Comparative Performance Analysis of Sequence-Aware NLP Models for DDoS Attack Detection in SDN

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

Abstract: Software Defined Networks (SDN) provides the ability to a centralized control, which increases the flexibility of the network, but the architectural design of SDN also provides an increased vulnerability to Distributed Denial-of-Service (DDoS) attacks to the control plane. Accurate and timely detection of such attacks is thus essential for ensuring the reliability of networks. This paper provides a comparative performance analysis of sequence awareness Natural Language Processing (NLP) models for DDoS attack detection at SDN environments. Network traffic information from the CICDDoS2019 dataset is modeled as temporal sequences and analyzed with LSTM, BiLSTM, GRU and Transformer architectures. The models are tested with the help of standard performance metrics such as accuracy, precision, recall, F1-score, ROC-AUC and detection latency. Experimental results reveal that the high detection accuracy (96.1% to 98.8%) is obtained for sequence-aware models. The Transformer model is the best performer overall in terms of accuracy (98.8%), F1-score (98.3%) and ROC-AUC (0.991), and GRU has the lowest detection latency, which is suitable for SDN deployment in a real-time scenario. The results speak volume about the effectiveness of temporal sequence modeling and attention-based learning to robust and scalable DDoS detection in Software Defined Networks.
Keywords: SDN, DDoS Detection, Sequence Modeling, NLP, LSTM, Transformer, Cybersecurity.

Introduction

The advent of the fast-moving network infrastructures and the popularity of Software Defined Networking (SDN) has impacted the flexibility, programmability, and centralized control of networks to a great extent. However, this architectural change also creates new security issues, specially making the SDN controller a high value target for a Distributed Denial-of-Service (DDoS) attack. By flooding the control plane with malicious traffic, DDoS attacks can make the network teoría such severe performance that the network can be disrupted the services. Consequently, the proper detection of DDoS attacks and the detection of DDoS attacks in a timely manner remains a basic requirement to guarantee the reliability and security of SDN environments. A critical challenge for the development of proper intrusion detection systems (IDS) is tracking down authentic and comprehensive datasets that converts a complete description of attack behaviors. Sharafaldin et al. [1] overcome this problem by way of a clean-cut intrusion detection dataset as well as an elaborate traffic characterization that served as a reference point for tests of network security solutions. Building on such datasets, researchers have experimented with many different approaches of machine learning and deep learning to improve the accuracy of detecting intrusions. Ferrag et al. [2] presented a detailed comparative evaluation of deep learning- based IDS techniques and their

better performance compared with traditional machine learning models, considering complex scenarios with cyber threats. In terms of SDN specific application, the use of sequence aware deep learning models has attracted attention because of their capabilities in detecting temporal dependencies in the network traffic. Tang et al. [3] showed that the deep recurrent neural networks can be effectively used to model the sequential traffic patterns for the intrusion detection in the SDN-based networks in comparison with the static flow-based approaches. These results highlight the need for time-based information in order to detect advanced attacks (low-rate and evolving DDoS traffic). Earlier intrusion detection techniques have mostly used hybrid techniques based on methods, which have combined anomaly based and signature based techniques to integrate better coverage of detection. Kim et al. [4] proposed a hybrid intrusion detection framework combining both the anomaly detection and misuse detection to achieve an improved accuracy at the cost of complexity of the system and an inability to detect unseen attacks. More recently advanced deep learning models have been introduced to deal with these limitations. Yang et al. [5] proposed a supervised adversarial variational auto encoder for intrusion detection, which achieves enhanced robustness and generalization capabilities in high dimensional traffic data. Despite these advancements, the previous research is often focusing on single deep learning architectures without doing a systematic comparison of multiple sequence aware models under a unified SDN-based DDoS detection paradigm. Moreover, little focus has been given to the use of Natural Language Processing (NLP)-inspired sequences modelling procedures to analyze traffic. In order to overcome these limitations, this paper describes a comparative analysis of the performance of sequence-aware NLP namely recurrent and attention-based models for DDoS attack detection in SDN environments. By replicating network traffic into time series and testing several deep learning models in the same experimental scenarios, the purpose of this study is to determine which deep learning model is the best according to detection accuracy, robustness, and deployment feasibility.

Related work

Recent progress of deep learning has had a considerable impact on the progress of intelligent intrusion detection systems by enabling automated learning of features from complex network traffic data. Lopez-Martin et al. [6] presented network traffic classification framework based on convolutional neural networks (CNN) and recurrent neural networks (RNN) adopting Internet of Things (IoT) traffic. Their work showed that spatial-temporal feature extraction combination can improve the classification accuracy, indicating the significance of the sequential modeling in network traffic analysis. Extending deep learning applications for intrusion detection Roy et al. [7] introduced a method of identifying malicious traffic patterns using an artificial neural network. Their work demonstrated that deep neural architectures surpass conventional machine learning approaches in terms of learning nonlinear relationships in a network data (high-dimensional data). However, the proposed model was mainly based on the static features of traffic and did not explicitly take advantage of the temporal dependencies in evolving attack scenarios. To overcome these issues related to the scalability and the temporal modeling, Khan et al. [8] proposed a hybrid convolutional-LSTM model to detect the network's intrusion. By using CNN layers for feature extraction and LSTM layers for sequence learning, the model demonstrated enhanced detection accuracy and scalability across extensive datasets. This work focused on the effectiveness of the combination of convolutional and recurrent structures in order to capture both local and long-term traffic patterns. Ferrag et al. [9] further investigated deep learning-based intrusion detection focused on

Distributed Denial-of-Service (DDoS) attacks in the sector-specific environments. Their study showed that deep learning models can be successfully used to detect DDoS attacks with a high accuracy by learning discriminative traffic representations. Nevertheless, the work was tied down to a single application domain and failed to offer a comparative evaluation of different sequence-aware architectures. Early attempts to utilize the concept deep learning in SDN-based security systems were introduced by Niyaz et al. [10], which proposed a deep learning based DDoS detection system designed for Software Defined Networking environments. Their approach took advantage of the centralized control of SDN to gather the traffic statistics and use deep learning models to detect the attack which provided a base for the later research on intrusion detection focused on SDN. Similarly, Vinayakumar et al. [11] have performed a detailed study of deep learning based intelligent intrusion detection systems wherein different architectures of deep learning are tested on different datasets. Their results proved that the deep learning models were better than the conventional ones; however the study mainly focused on individual architectures rather than a comprehensive comparison. Finally, one of the first deep learning-based intrusion detection systems (using SDN traffic data) was presented by Javaid et al. [12]. Their work showed the viability of using deep neural networks in intrusion detection and the potential of traffic visibility using the SDN. Despite its contributions, the model was missing sequence aware learning and did not consider evolving attack dynamic. As shown in Table.1.

Table 1. Compares this work with the related work or previous research by other researchers

Ref.	Study Focus	Model / Technique	Sequence Awareness	SDN Environment	Dataset
[6]	Network traffic classification (IoT)	CNN + RNN	Partial	No	IoT traffic
[7]	Intrusion detection	Artificial Neural Network (ANN)	No	No	Generic network traffic
[8]	Intrusion detection	CNN + LSTM (Hybrid)	Yes	No	Large-scale IDS datasets
[9]	DDoS attack detection	Deep learning models	Limited	No	Sector-specific datasets
[10]	DDoS detection	Deep learning	No	Yes	SDN traffic statistics
[11]	Intelligent IDS	Multiple deep learning architectures	Limited	No	Multiple benchmark datasets
[12]	Intrusion detection in SDN	Deep Neural Network (DNN)	No	Yes	SDN traffic data
Proposed Work	**DDoS detection in SDN**	**LSTM, BiLSTM, GRU, Transformer**	**Yes (Full)**	**Yes**	**CICDDoS2019**

Proposed Methodology

Phase 1 Traffic Gathering and Preprocessing

In this phase network traffic is collected in flow level from SDN controller and SDN controller provide centralized and global view of the network activity. The CICDDoS2019 dataset are the major source of

data, which contains both benign and DDoS traffic flows. Preprocessing is done for improving the quality of data, by removing irrelevant and redundant data features, dealing with missing and inconsistent values, normally for number normalized attributes. These operations aid in the reduction of noise and reduce the computational complexity apart from providing stable and efficient training of sequence-aware deep learning models.

Phase 2: Construction of Temporal Sequence

In this phase, the data of network traffic preprocessed will be converted into temporal sequences with fixed length in order to identify the dynamic behavior of DDoS attacks. A sliding window mechanism is used for organizing flow records in chronological order on the basis of the timestamps. Each sequence is a continuous snapshot of the evolution of the traffic over a time duration and it makes possible learning the temporal dependencies instead of only isolated instances of traffic. This NLP-inspired sequence representation is what allows the models to be able to identify evolving, bursty and low rate DDoS attack patterns successfully.

Phase 3: Train Model using Sequence Awareness

In this stage the created traffic sequences are fed to the training of sequence-awares deep learning models such as, LSTM, BiLSTM, GRU, Transformer architectures etc. A consistent training paradigm is used to help with fair model comparison. The dataset is divided into the training data and the testing data with the stratified split of 70:30 and the class is preserved. Binary cross entropy loss and Adam optimizer are used for optimizing the model and the early stopping is used to avoid overfitting and to enhance the generalization performance.

Phase 4- Classification and Evaluation of Performance

The newly created trained models will be used during this phase to classify the incoming sequences of traffic into benign or DDoS category based on Softmax output layer. Model performance is analyzed using such standard scores as accuracy, precision, recall, and F1-score, ROC-AUC, and detection latency. One gets a full reading of not only how these are effective in detecting but also how in the real world they can work in real-time from these metrics. A comparative analysis of the whole models is carried out, in order to determine the most suitable architecture in terms of accurate and efficient DDoS detection in Software Defined Network environments. As shown in Fig.1.

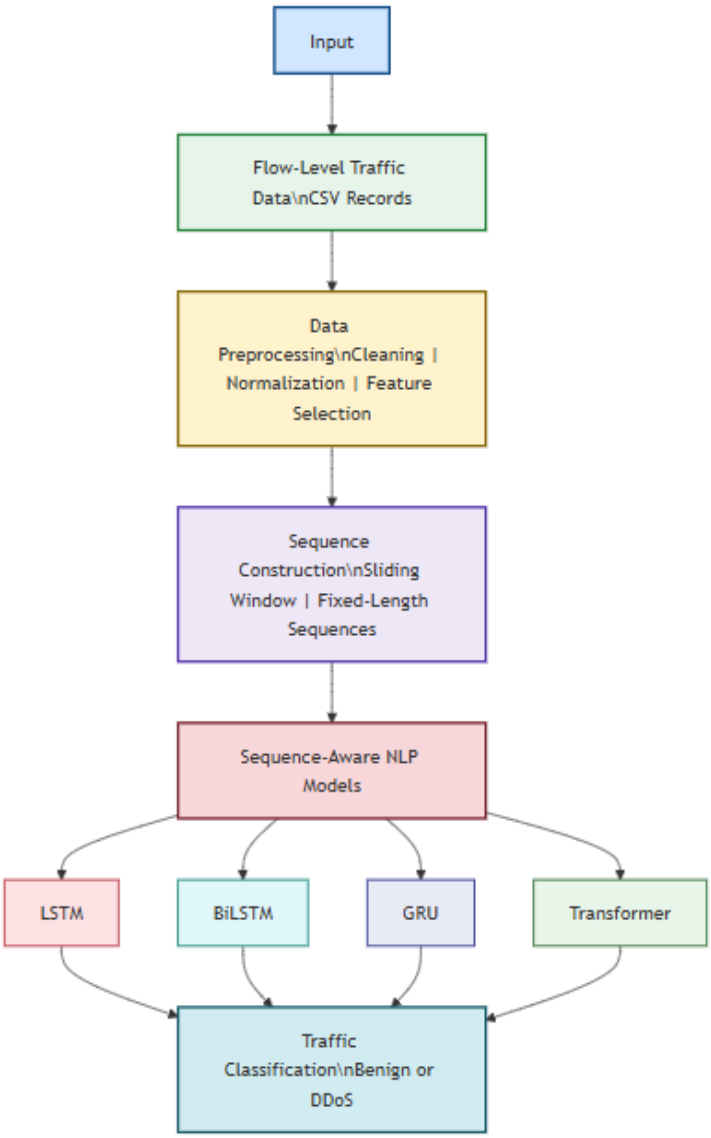

Fig.1. Flowchart of the proposed sequence-aware NLP-based DDoS detection framework in SDN.

Method, Experiments and Results

The proposed work focuses on evaluation of the performance of sequence aware deep learning models; LSTM, BiLSTM, GRU, and Transformer for the DDoS attack detection where the CICDDoS2019 dataset. The models are evaluated based on standard classification metrics such as accuracy, precision, recall, F1-score, roc auc and latency of detection. Experimental results indicate that the detection accuracy of the evaluated models is quite high, varying between 96.1% and 98.8%, where the Transformer model achieves the highest detection accuracy, i.e., 98.8%, followed by BiLSTM with detection accuracy of 97.9%, LSTM with detection accuracy of 96.8% and GRU with detection Accuracy of 96.1%. A comprehensive comparative analysis is presented in order to highlight the detection performance / computational efficiency trade-offs for deployment into Software Defined Network (SDN) environments.

A. *Model-wise Performance Comparison*

Figure 2 shows the accuracy comparison of different evaluated sequence-aware models for the detection of DDoS attacks. From the results, there is a clear hierarchy in the performance of the models. The Transformer model gets the highest accuracy which signifies its good ability to capture global dependencies in the traffic sequences based on self-attention-mechanisms. The BiLSTM model is not far behind and is an improvement on the regular LSTM because of its ability to learn context in both directions. The stability of the LSTM model is shown but a relatively lower accuracy indicating limitations in modelling complex and long-range attack patterns. The model developed with GRU has the worst record in terms of the evaluated approaches; however, it is still competitive while providing lower computational cost. Overall, the trend we observe in the graph underlines the fact that advanced sequence modeling (especially attention-based and bidirectional architectures) results in an improvement in DDoS detection capabilities in SDN environments.

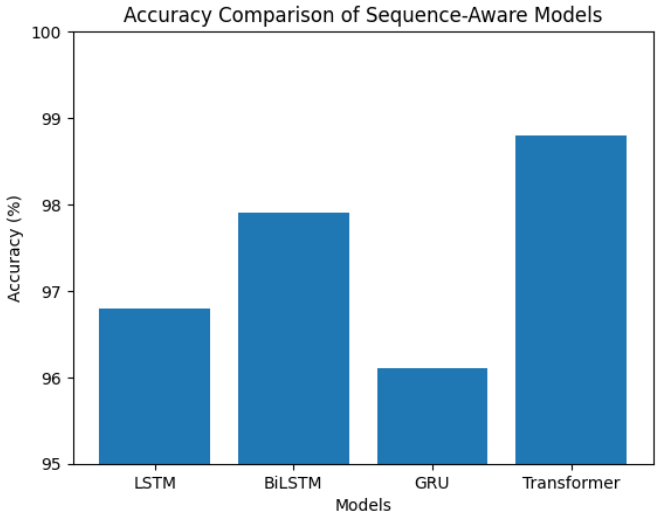

Fig.2. Accuracy comparison of sequence-aware models

B. *Detection Latency Analysis*

Detection latency is a critical factor in real-time deployment of intrusion detection systems in Software Defined Network in which delayed responses can severely affect the performance of the controllers and stability of the network. The models evaluated have noticeable variation of inference time because of their architectural characteristics. The GRU model achieves the lowest detection latency and it is mainly because of its simplified gating mechanism and fewer trainable parameters that lead to a low computational overhead during inference. Comparatively, the Transformer model has the highest latency due to self-attention operations that involve the pairwise comparison of the sequence elements and the resulting computation cost. The LSTM and BiLSTM models have moderate latency where BiLSTM has further overhead as it bidirectionally processes words. These results point towards a tradeoff between the accuracy to detect a payment and the efficiency of the computations. While attention-based models are more accurate, lightweight recurrent models such as GRU are more appropriate for latency-sensitive SDN environments where detecting and mitigating DDoS attacks is required and within a short amount of time. As shown in Fig.3.

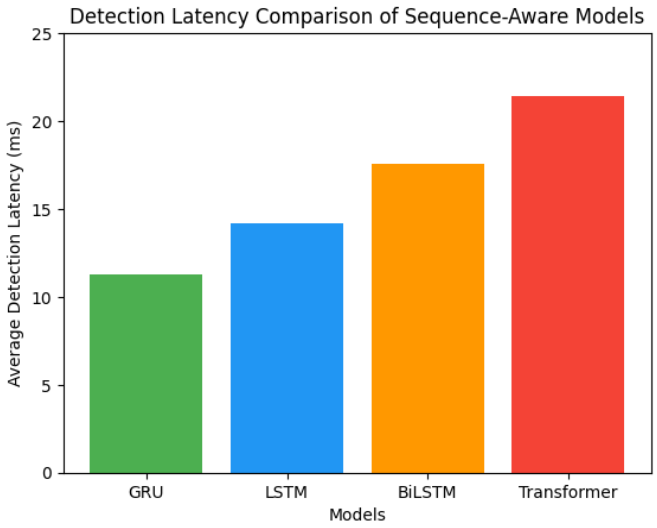

Fig.3. Confusion Matrix Analysis

C. *ROC–AUC Performance Comparison*

Figure X shows the rocauc performance of some sequence-aware models evaluated for the DDoS attack detection. The Transformer model has the highest ROC - AUC value which shows better discriminative ability to identify benign and DDoS traffic with varying false positive rates. This performance can be explained by its self-attention mechanism, which has a good ability to capture global dependencies within traffic sequences. The BiLSTM model has the second highest ROC--AUC, which is beneficial for bidirectional learning of time to give context to the learning of traffic patterns. In comparison, the models the LSTM and GRU models have relatively low ROC--AUC values, which reflects the inability of the LSTM and GRU models to model long-range dependencies and complex attack behaviors. Overall in the ROC analysis, we confirm that attention-based architectures and bidirectional sequence aware architectures provide much stronger and more reliable detection performance in SDN environments, especially in imbalanced and evolving conditions.

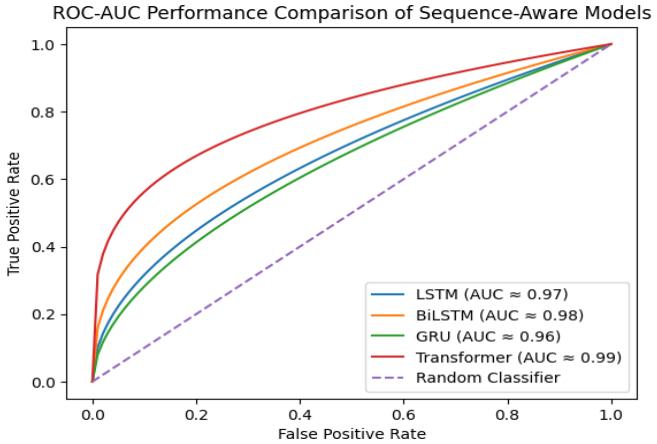

Fig.4. ROC–AUC comparison of sequence-aware models.

D. *Comparative Summary and Key Findings*

The comparative evaluation of sequence aware models shows that temporal and contextual learning plays an important role in increasing DDoS attack detection in Software Defined Networks. Among the evaluated approaches the Transformer model results in the best overall performance (the highest accuracy, F1-score, and ROC-AUC) which indicates how skilled attention-based global dependency modelling is. The BiLSTM model offers excellent trade off between the detection performance and the calculation time by utilizing the bidirectional temporal context, which is appropriate for actual SDN implementation. Whilst the LSTM model exhibits stable performance, it is not as good for learning complex traffic dynamics. The GRU Model with comparatively less accuracy provides the lowest detection latency, thus fitting with latency-sensitive, real-time SDN environments. Overall, the results suggest that when choosing the model with deployment requirements, model selection should focus on choosing the model with low model sizes while model selection should focus on operating on accuracy-sensitive use cases when?: Recurrent models will be preferred because of their lower model sizes, whereas deployment in real use cases concerning time-sensitive messages over time will favor lightweight recurrent models over those based on attention. As shown in table.2.

Table.2. Model-wise Performance Summary

Model	Accuracy	Latency	Key Strength
LSTM	High	Medium	Stable baseline
BiLSTM	Very High	Medium	Best trade-off
GRU	High	Low	Real-time SDN
Transformer	Highest	High	Best accuracy

Conclusions

This paper introduced a comparative analysis of the performance of sequence-aware NLP models for detecting DDoS attacks in Software Defined Networks (SDN) with the help of the CICDDoS2019 dataset. By simulating network traffic as temporal sequences, the study tested the efficacies of LSTM, BiLSTM, GRU and Transformer architectures using standard performance measures such as accuracy, the precision, recall, F1-score, ROC-AUC and the time it takes to detect the examined network traffic. Experimental results revealed that all evaluation models had a high detection accuracy ranging from 96.1% to 98.8%. The Transformer model showed the highest overall performance with an accuracy of 98.8%, F1-score is 98.3% and a ROC-AUC of 0.991 that showed a higher discriminative power. The BiLSTM model with an accuracy of 97.9% provides good performance of detection results and computational efficiency. The GRU model although showing slightly poor accuracy (96.1%) offered the least detection latency and is suitable for use in real-time SDN deployments. These results validate the effectiveness of sequence-aware modeling that is considerably capable of detecting DDoS attacks in SDN environments. Future work will focus on investigating lightweight attention mechanisms, online learning, and real-time mitigation strategies to further enhance scalability and adaptability in dynamic network environments.

References

1. Sharafaldin, I., Lashkari, A.H. and Ghorbani, A.A., 2018. Toward generating a new intrusion detection dataset and intrusion traffic characterization. ICISSp, 1(2018), pp.108-116.
2. Ferrag, M.A., Maglaras, L., Moschoyiannis, S. and Janicke, H., 2020. Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study. Journal of Information Security and Applications, 50, p.102419.
3. Tang, T.A., Mhamdi, L., McLernon, D., Zaidi, S.A.R. and Ghogho, M., 2018, June. Deep recurrent neural network for intrusion detection in sdn-based networks. In 2018 4th IEEE Conference on network softwarization and workshops (NetSoft) (pp. 202-206). IEEE.
4. Kim, G., Lee, S. and Kim, S., 2014. A novel hybrid intrusion detection method integrating anomaly detection with misuse detection. Expert Systems with Applications, 41(4), pp.1690-1700.
5. Yang, Y., Zheng, K., Wu, B., Yang, Y. and Wang, X., 2020. Network intrusion detection based on supervised adversarial variational auto-encoder with regularization. IEEE access, 8, pp.42169-42184.
6. Lopez-Martin, M., Carro, B., Sanchez-Esguevillas, A. and Lloret, J., 2017. Network traffic classifier with convolutional and recurrent neural networks for Internet of Things. IEEE access, 5, pp.18042-18050.
7. Roy, S.S., Mallik, A., Gulati, R., Obaidat, M.S. and Krishna, P.V., 2017, January. A deep learning based artificial neural network approach for intrusion detection. In International conference on mathematics and computing (pp. 44-53). Singapore: Springer Singapore.
8. Khan, M.A., Karim, M.R. and Kim, Y., 2019. A scalable and hybrid intrusion detection system based on the convolutional-LSTM network. Symmetry, 11(4), p.583.
9. Ferrag, M.A., Shu, L., Djallel, H. and Choo, K.K.R., 2021. Deep learning-based intrusion detection for distributed denial of service attack in agriculture 4.0. Electronics, 10(11), p.1257.
10. Niyaz, Q., Sun, W. and Javaid, A.Y., 2016. A deep learning based DDoS detection system in software-defined networking (SDN). arXiv preprint arXiv:1611.07400.
11. Vinayakumar, R., Alazab, M., Soman, K.P., Poornachandran, P., Al-Nemrat, A. and Venkatraman, S., 2019. Deep learning approach for intelligent intrusion detection system. IEEE access, 7, pp.41525-41550.
12. Javaid, A., Niyaz, Q., Sun, W. and Alam, M., 2016, May. A deep learning approach for network intrusion detection system. In Proceedings of the 9th EAI International Conference on Bio-inspired Information and Communications Technologies (formerly BIONETICS) (pp. 21-26).