SSRG International Journal of Electronics and Communication Engineering
ISSN: 2348-8549/ https://doi.org/10.14445/23488549/IJECE-V12I8P101

Volume 12 Issue 8, 1-10, August 2025

Original Article

Information Gain-Based Detection of Low and High Severity DDoS Attacks in SDN with Automated Mitigation Responses

Jaimin M Shroff[1], Sanjay M Shah[2]

[1]*Computer Engineering, Gujarat Technological University, Ahmedabad, India.*
[2]*Department of Computer Engineering, Government Engineering College, Rajkot, India.*

[1]*Corresponding Author : jaimin_shroff22@yahoo.co.in*

Received: 01 June 2025 Revised: 03 July 2025 Accepted: 02 August 2025 Published: 30 August 2025

Abstract *- Distributed Denial of Service (DDoS) attacks continue to be a significant danger to network infrastructure, especially in Software-Defined Networking (SDN) environments, because of their centralized management mechanisms. This study presents a dynamic, multi-tiered DDoS detection and mitigation framework utilizing entropy and Information Gain (IG) for real-time severity assessment. In contrast to conventional single-threshold models, our methodology differentiates between normal, low-intensity, and high-intensity DDoS attacks by analyzing statistical traffic entropy fluctuations and IG thresholds. Low-severity attacks are diverted to honeypots for isolation and examination, but high-severity threats activate automatic port-blocking protocols at the switch level. The proposed method demonstrates significant responsiveness in mitigation while causing minimum disturbance to legal traffic. Our architecture offers a strong, automated defensive strategy that corresponds with the evolving characteristics of contemporary network threats. This research represents a substantial advancement in intelligent, SDN-based DDoS mitigation. It establishes a basis for future integration with deep learning and cloud-native architectures to manage encrypted and large-scale traffic environments.*

Keywords *- DDoS, SDN, Information Gain, Mitigation, Packet-Per-Second.*

1. Introduction

Distributed Denial of Service (DDoS) assaults constitute a widespread and rising cybersecurity menace when assailants inundate a target system with excessive traffic, thereby incapacitating it for legitimate users. Such attacks can impair enterprises, essential infrastructure, and network services, resulting in considerable operational and financial detriment. DDoS assaults generally exploit bandwidth, protocol, or application weaknesses and are executed via botnets, extensive networks of infected devices under remote control [1, 2]. DDoS attacks can be broadly categorized into three types [3].

- Volumetric Attacks: These encompass UDP floods, ICMP floods, and DNS amplification, with the objective of overwhelming the target's bandwidth.
- Protocol Attacks: Examples include SYN floods and Ping of Death, which exploit transport or network layer protocol vulnerabilities.
- Application Layer Attacks: These are more covert, focusing on the application logic (e.g., HTTP floods) and frequently circumvent conventional defenses.

With the rapid growth of internet-connected systems, Distributed Denial of Service (DDoS) attacks have become a major and persistent threat. These attacks overwhelm networks or services with illegitimate traffic, making them inaccessible to legitimate users. Software-Defined Networking (SDN), which separates the control and data planes, offers flexibility and increases vulnerability, making it an attractive target for DDoS attacks [4, 5]. Real-time, context-aware DDoS detection and mitigation are essential in this dynamic environment. Traditional security methods rely on static thresholds and often fail to scale or adapt to varying DDoS attacks. They struggle to differentiate between low-rate stealthy attacks and high-rate floods, leading to delayed responses and disruptions [6]. Many existing approaches use metrics like Packet-Per-Second (PPS) rates or entropy to detect anomalies, but they often rely on fixed thresholds, making them prone to misclassification. These methods also lack detailed severity classification, preventing appropriate adjustment of mitigation strategies [7-10].

To detect anomalies, SDN-DDoS detection methods mostly use static thresholds, packets per second, or Shannon entropy statistics. These approaches have trouble adapting to

attacks in real time. It can often give false positives or negatives, especially with low-rate stealthy DDoS assaults or traffic bursts that imitate legitimate flows. Their binary response to attacks limits mitigation measures since they cannot determine attack severity. Critical services may be subject to slow answers or excessive blocking of genuine users.

This study presents an information gain-based multi-level DDoS detection and mitigation system to address the incapacity of SDN-DDoS detection techniques to respond to dynamic assault patterns and assess attack severity. Using entropy and IG values, the suggested system classifies arriving packets as regular, low-rate, or high-rate DDoS activity. Unlike binary alternatives, this idea classifies traffic into regular, low-severity, and high-severity DDoS. Mitigation methods automatically redirect low-severity attacks to a honeypot and shut down switch ports for high-severity attacks. This context-aware technique reduces false positives, enables real-time flexibility, and ensures network availability during active attacks. Major contributions of this research:

- Developed a multi-level mitigation system for severity-aware responses via knowledge acquisition.
- Seamless interaction with SDN controller, verified by Mininet simulations.
- Evaluated numerous DDoS attack types, TCP, SYN, and ICMP and found improved detection accuracy and fewer false alarms than traditional approaches.

2. Related Work

DDoS detection for SDN environments now uses statistical entropy analysis, clustering, and machine learning techniques to improve accuracy and adaptability. These methods classify traffic by behaviour to decrease false positives and improve real-time responsiveness. Many previous approaches use fixed thresholds or static models, which restrict their effectiveness against changing or low-rate attacks. Current methods struggle with scalability and high-traffic delay mitigation.

A.Apostu et al. explored ways to detect and mitigate SDN DDoS attacks. Conventional methods use volume-centric measurements like PPS and sometimes fail to distinguish between malicious and genuine traffic surges. Recent methods increase detection model precision and versatility with machine learning [11].

Amany I. Hassan et al. describe a hybrid DDoS detection system that uses entropy-based traffic analysis and k-means clustering in SDNs to discriminate normal, suspicious, and attack traffic in real time. They reduce false positives with adaptive thresholding and traffic categorization to achieve > 99.9% accuracy on benchmark datasets like CICIDS2017, CSECIC2018, and CICDDoS2019. Using statistical entropy and unsupervised machine learning, the approach detects volumetric and low-rate attacks. Static k-means clustering (k=3) is less adaptable to evolving or zero-day attacks. Entropy-based detection may miss concealed or slow-growing DDoS traffic until clustering confirms anomalies [12].

Two-Phase Authentication of Attack Detection (TPAAD) by Najmun Nisa et al. detects and stops DoS attacks using packet filtering and machine learning classifiers (SVM and KNN) in an SDN framework. The device restricts incoming traffic by threat level using machine learning models. The model achieves 99.56% detection accuracy while reducing CPU utilization, control channel bandwidth, and false positives. The CICDoS2017 dataset improves Mininet-SDN testbed packet delivery and controller responsiveness.

The system uses established criteria and models that may not adjust quickly. Real-time traffic diversity may affect categorization [13]. Results vary by dataset. Hurst coefficients and fuzzy c-means clustering help Sergii Lysenko et al. identify botnet-induced low-rate DDoS attacks in SDNs. Despite processing demands and precision degradation from bot and user traffic patterns, BotGRABBER achieved over 97% detection accuracy in testing [14].

Pritam Raut et al. present the Rényi Entropy with Packet Drop (REPD) method to detect low-rate DDoS attacks by examining packet flow destination address homogeneity. They successfully identified low-rate threats and conserved resources in the SDN data plane; however, all packets aimed at a single node result in zero entropy and false negatives [15].

In a Mininet-Ryu-based Software-Defined Network, Nirzari Patel et al. use Logistic Regression, Random Forest, Decision Tree, Naive Bayes, and K-Nearest Neighbors to detect and mitigate DDoS attacks. They successfully detected DDoS using ML algorithms and mitigated it with a controller-embedded module; however, they did not investigate false positives and mitigation delay under high-traffic scenarios [16].

Jin Wang and Liping Wang developed a hybrid GCN-GRU deep learning model, wavelet feature extraction, and a dual sliding window for SDN real-time LDDoS detection and mitigation. They achieved high detection accuracy with low false positives, enabling real-time OpenFlow-based port blocking mitigation. The approach may have limited scalability in highly dynamic topologies and may have trouble identifying novel attack variants not in the training data [17]. Pooja Chaudhary et al.'s three-phase fog-enabled IoT system uses entropy-based detection, symmetrical uncertainty mixed with K-means for feature selection, and RF and SVM for multi-class DDoS classification and mitigation. Random Forest accuracy was 98.71%, while fog-based architecture lowered reaction time by 35% over central systems. The dynamic threshold method is adaptive but may be affected by rapidly changing benign traffic [18].

Table 1. Comparison of DDoS mitigation approaches

Paper	Dataset	Mitigation Strategy	Accuracy (%)	Limitations
Jishuai Li et al. [19]	Custom Dataset	Switch Rule Filtering	97%	High config overhead for rule matching
Hao Chen et al. [20]	Real-time Traffic	Manual Rule Drop	91%	Scalability issue
Phan The Duy et al. [21]	Simulated SDN Topology	Flow Rule Blocking	92%	Dependency on the controller
Sanjeetha R et al. [22]	Simulated SDN Topology	Controller Alert & Rule Suppression	93%	More False positives
Jisi Chandroth et al. [23]	Real-time Traffic	NA	NA	No detection mechanism
Jin Wang et al. [24]	Simulated SDN Topology	Flow Drop and Blocking	95%	Overhead under high traffic
Harun Jamil et al. [25]	Real-time Traffic	Static Rule Update	90%	Rigid rule
Diego S. M. Gonçalves et al. [26]	Simulated SDN Topology	Blacklist and Flow Drop	92%	Issue in evolving HTTP flood
Jisa David et al. [27]	Real-time Traffic	Dynamic Threshold Blocking	96%	Parameter tuning needed for thresholds

Many current approaches use fixed thresholds or unique indications like entropy, limiting their ability to adapt to changing network conditions and distinguish DDoS attacks. Many techniques lack real-time mitigation or focus on certain threat types, making them rigid and scalability-limited. To overcome these issues, our research proposes an Information Gain-based, multi-tier detection and automatic mitigation technique in SDNs for more flexible, precise, and severity-aware DDoS defense.

The centralized controller in Software-Defined Networks (SDNs) gives flexibility in regulating network flows, but forwarding devices' limited threat awareness makes them vulnerable to DDoS attacks. Traditional detection methods that use packet rates, entropy, or fixed thresholds cannot adapt to dynamic traffic patterns, resulting in inaccurate classifications and slow responses.

IG powers our multi-level DDoS detection and mitigation platform. Shannon entropy and information gain are utilized to analyze real-time traffic and assess the severity of potential DDoS attacks. High-severity attacks block time-bound ports, whereas low-severity attacks are redirected to a designated honeypot. The system logs essential traffic parameters for post-event verification, facilitating adaptive, real-time mitigation while preserving the integrity of legitimate network flows.

3. Proposed Method

A proposed mathematical approach integrates entropy and information gain to identify and mitigate DDoS attacks based on their intensity in Software-Defined Networks. This model enables real-time traffic categorization and response using threshold-based logic derived from statistical traffic distribution.

3.1. Traffic Aggregation

Let P {p1,p2,...,pn} be the set of observed packets during an interval t. The source MAC address is recorded as MACsrc(pi) for each packet pi. The frequency count Cj for each source MACj is given by:

$$C_j = \sum_{i=1}^{n} 1_{\{MAC_{src}(p_i)=j\}} \quad (1)$$

The Total Packet Count T has been calculated based on the frequency count.

$$T = \sum_j C_j \quad (2)$$

3.2. Entropy Calculation

For each source of j, compute the traffic probability of P_j.

$$P_j = \frac{C_j}{T} \quad (3)$$

Entropy H(X) is computed over the traffic distribution:

$$H(X) = -\sum_j P_j \log_2 P_j \quad (4)$$

Entropy reflects the uncertainty in source traffic. High entropy implies normal behavior, while low entropy suggests a possible attack.

3.3. Conditional Entropy on Suspicious Subset

Define suspicious sources as those with Pj < 0.2. Let A be the set of such sources:

$$A = \{j | P_j < 0.2\}, \quad A_{count} = |A| \quad (5)$$

Compute conditional entropy:

$$H\left(\frac{X}{Y}\right) = -\sum_{j \in A} \frac{P_j}{A_{Count}} \log_2 \left(\frac{P_j}{A_{Count}}\right) \quad (6)$$

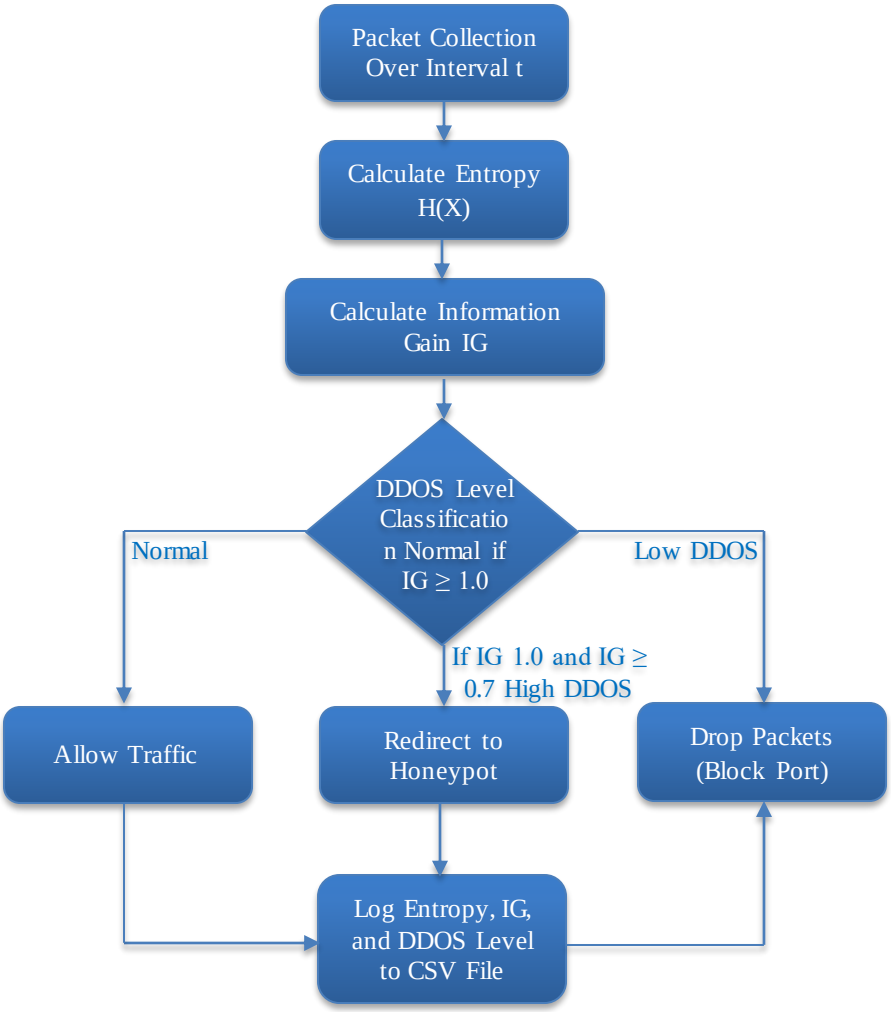

Fig. 1 Flow chart of the proposed method

3.4. Compute the Information Gain

Information gain quantifies the knowledge gained by isolating the suspicious subset.

$$IG = H(X) - H\left(\frac{X}{Y}\right) \tag{7}$$

3.5. Classification of Traffic Severity

$$DDOS\ Level = \begin{cases} Normal, if\ IG \geq 1.0 \\ Low\ DDoS, if\ 0.7 \leq IG < 1.0 \\ High\ DDoS, IG \leq 0.4 \end{cases} \tag{8}$$

Based on the classified severity level, appropriate mitigation actions are dynamically applied.

$$Mitigation = \begin{cases} Allow\ Traffic, Normal \\ Redirect\ to\ Honeypot, Low\ DDoS \\ Drop\ Packet, High\ DDoS \end{cases} \tag{9}$$

The system also initiates automatic unblocking of the T_{block} using flow deletion.

3.6. Logging

All traffic features, including entropy, IG, and classification results, are logged to a CSV file for monitoring and future analysis.

Equations (4) and (7) constitute the foundation of the detection algorithm by calculating entropy and Information Gain from real-time MAC address distributions, thereby facilitating the evaluation of traffic unpredictability.

Suspicious sources are discovered by Equation (5), which assesses low occurrence probability, and their unpredictability is subsequently examined using conditional entropy (Equation (6)). IG is utilized to categorize traffic severity into Normal, Low DDoS, or High DDoS based on the thresholds specified in Equation (8). According to this classification, Equation (9) dictates the mitigation strategy: normal traffic is allowed, low-severity traffic is sent to a honeypot, and high-severity traffic is obstructed at the ingress switch. These actions are temporally regulated and thoroughly documented for oversight and evaluation.

4. Implementation Setup

4.1. Environment Setup

The proposed detection and mitigation framework was deployed within a virtualized Software-Defined Networking testbed using Mininet, an emulation platform for building large-scale virtual networks [28]. The setup included:

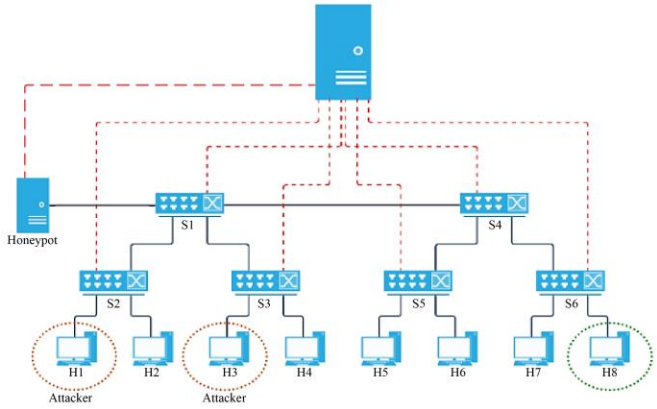

Fig. 2 SDN topology for simulation

The RYU controller administered the SDN environment's control plane, a lightweight framework compliant with OpenFlow that is suitable for Python application development. A custom controller module was created by modifying simple_switch_13 to provide real-time flow monitoring and entropy-based analytics. The testbed topology comprised six OpenFlow-enabled switches (s1–s6) and nine hosts, with h8 as the victim, a dedicated honeypot managing redirection, and h1 and h3 as attackers. Traffic data were collected every 5 seconds using OFPFlowStatsRequest, recording source and destination MAC addresses, packet counts, and timestamps. A centralized logic engine calculated entropy and Information Gain metrics to identify anomalies and implement mitigation strategies—either rerouting traffic to a honeypot or obstructing the ingress port—by injecting dynamic flow rules directly into the network switches.

4.2. Hardware and Software Configuration

Table 2. System specification

Component	Specification
Operating System	Ubuntu 20.04 LTS
RAM	8 GB
Processor	Intel Core i5 (8th Gen) or equivalent
Mininet Version	2.3.0
RYU Controller	Version 4.34
Python	3.8+
Tools Used	ping3, hping3, ovs-ofctl

4.3. Attack Simulation and Response Mechanism

To evaluate the effectiveness of the proposed detection system, controlled simulations of both normal and attack traffic were executed utilizing ICMP-based flows:

- Normal Traffic: Standard ping traffic was generated from benign hosts with default configurations.
- Low DDoS Attack: The command H1 ping3 -c 500 -d 120 -S -w 64 --rand-source H8 sent moderate-rate ICMP packets with randomized source addresses directed at the target H8.
- Severe DDoS Attack: Executed using h1 ping3 -c 10000 -d 120 -S -w 64 -p 80 --flood --rand-source h8, inundating the target with over 100,000 packets per second, substantially diminishing entropy and IG (~0).

Mitigation Triggers:

- Low Severity DDoS: Identified by IG values ranging from 0.7 to 1.0, leading to traffic diversion to a honeypot.
- High Severity DDoS: Recognized by IG $\leq$ 0.4, necessitating fast port blocking on the assailant's switch. The regulation is automatically rescinded upon a specified BLOCK_DURATION, facilitating a seamless recovery.

5. Experimental Results & Discussion

5.1. Detection Outputs

The proposed system dynamically calculates entropy and information gain from real-time traffic data across OpenFlow switches. The detection results were examined through Ryu controller terminal logs and corroborated using CSV logs and Mininet ping answers.

The terminal output in Figure 3 indicates that the system has identified a Low DDoS condition based on the computed Information Gain values. The controller dynamically initiates a mitigating response when Information Gain falls below the threshold. The dubious traffic from switch s3 is rerouted to a honeypot on port 1 for the purpose of isolating and examining the attack.

This terminal output in Figure 4 identifies Low DDoS threats based on IG thresholds and responds by routing suspect traffic from switch s1 to a honeypot. The ping activity from attacker hosts such as H1 and H3 persists without interruption, maintaining network continuity while isolating the possible threat effectively. This underscores the unobtrusive character of mitigation in the context of low-severity attacks.

Figure 5 illustrates real-time terminal outputs from nodes H1 and H3, which are persistently transmitting ICMP echo requests to the target node H8. Notwithstanding the categorization of a Low DDoS attack, the ping answers persist without interruption.

This occurs when the system redirects traffic to a honeypot rather than terminating it. This conduct guarantees uninterrupted service for the attacker nodes, while segregating their traffic for examination—illustrating an efficient and non-intrusive mitigation approach appropriate for low-severity DDoS situations.

Figure 6 depicts the terminal output during a severe DDoS attack, characterized by a traffic rate surpassing 100,000 packets per second. Consequently, the computed Information Gain value decreases to 0.0000. The substantial reduction in IG serves as a robust indicator of a high-intensity DDoS incident. The system autonomously implements a mitigation measure by obstructing the attacker's ports on the compromised switches for a specified interval (e.g., 120 seconds). This response mitigates additional traffic surges and safeguards the network infrastructure.

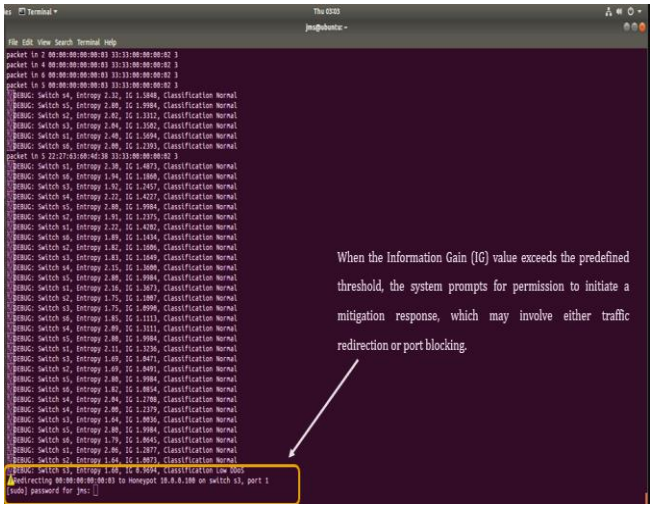

Fig. 3 Low DDoS condition based on calculated information gain

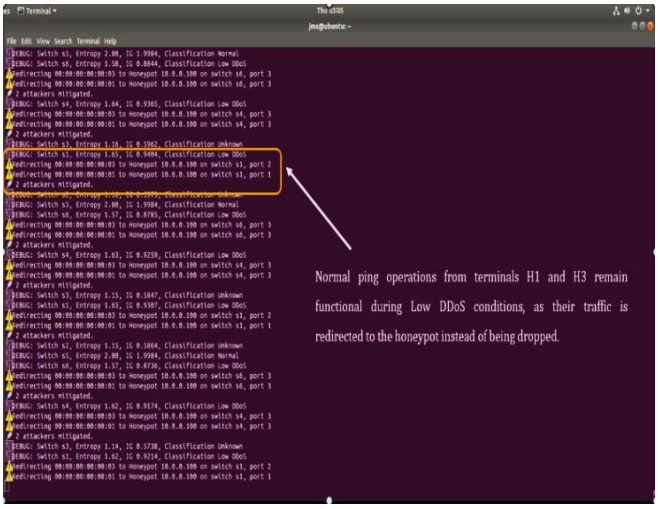

Fig. 4 Low DDoS threats based on IG thresholds

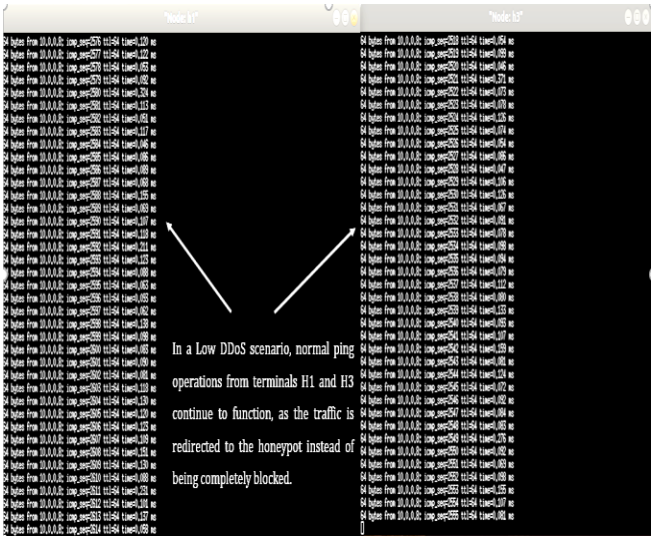

Fig. 5 Ping activity from H1 and H3 during low DDoS attack

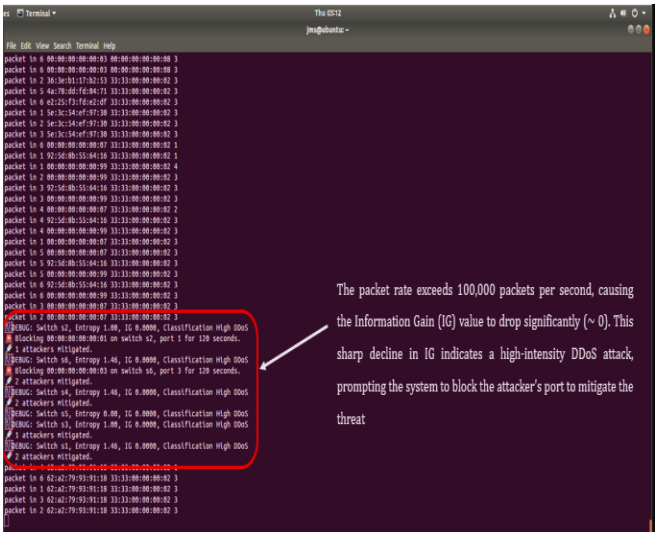

Fig. 6 High DDoS detection and mitigation via port blocking

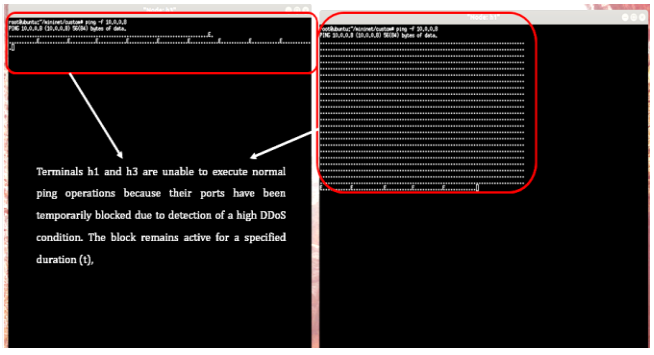

Fig. 7 Port blocking response during high DDoS attack

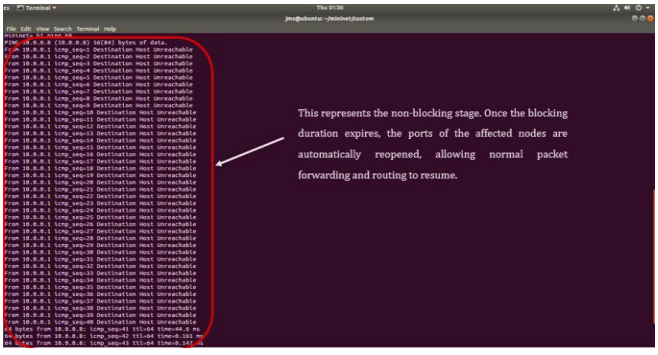

Fig. 8 Port unblocking and packet forwarding resumption

5.2. Effectiveness of Information Gain in Severity Classification

Utilizing Information Gain as a severity classifier demonstrates dynamism and precision. Figure 9 illustrates the packet volume over time for TCP, SYN, and ICMP-based DDoS attacks, revealing pronounced spikes in packet volume that coincide with the initiation of the attack. These abrupt increases result in considerable entropy fluctuations, which are subsequently manifested in IG computation.

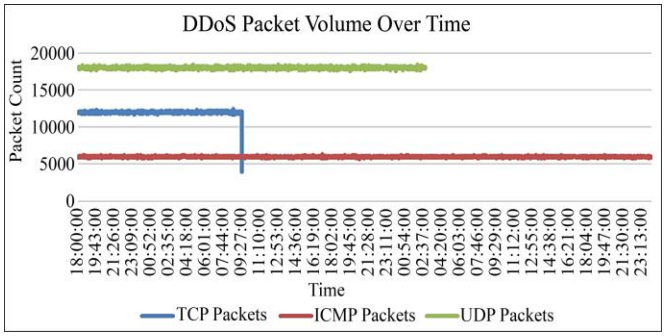

Fig. 9 Packet volume over time for different DDoS attacks

Figure 10 reinforces this understanding by illustrating entropy changes throughout time. A significant reduction in entropy levels correlates with heightened traffic abnormalities. The decrease in entropy activates the IG-based classifier, enabling it to differentiate among

- Normal Traffic (IG ≥ 1.0),
- Low DDoS (0.7 <= IG < 1.0) and
- High DDoS (IG ≤ 0.4).

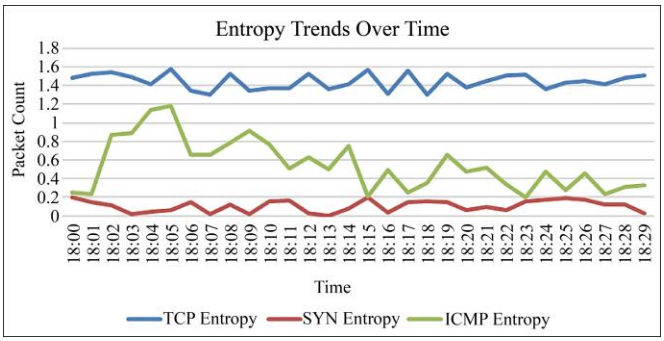

Fig. 10 Entropy trends over time

5.3. Second-Order Discussion Regarding Mitigation Timing and Effectiveness

Figure 11 illustrates the allocation of mitigation strategies like Forwarding, Port Blocking, and Redirection utilized against TCP, SYN, and ICMP attack categories. The data indicates increased port blocking in ICMP-based assaults, generally linked to high-volume floods. TCP and SYN attacks demonstrate a measured implementation of all three techniques, indicating the system's adaptive reaction according to IG classification. This time-sensitive response system:

- Redirects low-severity attackers to a honeypot, maintaining normal service (as evidenced by terminal log screenshots displaying uninterrupted pings from H1 and H3),
- Instantly blocks high-severity threats, terminating malicious traffic as indicated by "Destination Host Unreachable" messages, and
- Automatically reopens ports after a predetermined duration, reinstating normalcy without manual intervention.

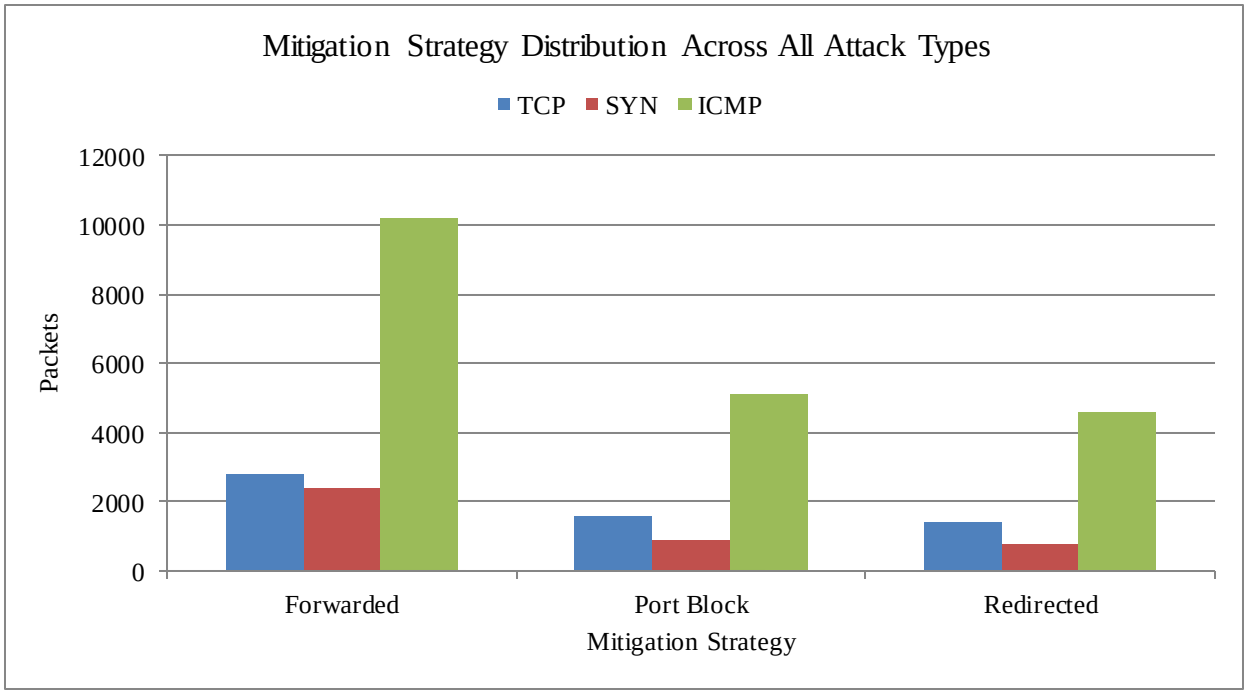

Fig. 11 Mitigation strategy distribution across attack types

Table 3. Evaluation metrics for DDoS in considering attack severity

Method	Severity	Accuracy (%)	Precision (%)	Recall (%)	F1 Score (%)
Deep Q-Network [29]	Low	27	30	25	27
Tsallis Entropy [30]	Low & High	50	52	48	50
Port & Traffic State [31]	Low	80	78	75	76
RNN [32]	Low	99	98	99	98.5
Deep MLP-based [33]	Low & High	97	95	96	95.5
Proposed Approach	**Low & High**	**98**	**97**	**98**	**97.5**

5.4. Discussion Regarding Evaluation Metrics

Table 3 shows the evaluation of various DDoS detection techniques based on severity levels and performance metrics, revealing significant differences in effectiveness. Methods such as Deep Q-Network and Tsallis Entropy demonstrate limited accuracy (27% and 50%, respectively) and lack the ability to adapt to both low and high-rate DDoS attacks, making them less suitable for real-world deployment. Port & Traffic State analysis and RNN-based methods offer improved detection for low-rate attacks, with the RNN approach achieving a notable 99% accuracy. However, they do not provide multi-level mitigation or severity-aware classification. Deep MLP-based detection shows balanced performance for both severity types but falls slightly short of the proposed method.

In contrast, the proposed Information Gain-based approach excels in both detection accuracy (98%) and balanced performance across all key metrics: precision (97%), recall (98%), and F1-score (97.5%). Importantly, it is one of the few models that explicitly distinguishes between low and high-severity attacks, enabling automated, context-aware mitigation through redirection or port blocking. This adaptability makes it a more robust and practical solution for SDN-based networks, where dynamic threat response is essential.

6. Conclusion and Future Work

This research provides an adaptive and intelligent framework for detecting and mitigating Distributed Denial-of-Service assaults in Software-Defined Networks utilizing Information Gain as a decision criterion. The system categorizes DDoS traffic into low and high severity levels, implementing multi-tiered mitigation strategies: low-severity traffic is diverted to a honeypot for isolation, whereas high-severity traffic activates temporary port blocking. Employing entropy and information gain facilitates real-time traffic analysis and accurate classification while minimizing false alarms.

- The system's primary contributions encompass a dynamic feature-based entropy and information gain calculation for precise severity identification.
- An automatic mitigation method driven by thresholds, customized according to the severity of identified assaults.
- Enhanced classification accuracy with minimized overhead, corroborated by experimental validation in a Software-Defined Networking testbed.

The suggested method markedly enhances responsiveness, scalability, and decision accuracy, representing a considerable advancement over conventional entropy or PPS detection techniques.

To augment the resilience and flexibility of the proposed framework, the subsequent avenues are suggested for future investigation:

- Encrypted Traffic Management: Enhance the methodology to analyse and categorize encrypted packets while preserving data security.
- Deep Learning Integration: Integrate the existing IG-based approach with sophisticated deep learning models to elucidate intricate attack patterns over time.
- Scalability Testing: Implement and assess the model on extensive, real-world datasets to verify its generalizability across various network contexts.

This study establishes a fundamental step towards developing self-adaptive and intelligent SDN security systems proficient in real-time threat detection and context-aware mitigation.

References

[1] Neelam Dayal et al., "Research Trends in Security and DDoS in SDN," *Security and Communication Networks*, vol. 9, no. 18, pp. 6386-6411, 2016. [CrossRef] [Google Scholar] [Publisher Link]

[2] Monika Sachdeva, Krishan Kumar, and Gurvinder Singh, "A Comprehensive Approach to Discriminate DDoS Attacks from Flash Events," *Journal of Information Security and Applications*, vol. 26, pp. 8-22, 2016. [CrossRef] [Google Scholar] [Publisher Link]

[3] Basheer Husham Ali et al., "Detection of Different Types of Distributed Denial of Service Attacks Using Multiple Features of Entropy and Sequential Probabilities Ratio Test," *Journal of Engineering Science and Technology*, vol. 18, no. 2, pp. 844-861, 2023. [Google Scholar] [Publisher Link]

[4] Chandrapal Singh, and Ankit Kumar Jain, "A Comprehensive Survey on DDoS Attacks Detection & Mitigation in SDN-IoT Network," *e-Prime - Advances in Electrical Engineering, Electronics and Energy*, vol. 8, pp. 1-17, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[5] Juan Camilo Correa Chica, Jenny Cuatindioy Imbachi, and Juan Felipe Botero Vega, "Security in SDN: A Comprehensive Survey," *Journal of Network and Computer Applications*, vol. 159, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[6] Bushra Alhijawi et al., "A Survey on DoS/DDoS Mitigation Techniques in SDNs: Classification, Comparison, Solutions, Testing Tools and Datasets," *Computers and Electrical Engineering*, vol. 99, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[7] Cameron S. Whittle, and Hong Liu, "Effectiveness of Entropy-Based DDoS Prevention for Software Defined Networks," *2021 IEEE International Symposium on Technologies for Homeland Security*, Boston, MA, USA, pp. 1-7, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[8] Mayadah A. Mohsin, and Ali H. Hamad, "Implementation of Entropy-Based DDoS Attack Detection Method in Different SDN Topologies," *American Academic Scientific Research Journal for Engineering, Technology, and Sciences*, vol. 86, no. 1, pp. 63-76, 2022. [Google Scholar] [Publisher Link]

[9] Mohammed Ibrahim Kareem, and Mahdi Nsaif Jasim, "Entropy-Based Distributed Denial of Service Attack Detection in Software-Defined Networking," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 27, no. 3, pp. 1542-1549, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[10] Debashis Kar Suvra, "An Efficient Real Time DDoS Detection Model Using Machine Learning Algorithms," *Arxiv Preprint*, pp. 1-7, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[11] Alexandru Apostu et al., "Detecting and Mitigating DDoS Attacks with AI: A Survey," *Arxiv Preprint*, pp. 1-35, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[12] Amany I. Hassan, Eman Abd El Reheem, and Shawkat K. Guirguis, "An Entropy and Machine Learning Based Approach for DDoS Attacks Detection in Software Defined Networks," *Scientific Reports*, vol. 14, no. 1, pp. 1-18, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[13] Najmun Nisa et al., "TPAAD: Two-Phase Authentication System for Denial of Service Attack Detection and Mitigation Using Machine Learning in Software-Defined Network," *International Journal of Network Management*, vol. 34, no. 3, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[14] Sergii Lysenko et al., "Detection of the Botnets' Low-Rate DDoS Attacks Based on Self-Similarity," *International Journal of Electrical and Computer Engineering*, vol. 10, no. 4, pp. 3651-3659, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[15] Anchal Ahalawat et al., "A Low-Rate DDoS Detection and Mitigation for SDN Using Renyi Entropy with Packet Drop," *Journal of Information Security and Applications*, vol. 68, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[16] Nirzari Patel, and Hiren Patel, "Novel Approach for Ddos Attack Mitigation in Software Defined Network," *Journal of Information Systems Engineering and Management*, vol. 10, no. 30s, pp. 2468-4376, 2025. [CrossRef] [Publisher Link]

[17] Jin Wang, and Liping Wang, "LR-STGCN: Detecting and Mitigating Low-Rate DDoS Attacks in SDN Based on Spatial–Temporal Graph Neural Network," *Computers & Security*, vol. 154, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[18] Pooja Chaudhary, A.K. Singh, and B.B. Gupta, "Dynamic Multiphase DDoS Attack Identification and Mitigation Framework to Secure SDN-Based Fog-Empowered Consumer IoT Networks," *Computers and Electrical Engineering*, vol. 123, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[19] Jishuai Li et al., "DoSGuard: Mitigating Denial-of-Service Attacks in Software-Defined Networks," *Sensors*, vol. 22, no. 3, pp. 1-17, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[20] Wajdy M. Othman, "Implementation and Performance Analysis of SDN Firewall on POX Controller," *2017 IEEE 9th International Conference on Communication Software and Networks*, Guangzhou, China, pp. 1461-1466, 2017. [CrossRef] [Google Scholar] [Publisher Link]

[21] Phan The Duy, Leduy An, and Van Hau Pham, "Mitigating Flow Table Overloading Attack with Controller-based Flow Filtering Strategy in SDN," *Proceedings of the 2019 9th International Conference on Communication and Network Security*, Chongqing China, pp. 154-158, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[22] R. Srivastava et al., "Mitigation of DDoS Attack Instigated by Compromised Switches on SDN Controller by Analyzing the Flow Rule Request Traffic," *International Journal of Engineering & Technology*, vol. 7, no. 2.6, pp. 46-49, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[23] Jisi Chandroth, Byeong-Hee Roh, and Jehad Ali, "Performance Analysis of Python Based SDN Controllers over Real Internet Topology," *2022 Thirteenth International Conference on Ubiquitous and Future Networks*, Barcelona, Spain, pp. 283-288, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[24] Jin Wang, and Liping Wang, "SDN-Defend: A Lightweight Online Attack Detection and Mitigation System for DDoS Attacks in SDN," *Sensors*, vol. 22, no. 21, pp. 1-21, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[25] Faisal Jamil, Harun Jamil, and Abid Ali, "Spoofing Attack Mitigation in Address Resolution Protocol (ARP) and DDoS in Software-Defined Networking," *Journal of Information Security and Cybercrimes Research*, vol. 5, no. 1, pp. 31-42, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[26] Diego S.M. Gonçalves, Rodrigo S. Couto, and Marcelo G. Rubinstein, "A Protection System Against HTTP Flood Attacks Using Software Defined Networking," *Journal of Network and Systems Management*, vol. 31, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[27] Jisa David, and Ciza Thomas, "DDoS Attack Detection Using Fast Entropy Approach on Flow- Based Network Traffic," *Procedia Computer Science*, vol. 50, pp. 30-36, 2015. [CrossRef] [Google Scholar] [Publisher Link]

[28] Amit Kumar Jaiswal, "DOS Attack Network Traffic Monitoring in Software Defined Networking Using Mininet and RYU Controller," *Research Square*, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[29] Yuyang Zhou et al., "Resource-Efficient Low-Rate DDoS Mitigation with Moving Target Defense in Edge Clouds," *IEEE Transactions on Network and Service Management*, vol. 22, no. 1, pp. 168-186, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[30] Mitali Sinha et al., "SynFloWatch: An Entropy-Based Live Defense System against SYN Spoofing DDoS Attacks in Hybrid SDN," *Journal of Network and Systems Management*, vol. 33, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[31] Dan Tang et al., "A Low-Rate DoS Attack Mitigation Scheme Based on Port and Traffic State in SDN," *IEEE Transactions on Computers*, vol. 74, no. 5, pp. 1758-1770, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[32] Thangavel Yuvaraja et al., "Detecting and Mitigating Low-Rate DoS and DDoS Attacks: Multimodal Fusion of Time-Frequency Analysis and Deep Learning Model," *Technical Bulletin*, vol. 31, no. 2, pp. 495-501, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[33] Abdullah Ahmed Bahashwan et al., "HLD-DDoSDN: High and Low-Rates Dataset-Based DDoS Attacks against SDN," *PLoS One*, vol. 19, no. 2, 2024. [CrossRef] [Google Scholar] [Publisher Link]