Enhancing DDOS Attack Detection In SDN Environments Using GRU

Mr.G.Dhanapaty[1], Mohamed Dhowfiq.A[2], Pretheshwaran.S[3], Malik Basha.A[4]
[1]Assistant Professor, Dept of Information Technology
[2, 3, 4]Dept of Information Technology
[1, 2 , 3, 4]RAAK College of Engineering and Technology

Abstract- *Distributed Denial of Service (DDOS) attacks continue to pose a serious threat to Internet security, aiming to render specific systems or networks inaccessible. Detecting diverse types of DDOS cyber attackss with improved algorithms while managing computational costs is critical for bolstering cyber security. DDOS attacks, originating from various distributed sources across multiple network locations, exploit vulnerabilities to degrade performance, exhaust resources, or monopolize networks, impeding legitimate users. This paper introduces a novel DDOS attack detection system in SDN environments employing a Deep Learning(DL) approach with a focus on the recently released CICDDoS2019 dataset. Our proposed model, leveraging the Gated Recurrent Unit (GRU) algorithm, demonstrates significant improvements in attack detection compared to bench marking methods, enhancing confidence in securing SDN networks against evolving DDOS attackss.*

Keywords- Gated Recurrent Unit (GRU) algorithm, Distributed Denial of Service (DDOS).

I. INTRODUCTION

1.1 SOFTWARE DEFINED NETWORKING(SDN)

Software-Defined Networking (SDN) introduces a transformative approach to network management, enhancing reliability by centralizing control through the separation of the control and data planes. However, this paradigm is susceptible to various security vulnerabilities and novel faults that malicious actors can exploit. Unlike traditional networks, SDN vulnerabilities can impact the entire system, involving devices from different vendors. One particularly menacing threat is Distributed Denial of Service (DDOS) attacks, which, in the era of the Internet of Things (IoT), can leverage numerous devices to flood the network with traffic, making detection challenging. In response to the escalating complexity of cyber security attacks, the adoption of Artificial Neural Networks (ANNs) emerges as a trend for more effective threat detection. ANNs offer resilience to attack pattern variations and do not rely on predefined thresholds, although their training for zero-day vulnerabilities poses challenges. Additionally, the study proposes a new taxonomy for DDOS attacks, specifically focusing on TCP/UDP-based protocols at the application layer, addressing a need for updated categorizations in this evolving security landscape.

1.2 EXPLOITATION-BASED ATTACKS

Are those kinds of attacks in which the dentity of the attacker remains hidden by utilizing legitimate third- party component. The packets are sent to reflector servers by attackers with the source IP address set to the target victim's IP address to overwhelm the victim with response packets. These attacks can also be carried out through application layer protocols using transport layer protocols i.e., TCP and UDP. TCP based exploitation attacks include SYN flood and UDP based attacks include UDP flood and UDP- Lag. UDP flood attack is initiated on the remote host by sending a large number of UDP packets.

1.3 PROBLEM DEFINITION

The classification process, integral to many applications, faces challenges due to the significant computational demands of commonly employed methods. These approaches are often computationally intensive, requiring substantial processing power and memory space, impacting both speed and user-friendliness. The complexity of installation and maintenance further hinders seamless integration, creating barriers for users with limited computational resources or expertise. Existing classification methods struggle to deliver optimal performance, limiting their effectiveness in real- world applications. Overcoming these challenges is crucial for enhancing usability and efficiency. Streamlining computational requirements, improving user-friendliness, simplifying installation and maintenance, and incorporating robust optimization mechanisms are essential steps to make classification techniques more accessible, adaptable, and effective across diverse applications and user scenarios.

II. LITRATURE SURVEY

A Flexible SDN-Based Architecture for Identifying and Mitigating Low-Rate DDoS Attacks Using Machine Learning. This paper addresses the persistent challenge of mitigating Low-Rate DDoS (LR-DDoS) attacks, especially in software-defined network (SDN) settings. The proposed solution introduces a flexible modular architecture designed for the identification and mitigation of LR-DDoS attacks. The intrusion detection system (IDS) is trained using six machine learning models and achieves a notable 95% detection rate, showcasing its effectiveness despite the inherent difficulty in detecting LR-DDoS attacks. The architecture's deployment involves the open network operating system (ONOS) controller running on Mininet, creating a simulated environment closely resembling real-world production networks. The testing topology reveals that the intrusion prevention detection system successfully mitigates all previously detected attacks, highlighting the practical utility of the proposed architecture in addressing LR-DDoS threats. The modular and flexible design of the architecture enables easy replacement of individual modules without affecting the overall functionality, enhancing adaptability and scalability in SDN environments.[1] ***Cochain-SC: An Intra- and Inter-Domain Ddos Mitigation Scheme Based on Blockchain Using SDN and Smart Contract.*** In response to the escalating impact of Distributed Denial-of-Service (DDoS) attacks, this paper introduces Cochain-SC, a novel blockchain- based approach for cost-effective and flexible DDoS mitigation. Operating at both intra-domain and inter- domain levels, the proposed scheme leverages software- defined networks (SDN) and smart contracts on the Ethereum blockchain. Intra-domain mitigation employs entropy-based and Bayes-based schemes to identify and mitigate illegitimate flows within a domain. Inter- domain collaboration is facilitated through smart contracts, allowing multiple SDN-based domains to securely share attack information in a decentralized manner. Cochain-SC uniquely combines SDN, blockchain, and smart contract technologies to achieve efficient mitigation along the attack path and near the attack origin. The implementation is deployed on Ethereum's official test network Ropsten, marking a pioneering effort in addressing both intra- and inter-domain DDoS mitigation challenges in a unified framework.

[2] ***Hybrid ddos detection framework using matching pursuit algorithm*** In addressing the persistent threat of Distributed Denial-of-Service (DDoS) attacks, this study proposes a novel detection framework utilizing the Matching Pursuit algorithm, particularly focusing on resource depletion type DDoS attacks. The method concurrently considers multiple network traffic characteristics, enhancing efficiency in detecting low- density DDoS attacks. The approach employs a dictionary generated from network traffic parameters using the K-SVD algorithm, providing adaptable models for both legitimate and attack traffic. Comparative evaluations with Matching Pursuit and Wavelet techniques, along with the introduction of a hybrid detection framework incorporating artificial neural networks, showcase the proposed method's superior performance. Achieving over 99% true positive rates and a false positive rate below 0.7% in low-density DDoS attack datasets, the study introduces the AMP method, offering a unique approach to DDoS detection by utilizing the Matching Pursuit algorithm. The proposed methodology is compared with existing methods, demonstrating its effectiveness in the detection of DDoS attacks, especially in low-density scenarios where resource depletion is a significant concern.**[3]** ***DDoS Attack Detection Method Based on Improved KNN With the Degree of DDoS Attack in Software-Defined Networks.*** This paper explores the potential of Software Defined Networking (SDN) as a defense mechanism against Distributed Denial of Service (DDoS) attacks. Two methods are proposed for DDoS detection in SDN:

one utilizes the degree of DDoS attack, and the other employs an improved K-Nearest Neighbors (KNN) algorithm based on Machine Learning (ML). Theoretical analysis and experimental results on datasets demonstrate the effectiveness of these methods in comparison to other existing approaches. Recognizing DDoS as a significant threat in SDN networks, the paper introduces four features and a novel concept called the "degree of attack." Two detection algorithms, DDADA and DDAML, are presented and show superior detection rates in experiments compared to existing solutions. The authors acknowledge the anonymous reviewers for their valuable input and express plans to enhance and apply the proposed algorithms in real SDN environments in future work.[4]***Identifying Application-Layer DDoS Attacks Based on Request Rhythm Matrices*** This paper addresses the growing threat of Application-layer Distributed Denial of Service (AL-DDoS) attacks on websites, which often evade traditional intrusion prevention systems. A novel statistical model, the Rhythm Matrix (RM), is proposed to detect AL-DDoS attacks by abstracting and accumulating access trajectories, including requested objects and dwell-time values. The RM efficiently compresses complex features into a simple structure, characterizing user access behavior. Abnormality degrees in the RM are utilized to detect AL-DDoS attacks, and malicious hosts are identified based on change-rate outliers. Simulated attacks using popular DDoS tools demonstrate the method's accurate and efficient detection. The proposed approach also exhibits excellent performance in distinguishing flash crowds from AL-DDoS attacks, with a True Positive Rate (TPR) exceeding 99% and a False Positive Rate (FPR) below 1%. The precision and recall of identifying malicious hosts approach 100% with parameter optimization, and simulation attacks are detected well in

advance of their impact. Results on modified datasets further illustrate the method's strong performance in flash crowd scenarios.[5]

III. EXISTING SYSTEM

The existing system focuses on enhancing the detection and classification of Distributed Denial-of- Service (DDoS) attacks by incorporating time-based features in the analysis of network traffic flows. Unlike previous research, this study explores the effectiveness of 25 time-based features across 12 types of DDoS attacks using binary and multiclass classification. The findings reveal that a majority of the models achieve 99% accuracy in detecting DDoS attacks in both control and time-based experiments, while maintaining 70% accuracy in classifying specific attack types. The introduction of a smaller time-based feature subset not only reduces training time but also diminishes dimensionality and noise, thus optimizing computational resources. Notably, the study highlights that models like LD, LGBM, and XGB benefit significantly from training on time- based features, leading to reduced training times with minimal accuracy loss. However, Random Forest (RF) may not warrant training on time-based features due to its longer training time and comparatively lower accuracy. Additionally, the study emphasizes the practicality of continuous learning, promoting the viability of the proposed time-based feature subset for near-real-time applications in the dynamic landscape of cybersecurity.

IV. ISSUES IN THE SYSTEM

- Classification process consumes large amount of computational time.
- Computationally intensive and require relatively large memory space It is not an easy-to-use method.
- High complexity of installing and maintaining.
- Difficulties to obtain better performance.

V. PROPOSED SYSTEM

The utilization of the Gated Recurrent Unit (GRU) algorithm for predicting Distributed Denial of Service (DDoS) attacks signifies a sophisticated approach to enhancing cybersecurity. The GRU, a type of recurrent neural network (RNN), excels in capturing temporal dependencies and patterns in sequential data, making it well-suited for analyzing the time-series nature of network traffic data associated with DDoS attacks. Unlike traditional machine learning models, the GRU has the ability to retain and selectively update information over time, making it particularly effective in recognizing evolving patterns of cyber threats. By leveraging the GRU algorithm, cybersecurity systems can predict diverse types of DDoS attacks with improved accuracy. The algorithm's capacity to model sequential dependencies allows it to discern subtle variations in network behavior that may precede or characterize different types of attacks. This nuanced understanding enables early detection, providing security systems with the opportunity to implement timely countermeasures and mitigate the impact of potential threats. Moreover, the GRU algorithm contributes to managing computational costs, a crucial consideration in cybersecurity applications. Its architecture, characterized by a more streamlined structure compared to other recurrent networks like the Long Short-Term Memory (LSTM), allows for efficient training and prediction without compromising on accuracy. This efficiency is particularly beneficial in real-time or near-real-time cybersecurity scenarios where swift responses are essential.

VI. ADVANTAGE OF THE PROPOSED SYSTEM

The proposed system brings several notable advantages to the field of cybersecurity. By integrating a time-based feature subset and utilizing machine learning classifiers, the system significantly improves the detection and classification of Distributed Denial of Service (DDoS) attacks. This approach not only achieves high accuracy in identifying attacks but also demonstrates a reduction in overall training time, enhancing efficiency for real- time applications. The smaller time-based feature set decreases dimensionality and noise, promoting continuous learning and adaptability to evolving cyber threats. Additionally, the careful selection of machine learning models optimizes computational resources, ensuring a balanced trade-off between accuracy and efficiency in the critical task of strengthening cybersecurity.

VII. ARCHITECTURE DIAGRAM

An architectural diagram is a visual representation that maps out the physical implementation for components of a software system. It shows the general structure of the software system and the associations, limitations, and boundaries between each element.

Fig 6.1 Architecture Diagram

- **DATA PREPROCESSING**
- **FEATURE EXTRACTION**
- **MODEL TRAINING**
- **EVALUATION**
- **ANALYZE AND PREDICTION MODULE**

DATA PREPROCESSING

In the process of data preprocessing, several crucial steps were undertaken to ensure the quality and relevance of the dataset for subsequent experimental operations. Initially, the dataset was inspected for null and infinite values. To address this, null values were replaced with the average, and infinite values were substituted with the maximum values, mitigating potential disruptions in the data. Subsequently, any remaining non-numerical null values were identified and removed from the dataset, leveraging the substantial number of available records. Encoding categorical columns was deemed essential to convert nonnumerical values into numerical counterparts, facilitating the dataset's compatibility with experimental operations. Another critical step involved the removal of columns exhibiting zero variance. A variance or standard deviation of zero indicates that all values within a particular column are identical, rendering that feature devoid of any impact on the final results. This removal process contributes to streamlining the dataset and enhancing the efficiency of subsequent analyses.

FEATURE EXTRACTION

Feature selection is used to reduce the number of variables and obtain a simpler model. It is an important preprocessing step in a number of machine learning applications. It employs a two- step process to extract numerical or categorical information (features) of the traffic observed, i.e., packet grouping and statistics computation. The former involves aggregating into flows packets generated between same pairs of applications, which can be achieved by monitoring origin, destination, and protocol fields. To address the difference between continuous and discrete features, we propose a novel forward search algorithm that combines correlation and mutual information to select the optimal features. Concretely, we use the linear correlation coefficient to measure the redundancy between a new feature and the existing feature subset. And we use mutual information to measure the relevance of the new feature to the target variable. The final feature score is calculated based on a weighted difference between the relevance and redundancy of the feature.

MODEL TRAINING

We divided the dataset into three segments: training, validation, and testing subsets. The model was constructed using the training set to adjust neural network weights. The validation set fine-tuned experimental parameters, such as classifier architecture (excluding weights), and the test set evaluated the model's accuracy or performance. This paper opted for the train-test split technique over the k-fold cross-validation method due to the unsuitability of the latter for time series data with inherent serial correlation. The convolution layer (CONV) manages data from a receiver cell, with hyperparameters like depth, stride, and zero-padding shaping the layer. The pooling layer (POOL) compresses information to reduce the intermediate image size, operating independently on each feature map. The rectified linear unit (ReLU) serves as the activation function in the correction layer. Transitioning to the Gated Recurrent Unit (GRU) architecture will enhance the model's ability to capture temporal dependencies in time series data.

EVALUATION

We focus on the following important performance indicators: false alarm rate (FAr), precision, F- score, detection rate (Dr), recall, True Negative rate (TNr), False Accept rate (FAr), rOC Curve, and accuracy. We use the receiver Operating Characteristic (rOC) curve to evaluate how well the model performs accurately. The rOC curve indicates the relation between two parameters: True and False classes. The area underneath the rOC Curve (AUC) measures separability between false positive and true positive rate. We also use various metrics to evaluate our proposed model, such as precision, recall, precision, F-score and accuracy, in order to have a systematic benchmarking analysis with other related approaches.

PERFORMANCE ANALYSIS

Once the dataset has been preprocessed and a machine learning model has been trained, you can evaluate its performance using various metrics depending on the nature of your task (classification, regression, etc.). Common performance metrics include:

Precision: The number of true positive predictions divided by the total number of positive predictions, indicating the model's ability to avoid false positives.

$$\text{Precision} = \frac{\text{TP}}{\text{TP} + \text{FP}},$$

Recall (Sensitivity): The number of true positive predictions divided by the total number of actual positives, demonstrating the model's ability to capture all positive instances.

$$\text{Recall} = \frac{\text{TP}}{\text{TP} + \text{FN}},$$

F1 Score: The harmonic mean of precision and recall, providing a balanced measure between the two.

$$C_{ij} = L_{ij}^{cls} + \lambda L_{ij}^{reg}.$$

$$\mathcal{L}_{\text{IoU}} = 1 - \text{IoU}^2.$$

Area Under the Receiver Operating Characteristic curve (AUC-ROC): Particularly useful for binary classification problems, this metric assesses the model's ability to discriminate between positive and negative instances.

VIII. CONCLUSION AND FUTURE WORK

The hybrid algorithm, integrating Gated Recurrent Units (GRU) for DDoS attack detection, proves to be a highly promising and effective strategy. This approach leverages the strengths of GRU, enabling the model to proficiently capture both sequential and temporal patterns in network traffic data. The hybrid algorithm outperforms conventional methods, demonstrating superior accuracy and efficiency in distinguishing between normal and malicious activities. Its recurrent and memory-preserving capabilities contribute to heightened adaptability to the dynamic nature of DDoS threats. Continuous research efforts are crucial for refining the hybrid algorithm to address emerging attack patterns. The integration of real-time monitoring and adaptive learning mechanisms further enhances its value as a resilient solution for fortifying network infrastructures against evolving cybersecurity threats. To enhance the effectiveness of the hybrid algorithm in countering evolving cybersecurity threats, further research is crucial. Investigating the integration of advanced real-time monitoring techniques and adaptive learning mechanisms will contribute to ongoing improvements in the model's responsiveness. Attention should also be given to scalability, ensuring the algorithm remains efficient in handling large- scale network environments. Collaboration with cybersecurity experts and industry practitioners is essential for gaining practical insights and validating the hybrid model in diverse network settings. The focus of future endeavors should be on advancing the algorithm's robustness, scalability, and real-world applicability, fortifying network infrastructures against the dynamic landscape of DDoS attacks.

REFERENCES

[1] T. Wang, Y. Feng, and K. Sakurai, “Improving the two-stage detection of cyberattacks in SDN environment using dynamic thresholding,” in *2021 15th International Conference on Ubiquitous Information Management and Communication (IMCOM)*, pp. 1–7, Seoul, Korea (South), January 2021. View at: Publisher Site | Google Scholar

[2] T. Omar, A. Ho, and B. Urbina, “Detection of DDoS in SDN environment using entropy-based detection,” in *2019 IEEE International Symposium on Technologies for Homeland Security (HST)*, Woburn, MA, USA, November 2019. View at: Publisher Site | Google Scholar

[3] R. Wang, Z. Jia, and L. Ju, “An entropy-based distributed DDoS detection mechanism in software- defined networking,” in *2015 IEEE Trustcom/BigDataSE/ISPA*, Helsinki, Finland, August 2015. View at: Publisher Site | Google Scholar

[4] L. Fawcett, S. Scott-Hayward, M. Broadbent, A. Wright, and N. Race, “Tennison: a distributed SDN framework for scalable network security,” *IEEE Journal on Selected Areas in Communications*, vol. 36, no. 12, pp. 2805–2818, 2018. View at: Publisher Site | Google Scholar

[5] H. D. Zubaydi, M. Anbar, and C. Y. Wey, “Review on detection techniques against DDoS attacks on a software-defined networking controller,” in *2017 Palestinian International Conference on Information and Communication Technology (PICICT)*, pp. 10– 16, Gaza, Palestine, May 2017. View at: Publisher Site | Google Scholar

[6] N. Ahuja and G. Singal, "DDoS attack detection & prevention in SDN using OpenFlow statistics," in *2019 IEEE 9th International Conference on Advanced Computing (IACC)*, pp. 147–152, Tiruchirappalli, India, December 2019. View at: Publisher Site | Google Scholar

[7] J. Pei, Y. Chen, and W. Ji, "A DDoS attack detection method based on machine learning," *Journal of Physics: Conference Series*, vol. 1237, no. 3, article 032040, 2019. View at: Publisher Site | Google Scholar

[8] M. Mittal, K. Kumar, and S. Behal, "Deep learning approaches for detecting DDoS attacks: a systematic review," *Soft Computing*, pp. 1–37, 2022. View at: Publisher Site | Google Scholar

[9] S. M. Mousavi and M. St-Hilaire, "Early detection of DDoS attacks against SDN controllers," in *2015 International Conference on Computing, Networking and Communications (ICNC)*, pp. 77–81, Garden Grove, CA, USA, February 2015. View at: Publisher Site | Google Scholar

[10] J. Wang, G. Shou, Y. Hu, and Z. Guo, "A multi- domain SDN scalability architecture implementation based on the coordinate controller," in *2016 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC)*, pp. 494–499, Chengdu, China, October 2016. View at: Publisher Site | Google Scholar