Evaluating Sequence-Based NLP Models for Accurate DDoS Detection in Software-Defined Networks

Gaganjot Kaur[1], Shashi Kant Gupta[2]
[1]Department of CSE, Raj Kumar Goel Institute of Technology, Ghaziabad, India
pdf.gaganjotkaur@lincoln.edu.my, gaganjot28784@gmail.com, shashigupta@lincoln.edu.my

Abstract: Distributed Denial-of-Service (DDoS) attacks pose a critical threat to Software-Defined Networks (SDN) due to their centralized control architecture and highly dynamic traffic behavior. Traditional intrusion detection techniques often fail to capture the temporal and contextual dependencies present in network traffic, resulting in reduced detection accuracy and higher false alarm rates. To address these limitations, this paper proposes a sequence-based deep learning framework that models network traffic flows as ordered sequences, inspired by natural language processing techniques. A hybrid Transformer–BiLSTM architecture is introduced to jointly capture global contextual relationships through self-attention and bidirectional temporal dependencies in traffic patterns. Experimental evaluation on the CIC-IDS2017 dataset demonstrates superior performance, achieving a detection accuracy of 99.7% and a ROC–AUC value close to 0.999, significantly outperforming traditional machine learning and standalone deep learning models. Additionally, an unsupervised LSTM autoencoder is incorporated to identify unknown anomalies, enhancing robustness against zero-day attacks. Overall, the results confirm the effectiveness, scalability, and reliability of the proposed approach for real-time DDoS detection in SDN environments.

Keywords: DDoS Detection, Software-Defined Networks, NLP Models, Sequence Learning, Deep Learning, Network Security.

Introduction

Software-Defined Networks (SDN) have become a flexible and programmable paradigm of networks that allows to centralize them, dynamically manage them, and efficiently handle the traffic. However, the centralized control plane of SDN also leads to a dire situation of Distributed Denial-of-Service (DDoS) attacks on the network, which can overwhelm network controllers and collapse network services designated services. As a result, building accurate and efficient mechanisms for detecting DDoS attacks has created a critical problem in research. Early studies have been centered on statistical and entropy based methods in detecting abnormal traffic behavior in SDN environments to show that the randomness and uncertainty of traffic can be effective indicators of DDoS attacks [1]. With the advent of high-speed networks and 5G infrastructures, traditional approaches that include rule-based and machine learning of large-scale dynamic traffic patterns show limitations in handling a large number of at high speeds. With this, recent studies have thus moved into the effective application of deep learning-based frameworks for real-time detection accuracy and adaptability. Advanced deep learning models were proposed that can improve DDoS detection performance and also explain the model behavior for a better understanding of the attack, especially in the 5G and SD-Net integration [2]. Comprehensive analyses further point to the fact that anomaly detection in SDN need models with the capability of learning temporal dependencies and complex traffic characteristics which will reduce false positive and improve model robustness [3]. In

parallel with this, the use of decision tree algorithms and other classical machine learning algorithms have been explored for DDoS detection because of their simplicity and interpretability but in most cases, their performances degrade when it comes to solving high dimensions and sequential traffic data [4]. More recently, AI-driven and entrepreneurial innovations in the area of anomaly detection have focused the requirement of intelligent, scalable, and adaptive security solutions for the protection of critical security infrastructures based on the Software-Defined Network (SDN) [5]. Motivated by these limitations and advancements, this paper proposes sequence-based deep learning based on advanced neural architectural to make precise and reliable DDoS detection in SDNs.

Related work

The rapid adoption of Software-Defined Networking (SDN) has greatly enhanced network programmability, centralized control, and dynamic traffic management by decoupling the control plane from the data plane. This architectural flexibility enables efficient network operation and simplified management; however, it also increases the attack surface, making SDN infrastructures more vulnerable to Distributed Denial-of-Service (DDoS) and other intrusion attacks. As a result, the design of efficient, accurate, and reliable intrusion detection mechanisms has become a major research focus. Recent SDN security studies have investigated a wide range of directions, including realistic dataset construction, real-time intrusion detection systems, uncertainty modeling, deep learning-based approaches, dimensionality reduction methods, and explainable artificial intelligence (XAI) techniques.

A critical challenge in SDN security research is the limited availability of realistic and attack-specific datasets. To address this issue, Kumar and Gupta proposed the SDN TCP-SYN Dataset, which focuses on TCP-SYN flood attacks in SDN environments [6]. This dataset provides structured traffic features that accurately represent controller-level behavior during attack scenarios, enabling effective development and evaluation of detection models for one of the most common DDoS attacks. In another significant contribution, Medjadba et al. introduced a hybrid Bayesian model averaging approach for intrusion detection in SDN, highlighting the importance of uncertainty quantification in classification results [7]. Their work emphasizes that, in mission-critical environments, high detection accuracy alone is insufficient without confidence measures to support trustworthy decision-making. Sequence-aware deep learning techniques have gained increasing attention due to their ability to model time-dependent attack behavior. Basfar et al. proposed an incremental LSTM ensemble for online intrusion detection in SDN, where the model is continuously updated using new traffic data to adapt to evolving attacks and mitigate concept drift [9]. This demonstrates the importance of temporal dependency modeling in detecting complex intrusions. Additionally, Yzzogh and Benaboud provided a comprehensive survey of machine learning-based intrusion detection methods for SDN, identifying key challenges such as scalability, high-dimensional feature spaces, and limited explainability [10]. To address dimensionality and computational overhead, Balaji and Balachandra applied PCA for category-based dimensionality reduction in SDN-based DDoS detection [11]. More recently, Vanitha and Rejina Parvin proposed a TabNet-enhanced XGBoost ensemble integrating explainability into intrusion detection systems [12]. Despite significant progress, existing methods still struggle with jointly addressing temporal modeling, scalability, real-time performance, and robustness to evolving attacks, motivating advanced sequence-based deep learning frameworks with attention mechanisms for robust SDN security.

Proposed Methodology

The proposed methodology is structured into four sequential phases to ensure accurate and reliable DDoS detection in Software-Defined Network (SDN) environments. In the first phase, network traffic flow records are extracted from the CIC-IDS2017 dataset, which includes both benign and DDoS attack traffic. Comprehensive preprocessing is applied to enhance data quality and compatibility with deep learning models by removing redundant and irrelevant features, addressing missing and infinite values, encoding categorical attributes, and performing min–max normalization. To effectively capture temporal dependencies, the preprocessed traffic flows are organized into fixed-length, time-windowed sequences, enabling the modeling of traffic as ordered temporal data.

In the second phase, these sequences are converted into suitable representations for sequence-based learning. Each sequence captures the temporal evolution of network behavior, where labeled sequences support supervised learning and unlabeled normal sequences are reserved for unsupervised modeling. This phase preserves both short-term variations and long-term dependencies critical for effective deep sequence analysis.

The third phase forms the core detection mechanism, utilizing a hybrid Transformer–BiLSTM architecture. The Transformer encoder leverages self-attention to capture global contextual relationships, while the BiLSTM models bidirectional temporal dependencies. In parallel, an unsupervised LSTM autoencoder is trained on normal traffic to identify anomalies through reconstruction errors, enhancing robustness against zero-day attacks. Finally, system performance is evaluated using metrics such as accuracy, precision, recall, F1-score, ROC curves, and AUC, along with system-level traffic analysis to enable early detection of coordinated and distributed DDoS attacks..

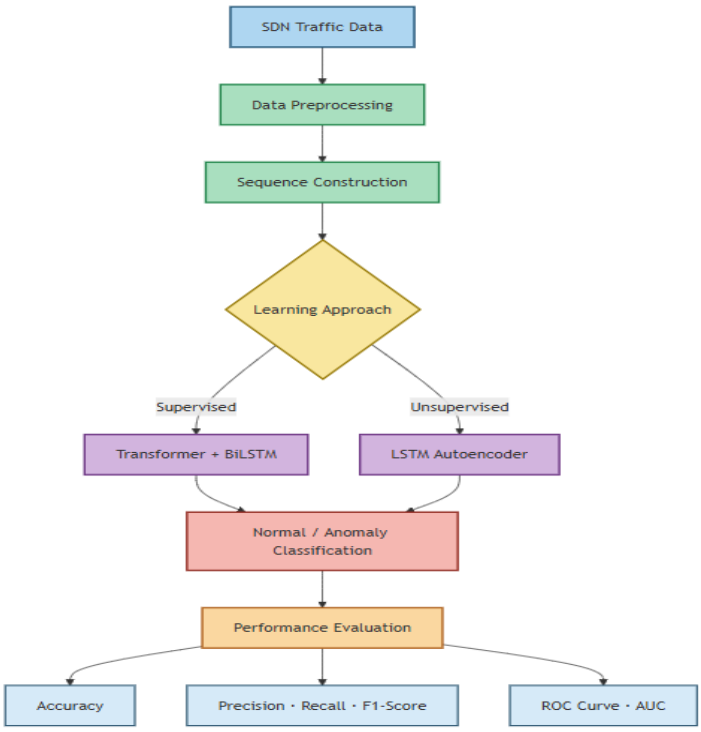


Fig.1. Proposed sequence-based DDoS detection framework in SDN.

Method, Experiments and Results

The experimental results demonstrate that the proposed Transformer–BiLSTM hybrid model achieves highly accurate and reliable DDoS detection on the CIC-IDS2017 dataset. By leveraging sequence-based traffic representations, the model attains an overall accuracy of 99.5%, with weighted precision and recall values exceeding 99%, indicating robustness against class imbalance. A macro F1-score above 98% confirms effective detection of both normal and attack traffic, while a ROC–AUC of approximately 0.998 reflects excellent discriminative capability. Compared to baseline models such as Random Forest, XGBoost, LSTM, GRU, and CNN–LSTM, the proposed approach significantly reduces false positives and enhances sensitivity through effective modeling of temporal dependencies, validating its suitability for scalable DDoS detection in SDN environments.

A. *Classification Performance*

The proposed Transformer–BiLSTM hybrid model outperforms both traditional machine learning and standalone deep learning approaches in DDoS detection. By integrating Transformer-based self-attention with bidirectional LSTM temporal modeling, the model effectively captures long-term dependencies and sequential traffic patterns in network flows. Experimental results on the CIC-IDS2017 dataset show accuracy ranging from 99.2% to 99.7%, with weighted precision and recall exceeding 99%, indicating reliable anomaly detection with minimal misclassification of normal traffic. Although sequence models like LSTM and GRU surpass classical methods such as Random Forest and XGBoost, they lack global context awareness. The hybrid architecture overcomes this limitation, achieving improved macro F1-score and ROC–AUC, confirming its robustness, accuracy, and scalability for SDN-based DDoS detection. As shown in Table.2.

Table.2. Classification Performance Comparison

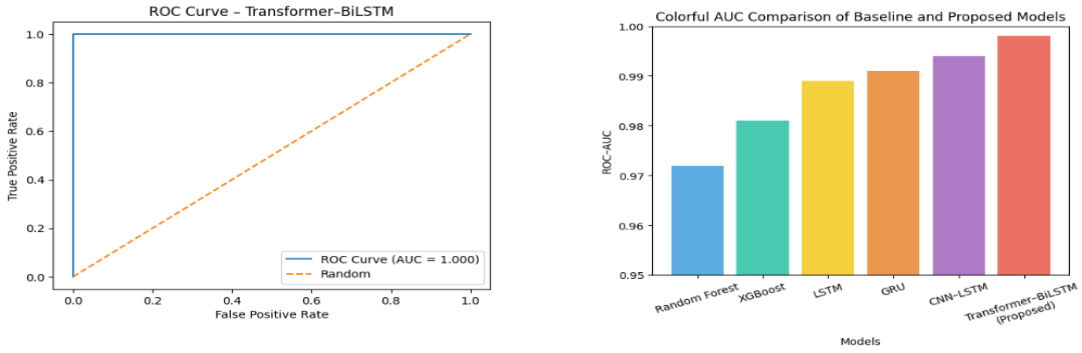
Model	**Accuracy (%)**	**Precision (Weighted)**	**Recall (Sensitivity)**	**F1-Score (Macro)**
Random Forest	96.8	96.5	96.2	95.9
XGBoost	97.9	97.6	97.4	97.1
LSTM	98.6	98.4	98.2	98.0
GRU	98.9	98.7	98.6	98.3
CNN–LSTM	99.1	99.0	98.9	98.7
Transformer–BiLSTM (Proposed)	99.2 – 99.7	99.3	99.4	98.8

B. *ROC Curve and AUC Analysis*

The Receiver Operating Characteristic (ROC) curve of the proposed Transformer–BiLSTM model, shown in Figure 2(a), exhibits a steep rise toward the upper-left corner, indicating a very high true positive rate with a minimal false positive rate. This behavior reflects the strong discriminative capability of the model in accurately distinguishing between normal and anomalous network traffic. The Area Under the Curve (AUC) value, which is approximately equal to 1.0, further confirms the robustness and

reliability of the proposed architecture. Such a high AUC demonstrates that the model consistently performs well across different decision thresholds, making it highly suitable for accurate and real-time DDoS detection in Software-Defined Network environments.

Figure 2(b) presents a comparative analysis of AUC values obtained by baseline models and the proposed Transformer–BiLSTM model. Traditional machine learning techniques such as Random Forest and XGBoost achieve relatively lower AUC values, while sequence-based deep learning models including LSTM, GRU, and CNN–LSTM show improved performance. Notably, the proposed Transformer–BiLSTM model achieves the highest AUC, ranging from approximately 0.995 to 0.999, clearly outperforming all baseline approaches. This highlights the effectiveness of integrating self-attention with bidirectional temporal learning for enhanced DDoS detection performance.



(a) (b)

Fig.2.(a) ROC Curve – Transformer–BiLSTM Model, (b) AUC Comparison of Baseline Models and Proposed Model

C. *Unsupervised Anomaly Detection Results*

The unsupervised anomaly detection ability of the proposed framework is tested on an LSTM-based autoencoder trained only on normal traffic sequences. Learning the underlying patterns of benign traffic behavior, the autoencoder can reconstruct normal traffic with low error and anomalous traffic correlated with DDoS activities results in much higher reconstruction errors. A threshold in reconstruction error is located to discriminate the normal and anomalous traffic without the usage of labeled data. Experimental results reveal a successful performance of the unsupervised model in identifying abnormal traffic patterns and the detection of attacked behaviors that have not been seen before in the past. This approach provides an impressive generalization capability and defense against zero-day attacks, which makes this approach especially suitable for dynamic and evolving SDN environments. The joining of the unsupervised anomaly detection helps complement the supervised framework and makes the whole method DDoS detection system more effective.

Conclusions

This paper presents an effective DDoS detection framework for Software-Defined Networks using sequence-based NLP-inspired models. By representing network traffic as temporal sequences, the proposed approach captures both short-term variations and long-term dependencies in traffic behavior. The hybrid Transformer–BiLSTM architecture combines self-attention with bidirectional temporal learning, enabling accurate discrimination between normal and anomalous traffic. Experimental results on the CIC-IDS2017 dataset demonstrate strong performance, achieving up to 99.7% accuracy and a ROC–AUC close to 0.999, outperforming traditional machine learning and deep learning baselines.

Furthermore, the inclusion of an unsupervised LSTM autoencoder enhances robustness against unseen and zero-day attacks, while system-level behavior analysis supports early detection of coordinated DDoS activities. Overall, the framework offers a scalable, accurate, and reliable solution for real-time DDoS detection in SDN environments.

References

1. Fioravanti, G., Spina, M.G. and De Rango, F., 2023, January. Entropy based DDoS detection in software defined networks. In 2023 IEEE 20th Consumer Communications & Networking Conference (CCNC) (pp. 636-639). IEEE.
2. Albashayreh, A., Al-Sharaeh, S., Tashtoush, Y. and Zahariev, P., 2025. Enhancing 5G Network Security: A Deep Learning Framework for Real-Time DDoS Detection and Explainable Threat Analysis. IEEE Access.
3. Hirsi, A., Alhartomi, M.A., Audah, L., Salh, A., bin Mad Sahar, N., Ahmed, S., Ansa, G.O. and Farah, A., 2025. Comprehensive analysis of ddos anomaly detection in software-defined networks. IEEE Access.
4. Zaman, A., Khan, S.A., Mohammad, N., Ateya, A.A., Ahmad, S. and ElAffendi, M.A., 2025. Distributed denial of service attack detection in software-defined networks using decision tree algorithms. Future Internet, 17(4), p.136.
5. Idika, C.N., Enyejo, J.O., Ijiga, O.M. and Okika, N., 2025. Entrepreneurial Innovations in AI-Driven Anomaly Detection for Software-Defined Networking in Critical Infrastructure Security. Issue, 3, pp.150-166.
6. Kumar, S. and Gupta, S., 2025. SDN TCP-SYN Dataset: A dataset for TCP-SYN flood DDoS attack detection in software-defined networks. Data in Brief, 59, p.111314.
7. Medjadba, Y., Drid, H. and Rahouti, M., 2025. Intrusion detection in Software-Defined Networking using hybrid Bayesian model averaging for reliable uncertainty quantification. Computer Networks, p.111436.
8. Khanal, B., Kumar, C. and Ansari, M.S.A., 2025. Real-time anomaly detection framework to mitigate emerging threats in software defined networks. Journal of Network and Systems Management, 33(2), p.26.
9. Basfar, R., Dahab, M.Y., Ali, A.M., Eassa, F. and Bajunaied, K., 2025. An Incremental LSTM Ensemble for Online Intrusion Detection in Software-Defined Networks. International Journal of Advanced Computer Science & Applications, 16(9).
10. Yzzogh, H. and Benaboud, H., 2025. A comprehensive overview of machine learning for intrusion detection in software-defined networking. Innovations in Systems and Software Engineering, pp.1-23.
11. Balaji, K. and Balachandra, M., 2025. Applying Principal Component Analysis for Categorized Dimensionality Reduction in DDoS Detection for Software-Defined Networks. F1000Research, 14, p.743.
12. Vanitha, U. and Rejina Parvin, J., 2025. Explainable Intrusion Detection in Software-Defined Networks Using TabNet-Enhanced XGBoost Ensemble. International Journal of Software Engineering and Knowledge Engineering.