Information Gain Driven Multi-level DDoS Detection and Mitigation for Software Defined Networks Using Machine Learning

Ph.D. Synopsis

Submitted To

Gujarat Technological University

for the Degree

Of

Doctor of Philosophy

In

Computer/IT Engineering

By

Shroff Jaimin Manharlal

Enrollment No: 189999913043

Supervisor:

Dr. Sanjay M. Shah

Professor & Head

Computer Engineering Department

Government Engineering College, Rajkot, Gujarat.

INDEX

1. INTRODUCTION

1.1 Distributed Denial of Service and Software Defined Networks

The rapid proliferation of Internet-connected gadgets, cloud services, and applications that depend on latency has rendered contemporary networks more susceptible to Distributed Denial of Service (DDoS) assaults. These assaults impair availability by inundating network resources, overloading bandwidth, depleting CPU capacity, and diminishing service performance. Conventional networks, constructed with vertically integrated architectures, lack comprehensive visibility and programmable control, hence complicating real-time DDoS mitigation.

Software-Defined Networks (SDN) is a transformative approach that decouples the control plane from the data plane, facilitating centralized management, programmability, and dynamic policy implementation. This architectural transition presents new security problems, notably the threat of DDoS attacks aimed at the SDN controller, which functions as the network's central intelligence. Consequently, there is a significant demand for intelligent, lightweight, and adaptive DDoS protection techniques that use the programmability of SDN while ensuring real-time performance. This research presents a comprehensive architecture that integrates feature reduction, multi-level detection, and real-time SDN mitigation to tackle these increasing difficulties [1, 2]

1.2 Background and Emergence of SDN

Conventional IP networks depend on decentralized routing and proprietary configurations that necessitate considerable manual intervention and provide restricted insight into overall network performance. The close integration of control and data planes results in network inflexibility, limited innovation, and challenges in implementing new security solutions.

SDN's centralized controller uses software-based policies and switches as OpenFlow-programmed forwarding devices to overcome these limitations. Programmability, dynamic rule implementation, and network-wide flow control are enabled by decoupling. However, centralization risks make the SDN controller a DDoS target. Network incapacitation can result from attackers flooding switches with destructive flows, packet_in messages, or communication channels between switches and controllers [3].Intelligent DDoS defense is essential for ensuring strong SDN functioning. This encompasses real-time surveillance of flow metrics, streamlined feature selection for rapid processing, multi-tier classification of attack intensity, and automated mitigation based on OpenFlow rules. Contemporary high-dimensional datasets like CICDDoS2019 underscore the necessity for effective feature optimization and scalable detection systems. The advent of SDN not only improves network programmability but also requires sophisticated security frameworks that can provide real-

time, adaptive, and resource-efficient DDoS mitigation.

1.3 Motivation

The escalating magnitude and complexity of contemporary DDoS attacks provide a significant risk to network availability, particularly in Software-Defined Networks (SDN), where the centrally managed controller is a primary target. Conventional detection techniques encounter difficulties with high-dimensional traffic, evolving attack patterns, and the necessity for real-time remediation. This research aims to establish an intelligent and efficient framework that minimizes feature complexity, precisely classifies attack severity, and implements timely mitigation in SDN contexts. This work seeks to substantially improve the resilience, speed, and scalability of SDN-based DDoS protection systems by the integration of hybrid entropy-based feature selection, machine learning-based severity prediction, and real-time OpenFlow rule enforcement.

1.4 Problem Statement

Contemporary DDoS datasets, such as CICDDoS2019, have as many as 88 traffic features, resulting in considerable computational burden for real-time categorization within SDN settings. Current methodologies frequently neglect feature optimization, resulting in cumbersome models that falter under extensive, high-velocity live traffic conditions. Furthermore, current approaches produce only binary attack classifications, rendering them unable of differentiating between low-severity and high-severity attack patterns, a crucial criterion for resource-efficient prevention.

Numerous contemporary systems also lack direct interaction with SDN controllers, resulting in delays between detection and mitigation. In the absence of automatic OpenFlow rule deployment, nefarious flows may persist in overburdening the controller or saturating switch flow tables.Therefore, an intelligent DDoS defense framework is required that optimally reduces features using a hybrid sequential method, facilitates multi-level machine learning detection, and implements real-time SDN-based mitigation via the Ryu controller in a Mininet environment.

1.5 Research Objectives

This study seeks to provide an intelligent and efficient DDoS defense framework based on SDN by incorporating optimized feature selection, multi-tier detection, and real-time mitigation within a programmable network context. The precise aims of this study are to:

I. To devise a hybrid entropy-based sequential feature selection methodology that efficiently diminishes high-dimensional DDoS traffic features while maintaining detection accuracy and alleviating computing burden.

II. To develop and assess a multi-tiered machine learning detection framework proficient in accurately categorizing normal traffic, low-severity DDoS attacks, and high-severity DDoS

attacks.

III. To execute real-time SDN-based mitigation through automated OpenFlow rules in the Ryu controller, facilitating adaptive responses such as traffic forwarding, redirection, and port blocking contingent upon attack severity.

IV. To assess the efficacy, scalability, and real-time performance of the proposed architecture utilizing a Mininet-based SDN testbed during active DDoS assault scenarios.

1.6 Contributions of Research

This study presents an extensive SDN-based DDoS defense mechanism that enhances feature optimization, attack classification, and real-time mitigation in programmable networks. This study's principal contributions encompass:

- ✓ Hybrid entropy-based feature selection framework: It is proposed, integrating mutual information and joint entropy in a sequential feature selection technique, resulting in substantial dimensionality reduction while preserving excellent detection accuracy.
- ✓ Multi-Level DDoS Detection Model: A machine learning-driven detection framework that categorizes traffic into normal, low-severity, and high-severity DDoS attacks, facilitating a more nuanced attack evaluation than binary classification models.
- ✓ Real-Time SDN-Integrated Mitigation Mechanism: An automated mitigation strategy based on OpenFlow rules is executed within the Ryu controller, facilitating dynamic actions including traffic forwarding, redirection to honeypots, and port blocking contingent upon the intensity of the attack.
- ✓ Live SDN Testbed Validation: Thorough validation of the proposed framework is conducted on a Mininet-based SDN testbed, showcasing efficient real-time detection, diminished latency, and significant decrease in network outage during active DDoS attacks.

2. LITERATURE REVIEW

2.1 DDoS Attack Landscape

DDoS attacks have evolved from bandwidth floods to complex, global organized campaigns backed by botnets, hijacked IoT devices, and protocol-level amplification. Modern attacks use spoofing, traffic surges, and reflection to drain network, computational, and financial resources. The included materials highlight the increasing frequency, scale, and complexity of DDoS attacks, making conventional defenses insufficient and requiring intelligent, adaptive, SDN-integrated detection systems.

Attackers use flow-setup to flood the control plane of the centralized controller in SDN, according to

Mahmood et al. SDN controller bottlenecks require rapid, automated in-network detection, making conventional defenses insufficient [4]. SDN provides centralized visibility and programmability, but packet-in floods can overload switches and controllers, according to Yan et al. AI-driven detection and dynamic OpenFlow mitigation can counter recent adaptive DDoS techniques [5]. Peng et al. explain how DDoS attacks use botnets, bogus traffic, and poorly constructed amplifiers to overwhelm networks with traffic. Instead of static signatures, the authors recommend entropy-based and behavior-driven analysis to distinguish assaults from flash crowds [6].

2.2 SDN-Based DDoS Detection

The controller's centralized visibility allows SDN-based DDoS detection to examine flow patterns, entropy fluctuations, and traffic data in real time. Entropy-based anomaly detection, statistical thresholding, and ML-driven classifiers can detect rapid flow behavior changes, according to studies. Most techniques have significant false positives, low scalability under bursty traffic, and lack multi-level decision-making for SDN mitigation.

A SDN early detection system for DDoS traffic uses Radial Basis Function (RBF) neural networks optimized by Particle Swarm Optimization and an entropy-triggered alarm, according to Dayal et al. Their findings show improved classification accuracy and controller-based mitigation, but training is expensive and real-time scaling during traffic surges is difficult [7]. The mitigation system SDN-Guard by Dridi et al. dynamically redirects suspect traffic, changes flow timeouts, and consolidates flow rules to reduce controller burden. Experiments show a 32% reduction in controller overhead and TCAM utilization, although the focus is on mitigation rather than detection and relies on IDS threat estimates [8].

Wang et al. develop OF-GUARD, an attack-oriented architecture that eliminates fraudulent traffic before it reaches the controller using packet migration and proactive rule caching. The method protects against control-plane saturation attacks, although it only addresses table-miss flooding attacks and not reflection, volumetric, or protocol misuse DDoS attacks [9]. JESS, the first SDN defensive system using joint entropy for detection and mitigation, dynamically picks optimal attribute combinations to identify abnormalities, according to Kalkan et al. The technology requires ongoing entropy profiling and may increase processing costs in densely populated high-speed networks, but it has excellent accuracy, low overhead, and efficacy against undisclosed attack routes [10].

Through packet-rate and packet-interval homogeneity detection, Lukaseder et al. improve their SDN-based mitigation system to detect and stop slow-rate DDoS attacks. Assessment shows reliable attacker identification without server adjustments, although it requires training and may misidentify legitimate slow customers under network unpredictability [11].

The comparative analysis indicates that the majority of SDN-based DDoS detection research

emphasizes entropy metrics, thresholding, and constrained machine learning models, attaining commendable detection performance while providing solely binary classification. Few methodologies tackle multi-level severity distinction, and the majority lack real-time connection with SDN controllers. This underscores a distinct research deficiency in lightweight, multi-tiered, and SDN-automated detection and mitigation frameworks, which your proposed work seeks to address.

Table 1:Overview of DDoS Detection Literature in SDN Environments

Paper	Proposed Approach	Results	Limitations
Hintaw et al.[12]	Rényi Joint Entropy with Dynamic Thresholding	High detection accuracy across varying traffic rates.	No severity classification and focuses on controller overload.
David et al.[13]	Fast Entropy with Adaptive Thresholding	Improved detection time & lightweight processing.	Binary detection only, limited SDN integration.
Kareem et al.[14]	Entropy Variation on SDN Flow Features	Reduced false positives using entropy-drop detection.	No severity differentiation, threshold sensitive to flash crowds.
Samta et al.[15]	Traffic Pattern Analysis with Mitigation Techniques	Effective SDN performance degradation mitigation.	No multi-level detection.
Ahalawat et al.[16]	Rényi Entropy with Packet Drop	Early detection of low-rate attacks.	Lacks multi-intensity classification and fails when entropy collapses.

2.3 Machine Learning Techniques

SDN categorizes DDoS traffic using flow-level patterns and anomalies using machine learning methods including Random Forest, SVM, Gradient Boosting, Neural Networks, and KNN. Due to high-dimensional input and controller overhead, these models are difficult to process in real time but improve detection accuracy over static threshold-based techniques. Most machine learning-based solutions only classify binary attacks, limiting their severity-aware SDN mitigation.

Ongshua et al.'s hybrid model uses ANN for feature extraction and RF for classification to detect 99.998% of application-layer DDoS datasets. Despite its high accuracy and fast detection, the system mostly uses binary classification and lacks SDN controller integration for severity-aware real-time remediation [17].Combinatorial Fusion Analysis by Owusu et al. integrates many machine learning models using cognitive diversity and rank–score analysis to detect multi-class denial-of-service attacks with improved precision, recall, and F1-score for both low-profile and high-frequency attacks. However, the strategy is computationally intensive and largely evaluated offline without real-time SDN correction [18].Rajkumar et al. introduced a semi-supervised Deep Extreme Learning Machine with SDN-based mitigation to identify DDoS assaults in IoT networks with 99.97% accuracy and increased bandwidth use. The approach reduces labeling and mitigation work but does not classify DDoS attacks by severity [19].

Machine Learning-based DDoS detection has advanced to high accuracy, however most methods lack severity aware classification or real-time SDN-integrated mitigation. As recommended in the study, a lightweight, multi-tiered DDoS detection and mitigation architecture directly coupled to SDN controllers is needed.

Table 2:Comparative Summary of DDoS Detection and Mitigation Techniques in SDN

Paper	Proposed Method	Results (Accuracy)	Dataset	Mitigation Method	Key Limitations
Zhang et al [20].	Hybrid Entropy & SSAE-SVM (HESS)	>98%	SDN traffic, IDS datasets	OpenFlow rule blocking	Binary classification. no severity levels
Najar et al [21].	CNN-based SDN DDoS Detection	98.64%	SDN simulated traffic	Filtering & rate limiting	Expensive computation, no severity mitigating
El-Sayed et al [22].	Multi-layer SD-IoT with ML	98.42%	CICIoT2023, real-time flows	Adaptive SDN based mitigation	Complex architecture; deployment overhead
Gebrye et al [23].	Feature Selection & ML Models	>90%	IoT datasets (IoTID20)	NA	No SDN integration; detection only
Makuvaza et al [24].	DNN-based IDS for SDN	97.59%	CICIDS-2017	Alert-based only	No mitigation; binary classification
Novaes et al [25].	LSTM & Fuzzy Logic	NA	CICDDoS2019	Flow blocking via SDN	No severity classification

2.4 Review of Benchmark Datasets

Diverse datasets have been utilized for DDoS detection research, each presenting unique benefits and drawbacks. A detailed DDoS assault taxonomy and a practical benchmark dataset, CICDDoS 2019, have been presented, encompassing many contemporary reflection-based and flooding attacks spanning the network, transport, and application layers. This dataset offers comprehensive labeled, high-dimensional flow characteristics and facilitates in-depth analysis at both the attack family and severity levels, rendering it very appropriate for machine learning-based DDoS detection studies [26]. A further study suggests a profile-based, testbed-driven approach for producing reproducible and realistic intrusion detection datasets, featuring comprehensive traffic capture and precise attack labeling. This methodology addresses the constraints of static and obsolete datasets by simulating typical network behavior and implementing multi-stage attack scenarios; still, it necessitates intricate experimental equipment and regulated environments [27].

A hybrid dataset has been introduced that integrates authentic modern network traffic with synthetically generated modern attacks within a controlled testbed environment. The UNSW-NB15 dataset enhances realism compared to older datasets and facilitates multi-class intrusion detection; nonetheless, it is not explicitly tailored for large-scale reflected DDoS attacks or comprehensive intensity-level analysis [28].

CAIDA UCSD DDoS 2007 Attack Dataset provides anonymized traffic traces from a major backbone link DDoS attack. The dataset provides significant insight into genuine attack behavior at the packet level, but it lacks flow-based characteristics, comprehensive attack labels, and attack intensity categorization, requiring extensive preprocessing before use in machine learning-based DDoS detection [29].

2.5 Summary of Literature Gaps Identified

An exhaustive examination of current DDoS detection and mitigation studies within SDN settings reveals numerous significant deficiencies. Primarily, most entropy-based detection techniques depend on static or binary thresholding, failing to distinguish the severity levels of DDoS attacks, which is crucial for adaptive mitigation in SDN. Secondly, although most machine learning-based methods get elevated offline accuracy, they frequently utilize high-dimensional features, resulting in augmented processing latency and rendering real-time implementation unfeasible. Third, most current studies fail to closely integrate detection with real-time SDN controller mitigation, leading to delayed or inefficient responses during high traffic surges. Fourth, several studies assess performance exclusively on datasets, with insufficient validation in actual SDN testbeds, neglecting controller overhead, flow-setup latencies, and real-time network dynamics. Ultimately, scant methodologies offer a lightweight, scalable, multi-tiered detection system that correlates attack intensity with various mitigation strategies, hence highlighting a significant research void for a pragmatic, severity-conscious, SDN-native protection solution.

2.6 Scope of Research

The study addresses research gaps by creating an intuitive and efficient multi-level DDoS detection and mitigation framework for SDN environments. The research develops a hybrid entropy-based feature reduction method to reduce high-dimensional DDoS traffic while keeping detection efficacy. The project comprises a machine-learning-based multi-severity classifier that distinguishes normal, low, and high-severity DDoS attacks. An Information Gain-driven, real-time mitigation engine in the Ryu controller is developed by automatic OpenFlow rule implementation.

The proposed framework will be tested on a Mininet SDN testbed during real attacks to assess detection performance, latency, controller overhead, and scalability. The study only covers flow-level SDN traffic, excluding application-layer signatures, deep packet inspection, and distributed multi-controller systems.

3. METHODOLOGY & SYSTEM ARCHITECTURE

3.1 Overview of the Proposed Framework

Figure 1 illustrates the detailed DDoS detection and mitigation technique represented in the model pipeline.

Following the completion of the preprocessing step, the dataset is next subjected to feature selection based on mutual information and hybrid entropy to maintain only the traffic features that are significantly relevant. The selected characteristics are then used in the process of training and evaluating several different machine-learning models, the effectiveness of which is analyzed and compared. The findings of the detection are used to classify the traffic in accordance with the severity of the distributed denial of service assaults. Attacks of low severity are redirected to a honeypot for observation, whilst attacks of high severity are used to elicit immediate mitigation through the blocking of ports.

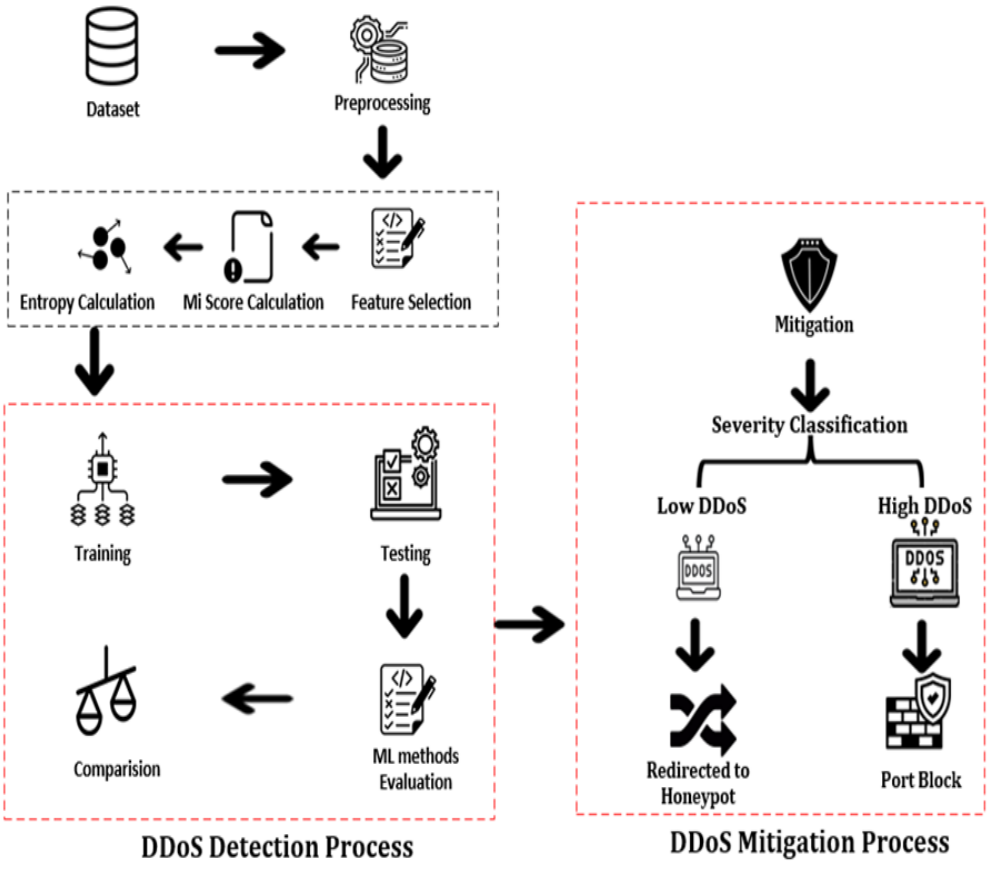


Figure 1:Proposed Model Pipeline

3.2 Sequential Feature Reduction Strategy

The suggested sequential feature selection method integrates Mutual Information score with Joint Entropy analysis to discern the most informative characteristics of network data. Mutual Information

is initially employed to prioritize features according to their significance to the attack class, followed by the application of Joint Entropy to systematically choose characteristics that optimize information gain and reduce redundancy. This guarantees an ideal, concise feature subset for precise and efficient DDoS detection.

Stage 1: Mutual Information (MI) Filtering:

The Mutual Information score $I\ (X;\ Y)$ identifies the relevance between traffic features and attack labels:

$$I\ (X;\ Y)\ =\ \sum_{x\in X}\sum_{y\in Y} p(x,y)\ log\ \frac{p(x,y)}{p(x)P(y)} \tag{1}$$

In this context, p (x, y) signifies the joint probability distribution function of X and Y, while p(x) and p(y) imply the marginal probability distribution functions of X and Y, respectively. The logarithm is typically base 2, signifying that the information is measured in bits.

Stage 2: Joint Entropy-Based Refinement:

Joint entropy measures the combined uncertainty of feature pairs. Joint entropy is defined as $H(X,Y)$:

$$H(X,Y)\ =\ -\sum_{x\in X}\sum_{y\in Y} p(x,y)\log p(x,y) \tag{2}$$

Let p (x, y) be the joint probability distribution function of the random variables X and Y. A revised entropy function H'(X, Y) is created to improve feature selection by integrating mutual information to discern the most relevant characteristics.

The sequential feature selection formula for H'(X, Y) is:

$$H'(X,Y)\ =\ -\sum_{x\in X}\sum_{y\in Y}(p(x,y)+\alpha\ I(X;\ Y))\ log\ p(x,y)+\alpha\ I(X;\ Y) \tag{3}$$

Where:

p (x, y): Original joint probabilities of X and Y.

α: A scaling factor that regulates the impact of mutual information on joint entropy. This ensures only interacting, high-impact feature combinations remain.

3.3 Machine-Learning-Based Classification

Following the sequential feature selection technique, the chosen features are employed to train various supervised machine learning classifiers for efficient traffic categorization. The framework accommodates widely utilized machine learning models, including Random Forest, Support Vector Machine, K-Nearest Neighbors, Gradient Boosting, and Neural Networks. These models analyze flow-level traffic patterns to differentiate between normal traffic and DDoS attacks. In contrast to traditional binary systems, the architecture is engineered to provide multi-level attack comprehension,

allowing for accurate distinction between benign, low-severity, and high-severity DDoS traffic without overwhelming the SDN controller.

3.4 Information Gain Based Mitigation Mechanism

The suggested SDN-based mitigation strategy utilizes an Information Gain (IG) driven decision model to facilitate severity-aware and automated DDoS responses in a SDN context. Utilizing the centralized control and programmability of SDN, mitigation decisions are dynamically implemented at the data plane according to real-time traffic characteristics analyzed at the controller.

Traffic flows are consistently aggregated at the SDN controller from OpenFlow-enabled switches, where packet-level information, particularly the frequencies of source MAC addresses, are gathered during a predetermined observation time. Entropy is initially computed using the aggregated traffic distribution to assess the randomness and uniformity of packet sources. A substantial decrease in entropy signifies traffic aggregation from a restricted number of sources, serving as a critical indicator of possible DDoS activity. The SDN controller continuously aggregates flow statistics and computes entropy H(X):

$$H(X) = -\sum_{j} P_j \log_2 P_j \tag{4}$$

Entropy signifies the unpredictability in source traffic. High entropy indicates typical behavior, but low entropy signifies a potential attack. A subset of suspect sources is chosen based on a low probability of occurrence to enhance the detection process. Conditional entropy is subsequently calculated for this subgroup to evaluate the uncertainty related to aberrant traffic producers.

To compute the conditional entropy suspicious sources as those with Pj < 0.2.

Let A be the set of such sources:

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

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

The distinction between global entropy and conditional entropy produces the Information Gain (IG) value, which measures the degree of irregularity in the observed traffic.

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

According to the established IG value, the parameters α and β denote the upper and lower dynamic thresholds, respectively, with $\alpha \geq \beta$. The observed traffic is categorized into three severity levels based on these thresholds: Normal, Low DDoS, and High DDoS.

$$DDOS\ Level = \begin{cases} Normal\ , & if\ IG \geq \alpha \\ Low\ DDoS\ , if & \alpha < IG < \beta \\ High\ DDoS\ , if\ IG \leq \beta \end{cases} \quad (8)$$

Where the calculation of α and β is given below.

Let μ_N, μ_L, and μ_H denote the mean Information Gain (IG) values of normal, low-severity, and high-severity traffic respectively. The dynamic thresholds α and β are defined as:

$$\alpha = (\mu_N + \mu_L)/2 \quad (9)$$

$$\beta = (\mu_L + \mu_H)/2 \quad (10)$$

This multi-level classification enables proportional mitigation strategies instead of aggressive blanket blocking.

$$DDOS\ Mitigation\ Rule = \begin{cases} Allow\ Traffic\ , & Normal \\ Redirect\ to\ Honeypot\ , & Low\ DDOS \\ Drop\ Packet(Block\ Port), & HighDDoS \end{cases} \quad (11)$$

When traffic is deemed normal, packets are transmitted without limitation. In instances of low-severity DDoS traffic, flows are dynamically rerouted to a honeypot by the implementation of suitable OpenFlow forwarding rules, facilitating isolation and subsequent investigation without interfering with legitimate users. In response to high-severity DDoS attacks, the SDN controller implements rapid blocking at the ingress switch by establishing drop rules or port-level limits to avert controller overload and network resource depletion.

To ensure network availability and avert permanent service interruption, the mitigation architecture includes automated unblocking procedures, wherein mitigation rules are rescinded after a specified timeout via flow deletion. Furthermore, all calculated metrics, encompassing entropy values, Information Gain scores, severity classifications, and mitigation measures, are methodically recorded for monitoring, auditing, and subsequent analysis.

3.5 SDN Testbed Design

To ascertain real-time viability, Figure 2 illustrates the proposed SDN testbed has eight end computers connected via six OpenFlow-enabled switches, with two hosts designated as attacker nodes, one host as the victim, and a specific honeypot implemented for redirecting low-severity attacks. This architecture facilitates detailed traffic monitoring, severity-sensitive attack classification, and instantaneous mitigation decisions at the controller level, thus enhancing responsiveness and minimizing service disruption during DDoS attacks.

To assess the efficacy of the proposed detection system, controlled simulations of both normal and attack traffic were conducted using flows:

- Normal Traffic: Standard ping traffic was produced from benign hosts with default setups.
- Low DDoS Attack: Conducted with the command h1 ping3 -c 500 -d 120 -S -w 64 --rand-source

h8, which transmitted packets at a modest pace with randomized source addresses aimed at the target (h8).

- Severe DDoS Attack: Conducted using h1 ping3 -c 10000 -d 120 -S -w 64 -p 80 --flood --rand-source h8, overwhelming the target with over 100,000 packets per second, significantly reducing entropy and IG (~0).

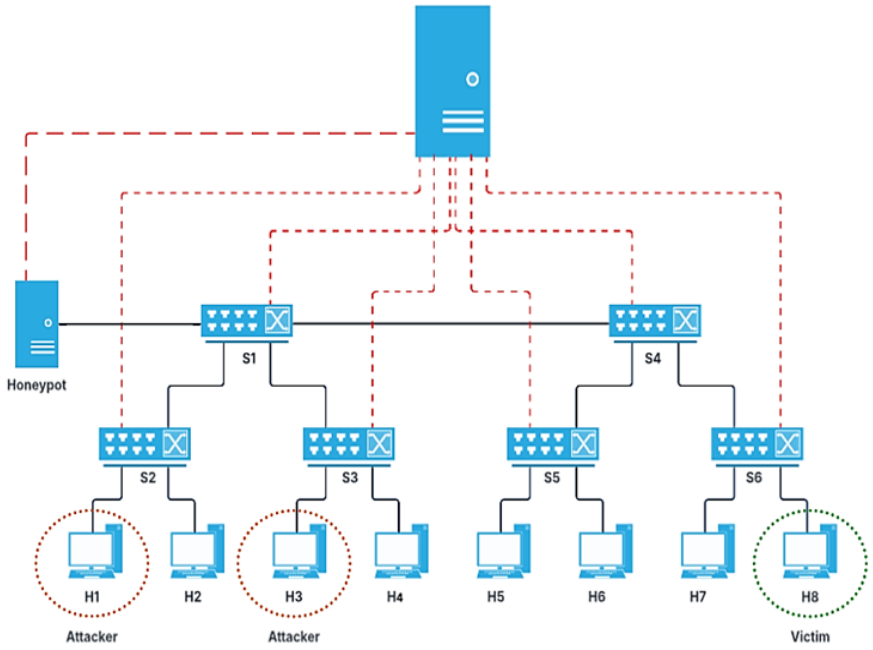


Figure 2: DARTNet-DDoS Attack Response Topology Network.

Following the detection results from the simulated normal and attack traffic flows, the mitigation process is initiated by categorizing the identified traffic based on attack severity and implementing suitable response measures, such as diverting low-severity DDoS flows to a honeypot and obstructing high-severity attack flows at the network level.

- Low Severity DDoS: Characterized by IG values between 0.7 and 1.0, resulting in traffic rerouting to a honeypot.
- High Severity DDoS: Identified by IG $\leq$ 0.4, requiring prompt port blockage on the attacker's switch. The regulation is automatically revoked after a designated BLOCK_DURATION, enabling a smooth restoration.

3.6 Evaluation Metrics and Experimental Procedure

The framework is evaluated using accuracy, precision, recall, F1-score, and processing time. Traffic flows are divided into training and testing sets for fair model learning. The assessment technique evaluates feature selection, classification stability across attack types, and mitigation consistency under changing traffic conditions. The SDN-based protection mechanism's strength and scalability are confirmed by these indications.

Confusion Matrix Parameters:

- True Positive (TP): The count of genuine DDoS attacks flows accurately identified as attacks, signifying proficient detection of malicious traffic.
- True Negative (TN): The count of benign flows accurately recognized as normal, indicating the system's capacity to maintain lawful network operations.
- False Positive (FP): Harmless traffic flows erroneously identified as assaults, resulting in false alarms and possibly unwarranted SDN mitigation measures.
- False Negative (FN): Attack flows erroneously labeled as benign, representing significant flaws that permit hostile traffic to evade detection.

Classification Performance Metrics:

- **Accuracy:** Accuracy evaluates the overall precision of the classification model by determining the ratio of correctly classified attack and benign flows to the total traffic instances.

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN} \tag{12}$$

- **Precision:** Precision quantifies the ratio of accurately detected attack flows to all flows designated as attacks, with elevated values signifying a reduction in false alarms and enhanced reliability in mitigation decisions.

$$Precision = \frac{TP}{TP + FP} \tag{13}$$

- **Recall (Detection Rate):** Recall is the capacity of the detection system to accurately identify genuine attack traffic, which is crucial for averting service damage caused by undetected DDoS flows.

$$Recall = \frac{TP}{TP + FN} \tag{14}$$

- **F1-Score:** The F1-score offers a balanced assessment by integrating precision and recall, rendering it especially appropriates for DDoS detection contexts characterized by class imbalance.

$$F1 - Score = 2 \times \frac{Precision \times Recall}{Precision + Recall} \tag{15}$$

Time-Based Performance Metric:

- $T_{\text{flow arrival}}$**:** The moment when a traffic flow initially arrives at the SDN controller for observation and evaluation.
- $T_{\text{classification}}$**:** The moment when the traffic flow is completely analysed and categorized by the machine learning model.
- **Processing Time:** Processing time is defined as the difference between $T_{\text{classification}}$ and $T_{\text{flow arrival}}$, representing detection and decision latency; lower values confirm the framework's suitability for

real-time SDN deployment.

$$Processing\ Time = T_{Classification} - T_{Flow\ Arrival} \quad (16)$$

The proposed DDoS detection and mitigation framework is comprehensive SDN-based framework integrates sequential entropy-driven feature reduction, multi-level machine-learning classification, and severity-aware SDN mitigation to improve current methods. Modern high-speed SDN systems benefit from the architecture's low computational cost, real-time responsiveness, and adaptive security management.

4. Result and Performance Analysis

The experimental evaluation of the SDN-based DDoS detection and mitigation system utilizing offline datasets and a live SDN testbed. Feature reduction, multi-level machine learning based detection and Information Gain–driven mitigation is tested under different attack intensities. Performance is measured by detection accuracy, severity classification reliability and SDN mitigation effectiveness.

4.1 Sequential Feature Selection Technique Analysis

The sequential feature selection method was tested using the CICDDoS2019 dataset, which includes benign traffic and numerous contemporary DDoS assault types. The labeled flow-based records provide 84 network traffic features, including packet statistics, flow durations, protocol characteristics, and attack identifiers. About 225,000 data instances per assault category provide diversity and scale for reliable evaluation.

Table 3 shows the number of actual features in the dataset and the number of features selected for each DDoS assault type after sequential feature selection. The dataset comprises 84 variables for all attack types, however the findings imply that only a few attributes are needed to accurately describe each DDoS attack. According to the attack approach, the selected features range from 74 to 81, showing that redundant and low-relevance qualities can be removed without affecting discrimination. This reduction shows that DDoS attacks have protocol-specific behavioural patterns, proving that a static feature set is not optimal for all attacks. By selecting the most important variables for each assault while keeping traffic characteristics, the suggested technique reduces processing overhead.

Data pretreatment eliminates non-numerical features and corrects missing or inconsistent records before examination. After that, Mutual Information (MI) scores are produced for each feature to determine its importance in distinguishing normal and attack traffic. These MI scores are used to rank and categorize features into incremental subsets of top 5, top 14, top 35, and the complete selected set to study feature dimensionality and detection efficacy. Joint Entropy analysis is sequentially

applied to MI-ranked features to remove duplicate attributes and preserve class-optimized attack combinations. The table shows how MI and Joint Entropy based selection reduces the initial 84 features to compact and informative subsets while preserving discriminative efficacy across DDoS assault types.

Table 3: Feature Usage in DDoS Attack Detection Methods on Dataset

Type	Actual Feature	Feature after MI Calculation	Feature after Joint Entropy Calculation	No of records
NTP	84	77	57	225001
DNS	84	79	57	225001
LDAP	84	74	54	225001
MSSQL	84	78	55	225001
NetBIOS	84	80	57	225001
SNMP	84	79	56	225001
SSDP	84	75	55	225001
UDP	84	79	57	235236
UDP-Lag	84	79	56	225001
SYN	84	76	55	225001
TFTP	84	81	56	225001

To evaluate feature interaction beyond singular relevance, an entropy-based analysis is conducted employing six recognized entropy methodologies: Shannon entropy, Renyi entropy, Tsallis entropy, Bhatia-Wolf entropy, Bhattacharya coefficient, and the Ubriaco technique. The suggested method enhances this analysis by calculating joint entropy, which encapsulates the collective informational contribution of many traits instead of considering them in isolation. The sequential joint entropy assessment constitutes the foundation of the suggested feature selection methodology.

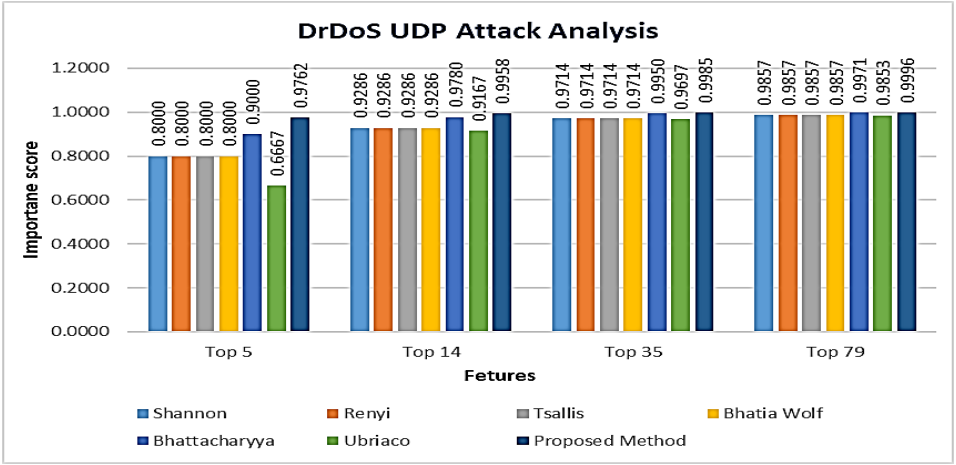
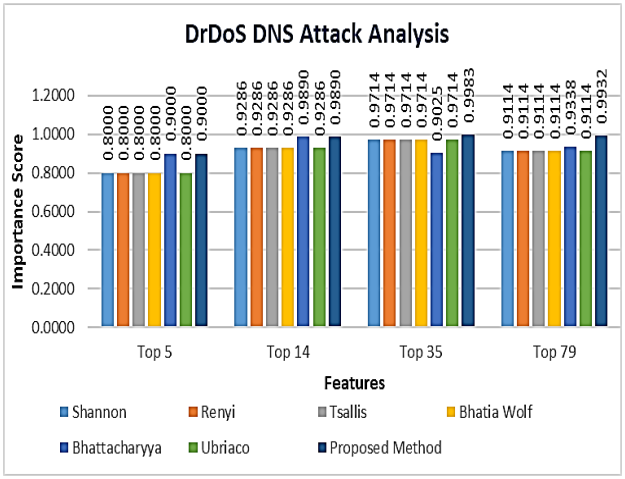


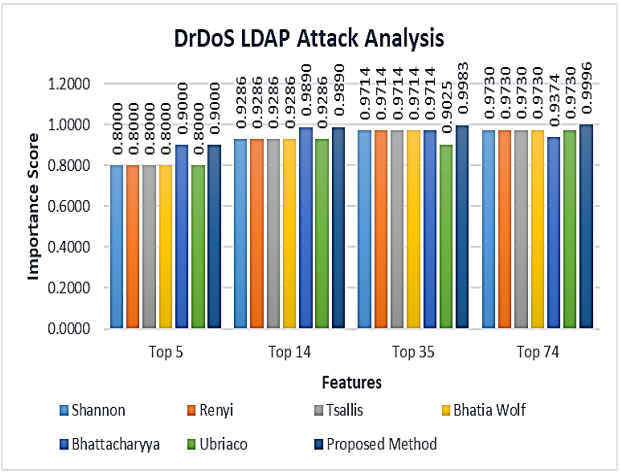
Figure 3: DrDoS UDP Attack Analysis

Figure 3 indicates that conventional entropy metrics exhibit moderate efficacy in assessing individual features or small subsets thereof. In UDP-based DDoS attacks, the significance score for the top five

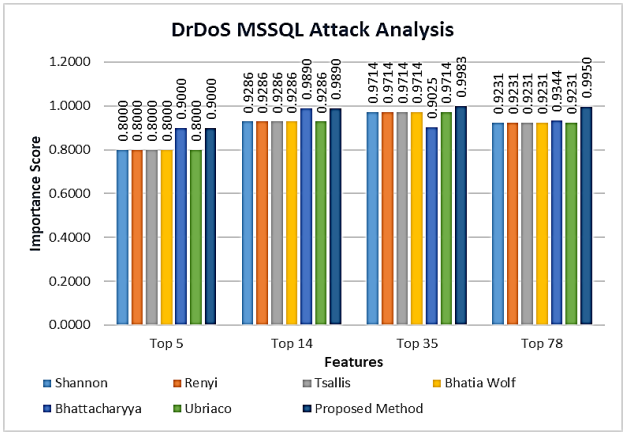
features, as determined by Shannon, Renyi, Tsallis, and Bhatia-Wolf entropy, consistently approximates 0.80, but the Ubriaco technique produces a diminished score of roughly 0.66. While the Bhattacharya coefficient achieves a commendable score near 0.90, the suggested joint entropy technique markedly enhances the score to roughly 0.97, underscoring its superior capacity to capture feature interdependencies.



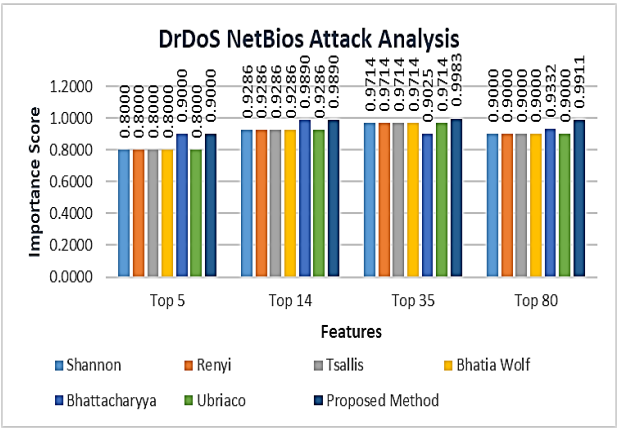
(a)



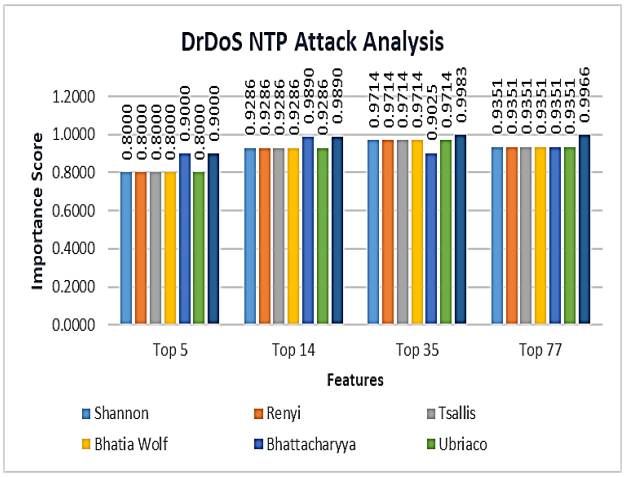
(b)



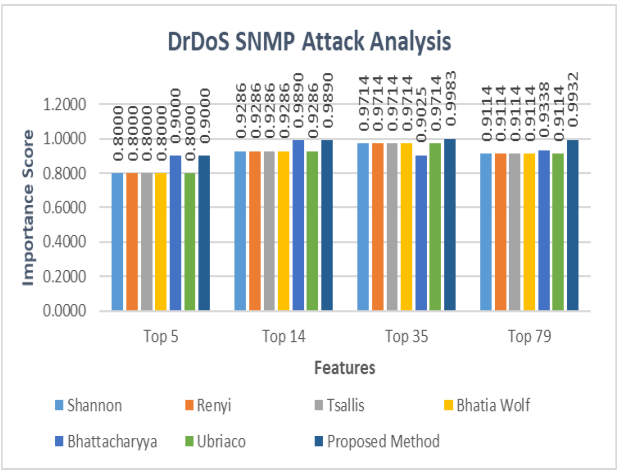
(c)



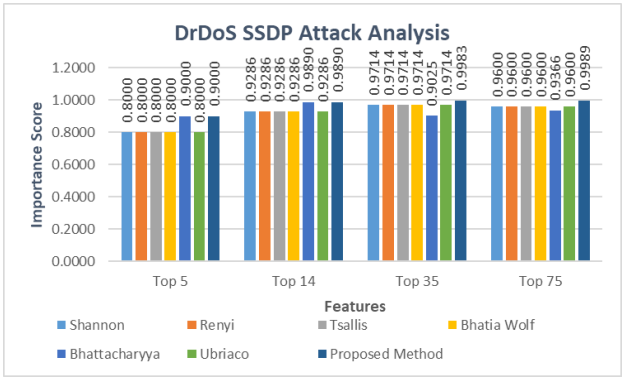
(d)



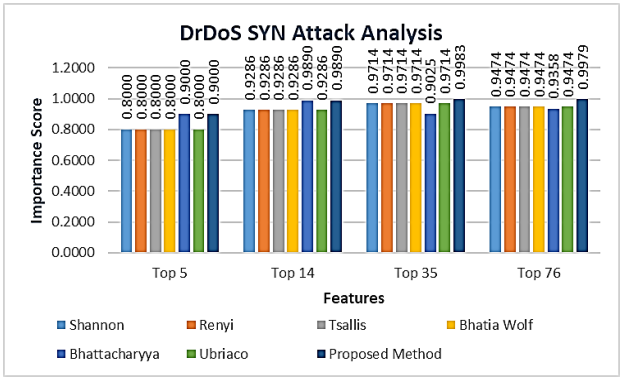
(e)



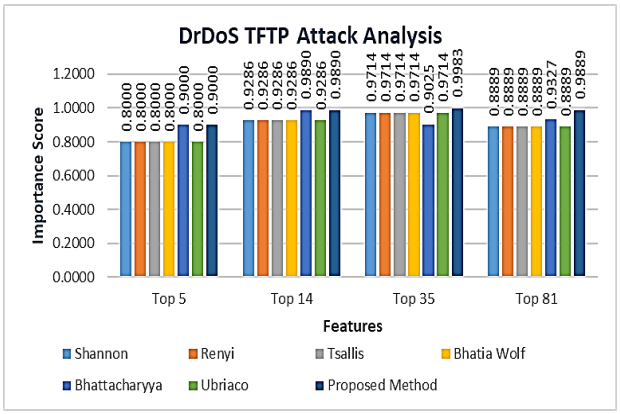
(f)



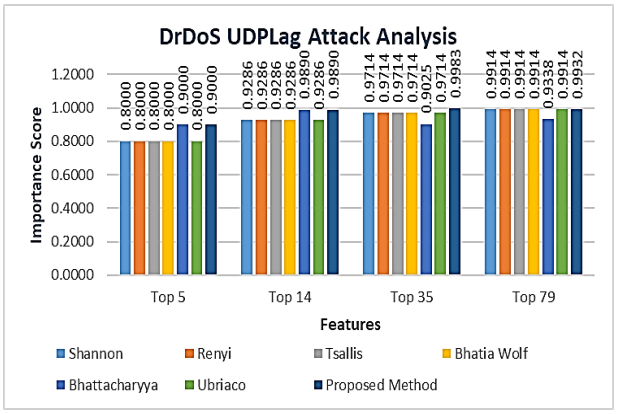
(g)



(h)



(i)



(j)

Figure 4: (a-j) Various DrDoS Attack Analysis on Dataset

As shown in Figure 4 (a-j) Comparable performance patterns are noted across several attack types, including DNS, LDAP, MSSQL, NetBIOS, NTP, SNMP, SSDP, SYN, TFTP, UDP, and UDP-Lag. In almost all instances, the suggested joint entropy-based method consistently attains superior feature importance scores relative to the six baseline entropy strategies. The uniformity across many protocols confirms the strength and broad application of the suggested feature selection mechanism. The findings indicate that the suggested sequential mutual information and joint entropy-based feature selection method efficiently discovers compact and highly informative feature subsets for various DDoS assault types. The suggested method surpasses traditional entropy-based approaches by capturing both individual feature significance and collective feature interactions.

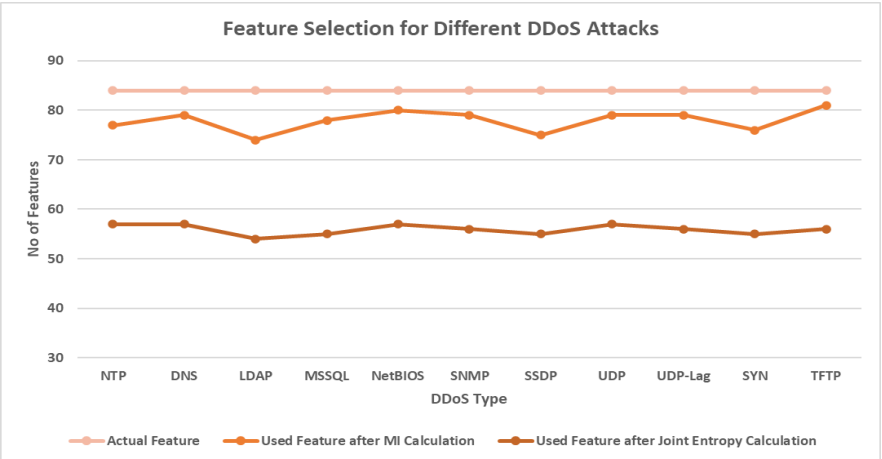


Figure 5: Selected features of different DrDoS attack on Dataset

4.2 Comparative Analysis with Existing Machine Learning Methods

This section provides a comparative assessment of the proposed detection framework related to existing machine learning-based methodologies, highlighting the influence of sequential feature selection and entropy driven feature refinement on detection efficacy across various DDoS attack types.

4.2.1 Selected Features on Dataset

The original dataset has 80–90 features spanning multiple DrDoS attack categories, as shown in Figure 5 MI-based feature assessment reduces relevant features to 70–80, removing non-informative properties. Next, the joint entropy-based technique reduces the feature set to 50–60 characteristics, keeping only the most discriminative combinations. This progressive decreases speeds processing and enhances detection system efficacy, which is crucial for real-time SDN settings.

4.2.2 Comparative Analysis of Machine Learning Algorithms on the Dataset

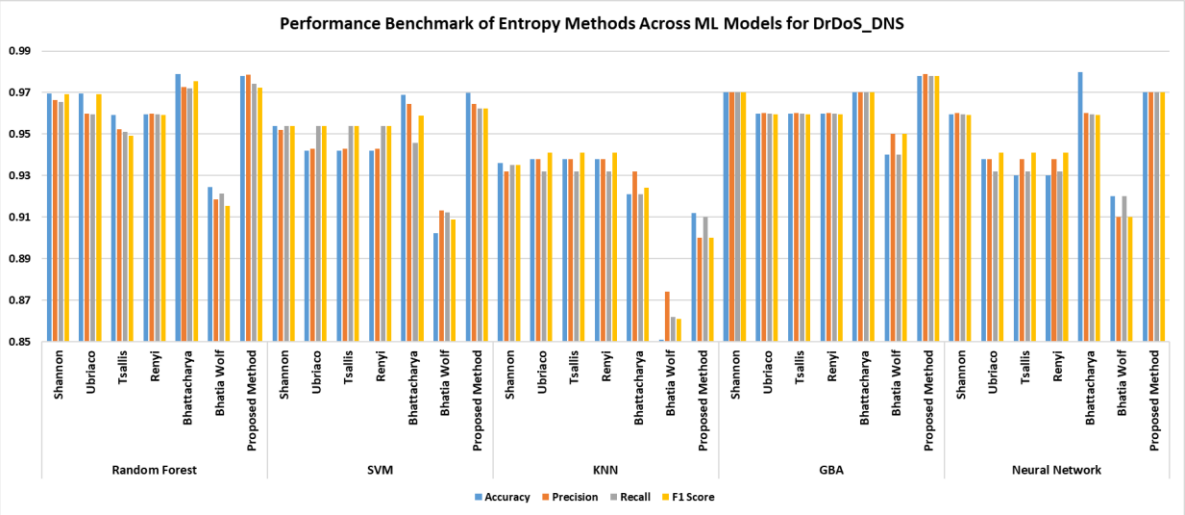
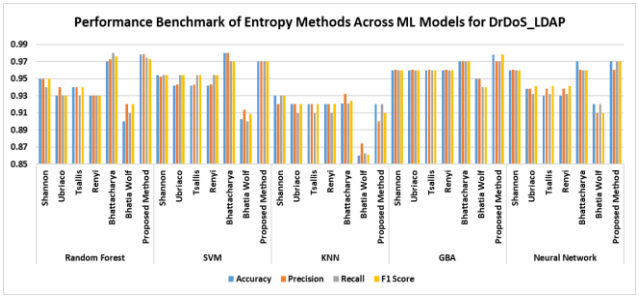


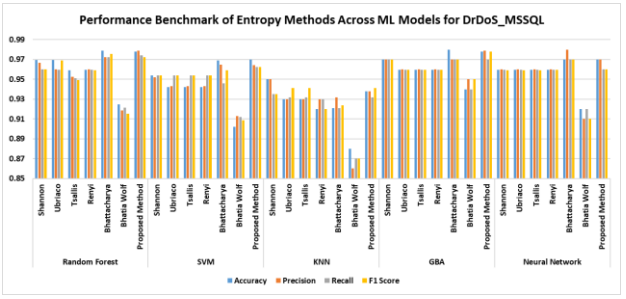
Figure 6: Performance Comparison of Entropy Methods Across ML Models for DrDoS_DNS

Entropy-based feature selection techniques are used to compare DrDoS DNS assault performance in Figure 6 Traditional entropy approaches like Shannon, Ubriaco, Tsallis, and Rényi perform similarly across most classifiers.

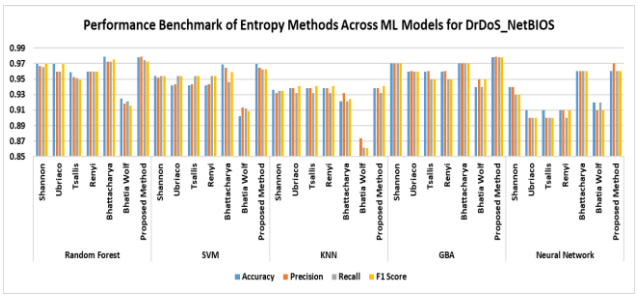
All evaluation metrics show higher results with the Proposed Joint Entropy-based Method. With the provided technique, Random Forest has the best detection performance, with Accuracy, Precision, Recall, and F1-score values over 0.97. This shows a strong ability to understand complex traffic patterns and detect DDoS attacks. Though somewhat behind Random Forest in recall and F1-score, Neural Networks perform well. SVM and GBA perform intermediately, but KNN constantly scores lowest, indicating its vulnerability to feature dimensionality and class overlap.



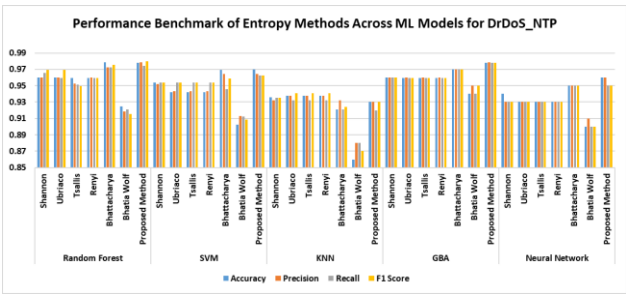
(a)



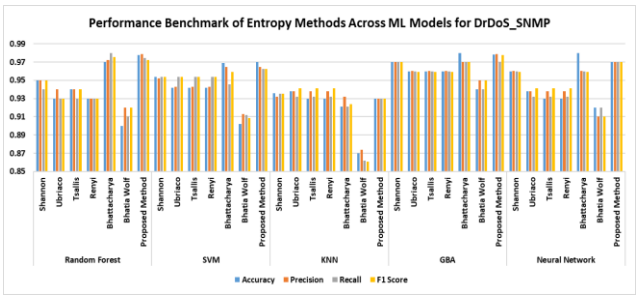
(b)



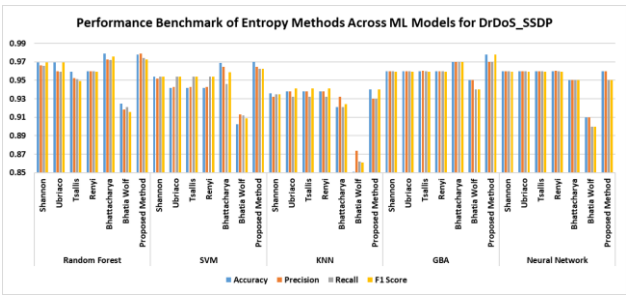
(c)



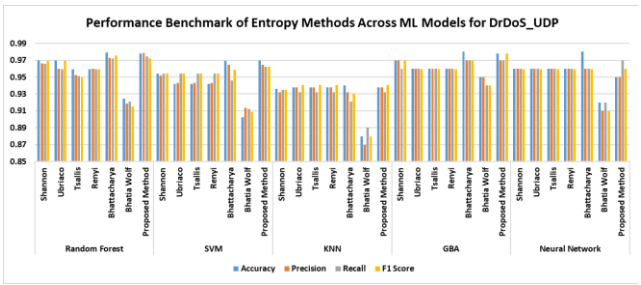
(d)



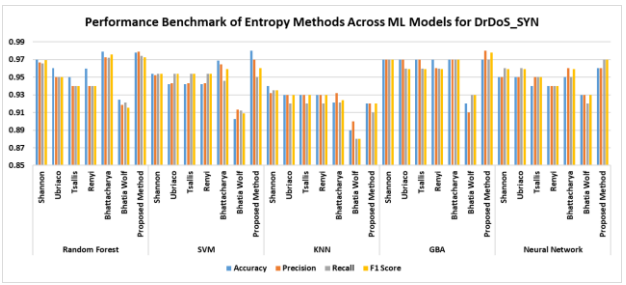
(e)



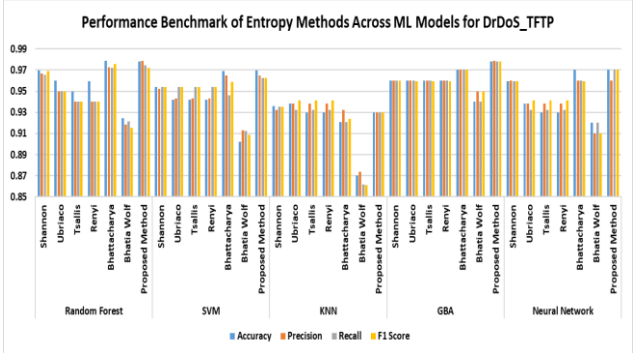
(f)



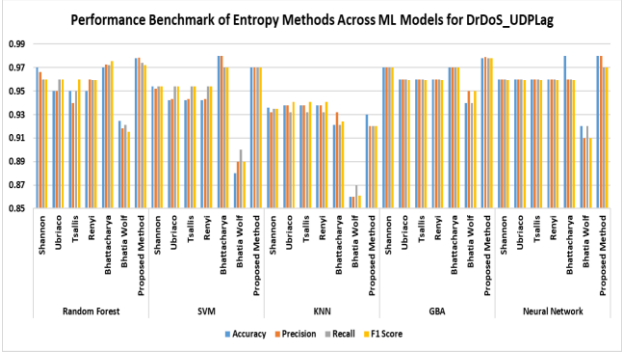
(g)



(h)



(i)



(j)

Figure 7 (a-j): Performance Comparison of Entropy Methods Across ML Models for Various DrDoS

Figure 7 (a-j) shows all machine learning models show that the Proposed Joint Entropy-based method

outperforms Shannon, Rényi, Tsallis, Ubriaco, and Bhatia-Wolf for all DrDoS attack types, including LDAP, MSSQL, NTP, SNMP, SSDP, SYN, TFTP, and UDP-Lag. Random Forest is the best classifier, with excellent Accuracy, Precision, Recall, and F1-score (typically above 0.97). Neural Networks are competitive but somewhat lower. KNN has poor recall, especially in high-frequency or burst attacks, compared to SVM and Gradient Boosting. The results demonstrate the architecture's robustness, generalizability, and attack-agnostic efficacy in various DrDoS attack scenarios.

Table 4: Processing Time of various DrDoS Attacks on Dataset

DrDoS Type	RF	NN	SVM	KNN	GBA
DNS	Fast	Fast	Slowest	Moderate	Moderate
NTP	Moderate	Fast	Slowest	Slow	Slow
SNMP	Fast	Fast	Slowest	Slow	Moderate
SSDp	Fast	Fast	Slowest	Slowest	Slow
TFTP	Fast	Fast	Slowest	Slowest	Moderate
UDP-Lag	Fast	Fast	Slow	Slowest	Slow
LDAP	Fast	Fast	Slowest	Slow	Moderate
NetBIOS	Fast	Fast	Slow	Slow	Moderate
MSSQL	Fast	Fast	Slowest	Slow	Slow
UDP	Moderate	Fast	Slowest	Slowest	Slow
SYN	Fast	Fast	Slowest	Slow	Moderate

Mapping Logic	
Less than 20 seconds	Fast
Between 21 to 35 seconds	Moderate
Between 36 to 65 seconds	Slow
Greater than 65 seconds	Slowest

In all machine learning models show that the Proposed Joint Entropy-based method outperforms Shannon, Rényi, Tsallis, Ubriaco, and Bhatia-Wolf for all DrDoS attack types, including LDAP, MSSQL, NTP, SNMP, SSDP, SYN, TFTP, and UDP-Lag. Random Forest is the best classifier, with excellent Accuracy, Precision, Recall, and F1-score (typically above 0.97). Neural Networks are competitive but somewhat lower. KNN has poor recall, especially in high-frequency or burst attacks, compared to SVM and Gradient Boosting. The results demonstrate the architecture's robustness, generalizability, and attack-agnostic efficacy in various DrDoS attack scenarios.

Table 4 processing-time analysis shows that machine-learning algorithms recognize DDoS attacks at varied speeds among DrDoS traffic categories. Due to its parallel decision structure and low inference

delay, Random Forest (RF) detects all threats quickly, making it ideal for real-time SDN scenarios. Neural Networks (NN) detect most assaults and UDP-Lag scenarios quickly, although their processing costs may increase with model depth and traffic volume. Due to its high computing complexity during categorization, SVM detects all attack categories slowly. Due to its reliance on distance computations throughout the dataset, KNN takes a long time to process SSDP and UDP-Lag assaults. GBA is slower than RF but balances speed and accuracy. On large, high-rate datasets, Random Forest provides the most reliable and scalable detection speed, making it the best choice for real-time DDoS detection.

4.3 Live Testbed Performance Evaluation

The live simulation demonstrates the real-time operation of the proposed Information Gain-driven DDoS detection and mitigation framework implemented using Mininet and the Ryu SDN controller.

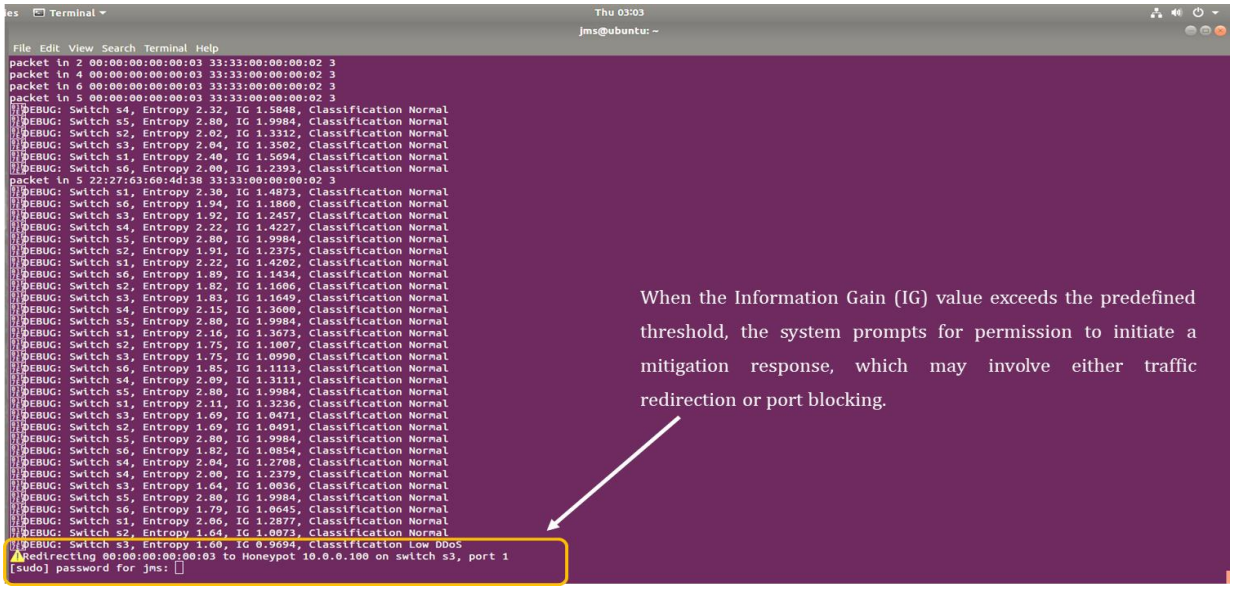


Figure 8:RYU-Mininet Simulation Environment Normal Traffic

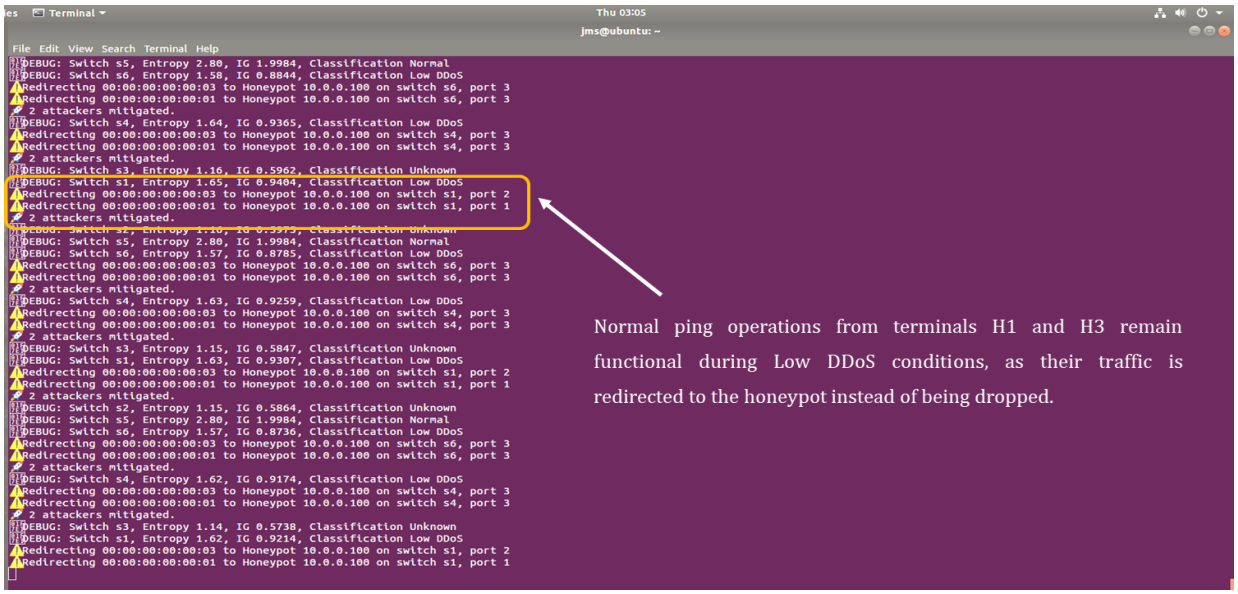


Figure 9: Low DDoS Detection

Figure 8 illustrates standard traffic behavior, where entropy levels stay elevated, and IG does not exceed the established adaptive thresholds. The controller logs indicate that traffic is categorized as Normal, and no mitigation measures are implemented. ICMP ping traffic from hosts (H1, H3) continues unimpeded, indicating that the framework does not obstruct genuine network connection under benign settings. Upon the commencement of a low-intensity DDoS attack, the IG value experiences a minor decline yet remains above the high-severity threshold, as illustrated in Figure 9. The controller categorizes the traffic as Low DDoS and dynamically implements OpenFlow redirection rules. The logs indicate that suspect traffic is diverted to the honeypot, whilst legal traffic proceeds uninterrupted.

The ping outputs from H1 and H3, as illustrated in Figure 10, corroborate this behavior, remaining operational throughout the attack. The redirection technique facilitates the isolation of attack traffic without interrupting services, hence confirming the efficacy of severity-aware mitigation.

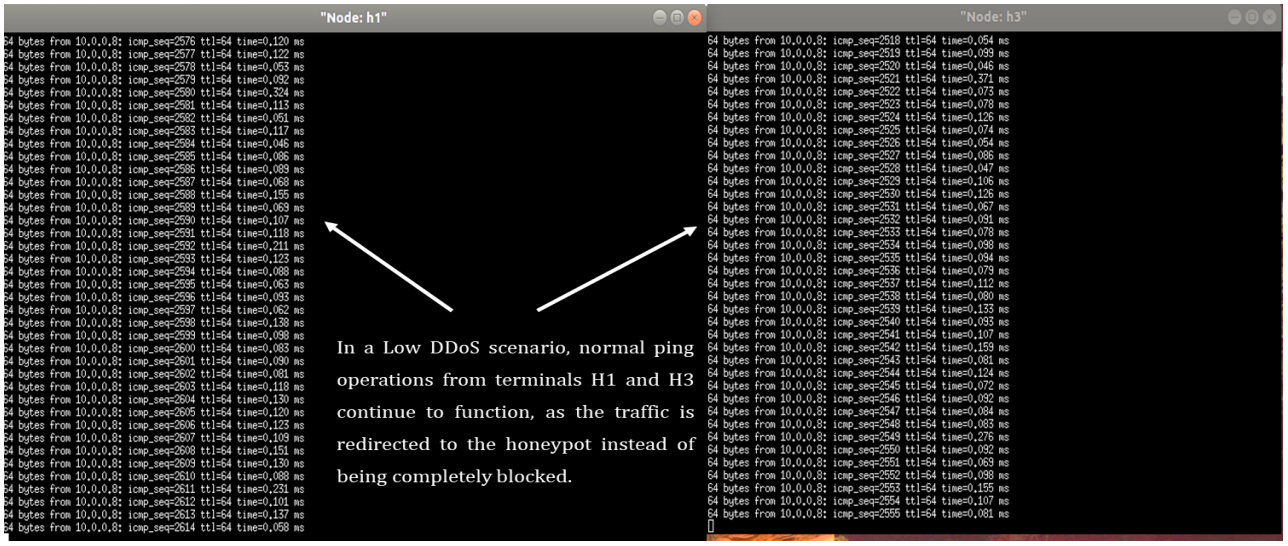


Figure 10:Ping output from H1 and H3 during Low DDoS

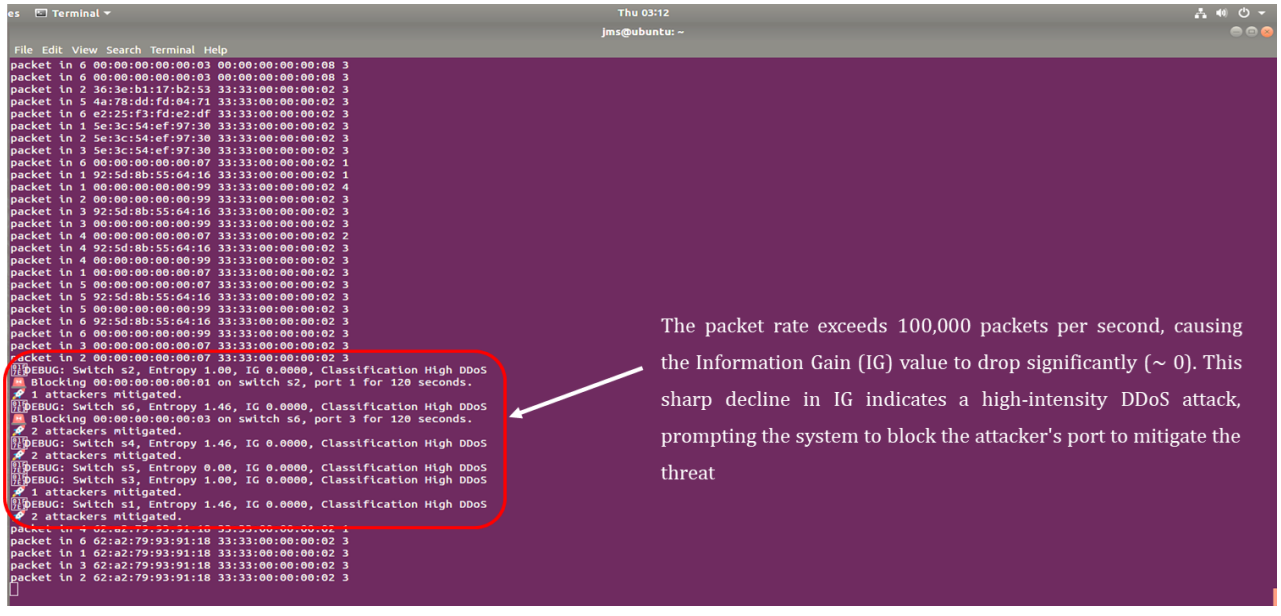


Figure 11:High DDoS Detection

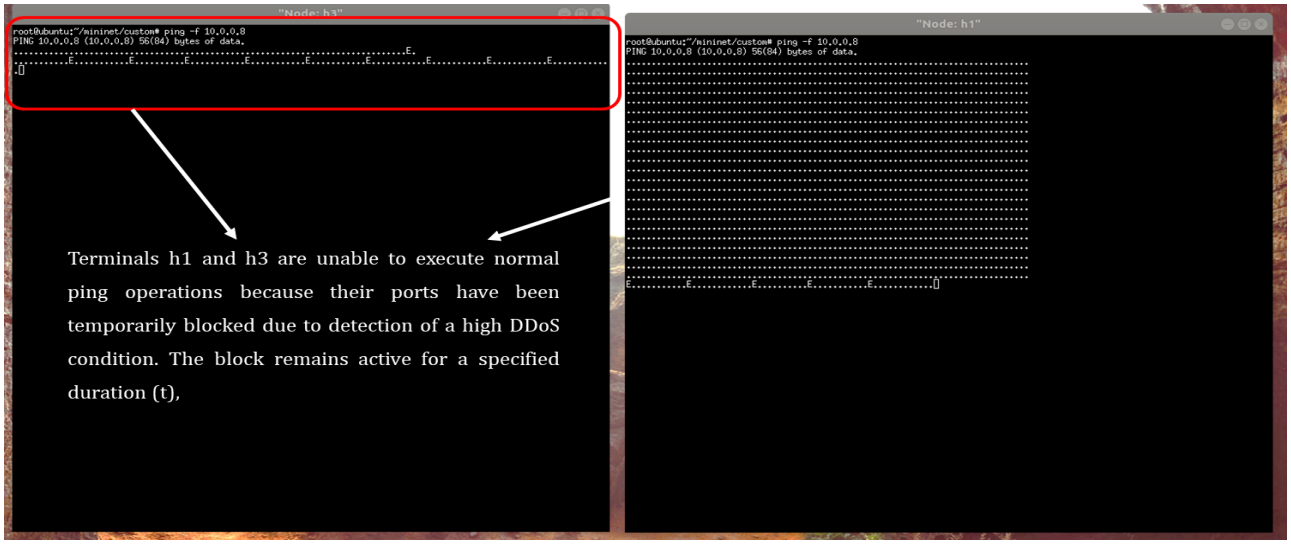


Figure 12:Ping output from H1 and H3 during High DDoS

Figure 11 illustrates a severe DDoS situation, where the packet rate surpasses around 100,000 packets per second, resulting in a significant decline in entropy and an almost negligible IG value. This substantial decreases warrants classification as High DDoS. The SDN controller promptly implements port-level blocking through OpenFlow drop rules. Figure 12, illustrates that terminal outputs and ping requests from compromised sites yield Destination Host Unreachable signals, thereby validating the successful blockage of the attacker's port. This swift reaction averts controller overload and network congestion.

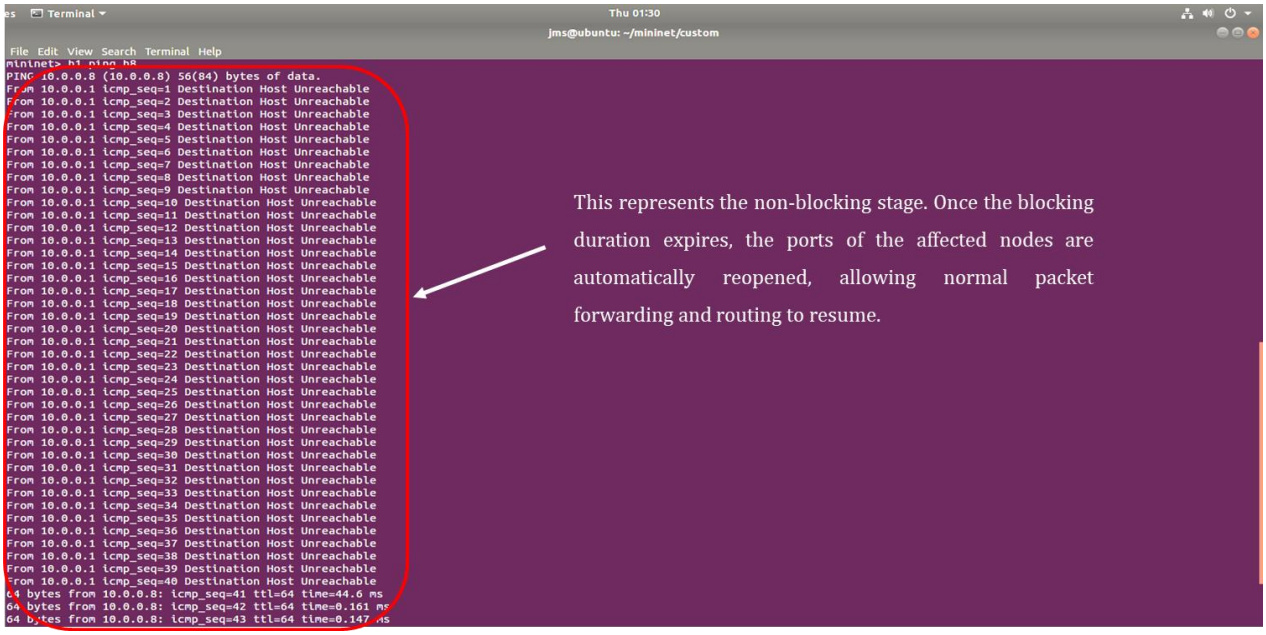


Figure 13: Automated time-based Unblocking

Time-limited blocking prevents persistent service denial in Figure 13 After the blocking duration, the controller automatically removes drop rules. As shown in the screenshots, ping traffic returns to normal after the rule expires. This proves the framework supports automated recovery and self-healing.

The live simulation shows that the proposed framework detects DDoS attack intensity in real time

and uses proportional mitigation. Honeypot redirection prevents low-severity assaults from interrupting genuine users, while high-severity attacks are prohibited to safeguard SDN resources. The suggested SDN-based protection mechanism's smooth transition between mitigation modes and automated unblocking shows its reliability.

4.3.1 Live Traffic Feature Selection Results

As shown in Figure 14, The suggested sequential feature selection strategy greatly decreases the number of features utilized for live ICMP, TCP, UDP, and SYN DDoS detection. Mutual Information selection decreases the live traffic feature set from seven raw features to four to five, and joint entropy refinement further reduces it to two dominating features. This significant reduction shows that the suggested strategy reduces duplicate and weakly informative features, speeding processing and lowering SDN controller overhead without affecting detection.

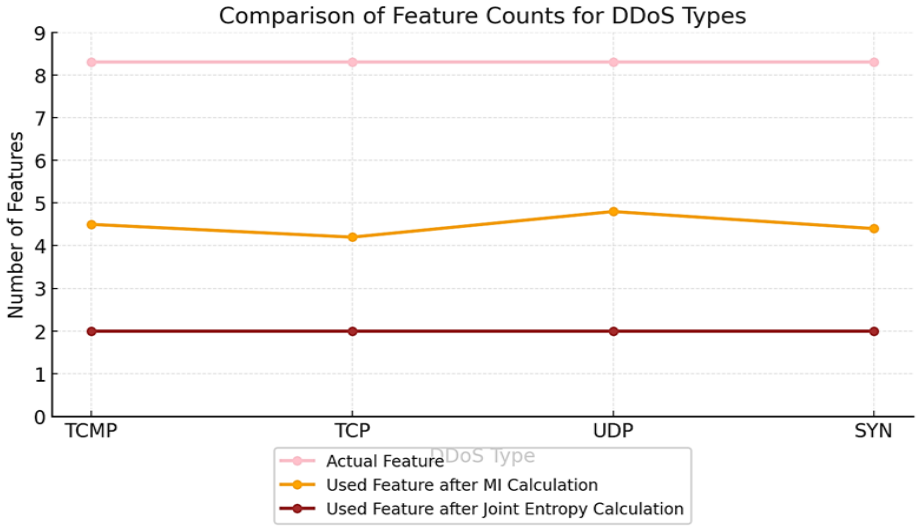


Figure 14:Selected feature of different DrDoS attack on Live Traffic

Figure 15(a) and (b) illustrate the live-traffic performance comparison for DDoS_ICMP and DDoS_SYN attacks utilizing the diminished two-feature set. The Random Forest classifier regularly attains superior Accuracy, Precision, Recall, and F1-score, nearing optimal performance in both attack scenarios. KNN and Neural Networks exhibit comparable performance, although display a marginal decline in recall during SYN flooding. SVM and Gradient Boosting demonstrate significantly diminished performance, suggesting susceptibility to feature sparsity and fluctuations in traffic dynamics.

Figure 15 (c) and (d) depict the detection performance for DDoS_TCP and DDoS_UDP live traffic. Comparable tendencies are noted, with Random Forest consistently surpassing all other classifiers across all assessment metrics. Neural Networks offer consistent, albeit somewhat worse performance, whereas KNN demonstrates adequate efficacy for UDP traffic but deteriorates with TCP traffic. Gradient Boosting and SVM exhibit relatively inferior recall and F1-scores, especially under variable

traffic conditions.

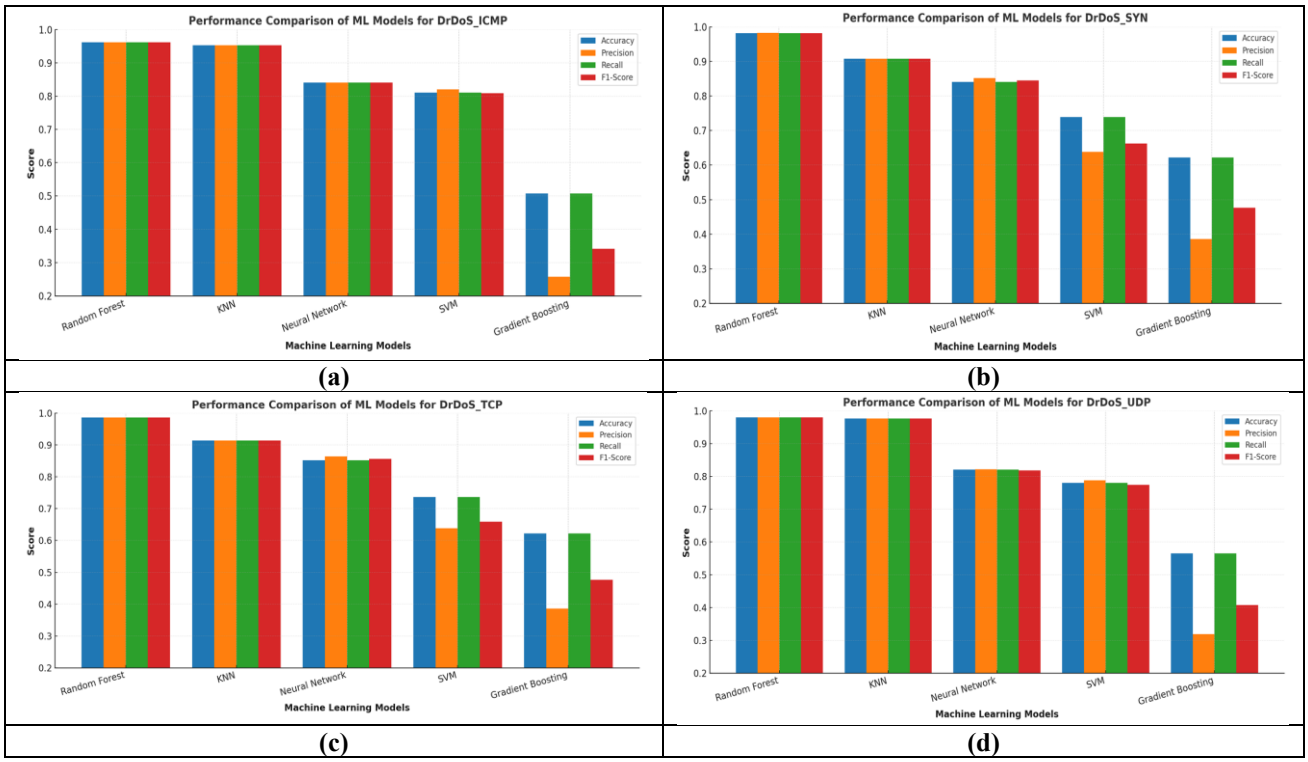


Figure 15 (a-d): Performance Comparison of Different ML Models on various Live DDoS Traffic

Table 5:Processing Time of various DrDoS Attacks on Live Traffic

DDoS Type	RF	NN	SVM	KNN	GBA
ICMP	Moderate	Moderate	Slowest	Slow	Moderate
SYN	Fast	Fast	Moderate	Fast	Fast
TCP	Fast	Fast	Moderate	Fast	Fast
UDP	Moderate	Moderate	Slow	Fast	Fast

Mapping Logic	
Between 0.04 to 0.30 seconds	Fast
Between 0.30 to 1.5 seconds	Moderate
Between 1.5 to 3.0 seconds	Slow
Greater than 3.0 seconds	Slowest

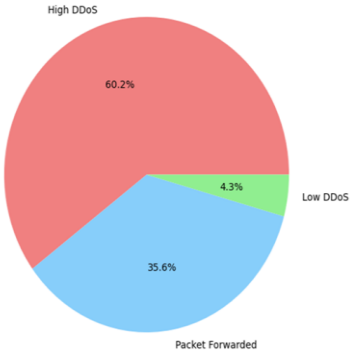
Processing time on real data shows that machine learning models for different DDoS attack types (ICMP, SYN, TCP, and UDP) have varied detection latency. Neural Networks (NN) and Gradient Boosting Algorithms (GBA) detect ICMP and UDP threats quickly, demonstrating effective dynamic flow pattern control. Random Forest (RF) performs well for TCP traffic but has modest overhead for ICMP, SYN, and UDP owing to ensemble evaluation. KNN has a moderate processing time due

to distance-based computations on live data streams, while SVM has a slow to high processing time across all attack types, indicating its computational complexity in real-time circumstances. Neural Networks (NN) and Random Forests (RF) achieve the best balance between detection speed and accuracy, making them better for real-time SDN-based DDoS detection than SVM and K-Nearest Neighbors.

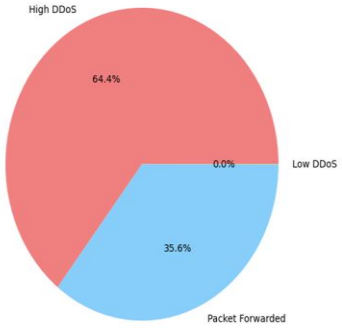
4.4 Multi-Level DDoS Mitigation Strategy:

4.4.1 Strategy Distribution for Dataset

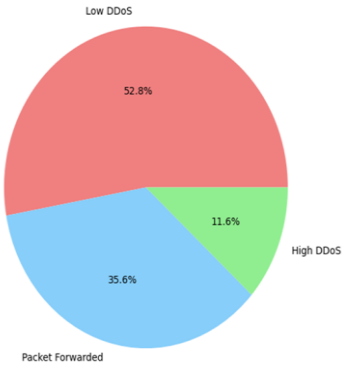
The suggested multi-tier detection system proficiently categorizes traffic into normal, low-severity DDoS, and high-severity DDoS, facilitating adaptive mitigation strategies within the SDN controller. Figure 16 (a-k), illustrates that a substantial amount of traffic is accurately classified as low-severity attacks, which are diverted to the honeypot, whilst high-intensity DDoS traffic is vigorously obstructed, safeguarding network resources. This technique maintains service continuity and security by continually forwarding approximately one-third of valid traffic while dynamically mitigating attack traffic according to severity levels.



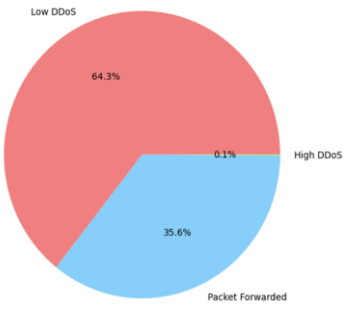
(a) DrDoS_DNS Attack



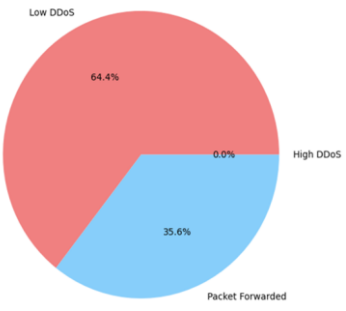
(b) DrDoS_LDAP Attack



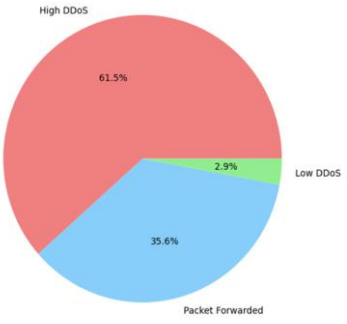
(c) DrDoS_MSSQL Attack



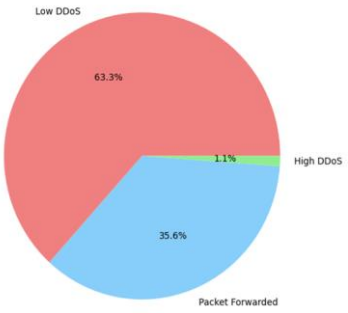
(d) DrDoS_NetBIOS Attack



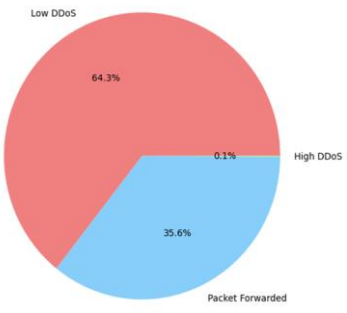
(e) DrDoS_NTP Attack



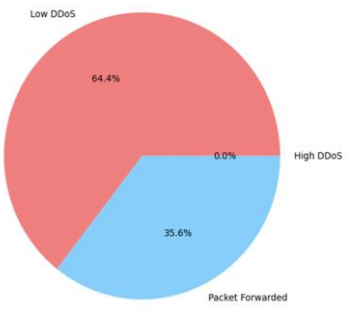
(f) DrDoS_SNMP Attack



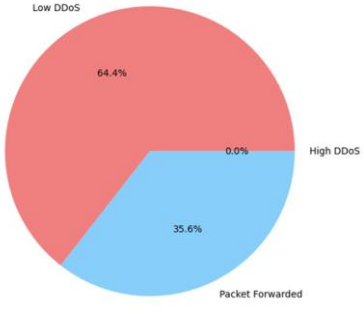
(g) DrDoS_SSDP Attack



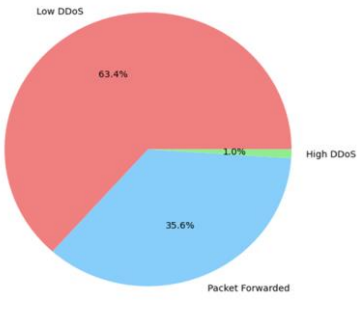
(h) DrDoS_UDP Attack



(i) DrDoS_SYN Attack



(j) DrDoS_TFTP Attack



(k) DrDoS_UDP-Lag Attack

Figure 16 (a-k):Strategy Distribution of Various DrDoS for Dataset

4.4.2 Strategy Distribution for Live Traffic

The actual traffic data demonstrates the efficacy of the proposed multi-tier DDoS detection and mitigation scheme within a real SDN context. The DDoS level distribution graphs indicate that most traffic is accurately recognized as normal, while significant segments are categorized as low-severity and high-severity DDoS attacks, hence validating the model's responsiveness to differing assault intensities in real network environments.

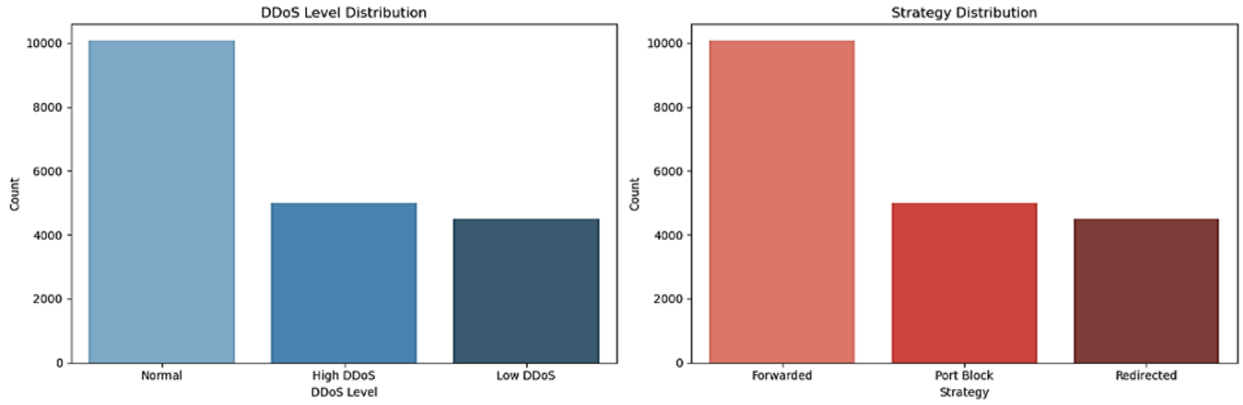


Figure 17:DDoS level and Strategy Distribution of Live DDoS_ICMP Traffic

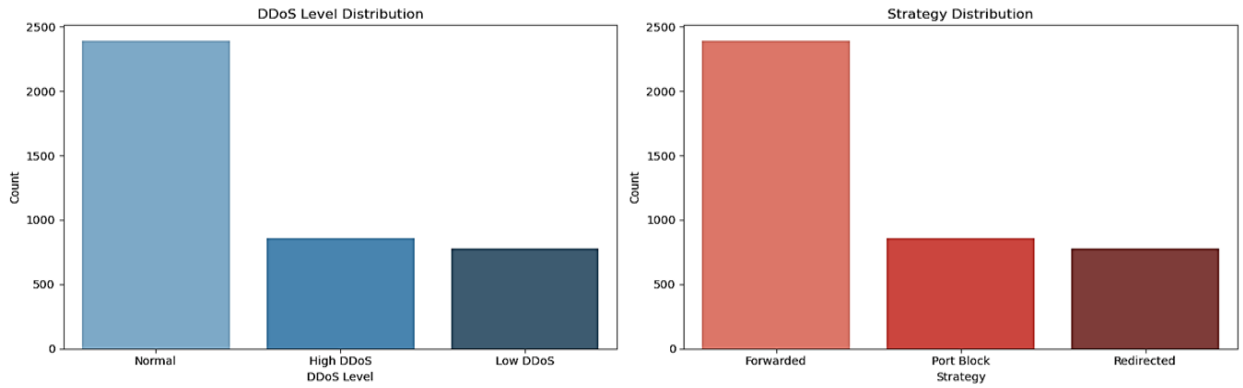


Figure 18:DDoS level and Strategy Distribution of Live DDoS_SYN Traffic

The Strategy Distribution graph mentioned in Figure 17 and Figure 18 depicts the mitigating steps implemented by the SDN controller in response to the identified DDoS severity. Most of the standard traffic is transmitted as usual, guaranteeing continuous network operation. Traffic categorized as Low DDoS is primarily diverted to the honeypot for controlled investigation without service interruption, whereas High DDoS traffic is addressed with port blocking. The evident correlation between detection levels and mitigation tactics in the accompanying graphs confirms that the proposed system executes adaptive, severity-aware mitigation, preserving network availability while efficiently countering active DDoS attacks.

4.5 Discussion on Results

The CICDDoS2019 dataset and live SDN testbed show that the proposed system detects and mitigates DDoS accurately, scalable, and in real time. The sequential feature selection method reduced feature dimensionality while maintaining discriminative efficacy, speeding processing and improving detection stability. The new joint entropy method consistently delivered higher feature significance ratings than conventional methods, proving its ability to capture significant feature interactions.

Random Forest was the most successful DrDoS attack model, with over 97% accuracy, precision, recall, and F1-score and low detection delay. Compared to SVM, KNN, and GBA, neural networks performed better. Live testbed assessments showed that Random Forest might improve detection accuracy with only two attributes per protocol. The Information Gain-based multi-level mitigation technique distinguished normal, low-severity, and high-severity assaults, executing appropriate SDN mitigation. Low-intensity assaults were routed to a honeypot without interfering with lawful traffic, whereas high-intensity assaults initiated rapid port blocking to prevent controller overload. Service continuity maintained by automatic unblocking. The findings show that the proposed architecture provides reliable, efficient, and flexible protection for modern SDN settings.

5. CONCLUSION

This study proposed an innovative, multi-tiered DDoS detection and mitigation solution for Software-Defined Networks. Using Mutual Information and Joint Entropy, a sequential feature selection strategy reduced feature dimensionality by 71% while preserving discrimination. Despite significant feature reduction, the system maintained 97% detection accuracy, showing that redundant and unimportant features may be removed without affecting performance.

Random Forest, Neural Network, Gradient Boosting Algorithm, K-Nearest Neighbors, and Support Vector Machine were trained on the optimized feature set to test identification skills. Random Forest was the most reliable classifier, with 97.8% accuracy and nearly 98% recall, making it ideal for real-time SDN scenarios. The comparison investigation showed that feature optimization greatly increases model efficiency and stability across attack types.

Multi-level mitigation was used on a live SDN testbed using Ryu and Mininet to validate the proposed architecture. Automatic OpenFlow-based port blocking neutralized high-severity DDoS activity, while low-severity traffic was dynamically diverted to a honeypot. The adaptive mitigation method ensured service continuity for authorized users and reduced network downtime by over 85% during active DDoS attacks. Gradient Boosting Algorithm had the fastest processing time, followed by Random Forest, which had 20% less latency than Support Vector Machine. All models achieved real-time detection within one second per flow, proving the method's viability in operational SDN networks.

This study shows that entropy-driven feature optimization, multi-tier machine learning detection, and software-defined networking-native mitigation can defend against modern DDoS attacks in real time.

6. FUTURE WORK

The proposed system provides many exciting ways to improve and use it. Deep learning models like CNNs, RNNs, or hybrid architectures may improve DDoS detection for dynamic and covert assault patterns in future research. Multi-protocol real-world SDN traffic and IoT-induced DDoS scenarios would improve validation and generalization across varied network environments. To improve scalability and fault tolerance, the framework can support distributed or multi-controller SDN designs, reducing controller dependence and strengthening resilience to large attacks. Future research may focus on AI-driven dynamic OpenFlow rule adaptation techniques in the Ryu controller to automatically modify mitigation reaction times to traffic patterns and attack intensity. These improvements will help the framework deploy in large, production-grade SDN networks.

7. PUBLICATION

7.1 Paper Publication

1 Shroff J, & Shah S. (2024). Entropy-Based Feature Selection for DDoS Detection: Enhancing Importance with Mutual Information Scores in SDN. J. Electrical Systems, 20 (3), 2510–2521. https://journal.esrgroups.org/jes/article/view/4232

2 Shroff, J. M., & Shah, S. M. (2025). Information Gain-Based Detection of Low and High Severity DDoS Attacks in SDN with Automated Mitigation Responses. SSRG International Journal of Electronics and Communication Engineering, 12(8), 1–10. https://doi.org/10.14445/23488549/IJECE-V12I8P101

7.2 Patent Publication

1. Design Patent Filed named with "DARTNet-DDoS Attack Response Topology Network."

8. REFERENCES

1. Putra Fajar A, Purboyo TW (2018) A Survey Paper of Distributed Denial-of-Service Attack in Software Defined Networking (SDN)
2. Srivastava A, Gupta BB, Tyagi A, et al (2011) A Recent Survey on DDoS Attacks and Defense Mechanisms. In: CCIS. pp 570–580
3. Nunes BAA, Mendonca M, Nguyen XN, et al (2014) A survey of software-defined networking: Past, present, and future of programmable networks. IEEE Communications Surveys and Tutorials 16:1617–1634. https://doi.org/10.1109/SURV.2014.012214.00180
4. Qiao Yan, F. Richard Yu (2015) Distributed Denial of Service Attacks in Software-Defined Networking with Cloud Computing. IEEE Communications Magazine
5. Bawany NZ, Shamsi JA, Salah K (2017) DDoS Attack Detection and Mitigation Using SDN: Methods, Practices, and Solutions. Arab J Sci Eng 42:425–441. https://doi.org/10.1007/s13369-017-2414-5
6. Peng T, Leckie C, Ramamohanarao K (2007) Survey of network-based defense mechanisms countering the DoS and DDoS problems. ACM Comput Surv 39:. https://doi.org/10.1145/1216370.1216373
7. Dayal N, Srivastava S (2019) Leveraging SDN for early detection and mitigation of DDoS attacks. In: Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics). Springer Verlag, pp 52–75
8. Dridi L, Zhani MF (2016) SDN-Guard: DoS Attacks Mitigation in SDN Networks. In: Proceedings - 2016 5th IEEE International Conference on Cloud Networking, CloudNet 2016. Institute of Electrical and Electronics Engineers Inc., pp 212–217
9. Wang H, Xu L, Gu G OF-GUARD: A DoS Attack Prevention Extension in Software-Defined Networks
10. Liu AX, Jie Zhang (2018) JESS: Joint Entropy-Based DDoS Defense Scheme in SDN. IEEE Journal on Selected Areas in Communications 36:2358–2372. https://doi.org/10.1109/JSAC.2018.2869997
11. Lukaseder T, Maile L, Erb B, Kargl F (2018) SDN-assisted network-based mitigation of slow DDoS attacks. In: Lecture Notes of the Institute for Computer Sciences, Social-Informatics and

Telecommunications Engineering, LNICST. Springer Verlag, pp 102–121
12. Aladaileh MA, Anbar M, Hintaw AJ, et al (2022) Renyi Joint Entropy-Based Dynamic Threshold Approach to Detect DDoS Attacks against SDN Controller with Various Traffic Rates. Applied Sciences (Switzerland) 12:. https://doi.org/10.3390/app12126127
13. David J, Thomas C (2015) DDoS attack detection using fast entropy approach on flow-based network traffic. In: Procedia Computer Science. Elsevier B.V., pp 30–36
14. Kareem MI, Jasim MN (2022) Entropy-based distributed denial of service attack detection in software-defined networking. Indonesian Journal of Electrical Engineering and Computer Science 27:1542–1549. https://doi.org/10.11591/ijeecs.v27.i3.pp1542-1549
15. Samta R, Sood M (2020) Analysis and Mitigation of DDoS Flooding Attacks in Software Defined Networks. In: Advances in Intelligent Systems and Computing. Springer, pp 337–355
16. Ahalawat A, Babu KS, Turuk AK, Patel S (2022) A low-rate DDoS detection and mitigation for SDN using Renyi Entropy with Packet Drop. Journal of Information Security and Applications 68:. https://doi.org/10.1016/j.jisa.2022.103212
17. Ongshu IA, Reza AW, Uddin Aksir ME, et al (2025) A Smart Approach for Early Detection of DDoS Attacks: Artificial Neural Network and Random Forest Hybridization. In: Procedia Computer Science. Elsevier B.V., pp 490–499
18. Owusu E, Rahouti M, Verma D, et al (2025) Generalizable Multi-Model Fusion for Multi-Class DoS Detection Using Cognitive Diversity and Rank-Score Analysis. ACM Transactions on Privacy and Security 28:1–37. https://doi.org/10.1145/3749374
19. Rajkumar K, shalinie SM (2025) Semi-supervised deep-ELM for DDoS attack detection and mitigation using the OptimalLink model in IoT networks. Comput Secur 152:. https://doi.org/10.1016/j.cose.2025.104323
20. Long Z, Jinsong W (2022) A hybrid method of entropy and SSAE-SVM based DDoS detection and mitigation mechanism in SDN. Comput Secur 115:. https://doi.org/10.1016/j.cose.2022.102604
21. Najar AA, Manohar Naik S (2024) Cyber-Secure SDN: A CNN-Based Approach for Efficient Detection and Mitigation of DDoS attacks. Comput Secur 139:. https://doi.org/10.1016/j.cose.2024.103716
22. El-Sayed A, Toony AA, Tolba A, et al (2025) Deception and cloud integration: A multi-layered approach for DDoS detection, mitigation, and attack surface minimization in SD-IoT networks. Computers and Electrical Engineering 126:. https://doi.org/10.1016/j.compeleceng.2025.110543
23. Gebrye H, Wang Y, Li F, Kahsay B (2025) Feature extraction and selection for flooding-based multi-class DDoS attacks detection in IoT network. International Journal of Critical Infrastructure Protection 51:100815. https://doi.org/10.1016/j.ijcip.2025.100815
24. Makuvaza A, Jat DS, Gamundani AM (2021) Deep Neural Network (DNN) Solution for Real-time Detection of Distributed Denial of Service (DDoS) Attacks in Software Defined Networks (SDNs). SN Comput Sci 2:. https://doi.org/10.1007/s42979-021-00467-1
25. Novaes MP, Carvalho LF, Lloret J, Proenca ML (2020) Long short-term memory and fuzzy logic for anomaly detection and mitigation in software-defined network environment. IEEE Access 8:83765–83781. https://doi.org/10.1109/ACCESS.2020.2992044
26. Iman Sharafaldin AHL (2019) Developing Realistic Distributed Denial of Service (DDoS) Attack Dataset and Taxonomy. In: International Carnahan Conference on Security Technology (ICCST)
27. Shiravi A, Shiravi H, Tavallaee M, Ghorbani AA (2012) Toward developing a systematic approach to generate benchmark datasets for intrusion detection. Comput Secur 31:357–374. https://doi.org/10.1016/j.cose.2011.12.012
28. Moustafa N, Slay J UNSW-NB15: A Comprehensive Data set for Network Intrusion Detection systems (UNSW-NB15 Network Data Set)
29. Shirsath V (2023) CAIDA UCSD DDoS 2007 Attack Dataset