Jurnal Elektro
p-ISSN: 1979-9780
e-ISSN: 2746-4288

Jurnal Elektro Vol. 19 No. 1 April 2026
journal homepage: https://ejournal.atmajaya.ac.id/index.php/JTE

Hierarchical SDN DDoS Detection in IoT Networks via Shannon Entropy and Adaptive Thresholding

Moh Febryan Dwi Cahyo, Diah Risqiwati*

Department of Electrical Engineering, Faculty of Engineering and Planning Ekasakti University, Padang 25115, INDONESIA

Article Info

Article history:

Received
26-06-2026

Accepted
29-07-2026

Keywords:
DDOS attack,
Internet of Think,
SDN,
Shannon Entropy

Abstract

Internet of Things (IoT) devices integrated with Software-Defined Networking (SDN) have increased network flexibility and centralized management. However, this architecture is increasingly vulnerable to volumetric Distributed Denial-of-Service (DDoS) attacks, which can degrade Quality of Service (QoS) and disrupt critical network services. Existing entropy-based detection approaches generally rely on flat SDN topologies and static thresholds, resulting in delayed attack isolation and increased false-positive rates during legitimate traffic surges. To address these limitations, this study proposes a lightweight DDoS detection and mitigation framework that combines Shannon Entropy with Adaptive Dynamic Thresholds in a hierarchical SDN architecture. The proposed system is implemented using Mininet, Open vSwitch, and Ryu Controller, and evaluated against UDP Flood, ICMP Flood, and TCP SYN Flood attacks. The hierarchical architecture enables mitigation at the Gateway layer, preventing malicious traffic from reaching the core network. Experimental results show that the proposed approach effectively recovers network performance after mitigation, increasing throughput from 0.09 Mbps during the attack to 6.36 Mbps while reducing packet loss from 100% to 0%. The classification performance achieves an overall accuracy of 91% with an AUC-ROC of 0.941, demonstrating strong capability in distinguishing malicious traffic from legitimate traffic. These results demonstrate that the proposed framework provides an effective and computationally efficient solution for securing SDN-based IoT networks against volumetric DDoS attacks while maintaining normal network performance.

1. INTRODUCTION

The exponential growth of resource constrained Internet of Things (IoT) devices has driven the adoption of Software Defined Networking (SDN) for centralized and efficient management [1], [2]. However, this integrated ecosystem remains highly vulnerable to volumetric Distributed Denial of Service (DDoS) attacks, such as UDP, ICMP, and TCP SYN floods, which rapidly exhaust network bandwidth and paralyze critical services[3] . [4]Furthermore, conventional detection systems relying on rigid static thresholds and flat SDN topologies often trigger false positives during legitimate traffic surges (Flash Crowds) and fail to isolate attacks early [5], [6], allowing malicious traffic to cause severe bottlenecks at the core network and server levels.[7], [8]

To address these limitations, the purpose of this study is to develop and evaluate a lightweight, adaptive DDoS detection and mitigation system using Shannon Entropy and Dynamic Threshold algorithms within a hierarchical SDN architecture [1], [6]. The scope of this research involves simulating a Three Tier SDN topology using Mininet and the Ryu Controller, where proactive attack blocking is delegated directly to the Gateway Switch to safeguard the core infrastructure. The system's effectiveness is strictly evaluated based on Quality of Service (QoS) recovery parameters—including throughput, delay, and packet loss against three main volumetric threat vectors. Finally, a Synthetic Minority Over sampling Technique (SMOTE) is applied to resolve dataset imbalance, ensuring a highly precise Confusion Matrix evaluation of the model's ability to isolate threats without disrupting legitimate IoT communications .

The novelty of this research lies in the integration of a hierarchical SDN architecture with a real-time Adaptive Dynamic Thresholding mechanism based on moving statistical mean and standard deviation. Unlike existing entropy-based methods that rely on rigid static thresholds and flat network topologies, this hierarchical approach distributes the detection workload to the edge layer (Gateway Layer). Consequently, this mechanism significantly improves computational efficiency, minimizes false-positive

*Corresponding author: Diah Risqiwati
Email address: risqiwati@umm.ac.id

rates during legitimate traffic surges (Flash Crowds), and proactively isolates malicious threats before malicious traffic impacts the core network infrastructure.

2. LITERATURE REVIEW

Internet of Things (IoT) devices integrated with Software Defined Networking (SDN) improve network management, but also expand the attack surface for volumetric Distributed Denial of Service (DDoS) attacks. Previous research has explored statistical algorithms for detecting traffic anomalies in SDN[6]. leverage Shannon Entropy on a flat SDN topology to measure the randomness of the originating IP distribution. However, this conventional static threshold-based method often triggers false alarms during legitimate traffic spikes (Flash Crowds) and fails to isolate attacks early. To address this weakness,[5], [9] proposed a variable entropy thresholding scheme, but the analysis is still concentrated on the Core Controller, thus creating a computational bottleneck in the centralized control layer.

To ensure the repeatability of the study, the new anomaly detection method in this study integrates Shannon Entropy in real-time. H(X) with the Adaptive Dynamic Thresholding algorithm[10], [11]. The lower threshold parameter T calculated dynamically using moving mean values (μ) and standard deviation (σ) from historical entropy $T=\mu-(K.\sigma)$ when $H(X) < T$, Ryu Controller proactively executes MAC/IP based blocking instructions with the OFPActionDrop rule.

3. METHODOLOGY

This research employs an experimental simulation approach using the Mininet network emulator to replicate a resource constrained Internet of Things (IoT) network ecosystem within a Software Defined Networking (SDN) framework. The data plane infrastructure is constructed using Open vSwitch (OVS) nodes supporting the OpenFlow 1.3 protocol, while the control plane is managed by a centralized Ryu SDN controller programmed in Python. These architectural components ensure a clean separation between the forwarding state and the centralized control logic[1].

This research method integrates real-time network monitoring and model classification evaluation in a single, systematic workflow. The flow begins in the Data Plane, where packet statistics are periodically extracted by the Ryu Controller using the Shannon Entropy algorithm to measure the randomness of the source IP address distribution. If the entropy value exceeds the Dynamic Threshold, the traffic is classified as a DDoS attack, and mitigation is immediately applied at the Gateway level. Next, all simulated traffic logs are collected as a dataset. Because the raw data is class-imbalanced, the SMOTE technique is applied specifically to the training data to balance the number of minority class (DDoS) samples without leaking the test data. Finally, the balanced dataset is evaluated using a Confusion Matrix to accurately measure the system's classification performance through Precision, Recall, F1-Score, and Accuracy metrics[4], [12]. which is injected specifically into the outermost Gateway Switch. This delegation of action isolates attack packets at the network entrance and prevents overloading of the Core Switch[13], [14].

3.1 Network topology

The proposed network design utilizes a hierarchical three-tier tree topology to logically separate layers and isolate malicious traffic anomalies. This architecture ensures a clean separation between the forwarding state and the [16]. The physical and logical structure of the simulated network environment is visually detailed in Fig 1:

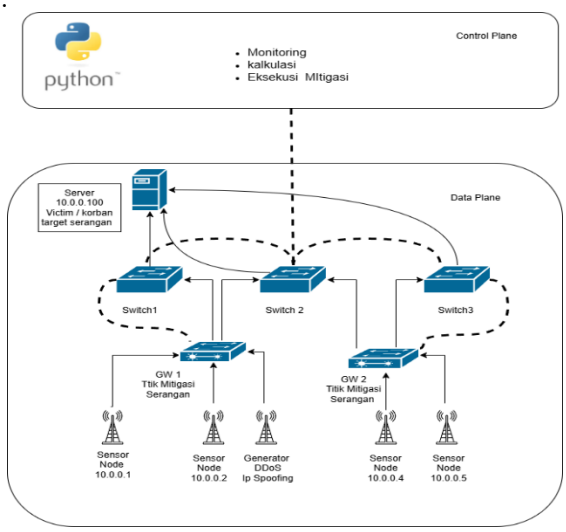

Figure 1. Hierarchical SDN IoT Network Topology the figure

As illustrated in Fig 1, the architecture is divided into two main operational planes: the Control Plane and the Data Plane. The Control Plane features a centralized Ryu SDN controller programmed in Python, which is responsible for traffic statistics monitoring, mitigation execution, and the calculation of Shannon Entropy and Dynamic Threshold boundaries. Beneath it, the Data Plane is organized into a hierarchical structure. The network backbone consists of three core switches (S1, S2, S3), while the edge layer is managed by two gateway switches (gw1, gw2). These gateway switches serve as the critical attack mitigation points, directly interfacing with the legitimate operational IoT sensor hosts (10.0.0.1, 10.0.0.2, 10.0.0.4, 10.0.0.5), the compromised DDoS generator host, and the target IoT server configured at the internet protocol address 10.0.0.100. This design enables proactive drop rules to be deployed at the network boundary, intercepting malicious traffic at the gateway before it impacts the core backbone [16].

3.2 DDoS Detection Framework

The anomaly detection mechanism relies on macroscopic traffic patterns. Flow statistical data are extracted periodically by the centralized controller through OpenFlow Packet In messages. To minimize computational overhead on the controller, the system measures the structural randomness of incoming packet distributions using the Shannon Entropy algorithm. The flow entropy H(X) within a specific observation time window is calculated as.

$$H(X) = -\sum_{i=1}^{n} P(xi)\ \log 2\, P(xi) \quad (1)$$

where $H, X,$ and P represent quantities and variable. The variable $P(xi)$ represents the probability of a specific source address xi appearing within the network. This probability is computed by dividing the individual packet count of a unique source address by the aggregate packet count arriving at the target server during the evaluation window.

To accurately differentiate between legitimate traffic spikes, such as flash crowds, and actual distributed denial of service (DDoS) attacks, an adaptive thresholding mechanism is developed[17]. The system continually monitors historical network behavior by calculating the moving statistical mean (μ) and standard deviation (σ) of the preceding entropy values. The mathematical formula for the historical mean is expressed as.

$$\mu = \frac{1}{n} \sum_{i=1}^{n} H_i \quad (2)$$

and the corresponding standard deviation is formulated as.

$$\sigma = \sqrt{\frac{1}{n}\ \sum_{i=1}^{n} (\ H_i - \ \mu\ )^2} \quad (3)$$

The symbol μ and σ represent constant statistical properties of the baseline traffic distribution. Based on the parameters derived from (2) and (3), the adaptive lower bound threshold T is mathematically defined as

$$T = \mu - (K.\sigma) \quad (4)$$

where K represents a configurable sensitivity constant. If real time monitoring indicates that the running entropy falls below the dynamic boundary, such that $H(X) < T$, the traffic flow is immediately classified as a volumetric DDoS attack.

3.2 Mitigation Strategy

During a positive attack classification via (4), the proactive mitigation module is executed. The controller constructs an OpenFlow flow modification message containing an *OFPActionDrop* command with the highest execution priority *(priority=1000)*. This packet drop rule is specifically configured based on the attacker's originating *MAC* and *IP addresses* with a time interval of *60 seconds*. To prevent the core backbone infrastructure from experiencing a buffer overflow, this drop rule is applied exclusively to the edge Gateway Switch associated with the attacker's ingress port. As a result, malicious packets are dropped immediately at the network boundary, isolating the threat while ensuring that legitimate data flows continue to reach the target destination server without experiencing packet loss or quality of service degradation.

4. RESULT AND DISCUSSION

4.1 Normal traffic characteristic

The system was first subjected to typical network operations to ensure that the integrated Shannon Entropy computation does not degrade legitimate communication channels. Under standard conditions,

legitimate Internet of Things (IoT) sensor nodes transmitted telemetry packets continuously to the central server. The Ryu Controller monitored a highly stable load fluctuating strictly between 40 and 55 packets per observation interval. Because the traffic distribution was evenly distributed across multiple valid source nodes, the computed entropy values remained well within the safe zone, allowing the controller to forward all data flows without inducing processing overhead or packet transmission delays. The operational steps and the system's traffic monitoring patterns under baseline configurations are visually captured in Fig. 2.

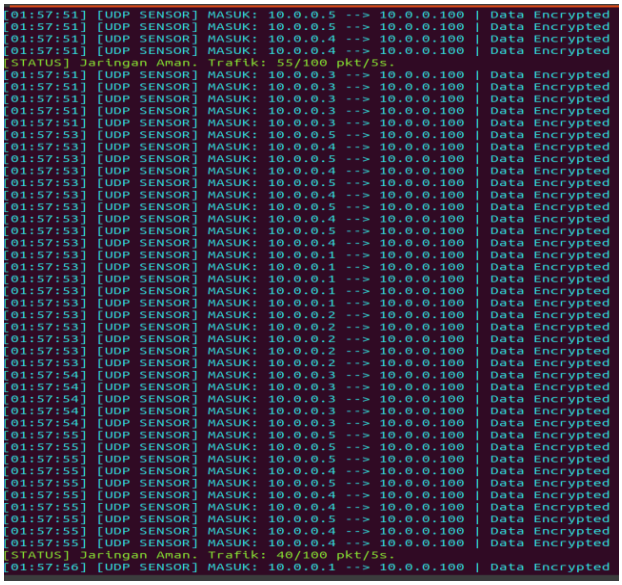

Figure 2. Traffic Monitoring Under Routine Normal Conditions

A sudden traffic burst was introduced to simulate an emergency event, i.e., a flash crowd. During this scenario, a legitimate operational host initiated an intensive transmission of high priority alert packets, causing the local load to rise rapidly to 143 packets per interval. Although the total volume expanded significantly, the overall entropy remained above the adaptive boundary because the remaining sensor nodes maintained a diverse distribution of source addresses. The dynamic threshold module successfully updated its limits to prevent a false positive classification, thereby guaranteeing that the target server successfully processed the emergency traffic alongside routine monitoring streams. The adaptive adjustments of the detection boundary during real time legitimate flash crowd events are depicted in Fig. 3

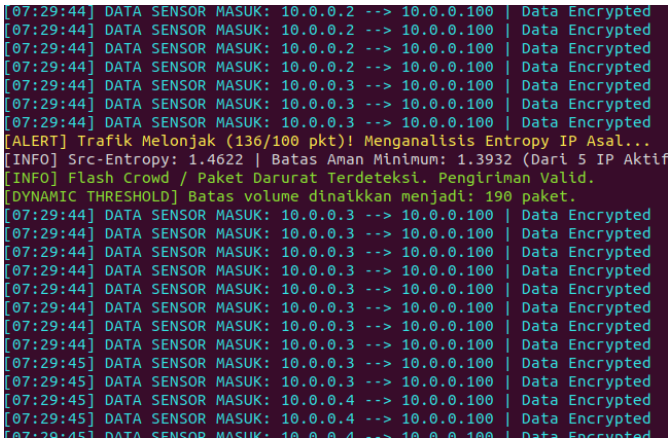

Figure 3. Monitoring of Flash Crowd

4.2 DDoS Detection and Mitigation

Based on the logs in Fig 4, the UDP Flood attack (hping3 --udp --flood) triggered a drastic traffic of up to 27,173 packets (5434.6 pps). This single packet concentration decreased the Shannon Entropy value to 12.4334. The Layer 2 system automatically confirmed this anomaly as a Spoofed Attack and executed the [BLOCK-MAC] rule on the attacker's IP (10.0.0.3) for 60 seconds on the Gateway Switch. After mitigation at 21:29:21, the attack traffic was completely interrupted and the legitimate sensor data flow ([UDP SENSOR]) returned to normal.

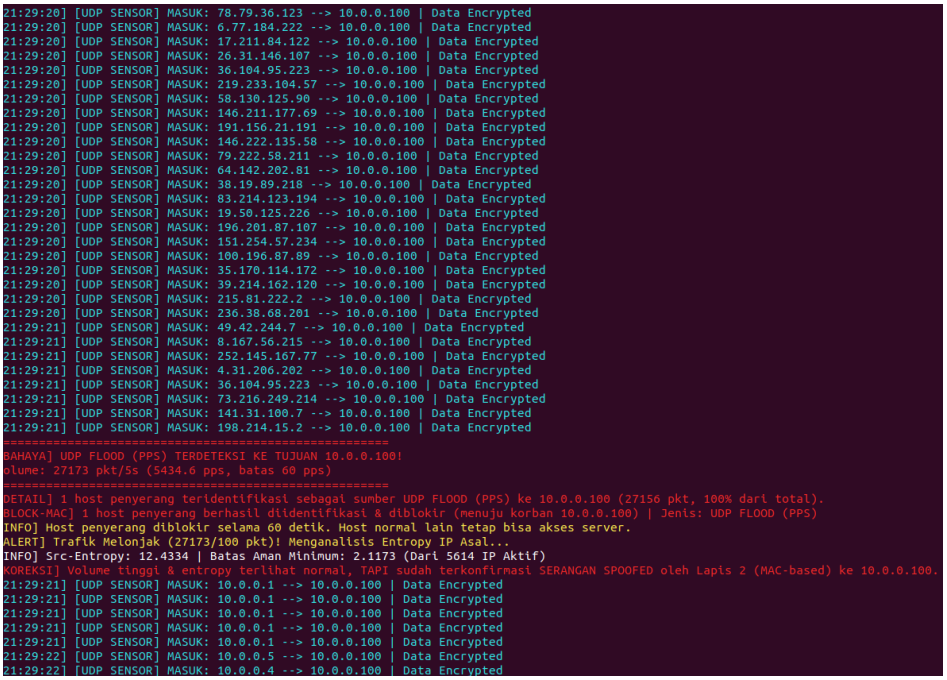

Figure 4. Statistical Detection and Mitigative Blocking of UDP Flood Attack

In the ICMP Flood test (hping3 -1 --flood) in Fig 5, the server was bombarded with [ICMP PING] packets reaching 3,812 packets (762.4 pps). The uniformity of packet types caused the entropy to drop to 9.7961, which is below the dynamic threshold (1.6947). Ryu Controller responded instantly by blocking the perpetrator's IP 10.0.0.3 for 60 seconds at the gateway level, which proved to immediately restore network stability and secure the IoT data flow.

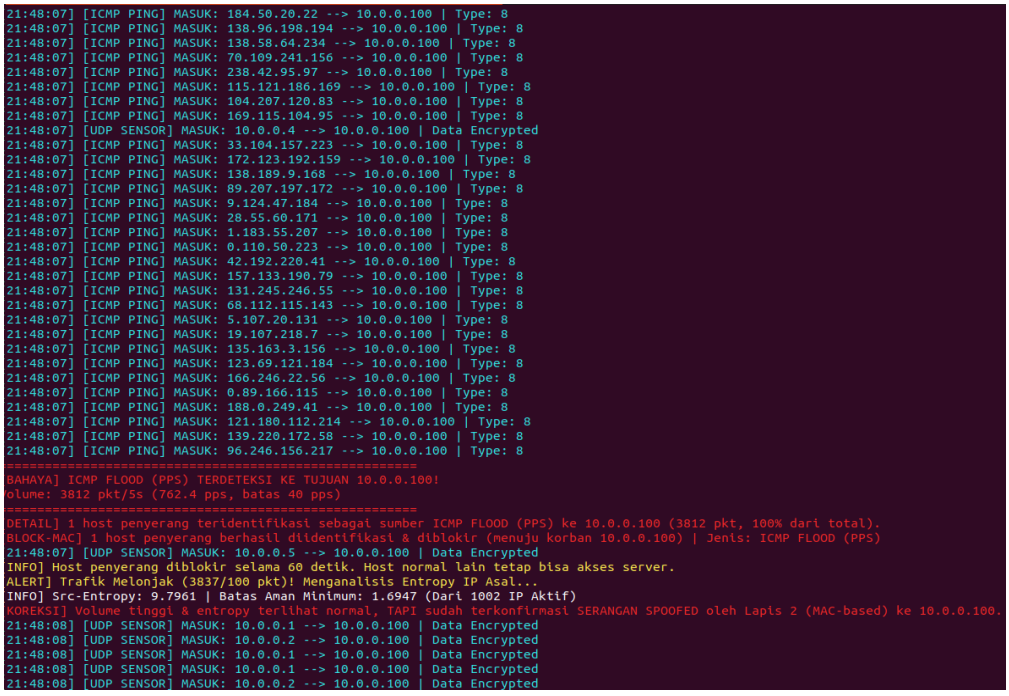

Figure 5. Statistical Detection and Mitigative Blocking of ICMP Flood Attack

In the protocol exhaustion evaluation via TCP SYN Flood attack (hping3 --flood -S -p 80) in Fig 6, the attacker flooded the server with [TCP TRAFFIC] packets reaching a volume of 8,281 packets per 5 seconds (1656.2 pps) with an absolute ACK/SYN ratio of 0.00. This connection flag monopolization decreased the entropy value to 10.7737, which was confirmed by the Layer 2 system as a Spoofed Attack because it was below the safe ratio < 0.3. The Ryu Controller responded instantly by triggering a [DANGER] state and applying a [BLOCK-MAC] rule on the attacker's IP (10.0.0.3) for 60 seconds on

the Gateway Switch. This mitigation step successfully cleared the buffer queue, allowing the normal sensor data flow ([UDP SENSOR]) to be received safely again immediately.

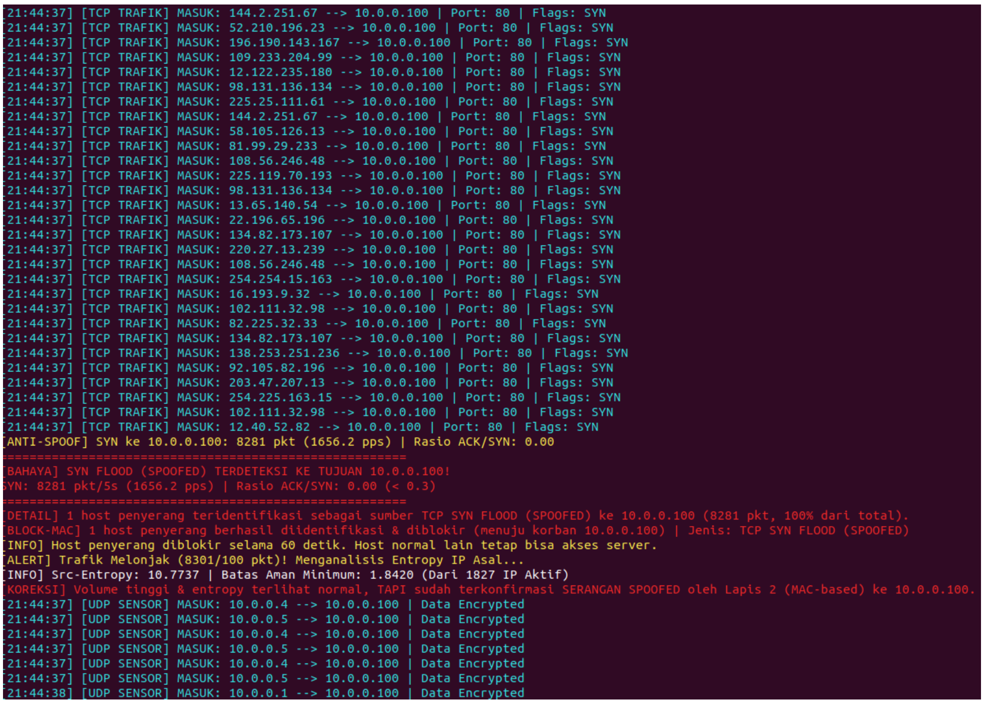

Figure 6. Statistical Detection and Mitigative Blocking of TCP SYN Flood Attack

4.3 Evaluation Quality of Service

To quantitatively validate network resilience, Quality of Service (QoS) telemetry comprising throughput, delay, and packet loss was recorded across three network states. The metrics are summarized in Table 1.

Table 1 . Quality of Service Evaluation Results

Network Condition	Throughput (Mbps)	Delay (ms)	Packet Loss (%)
Normal Operation	10.50	22.64	0
During DDoS Attack	0.09	Timeout	100
After Mitigation	6.36	22.64	0

The evaluation demonstrates that normal network operations achieve an optimal throughput of 10.50 Mbps with a stable delay of 22.64 ms and 0% packet loss. During an active unmitigated DDoS attack, the massive packet injection causes severe buffer overflow within the Gateway Switch queues, causing throughput to collapse to 0.09 Mbps and triggering an absolute 100% packet loss due to total destination unreachability. However, upon the automated activation of the mitigation rules, the malicious traffic is discarded directly at the ingress port. This proactive isolation allows network performance to recover substantially, successfully restoring throughput to 6.36 Mbps, returning latencies to the baseline level of 22.64 ms, and reducing packet loss back to 0% for all legitimate IoT node transmissions.

4.4 Detection performance

To comprehensively assess the classification capability of the proposed DDoS detection model, a total of 6,026 experimental traffic log instances were collected. Initial feature extraction revealed significant dataset cohesion, consisting of 5,893 normal traffic instances and only 133 attack instances.To prevent excessive false data loading and bias in the training process, the Synthetic Minority Over-sampling Technique (SMOTE) is applied specifically to the training data (training split) in a Stratified 5-Fold Cross-Validation scheme, so that the test data remains intact and represents the original network distribution. In addition, the evaluation stability is rigorously validated in each fold by measuring the Accuracy, Precision, Recall, F1-Score, and Receiver Operating Characteristic - Area Under Curve (AUC-ROC) metrics.

The baseline classification results obtained across the operational evaluation metrics are summarized in Table 2.

Table 2 . Classification Performance Metrics Across Evaluated Classes

	precision	recall	f1-score
Normal (0)	1.00	0.91	0.95
DDoS (1)	0.17	0.81	0.29
accuracy			0.91

As described in Table 2, the model achieved an Overall Accuracy of 0.91. To further analyze the prediction distribution, a 4-quadrant confusion matrix was derived. The model generated 1,074 True Negative (TN) instances, 22 True Positive (TP) instances, 105 False Positive (FP) instances, and only 5 False Negative (FN) instances. The structural distribution of these classification results is visually displayed in Fig 7.

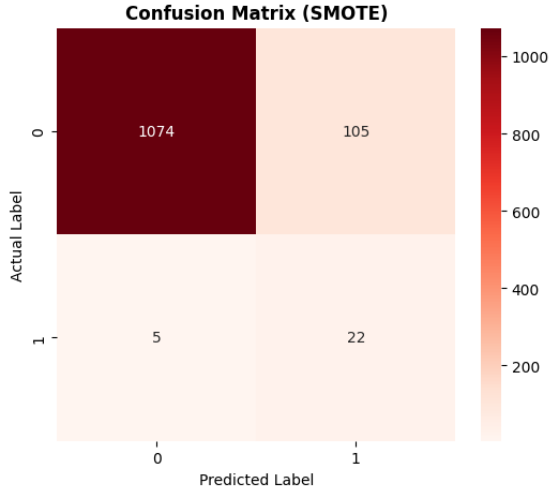

Figure 7. Confusion Matrix Heatmap for DDoS Classification Model

Based on the detailed analysis in Fig 7, the classification results demonstrate a critical level of operational security for IoT network infrastructure. The True Negative value (TN = 1.074) validates that most normal traffic is correctly recognized and maintained unimpeded. Meanwhile, the True Positive value (TP = 22) demonstrates the model's ability to identify volumetric attack patterns injected into the system. The most striking point of this matrix lies in the very low number of False Negatives (FN = 5). In the context of network security, False Negatives represent DDoS attack packets that slip through and fail to be detected by the system. This very low FN level confirms that the detection mechanism has very high sensitivity and recall in preventing attacks from bypassing the outermost layer of defense. The emergence of 105 False Positive (FP) instances was mostly triggered by sudden surges of legitimate traffic (Flash Crowds) that temporarily resembled an anomalous profile. However, thanks to the integration of Adaptive Dynamic Thresholding, the controller was able to tolerate these fluctuations so as not to cause mass service outages on legitimate IoT nodes.

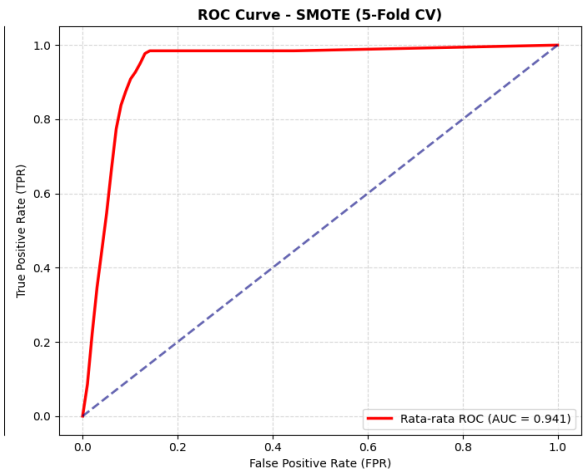

Figure 8. ROC Curve Analysis via 5-Fold Cross-Validation

As shown in the ROC curve in Fig 8, the red line (mean ROC) curves sharply toward the upper left corner of the graph, resulting in a very high average Area Under Curve score of AUC = 0.941. The dashed blue diagonal line represents the random guessing threshold (baseline chance level with AUC = 0.50). This highly significant performance difference between the model curve and the baseline empirically demonstrates that the classification model has very strong discriminatory power.

This AUC value of 0.941 confirms that combining the Shannon Entropy algorithm with the SMOTE training scheme on the training data successfully created a highly stable model. The system was proven to maintain a high True Positive Rate (TPR) while suppressing the False Positive Rate (FPR) at a very low level. This ensures that the Ryu Controller can consistently distinguish between destructive DDoS packet floods and legitimate IoT traffic variations across the Gateway layer, unaffected by data noise or fluctuations in daily communication patterns.

5. CONCLUSION

Based on comprehensive architecture design, experimental simulations, and performance evaluations, this study demonstrates several key findings related to SDN-IoT network security. The integration of the Shannon Entropy algorithm into a centralized Ryu SDN Controller presents a highly efficient and lightweight mathematical approach to identify anomalous traffic behavior caused by volumetric DDoS attacks. Furthermore, the implementation of an adaptive Dynamic Threshold mechanism successfully prevents false alarms by effectively distinguishing between flooding attack vectors and legitimate emergency data surges (flash crowds).

In terms of network resilience, a three-tier hierarchical topology proved optimal for threat isolation. By delegating OpenFlow flow modification rules directly to the Gateway Switch at the edge, this mitigation framework discards malicious traffic directly at the ingress port. This proactive border defense quickly restored the integrity of the core infrastructure, returning network throughput to 6.36 Mbps, latency to a baseline of 22.64 ms, and reducing packet loss to 0% for legitimate IoT transmissions.

Finally, the application of SMOTE specifically to the training data in the Stratified 5-Fold Cross-Validation scheme produces a classification model with an Overall Accuracy of 91.00% (0.91). The model evaluation shows a Recall rate of 0.81 (81.00%) for the DDoS attack class detection and 0.91 (91.00%) for the normal traffic class, as well as an average AUC-ROC score of 0.941.

REFERENCE

[1] C. Singh and A. K. Jain, "A comprehensive survey on DDoS attacks detection & mitigation in SDN-IoT network," *e-Prime - Advances in Electrical Engineering, Electronics and Energy*, vol. 8, 2024, doi:10.1016/j.prime.2024.100543.

[2] S. Vijay and M. K. Banga, "Managing Large IoT Network Using SDN and Hierarchical Tree Topology," *Theory and Practice*, vol. 2024, no. 5, pp. 6484–6495, 2024, doi:10.53555/kuey.v30i5.3969.

[3] J. G. Almaraz-Rivera *et al.,* "Toward the Protection of IoT Networks: Introducing the LATAM-DDoS-IoT Dataset," *IEEE Access*, vol. 10, pp. 106909–106920, 2022, doi:10.1109/ACCESS.2022.3211513.

[4] S. Qureshi *et al.,* "A Hybrid DL-Based Detection Mechanism for Cyber Threats in Secure Networks," *IEEE Access*, vol. 9, pp. 73938–73947, 2021, doi:10.1109/ACCESS.2021.3081069.

[5] F. M. Salem, H. Youssef, I. Ali, and A. Haggag, "A variable-trust threshold-based approach for DDoS attack mitigation in software defined networks," *PLoS ONE*, vol. 17, no. 8, Art. no. e0273681, 2022, doi:10.1371/journal.pone.0273681.

[6] C. Fan *et al*., "Detection of DDoS Attacks in Software Defined Networking Using Entropy," *Applied Sciences*, vol. 12, no. 1, Art. no. 370, 2022, doi:10.3390/app12010370.

[7] M. A. Ferrag et al., "Deep Learning for Cyber Security Intrusion Detection: Approaches, Datasets, and Comparative Study," *Journal of Information Security and Applications*, vol. 50, Art. no. 102419, 2020, doi:10.1016/j.jisa.2019.102419.

[8] J. P. Bharadiya, "Machine Learning in Cybersecurity: Techniques and Challenges," *European Journal of Technology*, vol. 7, no. 2, pp. 1–14, 2023, doi:10.47672/ejt.1486.

[9] D. T. T. Mai et al., "DDoS Attacks Detection Using Dynamic Entropy in Software-Defined Network Practical Environment," *International Journal of Computer Networks and Communications*, vol. 15, no. 3, pp. 113–128, 2023, doi:10.5121/ijcnc.2023.15307.

[10] T. Bai, Y. Liu, Y. Gao, and Y. Zhou, "ATS-DTA: Adaptive Two-Stage DDoS Detection with Dynamic Threshold Adjustment in SDN Networks," *Cybersecurity*, vol. 9, Art. no. 12, 2026, doi:10.1186/s42400-025-00414-0.

[11] T. Wang, Y. Feng, and K. Sakurai, "Improving the Two-stage Detection of Cyberattacks in SDN Environment Using Dynamic Thresholding," in *Proc. 15th Int. Conf. Ubiquitous Information*

Management and Communication (IMCOM), Seoul, South Korea, 2021, doi:10.1109/IMCOM51814.2021.9377395.

[12] V. Hnamte and J. Hussain, "DCNNBiLSTM: An Efficient Hybrid Deep Learning-Based Intrusion Detection System," *Telematics and Informatics Reports*, vol. 10, Art. no. 100053, 2023, doi:10.1016/j.teler.2023.100053.

[13] Y. Zhou, G. Cheng, and S. Yu, "An SDN-Enabled Proactive Defense Framework for DDoS Mitigation in IoT Networks," *IEEE Transactions on Information Forensics and Security*, vol. 16, pp. 5366–5380, 2021, doi:10.1109/TIFS.2021.3127009.

[14] A. Hirsi *et al.,* "Comprehensive Analysis of DDoS Anomaly Detection in Software-Defined Networks," *IEEE Access*, 2025, doi:10.1109/ACCESS.2025.3535943.

[15] J. L. Herrera et al., "Optimizing the Response Time in SDN-Fog Environments for Time-Strict IoT Applications," *IEEE Internet of Things Journal*, vol. 8, no. 23, pp. 17172–17185, 2021, doi:10.1109/JIOT.2021.3077992.

[16] Q. Syahputra, D. Akbi, and D. Risqiwati, "Deteksi dan Mitigasi Serangan DDoS pada Software Defined Network Menggunakan Algoritma Decision Tree," *REPOSITOR*, vol. 2, no. 11, pp. 1491–1502, 2020.

[17] M. N. Ali, M. Imran, M. S. Ud Din, and B. S. Kim, "Low Rate DDoS Detection Using Weighted Federated Learning in SDN Control Plane in IoT Network," *Applied Sciences*, vol. 13, no. 3, Art. no. 1431, 2023, doi:10.3390/app13031431.