Deep Learning Assisted Framework for Intelligent DDoS Detection and Network Defense in IoT

THOUDA YASHWANTH[1], Dr.S.SWATHI RAO[2]
[1]Student, Department of Computer Science and Engineering, Ellenki College of Engineering and Technology, Patelguda, Patancharu, Hyderabad, Telangana.
[2]Assistant Professor, Department of AI & ML, Ellenki College of Engineering and Technology, Patelguda, Patancharu, Hyderabad, Telangana.
[2]Email: swathirao1511@gmail.com

***Abstract*—** The rapid growth of Internet of Things (IoT) networks has increased the exposure of connected devices to distributed denial-of-service (DDoS) attacks, leading to service disruption, unauthorized access, and network instability. This paper presents an intelligent DDoS attack detection and mitigation framework that combines machine learning and deep learning techniques to identify malicious network traffic with high reliability. The proposed approach employs the IoT-23 benchmark dataset for model development, where data preprocessing includes feature encoding, missing value handling, normalization, and train–test partitioning to improve model effectiveness. XGBoost and Convolutional Neural Network (CNN) models are trained and evaluated using accuracy, precision, recall, F1-score, and confusion matrix analysis to assess classification performance across multiple attack categories. A web-based Flask application is integrated with the trained models to enable real-time analysis of incoming IoT traffic. Once malicious activity is detected, the corresponding source IP address is automatically marked for blocking, providing an additional mitigation mechanism to reduce repeated attacks. Experimental evaluation demonstrates that the CNN model achieves superior detection performance with approximately 98% accuracy, while XGBoost attains around **95% accuracy**, indicating the effectiveness of the proposed hybrid intelligent framework for securing IoT environments. The developed system offers a scalable and practical solution for automated attack detection and timely mitigation in modern IoT networks.

***Keywords*—** Internet of Things (IoT), Distributed Denial-of-Service (DDoS), IoT-23 dataset, XGBoost, Convolutional Neural Network (CNN), machine learning, deep learning, intrusion detection, network traffic analysis, cybersecurity, attack detection, attack mitigation, Flask web application, firewall-based IP blocking, intelligent network security.

INTRODUCTION

The widespread adoption of the Internet of Things (IoT) has revolutionized modern communication by enabling interconnected devices to exchange data across diverse application domains such as smart homes, healthcare, industrial automation, and intelligent transportation. Although IoT technology offers significant advantages in terms of automation and remote monitoring, its dependence on internet connectivity makes connected devices vulnerable to a wide range of cyber threats. Among these threats, Distributed Denial-of-Service (DDoS) attacks are particularly harmful because they overwhelm network resources, interrupt normal services, and reduce the reliability of IoT environments. Since many IoT devices possess limited computational power and memory, deploying conventional security mechanisms on these devices is often impractical. Consequently, there is an increasing need for lightweight and intelligent security solutions capable of detecting malicious activities accurately while maintaining low computational overhead **[12], [18]**.

Recent advances in machine learning and deep learning have provided effective approaches for identifying network intrusions by learning patterns from historical traffic data. Unlike traditional rule-based intrusion detection systems, data-driven models can recognize both known and previously unseen attack behaviors with higher detection accuracy. Algorithms such as Extreme Gradient Boosting (XGBoost) efficiently classify network traffic using engineered features, whereas Convolutional Neural Networks (CNNs) automatically learn complex feature representations from processed data. Combined with appropriate preprocessing techniques including categorical feature encoding, missing value handling, normalization, and data partitioning, these models provide reliable classification performance across multiple categories of IoT network attacks. The availability of benchmark datasets such as IoT-23 further supports the development and evaluation of intelligent intrusion detection systems **[10], [11], [15]**.

This work presents a web-based framework for intelligent DDoS attack detection and mitigation in IoT networks by integrating XGBoost and CNN-based classification models. The proposed system preprocesses IoT traffic records, trains both machine learning and deep learning models, and evaluates their performance using standard metrics including accuracy, precision, recall, F1-score, and confusion matrix analysis. A Flask-based application is incorporated to enable real-time detection of malicious traffic by allowing users to upload network data for analysis. Once an attack is identified, the corresponding source IP address is automatically flagged and blocked to prevent further unauthorized access. Experimental results demonstrate that the proposed framework achieves high detection accuracy while providing an efficient and scalable solution for enhancing the security of IoT-based communication environments **[7], [11], [15], [18], [20]**.

I. RELATED WORK

Y. Cao, Y. Deng, and J. Wu (2022) proposed **"Detecting and Mitigating DDoS Attacks in SDN Using Spatial-Temporal Graph Convolutional Network"** [7]. The authors introduced a graph convolutional network that captures both spatial and temporal characteristics of network traffic to improve the identification of distributed denial-of-service attacks in software-defined networks. By analyzing the relationships among traffic flows over time, the proposed model achieved better detection capability than conventional learning methods. The study also incorporated an effective mitigation strategy to reduce the impact of malicious traffic on network resources. Experimental evaluation demonstrated that the framework provided reliable detection performance while supporting secure and stable SDN operations. **[7]**

S. Kiranyaz, O. Avci, and O. Abdeljaber (2021) presented **"1D Convolutional Neural Networks and Applications: A Survey"** [5]. The study provided a detailed overview of one-dimensional convolutional neural networks and their application in processing sequential and time-series data. The authors discussed the capability of 1D CNN models to learn meaningful features directly from raw input without requiring extensive manual feature engineering. The survey highlighted the effectiveness of these models in several application areas, including fault diagnosis, signal analysis, and cybersecurity. The findings demonstrated that 1D CNN architectures offer high accuracy and computational efficiency for pattern recognition tasks. **[5]**

M. Assis, L. Carvalho, and J. Loret (2021) proposed **"A GRU Deep Learning System Against Attacks in Software Defined Networks"** [6]. The authors developed a deep learning framework based on Gated Recurrent Units (GRU) to identify malicious activities within software-defined networks. The proposed model learned temporal dependencies from network traffic data, allowing it to distinguish between legitimate and malicious flows with improved accuracy. Performance analysis showed that the GRU-based approach effectively reduced false detections while maintaining consistent classification results under different network conditions. The work demonstrated the potential of recurrent neural networks for strengthening SDN security against evolving cyber threats. **[6]**

L. Zhang and J. Wang (2022) proposed **"A Hybrid Method of Entropy and SSAE-SVM Based DDoS Detection and Mitigation Mechanism in SDN"** [15]. The researchers combined entropy-based traffic analysis with a stacked sparse autoencoder and support vector machine to improve the detection of DDoS attacks in software-defined networks. The hybrid framework extracted representative traffic features before performing attack classification, thereby enhancing detection accuracy while reducing computational complexity. Experimental results confirmed that the proposed approach successfully differentiated malicious traffic from normal network behavior and supported timely mitigation of detected attacks. **[15]**

S. Gao, Z. Peng, and B. Xiao (2020) proposed **"Detection and Mitigation of DoS Attacks in Software Defined Networks"** [18]. The authors presented an integrated framework that combines attack detection with mitigation mechanisms to protect software-defined networks from denial-of-service attacks. The proposed solution continuously monitored network traffic, identified abnormal flow patterns, and applied defensive measures to maintain network availability during attack scenarios. Experimental studies demonstrated that the framework effectively minimized the influence of malicious traffic while preserving normal network performance. The proposed approach provided a practical solution for enhancing the resilience and security of SDN infrastructures. **[18]**

II. DATASET DETAILS

The proposed DDoS attack detection framework is developed using the **IoT-23 dataset**, which contains network traffic collected from Internet of Things (IoT) devices operating under both normal and attack conditions. The dataset includes multiple

traffic attributes such as source and destination information, communication protocols, packet characteristics, and attack labels that represent different categories of network behavior. These records provide a comprehensive representation of real-world IoT communication patterns, enabling the learning models to distinguish legitimate traffic from malicious activities. Before model training, the dataset undergoes preprocessing steps including removal of missing values, categorical feature encoding, normalization, and random shuffling to ensure that the data is suitable for machine learning and deep learning algorithms. This preprocessing improves data consistency and enhances the reliability of the classification process.

The processed dataset is then divided into training and testing subsets using an 80:20 ratio to evaluate the performance of the proposed models. The training data is utilized to build both the XGBoost and Convolutional Neural Network (CNN) models, while the testing data is used to assess their ability to classify previously unseen network traffic. Model performance is measured using standard evaluation metrics such as accuracy, precision, recall, F1-score, and confusion matrix analysis. The dataset includes traffic generated from various attack scenarios, allowing the models to learn diverse malicious behavior patterns while maintaining accurate identification of normal network activity. This balanced evaluation process supports the development of a dependable intrusion detection framework capable of recognizing DDoS attacks under different network conditions.

The same dataset is further employed within the developed Flask-based web application for real-time attack detection and mitigation. Users can upload network traffic records through the web interface, after which the trained classification model analyzes each request and determines whether it represents normal communication or a potential DDoS attack. The application also extracts the source IP address associated with malicious traffic and automatically marks it for blocking to reduce repeated attacks from the same source. By integrating the IoT-23 dataset with machine learning, deep learning, and automated mitigation mechanisms, the proposed framework provides an efficient and scalable solution for protecting IoT networks against distributed denial-of-service attacks while supporting continuous monitoring of network security.

III. PROPOSED METHODOLOGY

The proposed framework presents an intelligent DDoS attack detection and mitigation system for Internet of Things (IoT) environments by combining machine learning and deep learning techniques with a web-based monitoring platform. The objective of the framework is to identify malicious network traffic accurately and respond promptly by preventing suspicious devices from accessing the IoT network. The system integrates data preprocessing, attack classification, performance evaluation, and automated mitigation within a unified architecture. A Flask-based web application provides an interactive interface through which users can upload network traffic data, perform attack analysis, and obtain detection results in real time. The framework also incorporates an automated IP-blocking mechanism that helps reduce the impact of repeated attacks by restricting malicious sources after successful detection.

The methodology begins with the preparation of the **IoT-23** dataset, which contains both normal and malicious network traffic generated from various IoT devices. Since the raw dataset contains categorical attributes and missing values, several preprocessing operations are performed before model training. These include label encoding to transform categorical features into numerical values, replacement of missing data, normalization of feature values, and random shuffling of records to improve data distribution. The processed dataset is then divided into training and testing subsets using an 80:20 ratio, ensuring that the learning models are evaluated on previously unseen network traffic. These preprocessing steps improve data quality and contribute to more reliable attack classification.

Following data preparation, two different learning models, namely **Extreme Gradient Boosting (XGBoost)** and **Convolutional Neural Network (CNN)**, are trained using the processed dataset. The XGBoost model performs supervised classification by constructing multiple decision trees to distinguish normal traffic from DDoS attacks, while the CNN model automatically extracts hierarchical feature representations to recognize complex attack patterns within network traffic. Both models are evaluated using standard performance measures including accuracy, precision, recall, F1-score, and confusion matrix analysis. The comparative evaluation enables the identification of the model that provides the best balance between detection accuracy and classification reliability for IoT network security.

The trained models are integrated into a Flask-based web application to support real-time DDoS attack detection and mitigation. Users upload network traffic files through the application interface, where each network request is analyzed using the trained classification model. The application classifies every record as either normal or malicious and extracts the corresponding source IP address for detected attacks. Once malicious traffic is identified, the system automatically initiates a mitigation process by blocking the associated IP address through firewall rules, preventing further unauthorized communication from the same source.

By combining efficient data preprocessing, intelligent classification, real-time traffic analysis, and automated mitigation within a single framework, the proposed methodology provides a scalable and practical solution for protecting IoT networks against distributed denial-of-service attacks while maintaining reliable network availability.

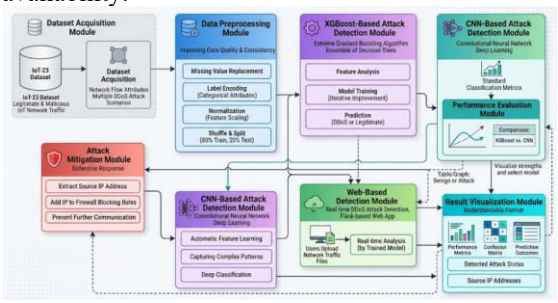


Figure 1: System Architecture of the Proposed IoT DDoS Attack Detection and Mitigation Framework

Figure 1 illustrates the architecture of the proposed IoT DDoS attack detection and mitigation framework. The process begins with the acquisition of the IoT-23 dataset, followed by data preprocessing, which includes missing value handling, label encoding, normalization, shuffling, and train–test splitting. The processed data is supplied to both XGBoost and Convolutional Neural Network (CNN) models for attack classification. Their performance is assessed using accuracy, precision, recall, F1-score, and confusion matrix analysis to determine the most effective detection model. The selected classifier is integrated into a Flask-based web application that performs real-time analysis of uploaded network traffic. When malicious activity is detected, the associated source IP address is automatically forwarded to the mitigation module for firewall blocking. Finally, the framework presents the detection outcome, blocked IP information, and model performance through graphical and tabular visualization, supporting efficient monitoring and protection of IoT networks.

V.RESULT AND DISCUSSION

The proposed IoT DDoS attack detection and mitigation framework was implemented to evaluate the effectiveness of machine learning and deep learning techniques in identifying malicious network traffic. The experimental study was carried out using the **IoT-23 dataset**, which contains both normal and attack traffic generated from IoT devices. Before model training, the dataset was preprocessed through label encoding, missing value replacement, normalization, and train–test splitting to improve the quality of the input data and ensure reliable model performance.

The developed framework integrates both **XGBoost** and **Convolutional Neural Network (CNN)** models with a Flask-based web application for real-time attack detection. Users can upload network traffic records through the application interface, where the trained model classifies each request as either normal or malicious. The application also extracts the corresponding source IP address and automatically initiates the mitigation process by blocking malicious IP addresses through firewall rules, thereby reducing the possibility of repeated attacks.

Experimental results indicate that both classification models successfully identify IoT network attacks with high accuracy. Performance evaluation using accuracy, precision, recall, F1-score, and confusion matrix analysis shows that the **CNN model achieves approximately 98% detection accuracy**, outperforming the **XGBoost model**, which achieves **approximately 95% accuracy**. The comparative analysis confirms that the proposed framework provides an efficient, scalable, and reliable solution for real-time DDoS attack detection and automated mitigation, thereby improving the security and resilience of IoT communication networks.

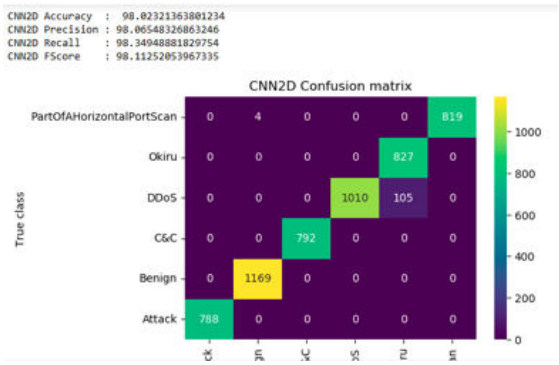
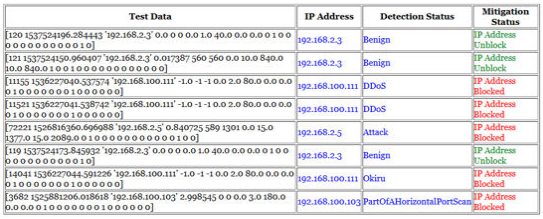


Figure 2: CNN2D Confusion Matrix

The above figure presents the **confusion matrix of the CNN2D model** used for classifying IoT network traffic into different categories, including **Attack, Benign, C&C, DDoS, Okiru,** and **PartOfAHorizontalPortScan**. The vertical axis represents the **actual class labels**, while the horizontal axis represents the **predicted class labels**. The diagonal elements indicate correctly classified instances, whereas the off-diagonal elements represent misclassified samples.

The performance metrics shown above the confusion matrix indicate that the CNN2D model achieved an **accuracy of 98.02%**, with a **precision of 98.07%**, **recall of 98.35%**, and an **F1-score of 98.11%**. Most samples are correctly classified along the diagonal, demonstrating the model's strong capability in distinguishing normal and malicious IoT network traffic. A small number of **DDoS** instances are misclassified as **Okiru**, indicating minor overlap between these attack patterns. Overall, the confusion matrix confirms that the proposed CNN2D model provides highly accurate and reliable detection of multiple IoT attack

categories, making it suitable for real-time DDoS attack detection and mitigation in IoT environments.



Test Data	IP Address	Detection Status	Mitigation Status
[120 1537524196.284443 '192.168.2.3' 0.0 0 0 0.0 1.0 40.0 0.0 0.0 0 1 0 0 0 0 0 0 0 0 0 0 0 0 1 0]	192.168.2.3	Benign	IP Address Unblock
[121 1537524150.960407 '192.168.2.3' 0.017387 560 560 0.0 10.0 840.0 10.0 840.0 1 0 0 1 0 0 0 0 0 0 0 0 0 0 0 0 0]	192.168.2.3	Benign	IP Address Unblock
[11155 1536227040.537574 '192.168.100.111' -1.0 -1 -1 0.0 2.0 80.0 0.0 0.0 0 1 0 0 0 0 0 0 1 0 0 0 0 0 0]	192.168.100.111	DDoS	IP Address Blocked
[11521 1536227041.538742 '192.168.100.111' -1.0 -1 -1 0.0 2.0 80.0 0.0 0.0 0 1 0 0 0 0 0 0 1 0 0 0 0 0 0]	192.168.100.111	DDoS	IP Address Blocked
[72221 1526816360.696988 '192.168.2.5' 0.840725 589 1301 0.0 15.0 1377.0 15.0 2089.0 0 1 0 0 0 0 0 0 0 0 0 0 0 0 1 0 0]	192.168.2.5	Attack	IP Address Blocked
[119 1537524173.845932 '192.168.2.3' 0.0 0 0 0 0.0 1.0 40.0 0.0 0.0 0 1 0 0 0 0 0 0 0 0 0 0 0 0 1 0]	192.168.2.3	Benign	IP Address Unblock
[14041 1536227044.591226 '192.168.100.111' -1.0 -1 -1 0.0 2.0 80.0 0.0 0.0 0 1 0 0 0 0 0 0 1 0 0 0 0 0 0]	192.168.100.111	Okiru	IP Address Blocked
[3682 1525881206.018618 '192.168.100.103' 2.998545 0 0 0.0 3.0 180.0 0.0 0.0 0 1 0 0 0 0 0 0 0 1 0 0 0 0 0 0]	192.168.100.103	PartOfAHorizontalPortScan	IP Address Blocked

Figure 3: Real-Time IoT DDoS Detection and Mitigation Results

The above figure illustrates the **real-time prediction results** generated by the proposed IoT DDoS attack detection and mitigation framework through the Flask-based web application. The first column displays the uploaded **network traffic records**, while the second column shows the corresponding **source IP addresses** from which the requests originated. The **Detection Status** column presents the classification outcome produced by the trained CNN model, identifying each network request as **Benign**, **Attack**, **DDoS**, **Okiru**, or **PartOfAHorizontalPortScan**. Based on the prediction result, the **Mitigation Status** column indicates the action performed by the system. Legitimate traffic is marked as **"IP Address Unblock"**, allowing normal communication to continue, whereas malicious traffic is labeled as **"IP Address Blocked"**, preventing further access from the identified source. The displayed results demonstrate that the proposed framework can accurately classify multiple categories of IoT network traffic and automatically initiate mitigation by blocking malicious IP addresses, thereby enhancing the security and reliability of IoT communication networks through real-time attack detection and response.

DISCUSSION

The proposed IoT DDoS attack detection and mitigation framework integrates **XGBoost** and **Convolutional Neural Network (CNN)** models to identify malicious network traffic and improve the security of Internet of Things (IoT) environments. The framework utilizes the **IoT-23 dataset**, which undergoes preprocessing through label encoding, missing value handling, normalization, and train–test partitioning to ensure reliable model learning. A Flask-based web application provides an interactive platform for uploading network traffic data, performing real-time attack analysis, and initiating automated mitigation. The system also incorporates an IP-blocking mechanism that prevents further communication from identified malicious sources, thereby strengthening network protection.

Experimental observations demonstrate that both learning models effectively distinguish normal network traffic from DDoS attacks using standard performance measures such as accuracy, precision, recall, F1-score, and confusion matrix analysis. Among the evaluated models, the **CNN** classifier achieves superior detection performance compared to **XGBoost**, providing higher classification accuracy while maintaining consistent prediction reliability. The integration of intelligent attack detection, real-time traffic monitoring, automated firewall-based mitigation, and result visualization offers a practical, scalable, and efficient solution for protecting IoT networks against distributed denial-of-service attacks and improving the overall resilience of connected systems.

VI.CONCLUSION

This work presents an intelligent framework for **IoT DDoS attack detection and mitigation** by integrating **Extreme Gradient Boosting (XGBoost)** and **Convolutional Neural Network (CNN)** models within a web-based security platform. The proposed framework performs network traffic preprocessing, attack classification, performance evaluation, and automated mitigation to enhance the security of IoT environments. A Flask-based application enables users to upload network traffic for real-time analysis, while the mitigation module automatically blocks malicious source IP addresses through firewall rules after successful attack detection. Experimental evaluation demonstrates that both models provide reliable detection performance, with the CNN model achieving higher classification accuracy than XGBoost. The proposed framework offers an efficient, scalable, and practical solution for protecting IoT networks against distributed denial-of-service attacks while supporting continuous network monitoring and rapid response to malicious activities. Future work may focus on extending the framework to detect additional categories of cyberattacks, incorporating transformer-based deep learning models for improved detection accuracy, integrating cloud-based deployment for large-scale IoT environments, and implementing adaptive threat intelligence mechanisms to enhance real-time network security and resilience.

REFERENCES

[1] V. Nguyen, A. Brunstrom, and K. Grinnemo, "SDN/NFV-Based Mobile Packet Core Network Architectures: A Survey," IEEE Communications Surveys & Tutorials, vol. 19, no. 3, pp. 1567–1602, 2017.

[2] V. Varadharajan, K. Karmakar, and U. Tupakula, "A Policy-Based Security Architecture for Software Defined Networks," IEEE Transactions on Information Forensics and Security, vol. 14, no. 4, pp. 897–912, 2019.

[3] P. Bera, A. Saha, and S. Setua, "Denial of Service Attack in Software Defined Network," in Proc. 5th Int. Conf. Computer Science and Network Technology (ICSNT), Changchun, China, Dec. 2016.

[4] Open Networking Foundation, OpenFlow Switch Specification Version 1.4.0, 2014. [Online]. Available: https://www.opennetworking.org/wp-content/uploads/2014/10/openflow-spec-v1.4.0.pdf. Accessed: Sept. 11, 2022.

[5] S. Kiranyaz, O. Avci, and O. Abdeljaber, "1D Convolutional Neural Networks and Applications: A Survey," Mechanical Systems and Signal Processing, vol. 151, Art. no. 107398, 2021.

[6] M. Assis, L. Carvalho, and J. Loret, "A GRU Deep Learning System Against Attacks in Software Defined Networks," Journal of Network and Computer Applications, vol. 177, Art. no. 102942, 2021.

[7] Y. Cao, Y. Deng, and J. Wu, "Detecting and Mitigating DDoS Attacks in SDN Using Spatial-Temporal Graph Convolutional Network," IEEE Transactions on Dependable and Secure Computing, vol. 19, no. 6, pp. 3855–3872, 2022.

[8] S. Agha and O. Rehman, "Improving Discrimination Accuracy Rate of DDoS Attacks and Flash Events," in Proc. Int. Conf. Cyber Warfare and Security (ICCWS), Islamabad, Pakistan, Oct. 2020.

[9] T. Nam, P. Phong, and T. Khoa, "Self-Organizing Map-Based Approaches in DDoS Flooding Detection Using SDN," in Proc. 32nd Int. Conf. Information Networking (ICOIN), Chiang Mai, Thailand, Jan. 2018.

[10] V. Deepa, K. Sudar, and P. Deepalakshmi, "Design of Ensemble Learning Methods for DDoS Detection in SDN Environment," in Proc. Int. Conf. Vision Towards Emerging Trends in Communication and Networking (ViTECoN), Vellore, India, Mar. 2019.

[11] C. Li, Y. Wu, and Z. Qian, "DDoS Attack Detection and Defense Based on Hybrid Deep Learning Model in SDN," Journal of Communications, vol. 39, pp. 176–187, 2018.

[12] Y. Cui, L. Yan, and S. Li, "SD-Anti-DDoS: Fast and Efficient DDoS Defense in Software-Defined Networks," Journal of Network and Computer Applications, vol. 68, pp. 65–79, 2016.

[13] X. Yang, B. Han, and Z. Sun, "SDN-Based DDoS Attack Detection with Cross-Plane Collaboration and Lightweight Flow Monitoring," in Proc. IEEE Global Communications Conference (GLOBECOM), Singapore, Dec. 2017.

[14] J. Cui, J. T. He, and Y. Xu, "TDDAD: Time-Based Detection and Defense Scheme Against DDoS Attack on SDN Controller," in Proc. 23rd Australasian Conf. Information Security and Privacy (ACISP), Wollongong, Australia, Jul. 2018.

[15] L. Zhang and J. Wang, "A Hybrid Method of Entropy and SSAE-SVM Based DDoS Detection and Mitigation Mechanism in SDN," Computers & Security, vol. 115, Art. no. 102604, 2022.

[16] S. Shin, V. Yegneswaran, and P. Porras, "AVANT-GUARD: Scalable and Vigilant Switch Flow Management in Software-Defined Networks," in Proc. ACM SIGSAC Conf. Computer and Communications Security (CCS), Berlin, Germany, Nov. 2013.

[17] H. Wang, X. Lei, and G. Gu, "FloodGuard: A DoS Attack Prevention Extension in Software-Defined Networks," in Proc. 45th IEEE/IFIP Int. Conf. Dependable Systems and Networks (DSN), Rio de Janeiro, Brazil, Jun. 2015.

[18] S. Gao, Z. Peng, and B. Xiao, "Detection and Mitigation of DoS Attacks in Software Defined Networks," IEEE/ACM Transactions on Networking, vol. 28, no. 3, pp. 1419–1433, 2020.

[19] R. Macedo, R. Castro, and A. Santos, "Self-Organized SDN Controller Cluster Conformations Against DDoS Attacks Effects," in Proc. IEEE Global Communications Conference (GLOBECOM), Washington, DC, USA, Dec. 2016.

[20] Y. Wang, T. Hu, and G. Tang, "SGS: Safe-Guard Scheme for Protecting Control Plane Against DDoS Attacks in Software-Defined Networking," IEEE Access, vol. 7, pp. 34699–34710, 2019.