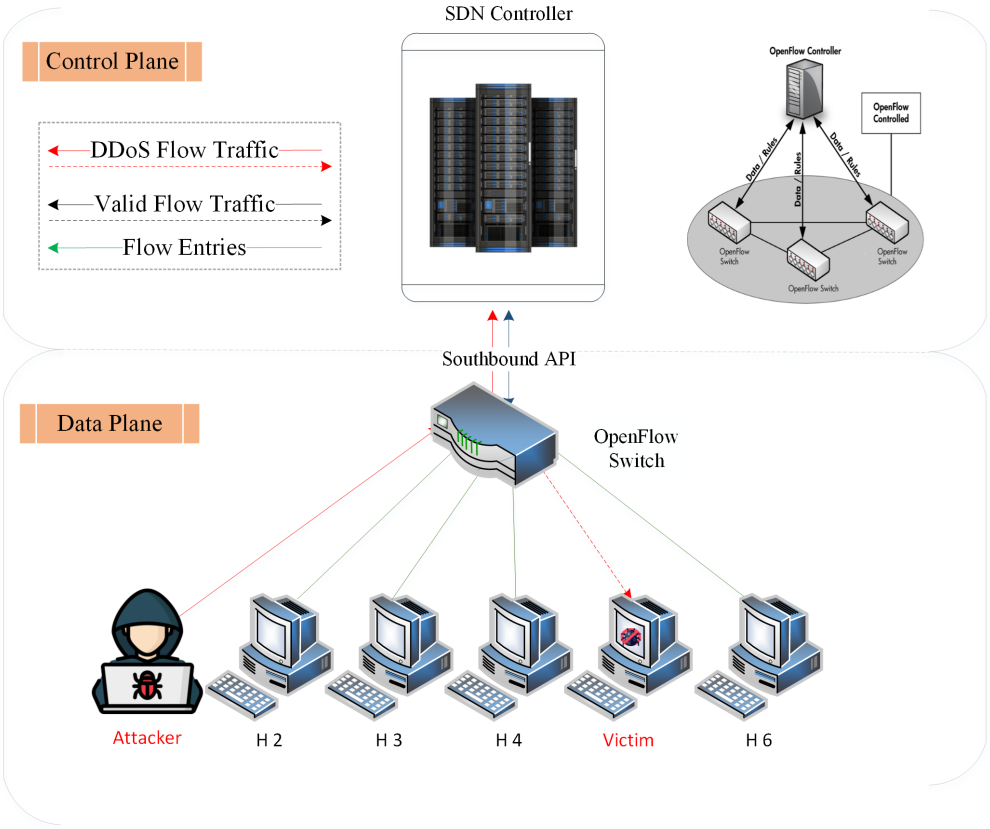


Figure 1. Hypothetical visualization of DDoS attacks on the SDN controller

However, as highlighted in the related works (section 2) the recently discussed deep learning (DL)-based approaches for detecting DDoS attacks exhibit certain limitations. Several of these approaches have been trained and tested on unrealistic datasets, which do not adequately reflect the unique characteristics of SDN networks. This disconnect leads to decreased accuracy and an increased false positive rate (FPR) in practical applications of SDN detection approaches in real world settings. While some approaches do utilize realistic datasets, they still deliver sub optimal performance.

In summary, the weaknesses of current DL-based approaches for detecting DDoS attacks on SDN network controller became evident. Despite their efficiency, these approaches have certain drawbacks: (i) many rely on unrealistic datasets that do not adequately capture the characteristics of SDN network architecture, which differs significantly from traditional network architecture; and (ii) many of these approaches exhibit low detection performance and suffer from high FPRs when identifying such attacks.

Therefore, the key contributions of this research paper are: (i) proposing a DL-based approach for detecting DDoS flooding attacks on SDN controller-based networks; (ii) evaluating and validating the proposed detection approach using a realistic dataset that reflects the characteristics of SDN network architecture; and (iii) enhancing detection performance while reducing FPRs. These contributions are directly addressing the challenges present in existing DL-based approaches.

The remaining sections of this research paper are organized to provide a comprehensive understanding of the proposed work. Section 2 presents a review of the relevant works in the field, highlighting existing approaches and their limitations. Following that, section 3 outlines the proposed detection approach based on DL, detailing its methodology and innovations. Section 4 discusses the results obtained from the proposed detection approach, along with a comprehensive analysis of the findings. Finally, section 5 concludes the paper by summarizing the key insights and provides recommendations for future works.

2. RELATED WORKS

This section examines the literature on DL approaches to detect DDoS attacks on SDN networks and their limitations. The approaches are listed as follows: in a comparative study by Ali *et al.* [11], various machine learning (ML) and DL techniques, including support vector machine (SVM), decision tree (DT), K-nearest neighbour (KNN), convolutional neural network (CNN), and multi-layer perceptron (MLP), were evaluated for detecting DDoS attacks in SDN with minimal time and complexity. The study utilized CIC-DoS2019 and ICIDS2017 datasets with 50 features. The study revealed that the SVM achieved the highest prediction accuracy at 95.5%, surpassing other algorithms. On the other hand, [12] proposed a DL approach employing recurrent neural network (RNN) for identifying DDoS attacks on the controller. However, it suffers from relatively low detection accuracy and high FPR.

Another approach by Gadze *et al.* [13] introduced a system for SDN-based detection of TCP, ICMP, and UDP DDoS attacks, employing DL algorithms like CNN and long short-term memory (LSTM), achieving an accuracy of 89.63%. Additionally, Alshra'a *et al.* [14] developed a DL-based intrusion detection system (IDS) for SDN defence against DDoS attacks, utilizing RNN, gated recurrent unit (GRU), and LSTM models, showcasing high accuracy in detecting attacks with 48 features using the InSDN dataset. DeepIDS, proposed by Tang *et al.* [15], is a DL-based IDS for SDN networks that employ DNN and GRU for anomaly detection and achieving comprehensive attack identification, including zero-day attacks. Meanwhile, DDoSNet, proposed by Elsayed *et al.* [16], utilizes RNN with autoencoder for SDN DDoS attack detection, boasting a 99% accuracy compared to traditional ML methods. The system also offers flexibility to implement null routing or forward attacks for further analysis on a honeypot server.

An additional approach by Haider *et al.* [17] is based on a CNN hybrid model for early detection of DDoS attacks, achieving an impressive accuracy of 99.45% with the CICDS2017 dataset. Further approach by Tang *et al.* [18] employed a GRU-RNN-based anomaly IDS for SDN networks to improve anomaly detection rates compared to their previous IDS; however, their approaches yielded relatively lower accuracies of 89% and 99% for the NSL-KDD and CICIDS2017 datasets, respectively, which may not faithfully represent SDN network characteristics. Moreover, an approach by Liu *et al.* [19] presents real-time mitigating flooding attacks. On the other hand, [20] proposed a defence and detection approach utilizing RNN, LSTM, and CNN for DDoS attacks in SDN, implemented in the OpenFlow switch, showcasing high validation accuracy of 98% and 99% for detection of DDoS attacks in test and training data, respectively, using the ISCX2012 dataset and a simulated SDN network dataset.

Overall, the recently mentioned DL approaches for detecting DDoS have some limitations. Some of these approaches have been trained and tested using unrealistic datasets, failing to capture the distinct characteristics of SDN networks. This mismatch results in reduced accuracy and higher FPR from a practical perspective when it comes to implementing SDN detection approaches in real-world scenarios. Although some approaches employ realistic datasets, they achieve low performance.

3. PROPOSED DETECTION APPROACH

The application of DL to SDN networks emerges as a crucial research area in recent years. One significant advantage of DL over traditional ML algorithms is its superior performance in analyzing large-scale datasets [21]. Additionally, the adoption of SDN technology gains momentum in various domains, including cloud computing and IoT systems, where substantial volumes of data are generated. Consequently, a multi-neural network architecture is well suited for handling the demands of these emerging technologies. This research paper adopted MLP, which comprises multiple processing layers that facilitate the training of data representations at varying levels of complexity [22].

Furthermore, MLP techniques demonstrate significant advancements in advanced applications compared to classical ML techniques [23]. The key reasons for choosing MLP are as follows: MLP is considered

one of the most efficient neural network techniques for detection approaches, consistently delivering impressive results [24]. Its capability allows the proposed detection approach to achieve notable accuracy and reduce FPRs in detecting DDoS attacks. Additionally, MLP is particularly well-suited for tabular datasets, which aligns with the input data format used in this study, provided as comma-separated values (CSV) [25].

Overall, this section provides a discussion of the phases of the proposed DL-based detection approach. It begins with dataset preprocessing, followed by SDN DDoS attack detection, and concludes with performance evaluation metrics used to assess the proposed approach. These phases are thoroughly discussed in the following subsections. Figure 2 visually illustrates the design and implementation of the overall methodology of the proposed detection approach. The following subsections discuss the methodology phases in more detail.

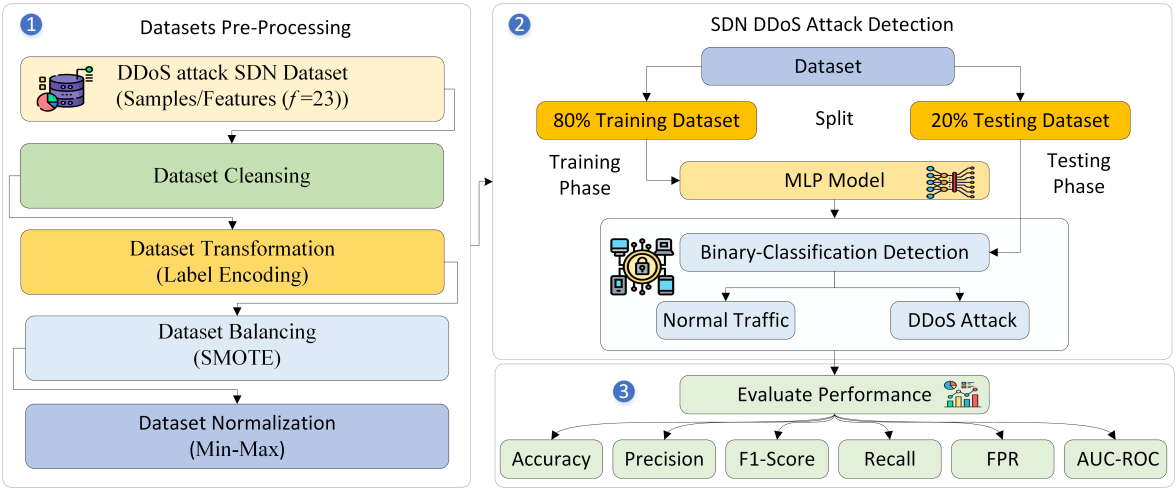


Figure 2. Overall proposed DL-based detection approach

3.1. Datasets preprocessing

The DL-based detection approach is evaluated using a realistic SDN benchmark dataset, "DDoS attack SDN dataset" [26], to overcome the limitation of existing approaches that rely on unrealistic datasets. Several preprocessing stages are applied to the dataset before training the proposed MLP model to prevent overfitting and ensure meaningful results. These stages are crucial for preparing the dataset for accurate detection:

- Dataset cleansing: this involves filling in missing or incomplete columns within the dataset and replacing missing values with 0 to ensure completeness and accuracy of the dataset values.
- Data transformation: the dataset is transformed to enhance readability and analysis. This includes converting data formats and replacing textual features with numeric values using label encoding, making it more suitable for the proposed MLP model.
- Dataset balancing: to achieve a balanced distribution of label classes, synthetic minority oversampling technique (SMOTE) is applied to oversample the minority class, reducing bias and improving model performance.
- Dataset normalization: finally, normalization ensures a consistent scale across all records, which helps the model learn more effectively.

Once these pre-processing stages are completed, the dataset is passed to the SDN DDoS attack detection stage for training and evaluation. Table 1 outlines the details and specifications of the benchmark datasets used.

Table 1. DDoS attack SDN dataset specifications

Dataset-specifications							
Ref.	Normal samples	Attack samples	Total samples	Normal label	Attack label	Dataset category	Total of features
[26]	62,344	62,344	124,688	0	1	Normal and DDoS attacks	22

3.2. SDN DDoS attack detection

This research adopted the MLP algorithm for feedforward supervised learning prediction, specifically classification. The MLP architecture makes it an efficient anomaly-based IDS for detecting DDoS attacks [27]. The supervised feedforward process technique analyses the data and detects such attacks accurately. Determining ideal hyperparameters relies on the problem, model architecture, and dataset characteristics. Consequently, experimentation with various values and continuous monitoring of model performance during training is necessary to identify the optimal combination.

This research underscores the importance of specific hyperparameters, such as categorical cross-entropy with SoftMax function, the Adam optimizer, and the number of epochs, in enhancing the proposed model's performance. Notably, balancing the number of epochs is crucial to avoid underfitting, where inadequate fitting to training used in this study achieved convergence in less than 50 iterations with a batch size of 100, considered optimal values. Critical factors like learning rate and momentum, set at 0.001 and 0.9, significantly impact detection accuracy. Incorporating techniques like L2 regularization, early stopping, and a flattened layer further contributes to the model's robustness and prevents overfitting. Table 2 presents the model hyper-parameters.

Table 2. DL-based MLP model parameters tuning

No	1	2	3	4	5	6	7	8	9	10	11
Hyper parameters	Losses function	Classification function	Optimizer	No of epochs	Batch size	Learning rate	Momentum	Regularization	No of hiding layers	Activation function	No of neuron
Optimized parameters	Categorical cross-entropy	SoftMax function	Adam	50	100	0.001	0.9	L2 (0.001)	4	ReLU	100

Additionally, the early stopping technique was used (monitoring loss with patience =3). For the proposed detection approach, the experiment was executed and formulated in Python, utilizing the TensorFlow, Keras, and Scikit-Learn libraries with 3.10.5, 2.11, 2.11, and 1.2, respectively. The detection approach is applied to the "DDoS attack SDN dataset" with all features. The assessment of this approach's performance involves split testing techniques to evaluate its generalization, which divides the datasets into a substantial 80% for the training set, enabling the model to learn diverse DDoS attack patterns. Simultaneously, the remaining 20% allocated to the testing set acts as a representative sample to assess approach performance on unseen data for reliable evaluation.

3.3. Evaluate performance

The proposed DL-based approach undergoes evaluation, and its performance, when integrated with data mining, is measured using several crucial matrices [28]. These metrics are calculated through a confusion matrix, illustrating the comparison between predicted and actual classes. The elements of the confusion matrix are clarified as follows: (i) true positive signifies the accurate identification of attacks by the detection approach. (ii) true negative denotes the precise identification of normal traffic as normal, while (iii) false positive indicates the misclassification of normal traffic as an attack. Lastly, (iv) false negative reflects the misclassification of an attack as normal traffic. Moreover, additional performance evaluation metrics were considered based on those metrics, including recall, F1-score, precision, overall accuracy, area under the receiver operating characteristic curve (AUC-ROC) score, and FPR.

4. EXPERIMENT RESULTS AND DISCUSSION

This section discusses and analyses the experiment results, highlighting the accuracy and reliability of the proposed approach for future SDN network security applications. It also provides a thorough comparison between the proposed detection approach and existing methods. Lastly, this section outlines key discussions, identifies limitations and suggests future works.

4.1. Results and analysis

The training model is generated using an MLP model architecture with all features ($f = 22$), as shown in Figure 3. The dataset used for training the proposed detection approach is described in Table 1. As shown in the table, the total number of instance samples is 124,688. The dataset is split into 80% for training and 20%

for testing. This is a straightforward approach and a commonly used technique. As a result, a confusion matrix is generated to represent and evaluate the performance of the proposed detection approach. It is commonly used to compare the predicted labels against the actual labels.

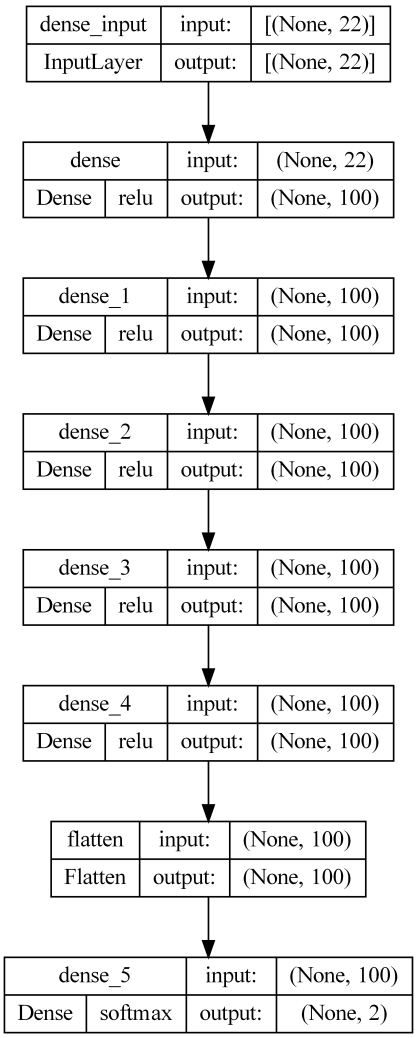


Figure 3. DL-based MLP model architecture

Moreover, Figure 4 presents the confusion matrix of DDoS flooding attack on SDN network. The detection approach achieved a high number of true positives (TP=15,655), which indicates the instances that were correctly detected as positive. The true negatives (TN=14,915) represent the instances that were correctly detected as negative. There was a relatively low number of false positives (FP=203), which indicates instances that were detected as positive but were actually negative. Also, there was a relatively low number of false negatives (FN=399), indicating the number of positive instances incorrectly predicted as negative by the proposed approach. In some cases, the proposed detection approach predicted a negative outcome, but the actual label was positive.

The confusion matrix analysis allows for the computation of various evaluation matrices, such as average accuracy, precision, F1-score, recall, and FPR, offering a comprehensive understanding of the overall performance of the proposed detection approach, as represented in Table 3. The detection DL approach archives 98.068% detection accuracy, 98.085% precision, 98.067% F1-score, 98.057% recall, and 1.34% FPR for detecting DDoS attacks on the SDN network. These evaluation results highlight the effectiveness of the proposed DL approach in accurately detecting such attacks.

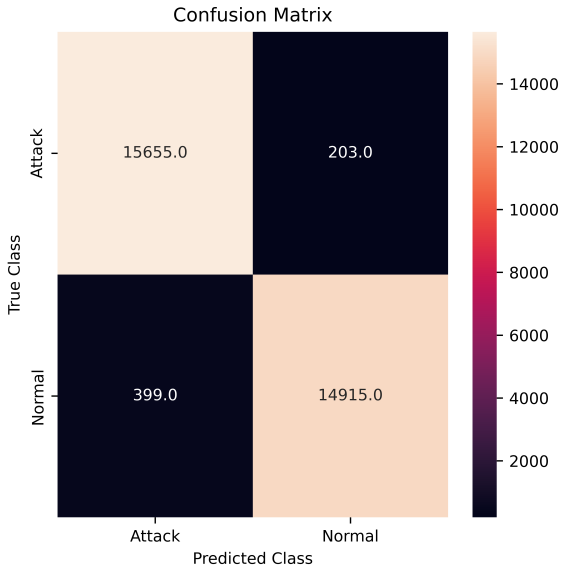


Figure 4. Confusion matrix of the DL-based MLP detection approach

Table 3. Average results of MLP detection approach

Performance evaluation metrics				
Accuracy (%)	Precision (%)	F1-score (%)	Recall (%)	FPR (%)
98.068	98.085	98.067	98.057	1.34

Further assessment is utilized, such as the AUC-ROC carve. The ROC curve represents the trade-off between true positive rates (TPR) and FPR for different classification thresholds. The AUC score quantifies the overall performance of the proposed approach with a perfect score of 1, indicating flawless detection. Conversely, if the AUC score approaches 0, it indicates poor performance by the proposed approach. As clearly shown in Figure 5, the AUC score value of the proposed approach is 98%, which indicates that the proposed approach excels at differentiating between normal traffic DDoS attacks.

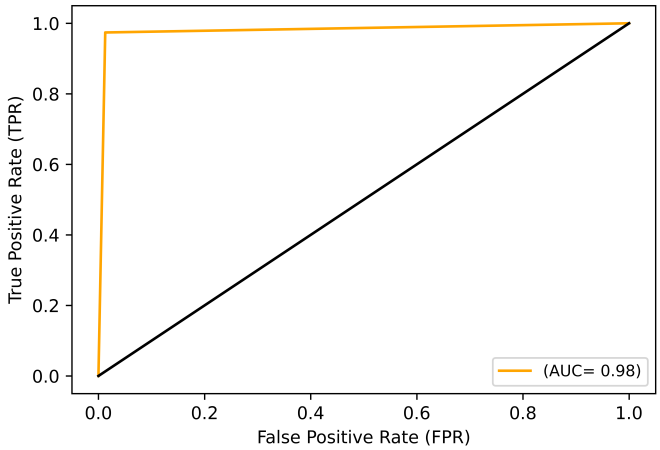


Figure 5. ROC-AUC carve of the DL-based MLP detection approach

4.2. Comparison of proposed detection

In addition to the previously mentioned results, this section provides a comprehensive evaluation of the proposed detection approach compared to the existing DLADSC approach [12], which utilizes RNN-based techniques for detecting DDoS attacks in an SDN controller environment. Both approaches aim to address

similar challenges; however, key differences emerge when evaluating their performance using several metrics, including (i) the SDN dataset itself, (ii) the average accuracy, (iii) precision, (iv) recall, (v) FPR, (vi) the F1-score, and (vii) time of DDoS attack detection (measured using Python time functions from inputting test data to producing the final prediction output).

As shown in Table 4, the proposed detection consistently achieves higher scores across most metrics: 98.068% detection accuracy, 98.085% precision, 98.057% recall, 1.34% FPR, and F1-score 98.067%. In contrast, DLADSC exhibits significantly lower performance, with 94.186% detection accuracy, 92.146% precision, 8.114% FPR, a an 94.276% F1-score. These results highlight the superior capability of the proposed detection approach in accurately identifying DDoS attacks with fewer false positives, where minimizing false alarms is paramount for enduring efficient networks management.

Table 4. A comparison of this approach with the DLADSC RNN approach

Approach	SDN dataset	Accuracy	Precision	Recall	FPR	F1-score	Times of detection
DLADSC RNN [12]	✓	94.186	92.146	✗	8.114	94.276	1.627
This approach (MLP)	✓	98.068	98.085	98.057	1.34	98.067	1.713

(✓) : matches the metrics, (✗) : does not match the metrics.

Despite the improved performance, the detection time reveals a slight trade-off. The proposed approach has a marginally longer detection time of 1.713 seconds compared to 1.627 seconds for DLADSC. While this difference is minimal, it could be relevant in extremely high-speed network environments where every fraction of a second counts. However, the slight increase in detection time is likely due to the use of four model hidden layers, which, while adding complexity and depth to the detection process, result in more accurate classification. This slight increase in detection time is justified by the significant improvements in accuracy and precision, making the proposed approach more comprehensive detection of DDoS attacks.

The implications of these results are substantial for future applications of DDoS detection in SDN environments. The enhanced accuracy and reduced FPR suggest that the proposed detection approach can better handle the complexity of SDN architectures, providing more trustworthy and efficient detection. Furthermore, the approach's ability to maintain high precision and recall across a realistic SDN dataset demonstrates its scalability and applicability in real-world scenarios. While DLADSC performance is marginally faster in detection time, the proposed approach offers a more robust solution with greater accuracy and fewer false alarms, making it the preferred choice for practical implementation in SDN-based networks.

4.3. Discussion and limitations

The enhanced accuracy and reduced FPR indicate that the proposed detection approach can handle the complexity of SDN architectures, offering trustworthy and efficient detection. Additionally, the ability to maintain high precision and recall across a realistic SDN dataset demonstrates its scalability and applicability in real-world scenarios, positioning it as a more robust detection approach compared to other ones, especially in practical SDN-based networks.

The results highlight the superior capability of the proposed detection approach in accurately identifying DDoS attacks with fewer FP, which is crucial for maintaining efficient network management. Despite the improved performance, there is a slight trade-off in detection time, where the proposed approach has a marginally longer detection time of 1.713 seconds compared to 1.627 seconds for the DLADSC approach. Although this difference is minimal, it may be due to the number of hidden layers, which adds complexity and depth to the detection process, resulting in more accurate detection.

5. CONCLUSIONS AND FUTURE WORKS

SDN technology provides flexible and cost-effective network management but remains susceptible to significant security vulnerabilities, especially DDoS attacks. To address these challenges, this research introduces a DL-based detection approach designed to overcome the shortcomings of existing approaches. By experimenting with a realistic SDN dataset and employing comprehensive features, the study detected both normal and malicious traffic patterns, ensuring accurate detection. The proposed detection methodology operates in three phases: dataset pre-processing, attack detection using DL algorithm, and rigorous evaluation based on performance metrics.

The results demonstrate a clear improvement, achieving a detection accuracy of 98.068% while minimizing FPRs to 1.34%, thereby outperforming other approaches in this space. These findings hold substantial implications for the field of SDN security and the broader network management community. The proposed approach not only enhances detection accuracy but also significantly reduces false alarms, contributing to more stable and efficient SDN operations. This advancement addresses a critical need for trustworthy and scalable solutions in real-world SDN environments. By aligning with modern DL practices, the study bridges gaps in current approaches, offering a robust and reliable solution for DDoS detection.

Future works could focus on several key areas to further improving the proposed detection approach. One potential direction is optimizing attack detection time without compromising accuracy. Additionally, incorporating feature selection techniques, such as ensemble methods, could help streamline the dataset by selecting the most relevant features, leading to faster processing times and reduced computational complexity. This would not only enhance detection efficiency but also make the model scalable and adaptable to SDN networks. Furthermore, the potential to extend this detection approach to safeguard against other attack types indicates a promising direction for future research and innovation, ultimately contributing to stronger and more secure network infrastructures.

ACKNOWLEDGEMENT

The Ministry of Higher Education Malaysia supports this work under the Fundamental Research Grant Scheme with project Code: FRGS/1/2022/ICT11/USM/02/1.

REFERENCES

[1] A. A. Bahashwan, M. Anbar, and N. Abdullah, "New architecture design of cloud computing using software defined networking and network function virtualization technology," in *Advances in Intelligent Systems and Computing*, vol. 1073, 2020, pp. 705–713.

[2] S. Scott-Hayward, S. Natarajan, and S. Sezer, "A survey of security in software defined networks," *IEEE Communications Surveys and Tutorials*, vol. 18, no. 1, pp. 623–654, 2016, doi: 10.1109/COMST.2015.2453114.

[3] M. I. Kareem and M. N. Jasim, "Entropy-based distributed denial of service attack detection in software-defined networking," *Indonesian Journal of Electrical Engineering and Computer Science (IJEECS)*, vol. 27, no. 3, p. 1542, Sep. 2022, doi: 10.11591/ijeecs.v27.i3.pp1542-1549.

[4] C. Kannan, R. Muthusamy, V. Srinivasan, V. Chidambaram, and K. Karunakaran, "Machine learning based detection of DDoS attacks in software defined network," *Indonesian Journal of Electrical Engineering and Computer Science (IJEECS)*, vol. 32, no. 3, p. 1503, Dec. 2023, doi: 10.11591/ijeecs.v32.i3.pp1503-1511.

[5] S. Singh and S. Prakash, "A survey on software defined network based on architecture, issues and challenges," in *2019 3rd International Conference on Computing Methodologies and Communication (ICCMC)*, Mar. 2019, pp. 568–573, doi: 10.1109/ICCMC.2019.8819785.

[6] M. A. Aladaileh *et al.*, "Effectiveness of an entropy-based approach for detecting low- and high-rate DDoS attacks against the SDN controller: experimental analysis," *Applied Sciences (Switzerland)*, vol. 13, no. 2, p. 775, Jan. 2023, doi: 10.3390/app13020775.

[7] E. Alomari, S. Manickam, B. B. Gupta, P. Singh, and M. Anbar, "Design, deployment and use of HTTP-based botnet (HBB) testbed," in *16th International Conference on Advanced Communication Technology*, Feb. 2014, pp. 1265–1269, doi: 10.1109/ICACT.2014.6779162.

[8] A. K. Al-Ani, M. Anbar, A. Al-Ani, and D. R. Ibrahim, "Match-prevention technique against denial-of-service attack on address resolution and duplicate address detection processes in IPv6 link-local network," *IEEE Access*, vol. 8, pp. 27122–27138, 2020, doi: 10.1109/ACCESS.2020.2970787.

[9] A. A. Bahashwan, M. Anbar, S. Manickam, T. A. Al-Amiedy, M. A. Aladaileh, and I. H. Hasbullah, "A systematic literature review on machine learning and deep learning approaches for detecting DDoS attacks in software-defined networking," *Sensors*, vol. 23, no. 9, p. 4441, May 2023, doi: 10.3390/s23094441.

[10] M. A. Aladaileh, M. Anbar, I. H. Hasbullah, A. A. Bahashwan, and S. Al-Sarawn, "Dynamic threshold-based approach to detect low-rate DDoS attacks on software-defined networking controller," *Computers, Materials Continua*, vol. 73, no. 1, pp. 1403–1416, 2022, doi: 10.32604/cmc.2022.029369.

[11] T. E. Ali, Y.-W. Chong, and S. Manickam, "Comparison of ML/DL approaches for detecting DDoS attacks in SDN," *Applied Sciences*, vol. 13, no. 5, p. 3033, Feb. 2023, doi: 10.3390/app13053033.

[12] A. Mansoor, M. Anbar, A. A. Bahashwan, B. A. Alabsi, and S. D. A. Rihan, "Deep learning-based approach for detecting DDoS attack on software-defined networking controller," *Systems*, vol. 11, no. 6, pp. 1–21, 2023, doi: 10.3390/systems11060296.

[13] J. D. Gadze, A. A. Bamfo-Asante, J. O. Agyemang, H. Nunoo-Mensah, and K. A.-B. Opare, "An investigation into the application of deep learning in the detection and mitigation of DDOS attack on SDN controllers," *Technologies*, vol. 9, no. 1, p. 14, Feb. 2021, doi: 10.3390/technologies9010014.

[14] A. S. Alshra'a, A. Farhat, and J. Seitz, "Deep learning algorithms for detecting denial of service attacks in software-defined networks," *Procedia Computer Science*, vol. 191, pp. 254–263, 2021, doi: 10.1016/j.procs.2021.07.032.

[15] T. A. Tang, L. Mhamdi, D. McLernon, S. A. R. Zaidi, M. Ghogho, and F. El Moussa, "DeepIDS: deep learning approach for intrusion detection in software defined networking," *Electronics (Switzerland)*, vol. 9, no. 9, pp. 1–18, 2020, doi: 10.3390/electronics9091533.

[16] M. S. Elsayed, N.-A. Le-Khac, S. Dev, and A. D. Jurcut, "DDoSNet: a deep-learning model for detecting network attacks," in *2020 IEEE 21st International Symposium on "A World of Wireless, Mobile and Multimedia Networks" (WoWMoM)*, Aug. 2020, pp. 391–396, doi: 10.1109/WoWMoM49955.2020.00072.
[17] S. Haider *et al.*, "A deep CNN ensemble framework for efficient DDoS attack detection in software defined networks," *IEEE Access*, vol. 8, pp. 53972–53983, 2020, doi: 10.1109/ACCESS.2020.2976908.
[18] T. A. Tang, D. McLernon, L. Mhamdi, S. A. R. Zaidi, and M. Ghogho, "Intrusion detection in sdn-based networks: deep recurrent neural network approach," in *Advanced Sciences and Technologies for Security Applications*, Springer, 2019, pp. 175–195.
[19] Y. Liu, M. Dong, K. Ota, J. Li, and J. Wu, "Deep reinforcement learning based smart mitigation of DDoS flooding in software-defined networks," in *2018 IEEE 23rd International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD)*, Sep. 2018, vol. 2018-Septe, pp. 1–6, doi: 10.1109/CAMAD.2018.8514971.
[20] C. Li *et al.*, "Detection and defense of DDoS attack–based on deep learning in OpenFlow-based SDN," *International Journal of Communication Systems*, vol. 31, no. 5, p. e3497, Mar. 2018, doi: 10.1002/dac.3497.
[21] I. H. Sarker, "Deep learning: a comprehensive overview on techniques, taxonomy, applications and research directions," *SN Computer Science*, vol. 2, no. 6, p. 420, Nov. 2021, doi: 10.1007/s42979-021-00815-1.
[22] B. A. Mohammed *et al.*, "Hybrid techniques of analyzing MRI images for early diagnosis of brain tumours based on hybrid features," *Processes*, vol. 11, no. 1, p. 212, 2023, doi: 10.3390/pr11010212.
[23] M. A. Al-Garadi, A. Mohamed, A. K. Al-Ali, X. Du, I. Ali, and M. Guizani, "A survey of machine and deep learning methods for internet of things (IoT) security," *IEEE Communications Surveys Tutorials*, vol. 22, no. 3, pp. 1646–1685, 2020, doi: 10.1109/COMST.2020.2988293.
[24] A. H. H. Kabla, A. H. Thamrin, M. Anbar, S. Manickam, and S. Karuppayah, "PeerAmbush: multi-layer perceptron to detect peer-to-peer botnet," *Symmetry*, vol. 14, no. 12, p. 2483, Nov. 2022, doi: 10.3390/sym14122483.
[25] N. S. Shaji, T. Jain, R. Muthalagu, and P. M. Pawar, "Deep-discovery: anomaly discovery in software-defined networks using artificial neural networks," *Computers and Security*, vol. 132, p. 103320, 2023, doi: 10.1016/j.cose.2023.103320.
[26] N. Ahuja, G. Singal, and D. Mukhopadhyay, "DDOS attack SDN dataset," *Mendeley Data*, vol. 1, no. September, p. 17632, 2020, doi: 10.17632/jxpfjc64kr.1.
[27] A. H. H. Kabla *et al.*, "Machine and deep learning techniques for detecting internet protocol version six attacks: a review," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 13, no. 5, pp. 5617–5631, Oct. 2023, doi: 10.11591/ijece.v13i5.pp5617-5631.
[28] M. Anbar, R. Abdullah, I. H. Hasbullah, Y.-W. Chong, and O. E. Elejla, "Comparative performance analysis of classification algorithms for intrusion detection system," in *2016 14th Annual Conference on Privacy, Security and Trust (PST)*, Dec. 2016, pp. 282–288, doi: 10.1109/PST.2016.7906975.

BIOGRAPHIES OF AUTHORS

Abdullah Ahmed Bahashwan earned his Ph.D. degree in internet infrastructures security from the National Advanced IPv6 Centre of Excellence (NAv6), Universiti Sains Malaysia (USM), where he also completed his M.Sc. in internet engineering. He also holds a Bachelor of Computer Applications (B.C.A.) from Osmania University (OU), Hyderabad, India. His research interests include cybersecurity, IDS, artificial intelligence (ML and DL), feature selection techniques, internet protocol version 6 (IPv6) security, software-defined networks (SDN) security, and the IoT. He can be contacted at email: a.a.o.bahashwan@gmail.com.

Mohammed Anbar obtained his Ph.D. in Advanced Internet Security and Monitoring from University Sains Malaysia (USM). He is a senior lecturer at National Advanced IPv6 Centre (NAv6), Universiti Sains Malaysia. His current research interests include malware detection, web security, IDS, intrusion prevention systems (IPS), network monitoring, IoT, and IPv6 security. He can be contacted at email: anbar@USM.my.

Selvakumar Manickam director and associate professor at Universiti Sains Malaysia Director and associate professor at National Advanced IPv6 Centre (NAv6), Universiti Sains Malaysia. His research interests include cybersecurity, the IoT, Industry 4.0, and machine learning. He has authored and co-authored more than 160 articles in journals, conference proceedings, and book reviews and graduated 13 Ph.D.. He has ten years of industrial experience prior to joining academia. He is a member of technical forums at national and international levels. He also has experience building IoT, embedded, server, mobile, and web-based applications. He can be contacted at email: selva@USM.my.

Taief Alaa Al-Amiedy received a B.Sc. degree in ECE engineering from the University of Kufa, Iraq, an M.Sc. degree in internet engineering from USM, Malaysia, and a Ph.D. degree in internet infrastructure security from the Nav6 Centre, USM, Malaysia. His research interests include mobile and wireless communication, artificial intelligence and optimization algorithms, network infrastructure security, IDS, and IoT security. He can be contacted at email: taiefalaa@gmail.com.

Iznan H. Hasbullah received a B.Sc. degree in electrical engineering from Rensselaer Polytechnic Institute, Troy, NY, USA. He is currently pursuing an M.Sc. degree in advanced network security. He has experience working as a software developer, a research and development consultant, and a network security auditor before joining the National Advanced IPv6 Centre (NAv6), Universiti Sains Malaysia, in 2010, as a research officer. His research interests include unified communication, telematics, network security, network protocols, and next-generation networks. He can be contacted at email: iznan@usm.my.