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

A Thesis submitted to Gujarat Technological University

For the Award of

Doctor of Philosophy

In

Computer / IT Engineering

By

Shroff Jaimin Manharlal

Enrollment No. 189999913043

Under supervision of

Dr. Sanjay M. Shah

GUJARAT TECHNOLOGICAL UNIVERSITY
AHMEDABAD

July-2026

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

A Thesis submitted to Gujarat Technological University

For the Award of

Doctor of Philosophy

In

Computer / IT Engineering

By

Shroff Jaimin Manharlal

Enrollment No. 189999913043

Under supervision of

Dr. Sanjay M. Shah

GUJARAT TECHNOLOGICAL UNIVERSITY
AHMEDABAD

July-2026

DECLARATION

I declare that the thesis entitled **"Information Gain Driven Multi-level DDoS Detection and Mitigation for Software Defined Networks Using Machine Learning"** submitted by me for the degree of Doctor of Philosophy is the record of research work carried out by me during the period from 2018 to 2026 under the supervision of **Dr. Sanjay M. Shah** and this has not formed the basis for the award of any degree, diploma, associateship, fellowship, titles in this or any other University or other institution of higher learning.

I further declare that the material obtained from other sources has been duly acknowledged in the thesis. I shall be solely responsible for any plagiarism or other irregularities if noticed in the thesis.

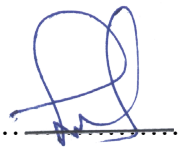
Signature of the Research Scholar: ……  …… Date: 27/07/2026

Name of Research Scholar: **Shroff Jaimin Manharlal**

Place: Ahmedabad

CERTIFICATE

I certify that the work incorporated in the thesis **"Information Gain Driven Multi-level DDoS Detection and Mitigation for Software Defined Networks Using Machine Learning"** submitted by **Mr. Shroff Jaimin Manharlal** was carried out by the candidate under my supervision/guidance. To the best of my knowledge: (i) the candidate has not submitted the same research work to any other institution for any degree/diploma, Associateship, Fellowship or other similar titles (ii) the thesis submitted is a record of original research work done by the Research Scholar during the period of study under my supervision, and (iii) the thesis represents independent research work on the part of the Research Scholar.

Signature of the Research Supervisor: ……  …… Date: 27/07/2026

Name of Supervisor: **Dr. Sanjay M. Shah**

Place: Ahmedabad

Course-work Completion Certificate

This is to certify that **Mr. Shroff Jaimin Manharlal** enrollment No.189999913043 is enrolled for PhD program in the branch **Computer / IT Engineering** of Gujarat Technological University, Ahmedabad.

(Please tick the relevant option(S))

☐ He has been exempted from the course work (successfully completed during M.Phil Course)

☐ He has been exempted from Research Methodology Course only (successfully completed during M.Phil Course)

☑ He has successfully completed the PhD course work for the partial requirement for the award of PhD Degree. His performance in the coursework is as follows-

Grade Obtained in Research Methodology (PH001)	**Grade Obtained in Self-Study Course (PH002)**
BB	AB

Supervisor's Sign

(Dr. Sanjay M. Shah)

Originality Report Certificate

It is certified that PhD Thesis titled **"Information Gain Driven Multi-level DDoS Detection and Mitigation for Software Defined Networks Using Machine Learning"** by **Shroff Jaimin Manharlal** has been examined by us. We undertake the following:

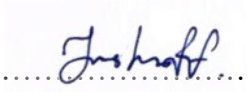
a. Thesis has significant new work / knowledge as compared already published or are under consideration to be published elsewhere. No sentence, equation, diagram, table, paragraph or section has been copied verbatim from previous work unless it is placed under quotation marks and duly referenced.

b. The work presented is original and own work of the author (i.e. there is no plagiarism). No ideas, processes, results or words of others have been presented as Author own work.

c. There is no fabrication of data or results which have been compiled /analyzed.

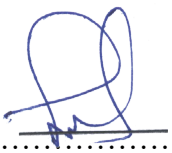
d. There is no falsification by manipulating research materials, equipment or processes, or changing or omitting data or results such that the research is not accurately represented in the research record.

e. The thesis has been checked using **Turnitin Software** (copy of originality report attached) and found within limits as per GTU Plagiarism Policy and instructions issued from time to time (i.e. permitted similarity index <=10%).

Signature of the Research Scholar:  Date: 27/07/2026

Name of Research Scholar: **Shroff Jaimin Manharlal**

Place: Ahmedabad

Signature of Research Supervisor:  Date: 27/07/2026

Name of Research Supervisor: **Dr. Sanjay M. Shah**

Place: Ahmedabad

Jaimin Shroff

Thesis

RESEARCH PAPER
Jaimin
Gujarat Technological University

Document Details

Submission ID
trn:oid:::1:3548711326

Submission Date
Apr 24, 2026, 11:29 AM GMT+5:30

Download Date
Apr 24, 2026, 11:34 AM GMT+5:30

File Name
final_thesis_v6.pdf

File Size
6.7 MB

142 Pages
33,772 Words
207,419 Characters

1% Overall Similarity

The combined total of all matches, including overlapping sources, for each database.

Filtered from the Report

- Bibliography
- Quoted Text

Exclusions

- 2 Excluded Matches

Match Groups

- 10 Not Cited or Quoted 1%
  Matches with neither in-text citation nor quotation marks
- 0 Missing Quotations 0%
  Matches that are still very similar to source material
- 0 Missing Citation 0%
  Matches that have quotation marks, but no in-text citation
- 0 Cited and Quoted 0%
  Matches with in-text citation present, but no quotation marks

Top Sources

1% Internet sources
1% Publications
1% Submitted works (Student Papers)

Integrity Flags

0 Integrity Flags for Review

No suspicious text manipulations found.

Our system's algorithms look deeply at a document for any inconsistencies that would set it apart from a normal submission. If we notice something strange, we flag it for you to review.

A Flag is not necessarily an indicator of a problem. However, we'd recommend you focus your attention there for further review.

Match Groups

- 10 Not Cited or Quoted 1%
  Matches with neither in-text citation nor quotation marks
- 0 Missing Quotations 0%
  Matches that are still very similar to source material
- 0 Missing Citation 0%
  Matches that have quotation marks, but no in-text citation
- 0 Cited and Quoted 0%
  Matches with in-text citation present, but no quotation marks

Top Sources

1% Internet sources
1% Publications
1% Submitted works (Student Papers)

Top Sources

The sources with the highest number of matches within the submission. Overlapping sources will not be displayed.

1 Internet
journal.esrgroups.org <1%

2 Internet
gtusitecirculars.s3.amazonaws.com <1%

PhD THESIS Non-Exclusive License to

GUJARAT TECHNOLOGICAL UNIVERSITY

In consideration of being a PhD Research Scholar at GTU and in the interests of the facilitation of research at GTU and elsewhere, I, **Shroff Jaimin Manharlal** having Enrollment No. **189999913043** hereby grant a non-exclusive, royalty free and perpetual license to GTU on the following terms:

a. GTU is permitted to archive, reproduce and distribute my thesis, in whole or in part, and/or my abstract, in whole or in part (referred to collectively as the "Work") anywhere in the world, for non-commercial purposes, in all forms of media.

b. GTU is permitted to authorize, sub-lease, sub-contract or procure any of the acts mentioned in paragraph (a).

c. GTU is authorized to submit the work at any National / International Library, under the authority of their "Thesis Non-Exclusive License".

d. The Universal Copyright Notice (©) shall appear on all copies made under the authority of this license.

e. I undertake to submit my thesis, through my university, to any Library and Archives. Any abstract submitted with the thesis will be considered to form part of the thesis.

f. I represent that my thesis is my original work, does not infringe any rights of others, including privacy rights, and that I have the right to make the grant conferred by this non-exclusive license.

g. If third party copyrighted material was included in my thesis for which, under the terms of the Copyright Act, written permission from the copyright owners is required, I have obtained such permission from the copyright owners to do the acts mentioned in paragraph (a) above for the full term of copyright protection.

h. I understand that the responsibility for the matter as mentioned in paragraph (g) rests with the authors / me solely. In no case shall GTU have any liability for any acts/ omissions / errors / copyright infringement from the publication of the said thesis or otherwise.

i. I retain copyright ownership and moral rights in my thesis, and may deal with the copyright in my thesis, in any way consistent with rights granted by me to my

university in this non-exclusive license.

j. GTU logo shall not be used / printed in the book (in any manner whatsoever) being published or any promotional or marketing materials or any such similar documents.

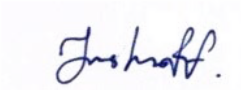
k. The following statement shall be included appropriately and displayed prominently in the book or any material being published anywhere: "The content of the published work is part of the thesis submitted in partial fulfilment for the award of the degree of Ph.D. in Computer/IT Engineering of the Gujarat Technological University".

l. I further promise to inform any person to whom I may hereafter assign or license my copyright in my thesis of the rights granted by me to my university in this nonexclusive license. I shall keep GTU always indemnified from all claims from the Publisher(s) or any third parties resulting or arising from the publishing or use or intended use of the book / such similar document or its contents.

m. I am aware of and agree to accept the conditions and regulations of Ph.D. including all policy matters related to authorship and plagiarism.

Date: 27/07/2026

Place: Ahmedabad



Signature of the Research Scholar

Recommendation of the Research Supervisor: **Approved**

Signature of Research Supervisor

Thesis Approval Form

The viva-voce of the PhD Thesis submitted by **Mr. Shroff Jaimin Manharlal** (Enrollment No. **189999913043**) entitled **"Information Gain Driven Multi-level DDoS Detection and Mitigation for Software Defined Networks Using Machine Learning"** was conducted on **Monday,27th July,2026** at Gujarat Technological University.

(Please tick any one of the following options)

☑ The performance of the candidate was satisfactory. We recommend that he/she be awarded the PhD degree.

☐ Any further modifications in research work recommended by the panel after 3 months from the date of first viva-voce upon request of the Supervisor or request of Independent Research Scholar after which viva-voce can be re-conducted by the same panel again.

☐ The performance of the candidate was unsatisfactory. We recommend that he/she should not be awarded the PhD degree.

Prof. S.M. Shah

Name and Signature of Supervisor with Seal

1) (External Examiner 1)Name and Signature

Dr. Arvind Kumar Tiwari

2) (External Examiner 2)Name and Signature

Abstract

Software Defined Networks (SDN) have undergone rapid development which now provides better programmability and centralized control and dynamic traffic management solutions. The control plane of SDN systems becomes highly susceptible to Distributed Denial of Service (DDoS) attacks because their systems depend on centralized architectural designs. Existing DDoS detection mechanisms often rely on high-dimensional traffic features and binary classification models and isolated mitigation strategies which result in increased computational complexity and limited severity awareness for real-time environments. This thesis proposes a DDoS detection and mitigation system for SDN environments which operates through an information gain-based intelligent system. The proposed solution uses a sequential feature selection method which combines mutual information and joint entropy to achieve feature dimensionality reduction while maintaining its ability to distinguish between different classes. The proposed method achieves significant feature reduction of approximately 70% because it maintains detection accuracy throughout the process. The system uses a three-level classification which classifies network traffic into three categories: normal traffic, low-severity attacks, and high-severity attacks. The framework was evaluated using the CICDDoS2019 benchmark dataset and validated through real-time SDN experiments implemented using Mininet and the Ryu controller. The experimental results demonstrate 97-98% detection accuracy together with low false positive rates and the ability to classify all data flows within one second. The severity-aware mitigation mechanisms use automated OpenFlow rule blocking and dynamic honeypot redirection to maintain service operations while minimizing network disruptions during ongoing attacks. The research results prove that the combination of sequential feature optimization and multi-level machine learning detection and SDN native mitigation methods provides a more robust defense against contemporary DDoS attacks. The proposed framework provides a scalable and lightweight solution that functions effectively in actual production SDN environments.

Acknowledgment

The research process does not always proceed smoothly. a journey often marked by challenges and setbacks. Yet it is necessarily a learning path directed on to higher grounds of growth and resistance supported and encouraged by the kindness of several individuals. First and foremost, I express my gratitude to the Almighty and my revered ancestors for their blessings and guidance throughout this journey. I have always felt blessed, guided, sheltered, and supported by them through all my time.

I would like to express my deepest gratitude to my supervisor, **Dr. Sanjay M Shah**, Professor, Computer Engineering Department at Government Engineering College, Rajkot, for their unwavering guidance, patience, and mentorship throughout this journey. His profound expertise, critical insights, and high standards for excellence have not only shaped this thesis but have also fundamentally influenced my growth as a researcher.

I am deeply thankful to the members of my Doctoral Progress Committee, **Dr. Chirag S. Thaker**, Professor, L. D. College of Engineering, Ahmedabad, and **Dr. Dhaval A. Parikh**, Professor, Government Engineering College, Gandhinagar, for their insightful suggestions, technical guidance, and valuable feedback throughout my research work. I sincerely acknowledge **Gujarat Technological University (GTU), Ahmedabad**, for granting me the opportunity to pursue the Doctor of Philosophy program and for providing essential academic and administrative support. I also gratefully acknowledge **Vishwakarma Government Engineering College, Chandkheda, Ahmedabad**, and **Government Engineering College, Modasa** for offering a supportive academic environment and necessary facilities to conduct this research.

I thank all my colleagues and friends: Prof. Nakul Dave, Prof. Jigna Jadav, Prof. Avani Dave, Prof. Vinod Thumar, Prof Uttam Chauhan, Prof. Kuntesh Jani, Prof. Bhavin Patel, Prof. Amit Vaishnav, Prof. Jignesh Vania, Prof. Amit Rathod, Prof. Nirav Suthar, Prof. Aniruddhsinh Dodiya, Prof. Pradeep Gamit, Prof. Shreyas Patel and Prashant Bhavsar for their technical help and moral support. I extend special thanks to the Head of the Department, **Prof. Kajal Patel**, for their guidance, cooperation, and encouragement, which significantly contributed to the successful completion of this research.

I extend my heartfelt thanks to my mother and father, **(Mrs. Ramilaben Makwana & Mr. Manharlal Makwana)** for their unconditional love and for the sacrifices you made to ensure I received the best education possible. You taught me the value of perseverance and the importance of dreaming big. I wish to convey my sincere appreciation to my wife **Mrs. Apeksha Shroff**; words cannot fully capture the depth of my gratitude. You have been my rock, my confidante, and my greatest cheerleader. Your unwavering support and encouragement were invaluable throughout this endeavour. I am grateful to my son, **Param**, whose joy and curiosity provided encouragement and balance throughout this research journey.

I am deeply thankful to my in-laws, **Anilkumar Rathod** and **Manjula Rathod**, for their kindness, assistance, and for providing me peace of mind to focus on my research work. I also appreciate my brother-in-law **Meet Rathod** and sister-in-law **Khyati Rathod** for creating a warm and uplifting atmosphere. My sincere thanks go to my sister **Sweta Parikh** and brother-in-law **Tarkesh Parikh** for their ongoing encouragement and support.

In the end, I convey my deep gratitude to my cherished companions whose unwavering motivation, encouragement, and moral support gave me the strength and determination required to complete this research journey.

Shroff Jaimin Manharlal
Research Scholar,
Gujarat Technological University.

Index

List of Abbreviations

Sr. No.	Abbreviations	Full Form
1	**ADA**	Adaptive Dragonfly Algorithm
2	**CICDDoS2019**	Canadian Institute for Cybersecurity DDoS 2019 Dataset
3	**CNN**	Convolutional Neural Network
4	**CRPS**	Continuous Ranked Probability Score
5	**CUSUM**	Cumulative Sum Control Chart
6	**DDoS/DrDoS**	Distributed Denial of Service
7	**DEHO**	Discrete Elephant Herding Optimization
8	**DL**	Deep Learning
9	**EGOA**	Enhanced grasshopper optimization algorithm
10	**ES**	Exponentially Smoothing
11	**FedAvg**	Federated Averaging
12	**FFT**	Fast Fourier Transform
13	**FN**	False Negative
14	**FP**	False Positive
15	**GAT**	Graph Attention Network
16	**GBA**	Gradient Boosting Algorithm
17	**GCT**	Gated Convolutional Temporal
18	**GRU**	Gated Recurrent Unit
19	**ICMP**	Internet Control Message Protocol
20	**IDS**	Intrusion Detection System
21	**IG**	Information Gain
22	**IIoT**	Industrial Internet of Things
23	**IoT**	Internet of Things

24	**IPS**	Intrusion Prevention System
25	**KNN**	K-Nearest Neighbor
26	**KPCA**	Kernel Principal Component Analysis
27	**LSTM**	Long Short-Term Memory
28	**MAC**	Media Access Control
29	**MI**	Mutual Information Score
30	**ML**	Machine Learning
31	**MLP**	Multilayer Perceptron
32	**NFV**	Network Functions Virtualization
33	**NN**	Neural Network
34	**OF**	OpenFlow
35	**PCA**	Principal Component Analysis
36	**QoS**	Quality of Service
37	**RF**	Random Forest
38	**RTT**	Round Trip Time
39	**SDN**	Software Defined Networks
40	**SSAE**	Stacked Sparse Autoencoder
41	**SsFLHT**	Semi-supervised Federated Learning with Hyperparameter Tuning
42	**SVM**	Support Vector Machine
43	**SHAP**	Shapley Additive Explanations
44	**TN**	True Negative
45	**TP**	True Positive
46	**VGG19**	Visual Geometry Group 19 Network
47	**XAI**	Explainable Artificial Intelligence

List of Figures

List of Tables

CHAPTER 1

INTRODUCTION

The rapid evolution of communication technologies and the unprecedented growth of Internet-based services have transformed computer networks into a critical backbone of modern society. From cloud computing and e-commerce to healthcare systems and smart infrastructures, the availability, reliability, and security of networks play a decisive role in ensuring seamless digital operations. However, this increasing dependence on networked systems has also made them highly vulnerable to sophisticated cyber threats, thereby emphasizing the urgent need for advanced and intelligent network security mechanisms.

1.1 Background of Network Security

With the dawn of the internet age, computer networks have become indispensable for a multitude of crucial societal operations, including cloud services, medical care, banking, industry, town planning, and the Internet of Things. The evolution of data transmission technologies, the proliferation of connected devices, and increasing application demands mean that systems increasingly require more robust, secure network architectures than before. Consequently, emphasis is placed on network security measures to ensure the confidentiality, integrity, and availability of assets and services. Traditional security measures, including firewalls, intrusion detection systems, and access control lists, were designed for static physical networks and are often inadequate for modern dynamic environments.

Increasingly, the prominence of networking paradigms beyond the fundamental stage, with the approach of virtualization, programmability, and centralization of management, has altered the threat profile. It is no longer practical to consider contemporary networks as isolated systems; in contrast, extra effort has been put in the design to formulate highly interlinked structures infused with software defined entities, cloud services and various devices of diverse makes and capacities. Such interconnected infrastructures increase the number of attack vectors available to malicious actors, enabling them to exploit architectural

weaknesses, software vulnerabilities, and configuration errors on a large scale. Consequently, contemporary network security must extend beyond traditional perimeter defenses and adopt advanced techniques such as threat intelligence, adaptive security approaches, and machine learning against cyber threats.

Next-generation network architectures like Software Defined Networks (SDN) are the focus of the most recent research articles, highlighting the potential and challenges that come with network security. In SDN, the separation of control plane from the data plane becomes the focus. As a result, centralized controllers of the network are made possible, giving additional management and monitoring functionalities of the network. Such rearrangements in the basic functioning of the network allow network management to come up with protection strategies suited to the threat environment, as well as analyze and defend the network from the attack. However, this level of centralization introduces security risks, as compromising key network components may significantly affect overall network operations. In this respect, the SDN controller and its communication channels represent critical components that are frequently targeted by cyber-attacks [1].

Moreover, with the advent of such technologies as SDN, NFV, and network slicing, particularly in 5G and later network versions, networks become more virtualized. Even though it seems quite comfortable to deploy such virtual networks due to their ease of scalability, adaptability and quicker pace of deployment, one must not forget that it inevitably broadens the attack possibilities as well as the vulnerabilities. Insufficient understanding of the scientific issues is observed in the work of Alnaim, particularly the problem of complex security analysis of virtual networks. Others, however, think that software defined concepts and systems have the possibility of a proactive defense, which warrants the use of additional security measures. Increasing network complexity introduces significant challenges in threat modeling and security management [2].

Fast growth of IoT devices, cloud services, and mobile applications has not only led to an increase in the attacks' rates but has also made the threats of the modern networks more acute, with the architectural vulnerabilities being added on top of them. An inherent challenge of SDN lies in its centralized architecture, which may introduce critical security vulnerabilities. Dayal et al. assert that SDN though giving ease of managing the network control and enforcing policies, makes its centralized controller particularly prone to availability based attacks such as a Distributed Denial of Service (DDoS) which can disrupt

the operation of the entire network by incapacitating a single entity. In comparison, it is suggested by new and recent research results that the 6G or next wireless network generation will require better security safeguards for their extremely low time delay, very high device density, and AI enabled automation [3]. Shahen et al. indicated that this milestone network will entail a prominent extent of use of intelligent security technologies, wherein artificial intelligence, blockchain and virtualization-posture-centric security mechanisms will be instrumental in enhancing trustworthiness, preparedness, and proactive defense capabilities [4]. This observation highlights the need to reform existing network security strategies toward dynamic and adaptive security frameworks.

The increasing adoption of SDN and virtualization technologies has encouraged the development of advanced security mechanisms capable of analysing traffic patterns, detecting attacks, and responding rapidly to emerging threats. Consequently, research efforts have increasingly focused on the detection, mitigation, and recovery from Distributed Denial of Service attacks, particularly within SDN environments. Developing effective and adaptive defense mechanisms for SDN-based DDoS attacks therefore constitutes the primary focus of this study.

1.2 Distributed Denial of Service (DDoS) Attacks

Distributed Denial of Service (DDoS) attacks have evolved into one of the most destructive and persistent security threats in modern network environments. DDoS attacks use multiple infected computers operating together to disable a target system unlike traditional Denial of Service (DoS) attacks which use a single attacking source. Compromised devices collectively form botnets that generate massive volumes of malicious traffic thereby depleting all available processing power and memory and network capacity of the targeted system. The denial of essential services to legitimate users results in financial losses and damage to reputation and interruptions to business operations.

Mirkovic and Reiher present their definition of a denial-of-service attack which requires attackers to make deliberate efforts that stop users from accessing their intended services, while DDoS attacks expand this definition through their ability to distribute attack traffic across multiple targets which creates substantial hurdles for detection and defense efforts. These findings demonstrate that DDoS attacks use multiple attacking methods which security experts need to defend against because hackers develop new strategies in response

to security measures. The diversity of attack methods creates major challenges for organizations attempting to detect and mitigate DDoS attacks because this problem continues to exist in real-world situations [5] .

Chaudhary and Mishra provide a thorough review of Distributed Denial of Service (DDoS) attacks within Industrial Internet of Things (IIoT) settings and their effects on industrial networks. It explains the architecture of IIoT systems and identifies vulnerabilities across different layers that can be exploited by attackers. The research classifies various DDoS attack categories, tools, and traffic generators utilized to initiate or emulate attacks in industrial networks. It also examines current defense strategies, including prevention and mitigation methods based on machine learning, deep learning, and other security techniques [6].

1.2.1 Evolution of DDoS Attacks

DDoS attacks have grown more extensive and complex during the last twenty years because attackers have developed new methods to launch these attacks. Early DDoS attacks primarily relied on brute-force flooding techniques, which involved attackers creating high traffic volumes to overwhelm their target's network connection. The basic DDoS attacks produced clear traffic spikes that made their detection easy during their initial period of operation. Attackers subsequently developed stealthy, protocol-aware, and application-specific techniques after defense mechanisms reached higher levels of effectiveness.

The comprehensive taxonomy developed by Singh and Bhandari demonstrates that cyber attackers develop new tools which they use to break through existing security measures. The cycle of defense development leading to attack strategy innovations has created various DDoS attack types that target different architectural and protocol-level weaknesses [7]. The current growth of Internet-connected devices has become a key factor which increases the effects of DDoS attacks. The main research study about DDoS defense systems shows that the primary method which attackers use to conduct DDoS attacks has changed because IoT-based botnets now serve as the main attack vector. The combination of low-cost IoT devices which operate continuously, and their security vulnerabilities has created perfect conditions for building extensive botnet networks. Current DDoS attacks today use multiple attack methods which they execute at the same time. The attackers use two separate attack

techniques to create detection problems through their simultaneous volumetric flood attacks and application-layer exhaustion attacks [8].

1.2.2 Types of DDoS Attacks

A Distributed Denial of Service (DDoS) attack is a malicious attempt to disrupt the availability of a network, system, or service by overwhelming it with a flood of traffic from multiple sources. The goal of a DDoS attack is to exhaust the target's resources, such as bandwidth, processing power, or memory, rendering it inaccessible to legitimate users. DDoS attacks can have severe consequences, including financial loss, reputation damage, and disruption of critical services. Here are the main types of DDoS attacks:

Volumetric Attacks: The purpose of volumetric attacks is to overwhelm a victim's network and upstream systems by generating extremely high amounts of traffic. The objective of these attacks is to saturate network links and exhaust available bandwidth. These attacks can generate traffic that exceeds both hundred gigabits per second and terabit-scale traffic levels. The recent DDoS defense systems survey shows that volumetric attacks create heavy traffic which consumes all network resources instead of attacking application functions. The enormous size of volumetric attacks forces security teams to use traffic scrubbing centers and rate-limiting systems and cloud-based filtering solutions for defense purposes [9].

Protocol-Based Attacks: These attacks use network and transport-layer protocol weaknesses to force servers into resource exhaustion attacks which consume their CPU cycles and memory and connection table resources. The attacks use protocol operations which include connection establishment and error handling as their basis for operation. The attacks create challenges for detection because they mimic standard protocol behaviour which makes it hard to differentiate between actual attacks and legitimate network activity [10].

Application Layer Attacks: These are more sophisticated as they target specific aspects of an application or service. They require less bandwidth to execute but can be very effective in disrupting the targeted service. Application-layer DDoS attacks target the operational functions of services which include web servers and DNS resolvers and database backends. The attacks do not attempt to overload network capacity but instead they try to deplete system resources through their use of fake requests that require heavy processing. The recent

survey about VANET-related DDoS attacks shows that application-layer attacks pose a major threat because they imitate standard user behaviour which makes them hard to detect. Financial systems and e-commerce platforms and cloud services use these attacks because even brief service interruptions result in major operational problems [11].

Reflective Attacks: Reflection attacks depend on attackers who use third-party servers to create their attack traffic. The attackers use this technique to fake the victim's IP address while they send requests to real servers which will send their responses back to the victim. This method enables attackers to remain anonymous while they create more incoming traffic. The DNS amplification study by MacFarland et al. explains that reflection attacks are attractive because they mask the attacker’s identity and enlist innocent servers as unwilling participants. The indirect method creates major challenges for both traceback and filtering processes [12].

Amplified attacks: These attacks operate as a distinct type of reflection attacks which use small requests to create massive response outputs. Attackers can achieve significant attack results by sending only little data to their targets. Zheng et al. demonstrate that DNS amplification attacks can achieve extreme amplification factors which enable attackers to generate floods exceeding 300 Gbps while transmitting only a small volume of data themselves. The asymmetrical relationship between attacker effort and victim damage makes amplification attacks highly dangerous [13].

1.3 Software Defined Networks (SDN)

Traditional computer networks depend on tightly coupled architectures which require networking devices to combine their control logic with their packet forwarding functions. The design of integrated systems which are tightly connected becomes more complex to handle when network systems experience growth in their size and operational requirements. The process of device configuration requires individual setups which depend on vendor specific commands, resulting in restricted network flexibility and delayed adjustments to new operational needs.

Software Defined Networks (SDN) was introduced to overcome these limitations by decoupling the control plane from the data plane which created a network that could be controlled through central management and operated as programmable infrastructure.

According to Sinha et al. SDN functions as a distributed network system which operates through its central controller to control network operations while its forwarding devices handle packet transmission tasks. This architectural separation enables network administrators to dynamically configure and manage the entire network through software which results in better scalability and operational efficiency [14].

1.3.1 Traditional Networks vs SDN

Network devices in traditional networks base their routing decisions on local data which they obtain from their distributed control protocols. This method restricts operators from viewing the entire network which creates challenges for managing network traffic in a unified way. The SDN framework enables network operators to monitor the complete network while making centralized decisions and applying network security policies throughout their entire system. Kurniawan et al. demonstrate that SDN enables application and service development to operate the entire network system as one unified system because it abstracts all network hardware components. The system uses network abstraction to create simplified network management and enables organizations to introduce new services at high speed without needing to alter their existing network infrastructure [15] .

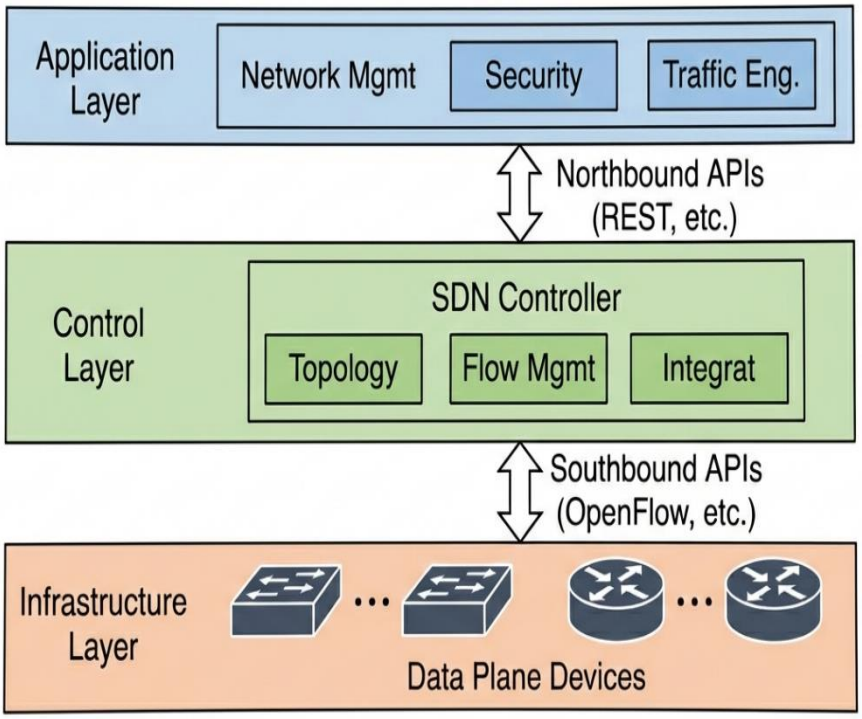


FIGURE 1.1 Software Defined Networks (SDN) Architecture

1.3.2 SDN Architecture

The SDN architecture uses a layered design which distributes different duties to multiple operational levels. The system design uses modular components to provide better operational flexibility and programmability while making it easier to manage and observe network activities. FIGURE 1.1 offers a complete overview of SDN architecture. The explanation of SDN shows three main components which include data plane and control plane and application plane. The system design enables separate development and optimization of each plane which supports both innovation and system expansion.

The data plane includes OpenFlow-supported switches as its forwarding devices that only handle packet transmission according to flow rules which the controller has set. The devices lack power for independent routing, but this feature simplifies their hardware construction. The SDN controller operates as the network's main control center from its position within the control plane. The system controls networkwide visibility while verifying operational rules and implementing data-plane device transmission guidelines. The controller functions as the SDN brain according to Meti et al. because any disturbance to the controller will result in total network downtime. The application plane contains network applications which establish high-level policies for routing, load balancing, intrusion detection and security monitoring. The applications use northbound APIs to interact with the controller which enables them to create automatic and real-time network operations [16, 17]. OpenFlow functions as the most used southbound interface which enables SDN controllers to communicate with data-plane devices. The system permits the controller to add new flow rules and modify existing rules and remove existing rules from the switch flow tables. Deb and Roy explain that OpenFlow allows the controller to directly control packet forwarding behaviour by manipulating flow entries, making it a fundamental enabler of SDN programmability. OpenFlow enables centralized control through its simplified interface yet introduces unprotected security risks which arise from the newly created security links between controller devices and switches [18].

1.4 Security Challenges in SDN

SDN provides important benefits through its ability to deliver flexible operations and central control functionality. The security of SDN systems becomes compromised because their architectural framework creates new vulnerabilities. The same features that make SDN

powerful, which include centralized control and programmability and frequent controller switch interactions create opportunities for attackers to exploit the system through Distributed Denial of Service (DDoS) attacks. Vykopal et al. demonstrate that SDN systems create a contradictory relationship with DDoS attacks because their unified monitoring system helps security teams detect threats, but attackers find it easier to target the system's central operations [19].

Table 1.1 Key Security Challenges in Software Defined Networks

Security Challenge	Description	Impact	Ref
Vulnerability	DDoS attack can be directed at the controller's logical structure, which can get its memory resources utterly depleted.	Service disruptions throughout the network due to the unavailability of a controller.	[20]
Flow Table Saturation	By creating many new flows, the switch can potentially run out of flow table space limited by TCAM.	Legitimate traffic that is admitted to the interface needs to be lost.	[21]
Packet-In Flooding	Attackers can use probing techniques to generate flow entries	Controller overload and severe performance degradation.	[22]

Table 1.1 provides an overview of the main security threats that Software Defined Networks present, which attackers can use to conduct DDoS attacks. The SDN controller serves as the main target for attackers because of its centralized control system, which enables them to cause resource depletion that will result in complete network failure. SDN switches face flow table saturation attacks because their TCAM based flow tables have restricted capacity, which results in service interruptions even when network traffic remains low. The packet-in mechanism serves as a basic communication link between controllers and switches, but attackers can use it to initiate controller overload through their control message generation activities. The system needs DDoS detection and mitigation solutions that operate efficiently in a scalable manner to protect both control and data planes of the system through our DDoS protection system.

1.5 Motivation for Research

The increasing popularity of cloud services and IoT ecosystems and latency-sensitive applications has created a situation where modern networks face greater risks from DDoS attacks. The risk associated with these threats increases in SDN environments because SDN employs a centralized controller as the main intelligence system which controls the entire network operations. The implementation of SDN enables organizations to program their networks and monitor all network activities while choosing different methods to manage network traffic, but this functionality introduces additional vulnerabilities that attackers can exploit to target the control plane. Existing DDoS detection systems face challenges in addressing the continuously evolving nature of attacks. The need to process high-dimensional traffic datasets results in significant computational demands which prevent real-time detection capabilities from functioning properly in SDN networks. The current solutions depend on binary attack classification systems which do not provide the detailed information needed to perform effective resource-based attack response systems. The application of aggressive mitigation methods across all situations leads to unnecessary interruptions of authentic network traffic, while the use of delayed response systems results in significant network performance declines. The research work uses three methods which combine entropy-based sequential feature selection with multi-level machine learning based attack detection and SDN based real-time defense systems to improve detection performance while providing immediate threat response based on attack intensity. This research focuses on developing a framework that combines accurate threat detection with effective live network protection to improve security measures in software defined networks setups.

1.6 Problem Statement

Despite significant research on DDoS detection and mitigation, several limitations remain in current SDN-based security solutions. Modern benchmark datasets, such as CICDDoS2019, contain many traffic features, which increase computational complexity and delay detection when applied in real-time SDN environments. Existing feature selection methods often fail to sufficiently reduce dimensionality while preserving important information for accurate detection. In addition, most current approaches perform only binary classification by distinguishing between normal and attack traffic, without identifying different attack severity levels. This limitation prevents the implementation of adaptive mitigation strategies that respond differently to low-severity and high-severity attacks.

Furthermore, many detection mechanisms operate independently of the SDN controller, creating delays between attack detection and mitigation. Therefore, there is a need for an integrated SDN-native framework that can effectively reduce feature dimensionality, classify attack severity, and enable automated, real-time mitigation through the SDN controller.

1.7 Research Objectives

This research aims to develop and evaluate an efficient, intelligent, and scalable DDoS detection and mitigation framework for SDN environments. The study will accomplish its main goal through these specific research objectives:

- Develop a hybrid entropy-based sequential feature selection method that reduces the dimensionality of DDoS traffic data while preserving discriminative information.
- Design a multi-level machine learning detection system capable of identifying network traffic as either normal or DDoS attacks with low or high severity.
- Implement a real-time SDN environment incorporating severity-aware mitigation strategies.
- Evaluate the proposed framework's effectiveness, scalability and real-time capabilities through evaluation on benchmark datasets and a Mininet-based SDN testbed that uses a Ryu controller.

1.8 Research Contributions

This research makes several significant contributions to the domain of SDN-based network security and DDoS mitigation:

- A hybrid entropy-driven feature selection framework is proposed that uses Mutual Information and Joint Entropy for sequential feature selection, thereby achieving high detection accuracy and substantial feature dimensionality reduction.
- A multi-level DDoS detection model is developed that enables more precise attack traffic assessment than standard binary classification through its ability to identify low-severity and high-severity attacks.

- The system implements a real-time SDN-integrated mitigation mechanism that uses automated OpenFlow rules to control system operations through the Ryu controller by enabling it to perform dynamic traffic forwarding, honeypot redirection, and port blocking according to attack severity.

- The proposed framework is validated on a live SDN testbed, which shows it can achieve faster detection times and needs fewer controller resources while maintaining network operation during ongoing DDoS attacks.

The presented findings together build up an advanced system which operates through SDN-native DDoS detection methods to determine attack severity and execute mitigation strategies.

1.9 Organization of the Thesis

The remainder of this thesis is organized as follows. Chapter 2 reviews existing literature on DDoS attacks, SDN security, machine learning-based detection techniques, benchmark datasets, and identified research gaps. Chapter 3 introduces the system model and problem formulation which defines the SDN architecture and DDoS threat scenario considered in this study. Chapter 4 describes the proposed methodology which includes the sequential feature selection approach and machine learning–based multi-level detection models and SDN-based mitigation mechanisms. Chapter 5 details the experimental setup and implementation process which includes datasets and model configurations and SDN testbed design. Chapter 6 presents and discusses the experimental results which evaluate detection accuracy and processing time and mitigation effectiveness. The thesis concludes in Chapter 7 which also describes possible research directions for future study.

CHAPTER 2

LITERATURE REVIEW

This chapter provides a comprehensive review of research related to DDoS attacks vector, botnet driven threats, detection techniques, and feature selection criteria, and discusses the defense mechanisms that can be enabled via the SDN. The intent is to analyse current trends, strengths, and limitations that exist in existing studies, while identifying the research gaps that motivate the development of the proposed framework of Information Gain based multi-level DDoS detection and mitigation framework elaborated upon in this thesis.

2.1 Introduction

DDoS attacks have evolved significantly over time, becoming increasingly sophisticated, diverse, and difficult to detect. Contemporary DDoS attacks differ substantially from traditional flooding-based approaches that primarily focused on overwhelming targets with high volumes of traffic. Modern attacks employ multiple attack vectors, exploit vulnerabilities in emerging network paradigms, and leverage large-scale botnets comprising compromised IoT devices. Understanding the evolving characteristics of DDoS attacks is essential for developing modern security solutions that are adaptive, intelligent, architecture-aware, and proactive. Existing studies indicate that DDoS attacks are characterized by anomalies in packet attributes, traffic volume, and the coordinated behaviour of multiple distributed sources. These evolving attack patterns highlight the limitations of conventional defense mechanisms and emphasize the need for advanced detection and mitigation strategies [23].

2.2 DDoS Attack Landscape

Over the years, the DDoS threat landscape has evolved significantly such that simple flooding attacks have been modified to highly organized, massive campaigns operated using botnet networks of co-opted machines at the disposal of a single adversary. Botnets have become increasingly sophisticated, enabling coordinated attacks and adaptive attack

strategies. Extensive survey confirms that botnets are now among the most serious cybersecurity threats supporting various malicious activities like the distribution of DDoS attacks, spam and phishing. The study highlights that botnet-driven attacks continue to increase in scale and sophistication, largely motivated by financial incentives and by the ease of availability of theoretically vulnerable devices [24].

Valdovinos et al provides a comprehensive review of SDN-based DDoS detection and mitigation techniques. They present a thorough taxonomy of detection strategies, including architectural, machine-learning-based, and statistics-based approaches, including the emerging technologies NFV, blockchain, honeynets, and moving target defense. Therefore, the present study also adds that while to date SDN has provided global visibility and programmability, its controller-centric design opens the door to several vulnerabilities naturally exploitable by DDoS attacks [25].

Kaur et al. analyzed 75 studies linked to the highest impact that summarize DDoS defense applications for SDN and grouped them based on the desired targets of the attacks, defense strategies applied, environments where testing was carried out and means with which traffic is used. This study reveals that attacks that continually rise in number focus their efforts on several planes within SDN, but that the available solutions mostly tackle the isolation of separate components rather than posing a holistic problem to control, data, and communication channels. It identifies scalability, controller centralization, and lack of resources within switch as major factors that define the SDN DDoS landscapes today [26].

According to Rathore et al., the IoT-driven smart civic environment has given rise to the extension of the DDoS landscape by the rapid rise of IoT devices combined with SDN-enabled infrastructure. Their study introduces a new IoT-specific DDoS taxonomy that focuses on MQTT, CoAP, and SSDP protocol vulnerabilities, not only articulated by traditional TCP/UDP-centric defense. Instead, the study illustrates that IoT botnets have been among the most used platforms in generating large-scale DDoS attacks [27]. Walfish et al. discuss application-layer DDoS attacks and their defense philosophy, focusing on the attacker's mirroring a legitimate client's behaviour pattern to exhaust the resources on the server side rather than network bandwidth. This exemplifies how DDoS attacks are going to exhaust resources by using legitimate-looking requests, making such detection primarily volume-based ineffective. Usually, it is noted that DDoS attacks have surpassed not only

brute-force tactics, but even cunning and intelligence they now demand an equally intelligent defense and countermeasures against them [28].

These findings suggest that modern DDoS attacks exploit architectural vulnerabilities, protocol-level weaknesses, malicious traffic patterns, and IoT-based botnets to launch large-scale and sophisticated attacks. The increasing complexity and multi-vector nature of these attacks highlight the limitations of conventional defense mechanisms. Consequently, effective mitigation requires adaptive and proactive security frameworks capable of continuously monitoring network behaviour, identifying evolving attack patterns, and responding dynamically to emerging threats.

2.3 SDN based DDoS Detection Techniques

2.3.1 Using Statistical Methods

DDoS attacks have continued to evolve and scale in complex ways, and the need for appropriate, faster detection have become increasingly important. Predetermined signatures and threshold-based traditional approaches have not been able to deal with new attack strategies, including low-rate and multi-vector attacks that often mimic valid traffic behaviour. As a result, researchers have been compelled to develop more adaptive detection techniques that analyse traffic patterns and learn behaviours rather than relying solely on static rules.

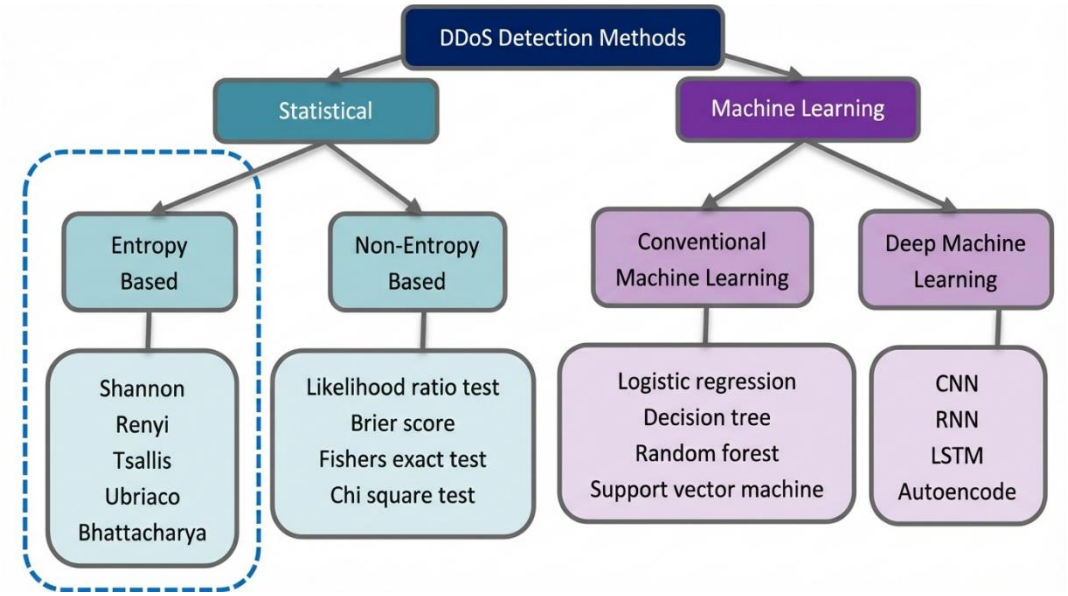


FIGURE 2.1 Classification of DDoS Detection Methods

As shown in FIGURE 2.1, DDoS detection techniques can be classified into purely statistical-based approaches and machine-learning-based strategies. Statistical strategies consider the properties of traffic, such as randomness, changes in frequency distributions, and start variations, as indicators of abnormal behaviour. Historical traffic from feeds and sensors is used to train artificial intelligence models that differentiate normal and malicious flows. Each of the methods has shown good promise, but they still have problems with accuracy, computational cost, and robustness to evolving attack patterns. This subsection will primarily review these techniques and explain the most important variations. The method of detecting DDoS also relies on model-based traffic analysis, using mathematical characteristics of network traffic to detect deviations from regular behaviour. Instead, it looks for anomalies that may indicate an attack by modelling the distribution, probability, or temporal patterns of network traffic, rather than relying on specific signatures or an intensive training dataset. Therefore, it is particularly suitable for the deployment and evaluation of real-time statistical approaches; in addition, if labelled data is scarce, statistical methods are light and easily explain facts. However, proper statistical metrics, in conjunction with thresholding mechanisms, can yield efficient results for these methods.

Bouyeddou et al. introduces a novel statistical method based on the continuous ranked probability score with exponential smoothing for detecting DoS and DDoS attacks. The Continuous Ranked Probability Score (CRPS) defines the deviation of data from normal traffic distribution profile, while Exponentially Smoothing (ES) enhances detection sensitivity for minute variations. A nonparametric threshold based on kernel density estimation is used, and therefore, it promises to perform well with high detection rates and low false alarms for high-rate as well as low-rate attack experiments [29]. Basicevic and Ocovaj did an in-depth study of entropy-based statistical methods for detection of DDoS in which they tested five entropy formulas, i.e., Shannon, Tsallis, Rényi, Bhatia–Singh, Ubriaco entropy. Evaluated on major input parameters as their features, the authors examined the efficiencies of detection, false positive rates, and delay for each entropy measure in the flow size distribution. As per their review, with a false positive rate lower than that of Tsallis entropy, both Rényi and Bhatia–Singh forms of entropy scored highest on detection accuracy relative to Shannon. Considering this, it is also indicated that no single entropy metric could perform optimally for all scenarios, which explains the need for adaptive or hybrid statistical detection strategies [30].

Table 2.1 Entropy-Based Statistical DDoS Detection

Ref	Entropy Type	SDN	Threshold	Method	Performance	Advantages	Limitations
Basicevic et al.[31]	Multiple	No	Static	Entropy Comparison	Low False Positive Rate	Generalized Entropy	Delay Tradeoff
Tsobdjou et al. [32]	Shannon	No	Dynamic	Online Entropy	High Detection Rate	Adaptive	No Severity
Aladaileh et al. [33]	Renyi	Yes	Dynamic	Joint Entropy	High Detection Rate	SDN Aware	Limited Victims
AbdelAzim et al. [34]	Hybrid	Yes	Adaptive	Entropy + KL	Stable Detection	Trust Based	No Benchmarks
M. Sinha et al. [35]	Shannon	Yes	Adaptive	Live Entropy	Low False Positive Rate	Real-Time	SYN Only
Kubra et al. [36]	Joint	Yes	Dynamic	Joint Entropy	High Accuracy	Multi-Feature	Small Dataset
Ahalawat et al. [37]	Renyi	Yes	Dynamic	Packet Drop	High Accuracy	Low rate Detect	Single Dest Issue
Kareem et al. [38]	Shannon	Yes	Static	Dest-IP Entropy	High Detection Rate	Early Detect	UDP Focus
Samta et al. [39]	Traffic Pattern	Yes	Static	Flood Analysis	Better RTT	Simple	Flood Only
David et al. [40]	Fast	No	Adaptive	Flow Entropy	High Accuracy	Low Cost	Not SDN

Table 2.1 and Table 2.2 detail the main entropy-statistical and non-entropy-statistical ways of detecting DDoS attacks. The reference is based on the employed statistical techniques, the applicability of SDN, thresholding strategies, and the performance shown with the corresponding drawbacks.

Basicevic et al., on one side, obtain generalized entropy measures falling in false positive rates compared to Shannon entropy, while they face increased delays in detection without the integration with SDN [31]. Tsobdjou et al. proposed a real-time Shannon entropy approach situated over a dynamic threshold if the provided correctness rate is massive although the framework provides limited support for severity-aware incident classification [32]. Aladaileh et al. described dynamically threshold methods applying the entropy of both Shannon and Renyi for big switch controllers of SDN under the provision of supposedly a high positive alarm detection rate, for innumerable instances in comparison with few evaluated cases [33]. On the other hand, AbdelAzim et al. assess how entropy is combined with Kullback-Leibler divergence and trust to test and increase detection stability within SDNs, albeit with limiting benchmark-based numerical validation [34].

M. Sinha et al. propose SynFloWatch, a live entropy-based defense system for hybrid SDN that dynamically detects and mitigates SYN spoofing DDoS attacks by identifying malicious switch ports and selectively blocking spoofed packets while allowing legitimate traffic, achieving reduced false positives and negatives [35]. Kubra Kalkan et al. Suggest the Ensemble Entropy Method of Detection using a couple of traffic features achieving high accuracy while using small datasets [36]. Enabling successful low-rate DDoS detection with Renyi entropy combined with packet-drop mitigation is demonstrated by Ahalawat et al. although they encounter limitations in the event of a multi-destination attack [37]. Kareem et al. apply Shannon's entropy for early detection in SDN with a focus on UDP-centric attacks [38]. Samta et al. classified flooding attacks based on traffic patterns-low weight with good coverage for silent attacks [39]. David et al. provides very rapid entropy-based flow analysis-very high bandwidth but not customized for SDN [40].

Leu et al. applied the Chi-square statistical test and received good detection accuracy with low complexity. However, performance depends on the static threshold selection [41]. Loukas et al. use the hybrid likelihood-ratio approach with a high precision but require training and not having SDN integration, attaining high with [42]. Oshima et al. uses short-term traffic statistics settings for higher detection early in the onset, it has a better vehicle

detection ratio [43], while Nosrati et al. combines Z-score and CUSUM for an adaptive online detection with low false positives and is mainly evaluated in VoIP environments with [44]. Shalini et al. addressed the flash-traffic filtering algorithm with the modified CUSUM scheme for SDN, the result of high accuracy attained but it increased computational complexity [45].

Most studies show that entropy-based and non-entropy-based statistical methods are highly effective at detecting DDoS attacks. However, this setup does not provide a single entropy metric, include a severity-aware classification, or incorporate SDN-mitigated mechanisms.

2.3.2 Using Machine Learning

The growth of Internet traffic and the increasing sophistication of DDoS attacks have sometimes made instances of signature-based intrusion detection technology often prove inadequate as part of an efficient protection system. Machine learning is often used to screen for DDoS at this scale, capable of detecting underlying patterns or learning the general principles of the flow of multiple attacks and counteracting them. ML-based DDoS detection systems extract information, classify the most efficient discriminative behavioural patterns, and then differentially classify legitimate and malicious flows to achieve significantly better identification with greater flexibility and tailoring to change, as opposed to rule-based methods. Consequently, the current principle of hybrid learning or ensemble learning to increase generalisation across most network environments and evolving attack types is still early research.

Melo et al. introduced a federated learning framework with an energy-based flow classifier for a better DDoS classification across heterogeneous networks. Accuracy evaluation of the bot-IoT, TON-IoT, and CICDDoS2019 datasets showed an enhanced cross-network generalization compared with stand-alone models and suggests the robustness of combining multiple learning paradigms [46]. The study related to managing resistant URL phishing compositions offers some findings on the influence of feature selection on classification accuracy through supervised machine learning. While the study is based on the task of detecting phishing Web sites, its findings are highly likely to benefit DDoS detection and further support benefit-centric feature-selection methodologies to handcraft efficient and accurate machine-learning-based security systems [47].

Table 2.2 Non-Entropy Statistical DDoS Detection

Ref	Method	SDN	Threshold	Technique	Performance	Advantages	Limitations
Leu et al. [41]	Chi-Square	No	Static	Stat Test	High Accuracy	Simple	Threshold Sensitive
Loukas G et al. [42]	LRT Hybrid	No	Static	Evidence Based	High Precision	Hybrid	Training Needed
Oshima et al. [43]	Short-term Stats	No	Static	Traffic Mean/Var	High Detection Rate	Early Detect	Not SDN
Nosrati et al. [44]	Z-score+ CUSUM	No	Adaptive	Change Detection	Low False Positive Rate	Online Detect	VoIP Focus
Shalini et al. [45]	Modified CUSUM	Yes	Adaptive	CUSUM + Flash Filter	High Accuracy	Flash Aware	Complexity

Table 2.3 Deep Learning Based DDoS Detection Methods

Ref	DL Method	Architecture	Feature Selection	Dataset	Accuracy	Severity	Limitations
Xu et al. [48]	Xatu	Multi LSTM	Aux Signals	ISP NetFlow	44%	No	Complex Model
Al-Eryani et al. [49]	Hybrid DL	GRU-BiLSTM	None	CICDDoS2019	99.9%	No	High Cost
Jayakrishna et al. [50]	Hybrid DL	CNN-LSTM	ADA & EGOA	CICDDoS2019	99.1%	Yes	High Complexity
Najar et al. [51]	CNN	Rule based	PCA	CICIDS2018	99.9%	Yes	SDN Specific
Makuvaza et al. [52]	DNN	Full Connected	None	CICIDS2017	97.5%	No	Binary Only

Table 2.4 Machine Learning Based DDoS Detection Methods

Ref	Method	Architecture	Feature Selection	Dataset	Accuracy	Severity	Limitations
Gebrye et al. [53]	FS + ML	RF, SVM, KNN	Boruta, RFE	CIC-IoT23	90%	No	Binary
Ongshu et al. [54]	Hybrid ML	ANN + RF	DS Optimizer	App-layer DDoS	99.9%	No	Single layer
Alam et al. [55]	Optimized ML	SVM-DEHO	KPCA	NSL-KDD	-	No	Not SDN
Coscia et al. [56]	Rule Gen ML	Decision Tree	Embedded	BUET-DDoS	99.7%	No	Signature based
Chen et al. [57]	Big Data ML	RF	Embedded	DNS Traffic	99.2%	No	DNS specific
Hill et al. [58]	ML	RF, SVM	None	Public SDN	-	No	Complexity
Hekmati et al. [59]	Correlation	Neural Network	Correlation	Urban IoT	81%	No	Complexity
Zhang et al. [60]	ML	SSAE-SVM	SSAE	Real-time	98%	No	Binary
Madathi et al. [61]	ML	KNN	None	SDN	97%	No	Binary
Rajakumaran et al. [62]	ML	GDA	None	SNMP	99.7%	No	TCP-SYN

Table 2.3 provides a summary of contemporary DDoS detection methods which use deep learning technology by showing their differences in network design, testing materials, system performance, and operational constraints.

Table 2.4 presents a comparative overview of representative machine learning–based DDoS detection methods in terms of employed models, feature selection strategies, datasets, detection accuracy, and limitations.

Xu et al. report a performance increase of 44% through their multi-timescale LSTM framework, although the method requires complex modeling and does not enable severity classification of results [48]. Al-Eryani et al. achieve 99.9% accuracy through their GRU-BiLSTM model, but the training expenses remain excessive [49]. Jayakrishna et al. develop a system that combines CNN and LSTM with optimization methods to achieve severity-level detection, yet the system now requires more complex implementation [50]. Najar et al. built a CNN-based SDN-specific framework that incorporates PCA and rule-based mitigation to reach 99.9% accuracy [51], whereas Makuvaza et al. used a fully connected DNN which produced 97.5% accuracy through its binary classification system [52].

The study by Gebrye et al. tested various classifiers through Boruta and RFE feature selection which resulted in a model that achieved 90% accuracy but only handled binary classification tasks [53]. Ongshu et al. created an ANN-RF hybrid system which they optimized through a DS optimizer to achieve 99.9% accuracy in their application-layer DDoS detection system that functioned at one detection layer [54]. Alam et al. combine SVM with DEHO and KPCA for optimized detection, but their framework does not support SDN environments [55]. Coscia et al. creates decision-tree-based rules through automatic generation which results in 99.7% accuracy although the system depends on signature-style rules [56]. Chen et al. use Random Forest on big-data platforms to detect DNS DDoS attacks which results in 99.2% accuracy although the method only works with DNS traffic [57]. Hill et al. examine various ML models through public SDN datasets [58].Hekmati et al. implement correlation-aware neural networks for IoT environments which results in 81% accuracy but demands more computational resources [59]. Zhang et al. use SSAE-SVM for their real-time detection system which achieves 98% accuracy [60] while Madathi et al. implement KNN in SDN to reach 97% accuracy [61]. Rajakumaran et al. used gradient descent-based prediction to achieve 99.7%accuracy in detecting TCP-SYN attacks [62].

The detection system achieves high accuracy through deep learning and machine learning; however, existing detection methods require high computational power and use binary classification, while lacking lightweight detection systems that can recognize multiple levels of system operation and leverage SDN-based mitigation methods for complete system protection.

2.3.3 Emerging Trends in SDN-Based DDoS Detection and Security

Shen et al. proposed an FFT-based traffic transformation method combined with transfer learning using an enhanced VGG19 network for DDoS attack detection. The model achieved 99.11% accuracy, 0.42% false positive rate, and 0.0183 s detection time on the CICDDoS2019 dataset. However, the approach requires computationally intensive FFT and deep CNN processing and may face challenges with encrypted traffic and large-scale SDN deployments also it focuses solely on attack detection and does not provide severity-aware attack classification or adaptive mitigation mechanisms [63]. Ahmed et al. proposed a Dynamic Graph Neural Network integrating GCT, Edge-Aware LSTM, and GAT for SDN-based DDoS detection. The model achieved 94.08% accuracy and 93.27% F1-score on an SDN dataset with over 700,000 flow records. However, the framework focuses only on attack detection, requires complex graph processing, and lacks severity-aware classification and mitigation capabilities [64]. Sumadi et al. proposed SsFLHT, a semi-supervised federated learning framework that combines pseudo-labeling, FedAvg aggregation, and GSCO-based hyperparameter tuning for DDoS detection in Software-Defined Internet of Drones Using the CIC-BCCC-NRC TabularIoTAttack-2024 dataset, the framework achieved 96.21% accuracy with MLP and 95.27% accuracy with CNN. However, the approach focuses on binary attack detection and requires complex federated training infrastructure [65]. Sbai et al. (2026) proposed a federated learning-based SIP-DDoS detection framework using GRU and RNN models with FedAvg, FedAvgM, and FedYogi aggregation algorithms for collaborative anomaly detection. The federated GRU model achieved up to 99.96% accuracy in detecting SIP flooding attacks. However, the framework focuses only on attack detection in SIP networks and requires federated coordination among multiple clients [66]. Komarchesqui et al. (2026) proposed an Explainable AI (XAI)-based intrusion detection framework that combines SHAP analysis with an optimized 1D-CNN-GAN model to improve transparency and feature selection for network attack detection. Using the CIC-DDoS2019 and CSE-CIC-IDS2018 datasets, the optimized model improved

F1-score by 3.65% and recall by 6.02% on CIC-DDoS2019, while achieving 19.9% higher F1-score and 32.3% higher Recall on CSE-CIC-IDS2018. However, the framework focuses primarily on explainability and attack detection and does not provide severity-aware DDoS classification or SDN-based mitigation mechanisms [67]. S. Niktabe et al. proposed an Explainable AI based IoT botnet detection and identification framework that combines XGBoost correlation-based feature selection, Bayesian-optimized LSTM, and SHAP analysis for bot profiling. Using the augmented BCCC-Aposemat-IoT-Bot-2024 dataset, the model achieved 99.99% accuracy, precision, recall, and F1-score. However, the framework is designed for IoT botnet detection and explainability rather than SDN-based DDoS defense and does not provide severity-aware attack classification or automated mitigation mechanisms [68].

2.4 Feature Selection and Dimensionality Reduction Methods

The analysis of high-dimensional network traffic data yields redundant data, irrelevant information, and noisy elements, thereby reducing detection accuracy while increasing processing demands. The techniques of feature selection and dimensionality reduction enable the identification of essential attributes that improve classification accuracy while decreasing training duration and making models more understandable. Detecting DDoS attacks requires efficient feature selection, as attackers use subtle alterations in traffic patterns to execute their attacks. Researchers have studied various methods for selecting or transforming features, including statistical, information-theoretic and projection-based methods, before using detection models.

2.4.1 Information Gain(IG) based Feature Selection Method

Information Gain (IG) is a popular filter-based feature selection method that relies on fundamental principles of information theory. The method determines the extent to which each feature helps decrease uncertainty about the target class. The system assigns higher ranks to features that deliver more precise information about determining whether network activity is normal or harmful. The combination of Information Gain's simple structure, minimal processing requirements, and independence from learning methods makes it a preferred tool for DDoS detection, helping identify key network attributes.

Several studies have demonstrated that IG is highly effective in reducing feature dimensionality while preserving discriminative information. Lee and Lee developed an Information Gain and divergence-based feature selection method that enables them to rank features according to their relevance while using novelty to select features without overlapping. Their approach achieves two benefits because it reduces the number of available features while boosting classification accuracy when compared to standard IG and greedy feature selection techniques. The method requires extra processing time because it needs to calculate dependencies between every pair of features which makes it unsuitable for real-time operations until it gets optimized [69]. Ramasamy and Kowshalya created an IG-based feature selection algorithm which identifies highly correlated features that scientists can use for their classification tasks. The results show better accuracy when scientists remove unnecessary and duplicate attributes from their research. The approach shows its main evaluation in textual sentiment analysis tests while researchers have not yet confirmed its ability to detect network traffic-based intrusions or DDoS attacks [70]. Shang developed a hybrid feature selection system which uses Information Gain and a Genetic Algorithm to find the best feature subset. The method successfully decreases vector dimensionality while boosting classification accuracy through the removal of nonessential and duplicate features. The genetic optimization method provides benefits, but it raises computational demands and it faces problems with reaching optimal solutions which affects its ability to handle extensive operations and quick processing needs [71].

Information Gain functions as an essential method for both feature selection and dimensionality reduction tasks. The implementation of standalone IG fails to account for redundant information while hybrid IG-based methods result in increased processing requirements. The research requires development of lightweight feature selection methods which enable better information representation through Information Gain and entropy-based measurement methods to assess feature selection relevance and diversity.

2.4.2 Mutual Information (MI) based Feature Selection Method

The Mutual Information (MI) measurement system quantifies the amount of information two entities share about a feature and its corresponding class label. The DDoS detection system uses MI-based feature selection to identify features with strong statistical links to attack patterns, thereby improving classification performance and system resilience.

The implementation of MI-based feature selection has become a common solution to tackle the problems of high dimensionality and dataset redundancy and noise present in complex datasets. Huang et al. presents a time-series feature selection method which uses MI together with Principal Component Analysis (PCA) to develop representative target variables that enable subsequent feature selection. Their method achieves successful dimensionality reduction which enhances condition recognition accuracy through the preservation of features that show strong system state dependency. The method needs PCA to produce target variables because this requirement leads to lower interpretability and higher preprocessing requirements according to reference [72].

Liu and Motani observe that most current MI-based feature selection methods believe they should select important features while they should eliminate redundant features because of their relevant yet distinct value. They introduced a boosted unique relevance assessment method which selected fewer features but increased classification performance by 2 to 5 percent. The method requires extra computational resources because it needs to calculate nearest neighbor distances which makes it better for offline work instead of immediate implementation according to reference [73].

The use of MI-based feature selection techniques results in both reduced dimensionality and improved classification accuracy. The existing MI methods struggle to control redundancy and select target variables, underscoring the need for hybrid methods that integrate MI with PCA and entropy-based approaches.

2.4.3 Entropy-Based Feature Selection based Feature Selection Method

Entropy-based feature selection techniques assess the uncertainty or randomness in individual features or feature subsets. The features become more discriminative when attackers exhibit entropy patterns different from those of normal users. Researchers have used various entropy measures, such as Shannon, Rényi, and Tsallis entropies, to evaluate features using both individual and combined methods. The approaches effectively detect DDoS attacks by showing how they disrupt normal traffic patterns.

Khan and Naeem present their framework for DoS attack feature selection which combines entropy and granular computing methods to evaluate traffic characteristics. Their findings demonstrate that entropy-based feature reduction methods successfully decrease feature

dimensions while maintaining classification performance. The method depends on specific granulation levels which cause performance issues when users select incorrect granularity options [74].

Lotfalizadeh and Kim study real-time entropy characteristics which they obtained from partial flow categories in SDN environments. The method uses flow grouping which combines time-based and packet-count properties to create more detailed traffic patterns that enhance DDoS attack detection at early stages. The research shows that entropy features can effectively track changes in attack distribution during cybersecurity attacks. Short time-window monitoring creates extra communication needs for switches and controllers which results in a trade-off between system detection performance and operational expenses [75]. Kachavimath and Narayan present a multi-feature selection framework for SDN which combines statistical feature ranking with ensemble learning. Their results demonstrate that using 10 of the 81 most relevant features leads to better detection performance and operational efficiency even though their approach does not depend entirely on entropy. The study shows that organizations need to adopt multiple feature selection methods because single techniques do not provide adequate results [76].

The study proves that entropy-based feature selection effectively detects changes in traffic distribution while decreasing the number of required features. The system still faces three unresolved problems which include its dependence on specific parameter configurations and the need to create time window settings and manage redundant information.

2.4.4 Principal Component Analysis (PCA) based Feature Selection Method

Principal Component Analysis is a widely used method for reducing dimensionality, as it transforms the original data into a smaller set of independent principal components that retain most of the original data variance. PCA reduces computational costs and enhances classifier accuracy by eliminating redundant information and unnecessary data elements. The attributes created through PCA transform the original data into new components that users find difficult to understand.

The application of PCA has become a widely used method for reducing dimensions and extracting features from high-dimensional datasets. Razzaque and Badholia demonstrate that applying PCA before feature selection significantly reduces thousands of original features to

a very small subset which enables efficient learning while improving classification accuracy for SVM, KNN and Naïve Bayes classifiers. Their results confirm that PCA effectively removes redundancy and noise; however, the transformed components lack direct interpretability which makes it difficult to associate principal components with original domain features [77]. Basicevic et al. investigate the integration of PCA with entropy-based DoS detection and show that using only the principal component of two basic traffic features (source and destination ports) can achieve strong detection performance. The study shows that PCA increases attack-related entropy changes which results in better detection performance through improved detection rate F1-score and detection delay when compared to using raw features. The approach evaluates SYN flood traffic but uses only a few features which makes it difficult to apply the method to different attack types [78].

Wang et al. present a moving-window PCA-based anomaly detection framework that protects SDN networks through traffic matrix analysis which identifies normal and abnormal traffic patterns. Their method successfully detects threats with high accuracy while maintaining low false alarm rates and achieves real-time threat control through defensive flow rule installation at switches. The method requires specific window size and threshold value selection because its lightweight design does not operate well under extreme traffic environment changes [79]. PCA enables dimensionality reduction of features which helps to increase learning speed and detection capabilities.

Information Gain, Mutual Information, Entropy-based methods, and PCA all reduce dimensionality while enhancing detection capabilities, but each address only feature relevance, with its own limitations. The analysis of traffic patterns requires multiple feature selection methods, as no single method can provide a complete understanding of both feature significance and traffic distribution patterns. The proposed Information Gain-driven framework, together with entropy-based analysis, will deliver effective DDoS detection that works under various conditions in SDN environments.

2.5 Multi-level and Severity-Aware Detection Systems

Most existing DDoS detection systems employ traditional binary classification approaches that categorize network traffic as either normal or malicious. Although these methods are effective in identifying the presence of attacks, they are unable to distinguish between different levels of attack severity or behavioural characteristics. DDoS attacks can vary

considerably in intensity, ranging from low-rate attacks that subtly degrade network performance to high-rate flooding attacks that rapidly exhaust bandwidth and computational resources. Each attack category exhibits distinct characteristics and may require different mitigation responses. Consequently, increasing attention has been directed toward multi-level, severity-aware detection systems capable of classifying traffic into categories such as normal traffic, low-severity attacks, and high-severity attacks. By incorporating severity awareness into the decision-making process, these systems enable more accurate threat assessment and facilitate adaptive mitigation strategies, thereby improving service availability and resilience in SDN-enabled network environments.

2.5.1 Binary vs multi-level DDoS detection

DDoS monitoring tools present a classic binary classification of observed traffic flows into normal versus attack traffic. Although good enough for simplistic detection, a binary scheme fails to capture various levels of attack intensity or behaviour, with multiple-level or -class detection frameworks have started to evolve that would classify traffic into finer categories, hence providing room for a much more precise and adaptive kind of mitigation for different attack severities. Kumavat and Gomes suggested a multi-layer DDoS detection and mitigation protocol for IoT-based networks with a trust-based approach across several protocol layers. While the implementation has led to improvements in network performance, it lacks the categorization of attacks into low or high volume [80]. In another study by Pradeesh et al. proposes a framework for hybrid and multiclass DDoS detection in SDN that categorise various attack types with high accuracy, for which a more computationally involved learning system has been used; however, the assigning of low and high-rate attacks is not clearly defined [81].

Given the summary of multi-class models being developed in the current scenario, the least of the techniques that have been used for binary classification is lightweight classification wrapped in severity, combined with SDN mitigation.

2.5.2 Low-rate vs High-rate DDoS Detection

Zhou et al. propose a low-rate DDoS detection method based on the expectation of packet size (EPS), which distinguishes attack traffic from legitimate traffic by identifying the consistent difference in packet size distributions, enabling effective detection of low-rate

DDoS attacks [82]. Bhuyan et al. used numerous information theoretic measures for the identification of both low-rate and high-rate DDoS attacks, showing that the proposed second-order interval statistics and entropy-based measures adequately reveal the dynamics of changes in traffic distribution. Their work does not consider any notion of selection of features on an adaptive basis or solid modeling at different levels of severity [83].

Na et al. use Rényi entropy in a hybrid Trans-KAN deep model to detect low-rate DDoS in SDN, and thus it attains a high accuracy and low false alarm rate. Nonetheless, the model only targets low-rate attacks, and it cannot perform severity-aware classification and mitigation discrimination [84]. Abu Al-Haija and Droos analyze adversarial low-rate DDoS attacks and reveal that IDS models have vulnerabilities against evasions. While also emphasizing issues on robustness, there exists no proposed multi-level or SDN-integrated way for detection [85].

Most of the present DDoS detection algorithms are inclined towards the binary or single-level system and do not portray varying attack severities at the low-rate and high-rate behaviours. Or else, a few researchers have undertaken case studies with respect to multi-class or low-rate detection, leaving most united with severity-aware modelling and not having tight integration with SDN-based mitigation. It was these very gaps which triggered the suggested framework.

2.6 SDN-Based DDoS Mitigation Strategies

Software Defined Networks (SDN) offer unique capabilities to counter the Distributed Denial of Service (DDoS) threats with centralised network visibility, programmability, and dynamic control over forwarding behaviour. Mitigation capabilities in traditional networks are either static or device-specific, but SDN enables the instant deployment of mitigation policies by modifying flow rules, controlling traffic rates, and diverting malicious flows in real time via the controller. Centralised control enables the network to respond to detected attacks quickly and to adapt mitigation strategies based on traffic conditions and attack characteristics. Various mitigation frameworks based on SDN have also been studied, such as rate limiting, flow rule blocking, honeypot etc. Each category addresses different aspects of the attack surface, but most works focus on a single mitigation action and lack tight integration with severity-aware detection, motivating the need for coordinated multi-level mitigation.

2.6.1 Rate Limiting Based Mitigation

Several studies endorse the view that rate limiting continues to be a lightweight and practical way by which to combat various flooding-based DDoS attacks that utilize traffic thresholding to restrict the flow of unwanted traffic prior to network resource exhaustion. Feraudo et al. enhanced the Manufacturer Usage Description standard by adding fine-grain packet rate and byte rate permission that IoT gateways can apply via either custom eBPF or iptables. Their system utilizes real datasets from IoTs in its continuous learning in obtaining normal thresholds in traffic and implementing device-level rate control, thus crushing botnet-savvy traffic spikes while preserving legitimate communications [86].

El Kamel et al. have suggested a sliding window rate limiting framework against dynamic online deep learning at the SDN controller side. Their approach is designed to tap into the controller queue occupancy and switch flow table usage to assign dynamic weights to hosts. Wicked hosts with low credibility are penalized by enabling rate limiting or temporarily blocking their PacketIn requests, which helps in substantively reducing controller overload or flow-table saturation under an attack [87]. Rouf et al. devised a security framework for IoT, which integrates a specific security layer featuring rate-based limiting and traffic control mechanisms between the middleware and communication layer. The purpose of the framework is to decrease excessive request rates coming from compromised devices and to deter these compromised devices from joining large-scale DDoS campaigns to enhance the overall IoT network resilience [88]. Molsa experimentally investigated how rate limitation could help in restraining TCP flood attacks: the intermediate rate limit managed to bring down the attack traffic while maintaining an appropriate throughput for benign TCP flows. Thus, among different measures including complete blocking it is better to use rate limiting as an early-response mechanism because that is how it partially degrades the attack without annulling service completely to good stuff [89]. Wang et al. introduce Flood Guard, integrating packet washout and rate-limited forwarding of table-miss flows in SDN. Flooding packets are temporarily stored at the data plane level and relayed to the controller using rate limiting and round-robin scheduling, ensuring that whatever happens, the controller and the data plane remain protected from saturating one another for policy enforcement [90].

Most existing rate-limiting approaches reduce the impact of DDoS attacks quite well, providing SDN controllers with adequate protection; however, they rely solely on fixed or

traffic-based thresholds and offer no guidance for selecting mitigation actions based on attack severity.

2.6.2 Flow Rule Blocking

Some researchers have applied the principle of flow rules to block and ameliorate malicious stuff like traffic that depletes the resources of switch and control in case of SDN-based mitigation mechanism. As observed by Srivastava et al., compromised switches produce excessive flow-rule requests, saturating controllers; their approach, however, detects changes in the flow-rule request traffic and isolates dangerous switches, completely blocking them so that no more harmful requests through these switches will go further [91]. A framework coined by Dridi and Zhani, SDN-Guard, that dynamically reroutes suspicious traffic, adjusts flow timeouts, and aggregates flow rules, thus effectively constricts malicious flow entries in switches. This is an approach aimed at reducing controller load and switching TCAM usage when it is under attack [92]. Shin et al. provide actors that extend OpenFlow switches with connection migration and activating triggers. Only successfully established TCP connections pressure the controller for rule installation. In this sense, AVANT-GUARD can work as a very effective means to filter out those spoofed or incomplete flows and at the same time to restrict slaughter at the control plane [93]. Phan The Duy et al. proposed a controller-based flow filtering approach to scrutinize PacketIn messages, identify and remove malicious flow entries, and block new rules from untrusted sources, thereby enhancing flow table availability during DDoS attacks [94].

For the effective security of SDN infrastructure, flow rule blocking mechanisms may prevent a malicious life flow from being installed. Too common for those to work with the preset rule and adaptive mitigation system representing thresholds rather than sharing intelligence between all factors.

2.6.3 Honeypot Based Mitigation

Attacks are lured to decoy systems by honeypots to waste hours of their time far from production resources and ultimately to become more easily threatened through intense introspection about their own actions. In combination with SDN, honeypots can be initialised and empowered as required, allowing traffic to be redirected to these decoys according to rules. Now they can respond to DDoS attacks automatically and flexibly.

The model of Rabah et al. discussed in the paper presents an SDN-UAV architecture that combines ensemble learning with the specially dedicated Honeypot UAV to detect and mitigate DDoS attacks. In this model, ensemble classifiers first work to identify malicious traffic, intercept attackers using a honeypot UAV to collect attack traces and thereby continue to refine learning models. Detected attack sources are then blocked or isolated by SDN controllers to improve the speed and efficiency of this detection and alerting core [95]. HoneyMix is a new kind of honey SDN-based honeynet that manages dynamically multi-honeypots and intelligently routes incoming suspicious traffic into the proper decoy nodes. The system offers the capability to distribute multiple decoy nodes, reducing visibility of real services for even serious attackers [96]. In another study, a novel traffic mis categorization technique that can be employed together with the H-Series profiling and SD-honeypot architecture and concentrate on generating a relatively classified and more interactive approach to identifying potentially malicious flows, which further hinders threat actors' behaviour [97]. One possible approach for Industrial IoT environment SDN-enabled honeypots involves lightweight decoy services mimicking genuine devices, where suspicious activities will be automatically directed by the controller to the proper honeypot pool. Operation system disruptions are minimized, and threat visibility is enhanced [98].

With the enhancement of the honeypot, a useful measure for attack mitigation, we now have an effective mechanism for attack isolation and intelligence gathering. However, most existing attack-mitigation methodologies focus primarily on binary prevention rather than traffic-based classification by attack severity.

2.6.4 Controller Based Mitigation

Mitigation strategies relying on the controller seek to defend the control plane of SDN through the introspection of the detection and response mechanics of the controller within. Considering that the controller is most vital and can present a single point of failure, such approaches emphasize attacking the problem of control-plane flooding by means of early detection of harmful traffic and immediate application of countermeasures.

The FLOODGUARD mitigation, as described by Wang et al., moves table-miss packet handling to the data plane and forwards packets to the controller using rate limiting and scheduling, and helps to prevent large amounts of malicious packets from directly attacking the controller [84]. Dridi and Zhani presented SDN-Guard, a controller-oriented mitigation

architecture making decisions such as rerouting suspicious traffic, adjusting flow timeouts, and aggregating flows to alleviate the adverse effects of the DoS attacks upon both controller and switches. Their model is significantly less aggressive in attack situations, thereby reducing TCAM exhaustion and control-plane traffic [92].

Kumar et al. proposed SAFETY, an early detection-cum-mitigation framework for SYN flooding attacks using TCP and entropy in the SDN which examines entropy in the destination IP address and patterns of order of the TCP flags through the controller to spot possible abnormal behaviours, so that mitigation could catch in before the latter spill over the controller resources. As the blueprint intensifies, therefore, the firm resisted the way to lessen the power of the buggy Controller [99]. Ishtiaq et al. study DHCP-based denial of service (DoS) and starvation attacks targeting SDN controllers and propose a verification mechanism that filters out malicious DHCP discovery packets at the controller. The only authenticated DHCP requests are passed on to switches, thus improving network throughput and minimizing packet loss in the presence of an attack [100]. While providing effectively robust SDNs, controller-based mitigation solutions focus on fortifying merely the control plane; they cannot improvise the system based on severity-aware decisions or coordinated multi-level mitigations, thus necessitating the input of an architecture.

Table 2.5 Comparative Summary of SDN Based DDoS Mitigation Strategies

Mitigation Category	Core Idea	Typical Actions	Strengths	Limitations
Rate Limiting	Restrict traffic rate	Packet In messages	Fast, lightweight	Static thresholds
Flow Rule Blocking	Drop malicious flows	Drop rules	Direct suppression	False blocking
Honeypot Based	Divert to decoys	Redirection	Attack isolation	Extra resources
Controller Based	Protect controller	Request filtering, caching	Controller resilience	Limited scope

Table 2.5 offers a comparative summary of the same SDN-based DDoS mitigation strategies that are identified into several categories such as rate limiting, difference in the way different strategies approaches mitigation ranging from traffic throttling to direct packet dropping or isolating attackers and protecting the control plane. All these mechanisms are effective forms of localized defense, working independently of one another and based on static or coarse-

grained punitive policies, without coordination and severity-based mitigation. Furthermore, the observation provides an insight into why the multi-level detection and adaptive mitigation system components designed in this work must be integrated.

2.7 Benchmark Datasets for DDoS Detection

Benchmark Datasets are very important when it comes to judging and comparing DDoS detection methods as these standard traffic traces contain the normal and attack behaviour. The availability of good quality datasets gives the researcher the opportunity to measure the detection power, stability, and adaptation of the detection system in conditions as close to the reality as possible. Various datasets have been put forward and utilized in DDoS research for various periods of time which include CICDDoS2019, ISCX2012, UNSW-NB15, and CAIDA DDoS 2007 datasets.

The new work by Sharafaldin et al. extends the CIC intrusion datasets by proposing the CICDDoS2019 dataset, which is centered on contemporary DDoS attack scenarios involving very large volumes of traffic. The dataset provides a range of labelled sealed flows for reflective, and flood based e.g., DNS, UDP, ICMP and SYN etc. as well as normal network traffic processed using CICFlowMeter. This paper explains that such a dataset may allow for an extensive study of various types of DDoS attacks and appropriate design methods for both ML and DL classes of models [101]. According to Shiravi et al., the shortage of realistic and well-labeled openly available data is the core complication of the intrusion evaluation as well as DDoS prevention systems. They propose to address the issue by providing a clear process for creating benchmark intrusion datasets ISCX2012 based on traffic patterns and attack scenarios observed from actual networks. Such methodology produces datasets that are reproducible, labeled and contain portions of the data-bearing packet payloads, which are useful for anomaly detection as well as signature detection studies [102].

Moustafa and Slay provide the UNSW-NB15 dataset, which was collected using the IXIA PerfectStorm tool and captures recent attack types as well as incorporates realistic background traffic. The dataset is rich in flow-based features and attack classes, which helps in the performance evaluation of the machine learning methods for intrusion and DDoS detection. UNSW-NB15, as they mention, reproduces some of the network behaviours more effectively than outsiders over old data sets [103]. The Centre for Applied Internet Data Analysis presents the CAIDA DDoS 2007 data set, which includes obfuscated backbone line

traffic collected during the period of a high intensity DDoS assault. In contrast to the artificial datasets, this segment represents the real activity of an attack and the related traffic flows, thus being useful for the investigation of volumetric attacks and the evaluation of detection mechanisms in practical scenarios [104]. Given diversity, volume, and normative labeling, these datasets have become judiciously used in current work. For that reason, the CICDDoS2019 dataset primarily selected with its quality coverage of attack possibilities relevant to all DDoS scenarios.

In this thesis, the term Distributed Denial of Service (DDoS) is employed in a broad sense. The CICDDoS2019 dataset classifies several attacks as DrDoS, which represents a DDoS variant based on reflection and amplification. Hence, to maintain consistency, the terms DDoS and DrDoS are treated as having the same meaning within this study's framework.

2.8 Research Gaps

Many works aim to detect and mitigate DDoS in Software Defined Networks using statistical and machine learning techniques. However, scrutinising the literature makes it clear that there are still some challenges in DDoS attack detection, and many more with changing attitudes and further elucidation.

First, most applied research on feature selection uses redundant methods such as mutual information, PCA-based, and entropy-based ranking. These techniques alone do not sufficiently reflect feature relevance nor the level of even traffic distribution. Given that there is no joint entropy- or information-gain-based approach to feature selection, this results in the inclusion of excess features or an incomplete picture of attack behaviour in most cases.

Second, it can be noted that many detection models focus on binary classification, assuming that all traffic is either normalised or malicious. There are a few works that consider classification and detection of multiple classes; severity-based classification to determine high- and low-threat attacks has yet to garner much interest. Lack of severity, however, may make it difficult to properly classify attacks and implement necessary remedial measures.

Third, though SDNs offer great programmability with centralised management, the coordination of existing systems for detection and utilising SDN-centred mitigation is weak. The detection or mitigation process is disjointed and, in many cases, the mitigative action, for example, rate limiting, traffic blocking, or redirecting such requests to honeynets, does

not arise from a decision of the detection mechanism. Finally, it has also been observed that advanced machine learning and deep learning-based solutions achieve high accuracy, but this results in higher computational complexity due to the large size of the features most of the time. It is because such complexity will make it difficult, or even impossible, to employ SDN in real-time mode.

These limitations emphasise the importance of designing a lightweight, functionally optimised, and severity-aware framework that combines Information Gain-driven sequential feature selection and joint entropy analysis, enabling DDoS detection and SDN-based mitigation across multiple steps. Along these lines, this thesis primarily aims to address these weaknesses.

2.9 Scope of Research

The research is directed to the design and development of a multi-level DDoS detection and mitigation System using a machine learning model. To do so, the research hinges on feature selection, a multi-level classification scheme, and SDN-based mitigation against DDoS. In this multi-level architecture, Sequential Feature Selection based on Mutual Information and Joint Entropy Analysis is applied to extract relevant traffic features. Machine learning Classifiers are used to subdivide traffic into normal, low-severity, and high-severity attacks. In addition, flow-based gear, such as flow blocking and redirection using a honeypot, is used in SDN to combat the active process and mitigate the extent of the problem. For experimental purposes, the benchmark dataset used is the CICDDoS 2019, while the Mininet–Ryu SDN emulation system is used to test and demonstrate the effectiveness of the detection and mitigation systems in real time.

The scope of this research is limited to DDoS attacks categorised as network and transport-layer attacks and to flow-based traffic analysis. The study excludes other types of attacks, such as application-layer attacks or application-specific attacks, insider threats, and risks caused by cyber threats, such as viruses, email sending, and other data breaches. There is no deep packet inspection or payload analysis. Additionally, this framework is designed only for the existing SDN architecture but does not seek to design any new SDN controllers or even hardware. This study considers machine learning models; however, it does not concern itself with the construction of such networks.

CHAPTER 3

SYSTEM MODEL & PROBLEM FORMULATION

This chapter presents the system model and problem formulation for the proposed Information Gain based multi-level DDoS detection and mitigation framework designed for SDN. It begins by describing the SDN-based threat model, which identifies potential attack surfaces across the data, control, and application planes. Subsequently, an attacker model is introduced to explain how adversaries can launch DDoS attacks at varying intensities, including both low-rate and high-rate attacks. The network model outlines the SDN architecture comprising controllers, switches, and end hosts, which collectively facilitate traffic monitoring and feature extraction. Furthermore, the chapter formally defines DDoS attack severity and categorise network traffic into three classes: normal traffic, low-severity attacks, and high-severity attacks. The system constraints and operational assumptions considered in this study are also presented. Finally, a mathematical formulation of the multi-level DDoS detection and mitigation problem is developed, and the design objectives of the proposed framework are established.

3.1 SDN-Based Threat Model

Essentially, SDN architecture is made up of three logical planes, namely, the application plane, the control plane, and the data plane. FIGURE 3.1 shows the final architecture with places where Distributed Denial of Service (DDoS) may be located. These three planes have well-defined boundaries within an SDN architecture-and with attackers' clever handling and understanding of these boundaries, SDN elements can be made vulnerable and exploited.

At Application plane, DDoS attacks victims and SDN applications and network services are there, they do so by flooding those services at application-layer levels and using reflection-based techniques through LDAP, MSSQL, NetBIOS, Portmap. In essence, these attacks starve out application resources or disrupt the policy and management functions, ultimately afflicting the global control logic in the network.

In the case of control plane, the SDN controller holds a most crucial position as well as a significant failure point. Enormous amounts of attack traffic on SYN, UDP, or DNS are created, thereby causing extensive PacketIn messages and flow setup requests that lead to overload and fill the controllers. Such attacks significantly disrupt the controller's ability to manage the switches and enforce forwarding rules, resulting in disruption of services across the entire network.

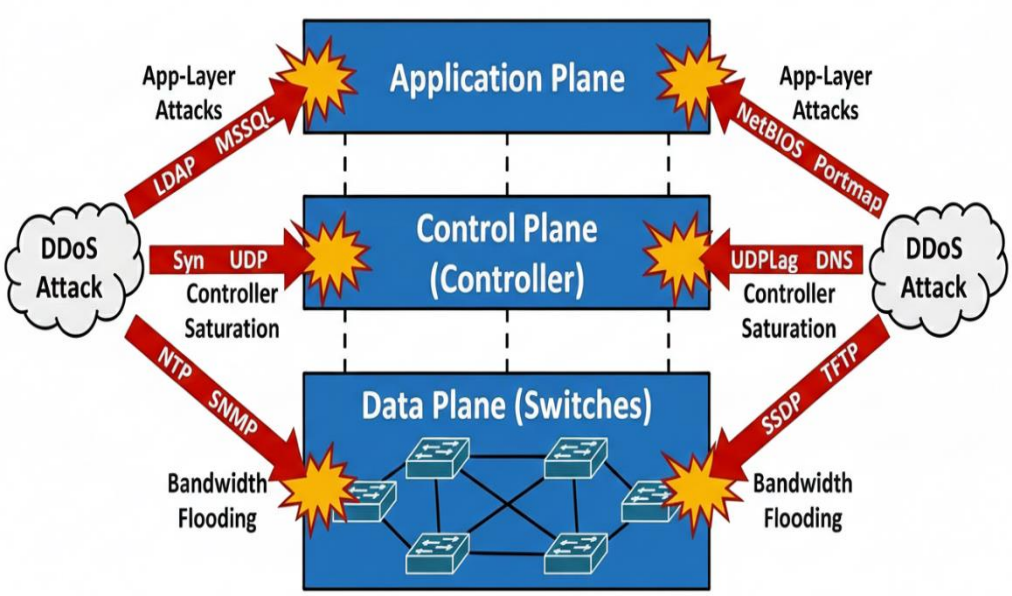


FIGURE 3.1 SDN Architecture with Threat (DDoS) Locations

At the data plane, switches and forwarding entities are typically attacked using volumetric floods and reflection-based attacks like NTP, SNM, SSDP, and TFTP attacks. These consume volumetric bandwidth and switch resources, leading to the blockage of flow table exhaustion with some dash packets delivered to rightful users.

This typical threat model, in its examination consists of several parts which include the attackers' launching attacks of low intensity that stifle the system's performance much more or less in a stealthy way, and it also includes attacks of high intensity such as floods which consume the resources of the network in a quick span of time. The model put forward proposes that traffic within these planes is examined, and as soon as any degree of abnormal activity is experienced, measures are implemented such as SDN active protection of the network's resources.

3.2 Attacker Model

The suggested framework accounts for a remote adversary able to initiate Distributed Denial of Service (DDoS) attacks against an SDN-enabled network. Assumptions forming the attacker model include:

- Many compromised systems are distributed across the Internet and controlled by the attacker.
- The attacker can generate both low-rate stealthy and high-rate flooding attacks. Low-rate attacks seek to slowly reduce network performance gradually and evade simple threshold-based detection. High-rate attacks seek to quickly drain bandwidth, switch flow tables, or controller processing resources.
- The attacker can employ various protocols such as TCP, UDP, ICMP, DNS, and reflection-based services. The attacker may spoof source addresses and alter traffic patterns dynamically.
- The intruder lacks direct access to the SDN controller and is unable to alter controller applications.
- Network switches and the controller are assumed to be trusted but susceptible to resource exhaustion.

Under this attacker model, the adversary's goal is to reduce network availability and disrupt legitimate services. The proposed framework seeks to identify malicious activities across varying severity levels and implement suitable SDN-based countermeasures.

3.3 Network Model

The proposed framework in FIGURE 3.2 envisions an SDN-enabled network consisting of a collection of forwarding devices, a centralized SDN controller, and various end hosts. The network is logically centralized yet physically dispersed, where switching decisions are carried out by switches according to flow rules set up by the controller. The data plane contains OpenFlow-enabled switches that route packets by entries in their flow tables. These switches gather traffic statistics such as the number of packets, bytes, and flow period and send it to the controller for analysis, on a periodic basis. The control plane is effectively

where the central SDN controller maintains a global network view, installs flow rules, and coordinates an action-to-detection sequence. The application layer being part of the network management and security application encompasses those applications, stages, or considerations of various abstraction levels, the suggested multi-tiered DDoS detection and mitigation module first and foremost.

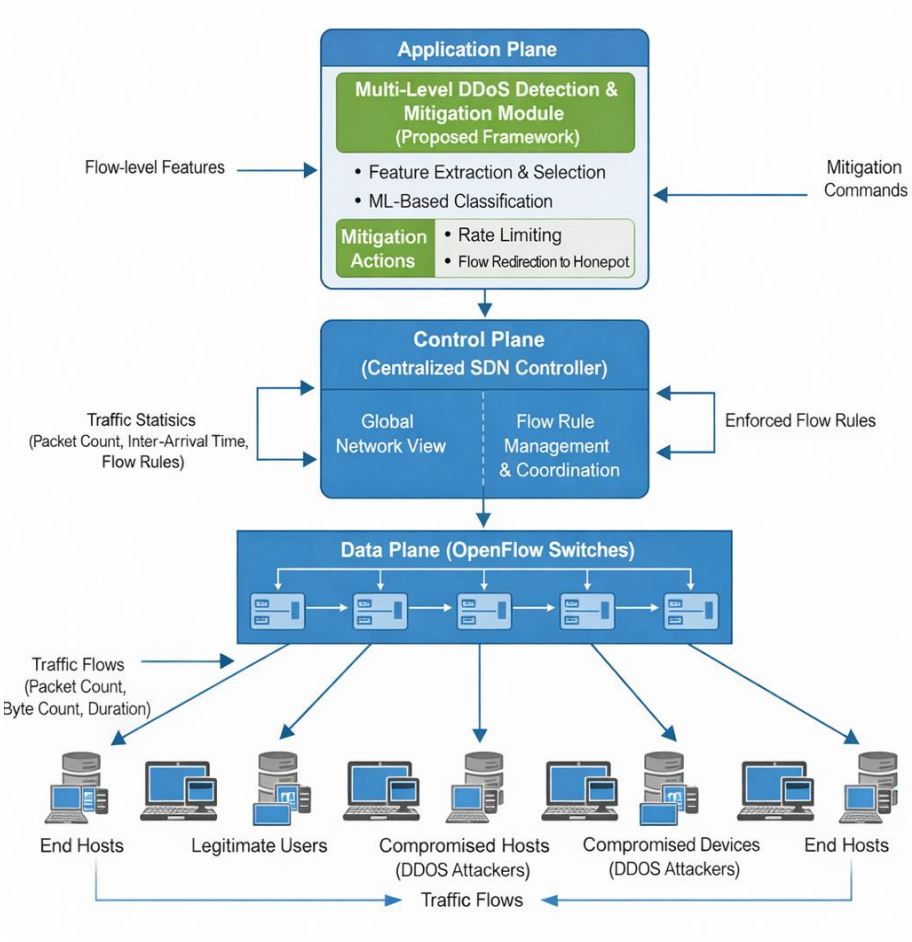


FIGURE 3.2 Multi-level DDoS Detection and mitigation framework in SDN

The end hosts should be well connected to the switches, which could indicate legitimate users or compromised devices participating in DDoS attacks. Their traffic flows are generated through the data plane and observed by the controller. Then, the controller extrapolates flow-level features and implements the given sequential feature selection and ML-based classification. When a decision is made, the controller will enforce mitigation actions like rate limiting, flow blocking, or redirection to honeypots. Communication assumes that it is reliable and secure between the controller and switches. This network model is a simple yet representative abstraction of a real SDN environment, which could help in implementing and analysing the proposed architecture.

3.4 DDoS Severity Definition

Any DDoS attack varies in comparison to another DDoS attack with respect to volumes of traffic, duration, and the degree of impact on the network's performance. A few attacks, for instance, generate very high level of traffic when bandwidth and computer resources are exhausted within a short period of time while, in other cases, the rate of attack is at low rates and the differences between outgoing and incoming traffic are not detected. So, it is not enough to consider DDoS attack as one class because one cannot treat them all at once and expect to detect or mitigate them effectively. In this research, the severity level of DDoS is characterized by the power and effect of attack traffic on network resources.

- Normal Traffic: Authentic network traffic adhering to standard usage patterns and does not degrade network performance.

- Low-Severity DDoS Traffic: Low-rate attack traffic that results in slow performance decline, increased latency, or slight packet loss but does not immediately overwhelm network resources.

- High-Severity DDoS Traffic: Aggressive flooding data that quickly uses up bandwidth, switch flow capacity, or controller processing resources, causing major service interruptions.

The severity levels are established based on flow-level statistical and information-theoretic attributes that are extracted at the controller and chosen via the proposed sequential feature selection process. Severity-informed classification permits the system to implement proportional mitigation strategies, such as moderate rate limiting for low-severity attacks and rigorous flow blocking for high-severity attacks.

3.5 Assumptions

The designed hierarchical DDoS detection and mitigation framework is developed under the following assumptions:

- The SDN network is made up of six OpenFlow-enabled switches and includes eight end hosts, creating a representative testbed topology.

- The SDN controller is considered trustworthy and functions correctly but may be vulnerable to resource exhaustion attacks. Communication between the controller and switches is secured and dependable.

- End hosts may behave as legitimate users or may be compromised to generate DDoS traffic. The framework considers four types of DDoS attacks, including volumetric and reflection-based flooding attack vectors.

- Both live traffic generated in the SDN testbed and offline benchmark data are used utilized for evaluation.

- The CICDDoS2019 dataset is considered to accurately reflect modern DDoS attack characteristics and benign traffic.

- Flow-level statistics collected at the controller are sufficient for feature extraction and classification.

- Machine learning models are trained offline and deployed online to facilitate real-time detection capabilities.

- Mitigation measures initiated by the controller are executed immediately by switches.

CHAPTER 4

PROPOSED METHODOLOGY

4.1 Overview of Proposed Framework

In this chapter, we introduce a model Information Gain Driven Multi-Level DDoS Detection and Mitigation Framework for Software Defined Networks using Machine Learning. The aim of the framework is to accurately detect the severity levels of DDoS attacks and to provide adaptive, SDN-native mitigation with low computational overhead and high detection reliability.

The proposed framework is divided into two main parts: offline training data and real-time detection and mitigation data within the SDN framework. In its offline stage, flow-level features are extracted from the traffic data, labelled by the CICDDoS2019 dataset, and the live SDN testbed traffic. Subsequently, a sequential feature reduction strategy would select the most informative ones using Mutual Information for first selection and Joint Entropy for redundancy reduction. That way, a compact yet discernible feature subset is created. The machine learning models are deployed using the selected features, enabling them to learn a range of multilevel traffic patterns associated with normal, low-intensity, and high-intensity DDoS attacks.

Switch-level performance measurements are fetched from SDN switches using a controller that helps in online traffic collection, essentially enabling real-time statistics. After receiving flows from online traffic instances, feature extraction and feature selection are performed. Trained machine learning models classify these considering the degree of severity. The outcomes also help the controller to act in terms of actions that could be mitigated-like rate limiting when it is at low-severity level and flow rule blocking, when it is at a high-severity level. This close loop between detection and mitigation leads to fast reaction and reduced impact of the attack.

What distinguishes the proposed framework is the key novelty of Information Gain-driven sequence feature selection, layered with joint entropy assessment, while considering

different degrees of attack intensity and reinforcing SDN mitigation capacities. By maximising feature robustness, classification precision, and mitigation sensitivity concurrently, the framework successfully meets the modern need to protect SDN infrastructure against variant DDoS threat vectors.

4.2 Architecture of the Proposed System

The suggested design that is Information Gain–driven multi-level DDoS detection as well as mitigation scheme comprises of few inter-related modules within a SDN framework. The system proposed has a workflow explained in a diagram in FIGURE 4.1 The aspects of the functional architecture are as follows.

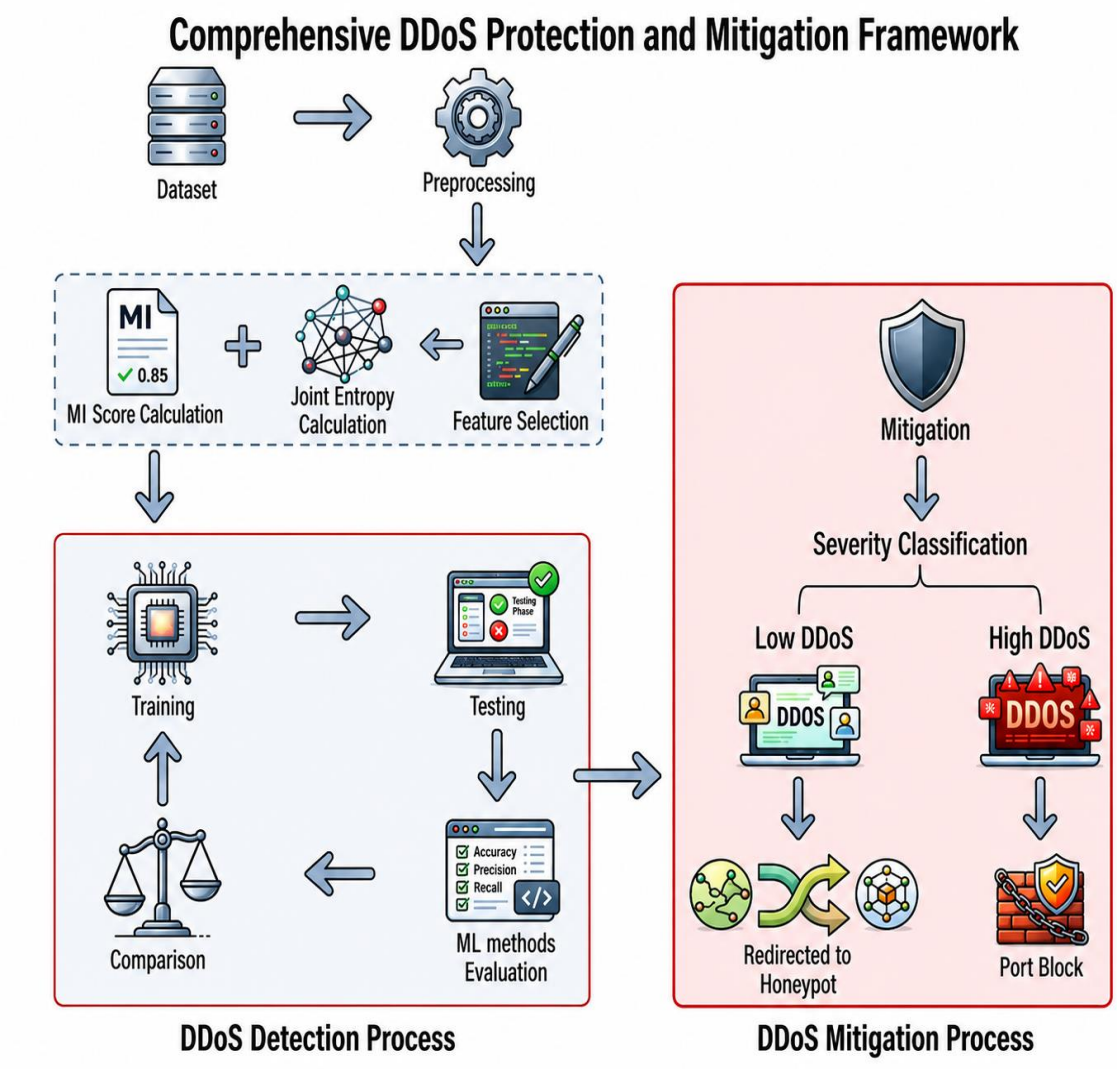


FIGURE 4.1 Workflow of the Proposed Framework.

4.2.1 SDN-Based Implementation Environment

The proposed framework has been realized in an SDN domain comprising an SDN controller, OpenFlow switches, and hosts. In a typical deployment, the controller, which has a centralized view of the network, connects to the switches via the southbound interface to aggregate flow statistics and enforce forwarding rules. Any flow sourced by an end host traverses the switches, which monitor packet headers and flow statistics. These are sent to the controller in a timely manner. The centralized approach of SDN enables rapid rule revision and the implementation of detection and mitigation mechanisms within the network.

4.2.2 Feature Selection Module

Algorithm 4.1 begins by preprocessing the network traffic dataset to remove missing values, duplicate records, and normalize feature values. Mutual Information (MI) is then computed for all features, and the top-ranked features are selected based on their MI scores. Joint Entropy is applied to the selected features to evaluate their relevance and redundancy, resulting in an optimal feature subset. The selected features are used to train and validate a machine learning model, and performance metrics such as accuracy, precision, recall, and F1-score are evaluated. Finally, dynamic thresholds (α and β) are calculated from the mean Information Gain values of different traffic classes and stored along with the trained model for real-time DDoS detection and severity classification.

Algorithm 4.1: Feature Selection Module

Input*: Network Traffic Dataset D*
Output*: Trained Model M, Thresholds α and β*
1: *Load dataset D*
2: *Preprocess dataset*
   a. Remove missing values
   b. Remove duplicate records
   c. Normalize feature values
3: *Calculate Mutual Information (MI) score for each feature Fi*
4: *Rank features in descending order of MI score*
5: *Select Top K ranked features*
6: ***For*** *each selected feature Fi* ***do***
7: *Compute Joint Entropy H (X, Y)*
8: *Evaluate feature relevance and redundancy*
9: ***End For***
10: *Select optimal feature subset Fs*

11: *Split Fs into Training Set and Testing Set*
12: *Train Machine Learning Model M using Training Set*
13: *Compute mean Information Gain values:*
    μN ← Mean IG of Normal Traffic
    μL ← Mean IG of Low DDoS Traffic
    μH ← Mean IG of High DDoS Traffic
14: *Calculate dynamic thresholds:*
    α ← (μN + μL)/2
    β ← (μL + μH)/2
15: *Validate model M using Testing Set*
16: *Evaluate Accuracy, Precision, Recall, and F1-Score*
17: *Store M, α, and β*
18: ***Return*** *M, α, and β*
End

4.2.3 Detection Module

Algorithm 4.2 performs real-time analysis of incoming network traffic flows using the trained machine learning model. First, the selected features are extracted from each traffic flow and classified as normal or attack traffic. If the traffic is identified as an attack, its Information Gain (IG) value is computed and compared with the predefined thresholds α and β. Based on the IG value, the traffic is categorized as Low DDoS or High DDoS, while traffic with IG values greater than or equal to $\alpha$is considered Normal.

Algorithm 4.2: Online DDoS Detection and Severity Classification

Input*: Traffic Flow T, Model M, Thresholds α and β*
Output*: Traffic Class C*
1: *Receive incoming traffic flow T*
2: *Extract selected feature subset Fs*
3: *Predict attack status using model M*
4: ***If*** *M(T) = Normal* ***then***
5: *C ← Normal*
6: ***Else***
7: *Compute Information Gain (IG)*
8: ***If*** *IG ≥ α* ***then***
9: *C ← Normal*
10: ***Else If*** *β < IG < α* ***then***
11: *C ← Low DDoS*
12: ***Else***
13: *C ← High DDoS*

14: ***End If***
15: ***End If***
16: ***Return*** *C*
End

4.2.4 Classification Module

The classification module is based on machine learning algorithms that are trained on a selected set of features. Each flow is classified into one of three categories: normal traffic, low-severity DDoS or high-severity DDoS. The trained model operates in real time within the controller, enabling rapid identification of attack severity. Again, multi-level classifications enable diverse response policies and generally improve detection performance.

4.2.5 Mitigation Module

Algorithm 4.3 shows the mitigation module correlates classification results with countermeasures implemented in SDN. When the attack flow is recognized as a low-severity DDoS attack, the flows are redirected to honeypots. In high-severity DDoS flows, port blocking is used as a mitigation measure. Conducting such actions is achieved by updating flow rules in the switches via the controller. A close integration of detection and mitigation enables a quick, appropriate response to the severity of the DDoS.

Algorithm 4.3: Severity-Aware DDoS Mitigation

Input*: Traffic Class C*
Output*: Mitigation Action*
1: *Receive classification result C*
2: ***If*** *C = Normal* ***then***
3: *Allow traffic forwarding*
4: *Continue normal network operation*
5: ***Else If*** *C = Low DDoS* ***then***
6: *Identify suspicious flow*
7: *Generate OpenFlow redirection rule*
8: *Redirect traffic to Honeypot*
9: *Monitor attacker behaviour*
10: *Log attack information*
11: ***Else If*** *C = High DDoS* ***then***
12: *Identify malicious source*

13: *Generate OpenFlow blocking rule*
14: *Install rule in SDN switch*
15: *Block source Port*
16: *Drop attack packets*
17: *Record mitigation event*
18: ***End If***
19: *Verify network status*
20: ***Return*** *Mitigation Status*
End

4.3 Data Preprocessing

Data preprocessing refers to the method of converting raw trace values into a format that machine learning techniques can readily work with. The flow records from the CICDDoS2019 dataset and the live SDN testbed are cleansed first by removing insignificant and problematic entries such as incompleteness, redundancy, and corruption. Only meaningful samples are used in the next stage of processing. Any categorical parameters, if found, would be converted to the numerical type with the help of appropriate encoding methods. After that, every numerical feature is subjected to a min-max transformation so soon as to avoid the relative importance of features with respect to distance. Finally, the cleaned and normalized dataset is divided into training and testing subsets for model learning and evaluation. The same preprocessing steps are applied to both offline and online traffic to maintain consistency across experiments.

4.4 Entropy-Based Feature Selection Techniques

Network traffic features use entropy-based measures to measure uncertainty which include random elements and variable distribution patterns. DDoS detection uses entropy to differentiate between normal network traffic and malicious network traffic through its analysis of abnormal distribution patterns and flow statistics and protocol behaviour. Statistical metrics use entropy-based methods to measure traffic streams because they reveal both nonlinear links and the complex nature of traffic flow patterns. The study uses six different entropy measurements which include Shannon, Rényi, Ubriaco, Bhatia–Wolf, Bhattacharyya, and Tsallis entropy to improve the ability of features to separate different data classes. The different entropy formulations show different uncertainty aspects and

distribution sensitivity aspects which help assess feature importance for multi-level DDoS detection.

4.4.1 Shannon Entropy

Shannon entropy is the foundational measure of information uncertainty. It quantifies the average information content in a probability distribution and is defined as:

$$H(x) = -\sum_{i=1}^{n} p_i \log p_i \tag{1}$$

where $p_i$represents the probability of occurrence of the i^{th}event. In network traffic analysis, Shannon entropy measures packet-level attributes which include source IP and destination port and flow size. The traffic behaviour shows higher entropy values when the network experience random or evenly distributed traffic patterns which can indicate ongoing distributed attacks.

4.4.2 Rényi Entropy

Rényi entropy generalizes Shannon entropy by introducing an order parameter α, which controls sensitivity to probability distribution tails:

$$H_\alpha(x) = \frac{1}{1-\alpha} \log\left(\sum_{i=1}^{n} p_i^\alpha\right), \ \alpha > 0, \alpha \neq 1 \tag{2}$$

When $\alpha \to 1$, Rényi entropy function reaches its limit at Shannon entropy. The Rényi entropy measure enables users to control their focus between common and uncommon events. The system helps DDoS detection work by showing unusual traffic patterns and identifying heavy-tailed distributions which result from volumetric attacks. The various α values provide users with the ability to adjust their feature sensitivity at different levels.

4.4.3 Tsallis Entropy

Tsallis entropy is another generalized entropy model that introduces a non-extensive parameter q:

$$H_q(x) = \frac{1}{q-1} \log\left(\sum_{i=1}^{n} p_i^q\right), \mathrm{q} > 0, \mathrm{q} \neq 1 \tag{3}$$

Shannon Entropy appears as the limit when q approaches 1. The Tsallis entropy method works best for assessing systems which display both long-range interactions and non-linear relationships. The non-uniform traffic patterns generated by DDoS attacks enable Tsallis entropy to detect deviations more effectively than traditional entropy methods.

4.4.4 Ubriaco Entropy

Ubriaco entropy is a fractional entropy formulation derived from non-extensive statistical mechanics. It introduces fractional power components to better capture deviations from equilibrium distributions.

$$H_U(x) = \sum_{i=1}^{n} p_i \, (-\ln p_i)^{\beta} \tag{4}$$

Where, $p_i$is the probability of event i and $\beta$is a fractional parameter controlling nonlinearity. When $\beta = 1$, Ubriaco entropy reduces to Shannon entropy.

4.4.5 Bhatia–Wolf Entropy

Bhatia–Wolf entropy extends classical entropy by incorporating logarithmic normalization factors to improve discrimination among similar probability distributions.

$$H_{BW}(x) = -\sum_{i=1}^{n} p_i \, \log\left(\frac{p_i}{\max(p)}\right) \tag{5}$$

Where max(p) is the maximum probability in the distribution. This entropy improves discrimination by emphasizing dominant traffic components, which is helpful in identifying volumetric DDoS attacks.

4.4.6 Bhattacharyya Coefficient

Bhattacharyya Coefficient is derived from the Bhattacharyya distance concept and measures similarity between probability distributions. It quantifies overlap between two distributions:

$$H_B(x) = -\log\left(\sum_{i=1}^{n} \sqrt{p_i q_i}\right) \tag{6}$$

where P and Q represent normal and attack class distributions. This entropy is derived from the Bhattacharyya coefficient and measures class separability between normal and attack traffic distributions. It is useful in evaluating feature discrimination strength.

4.5 Sequential Feature Reduction Strategy

High-dimensional network traffic data contains various features, including redundant components, irrelevant elements, and noisy attributes, which decrease detection accuracy and require the system to use more resources to operate. The full feature set of machine learning needs to be avoided because it results in extended training durations and excessive memory requirements, and it reduces system capacity to handle multiple tasks, making it unsuitable for real-time SDN environments. To address these challenges, this research proposes a Sequential Feature Reduction Strategy that integrates Mutual Information (MI) and Joint Entropy in a two-stage selection process. The objective is to retain features that are highly relevant to attack severity while eliminating redundant attributes. This strategy produces a compact yet informative feature subset that improves multi-level DDoS detection performance and reduces controller processing burden.

4.6 Motivation for Sequential Feature Selection

Single-stage feature selection techniques typically focus either on feature relevance or redundancy but not both. Relevance-based methods may select correlated features, while redundancy-aware methods may discard informative attributes. The complex DDoS traffic patterns require multiple techniques due to their varied patterns and severity levels. The proposed sequential approach first emphasises relevance using Mutual Information and then addresses redundancy using Joint Entropy. The design uses multiple layers to guarantee that chosen features provide both maximum informational value and distinctive characteristics needed to differentiate between normal, low-severity, and high-severity DDoS traffic.

4.6.1 Mutual Information-Based Initial Filtering

Mutual Information (MI) measures the statistical dependency between a feature and the class label. The classification performance of a feature increases with higher MI values because the feature provides more information about traffic class identification. The Mutual Information between a feature X and the class label Y is defined as:

$$I\ (X;\ Y)\ =\ \sum_{x\in X}\sum_{y\in Y} p(x,y)\ log\ \frac{p(x,y)}{p(x)P(y)} \tag{7}$$

where $p(x,y)$ denotes the joint probability distribution of X and Y, and $p(x)$ and $p(y)$represent their marginal probabilities.

The system orders feature from their highest to lowest MI scores. The top-k selection method is used to keep the most important features. This stage achieves major dimensionality reduction while maintaining the ability to distinguish between different classes.

4.6.2 Joint Entropy-Based Feature Refinement

The MI-based filtering method identifies important features, but it continues to keep features that show correlation and duplication. The researchers used Joint Entropy to examine how selected features depend on each other because they wanted to improve their feature set analysis. The joint entropy of two variables X and Y is defined as:

$$H(X,Y)\ =\ -\sum_{x\in X}\sum_{y\in Y} p(x,y)\log p(x,y) \tag{8}$$

The selection process chooses feature combinations which produce higher joint entropy measurements because this metric demonstrates better informational variety between the selected features. Redundant features which do not enhance joint entropy measurement must be eliminated from the system.

4.6.3 Final Feature Subset Construction

The final feature subset is obtained by selecting MI-ranked features that also satisfy the Joint Entropy refinement criterion. The system uses a weighted entropy formulation to achieve its goal of combining relevance with diversity.

$$H'(X,Y)\ =\ -\sum_{x\in X}\sum_{y\in Y}(p(x,y)+\alpha\ I(X;\ Y))\ log\ p(x,y)+\alpha\ I(X;\ Y) \tag{9}$$

where α is a weighting factor controlling the influence of Mutual Information. This sequential integration ensures that selected features are both highly relevant and minimally redundant. As a result, the proposed strategy achieves

- Reduced feature dimensionality
- Improved detection accuracy

- Lower computational complexity
- Better generalization across severity levels

This sequential feature reduction strategy forms the foundation of the proposed multi-level DDoS detection framework.

4.6.4 Selection of Information Gain for Feature Reduction

Information Gain was selected as the primary feature evaluation and severity assessment metric due to its simplicity, interpretability, and suitability for real-time SDN environments. Unlike Principal Component Analysis (PCA), which transforms original features into new orthogonal components and reduces feature interpretability, IG preserves the original network traffic features and directly measures their contribution to distinguishing normal and attack traffic. This characteristic is particularly important in SDN-based security systems where understanding the influence of individual traffic attributes is necessary for effective attack analysis and mitigation.

ReliefF is a feature-ranking algorithm that estimates feature importance based on the ability to distinguish neighboring instances from different classes. Although effective in many classification tasks, ReliefF requires repeated nearest-neighbor computations, resulting in higher computational overhead when processing large-scale network traffic datasets. In contrast, IG computes feature relevance directly from entropy measures, making them computationally efficient and more suitable for real-time DDoS detection.

Furthermore, the proposed framework employs entropy-based traffic analysis for severity classification and mitigation decisions. Since Information Gain is inherently derived from entropy concepts, it naturally integrates with the proposed entropy-based detection model.

4.7 Machine Learning-Based Multi-Level Detection

The selected feature subset obtained from the sequential feature reduction strategy is used as input to the machine learning–based multi-level detection module. The module classifies traffic flow into three different severity categories which include normal traffic and low-severity DDoS and high-severity DDoS attacks. The system uses multi-level classification to identify attack strength which enables it to execute severity-based defense strategies instead of traditional binary detection methods. The system uses different supervised

machine learning algorithms to test its performance in detecting threats and staying dependable under various conditions. The system uses labeled data to train its models which operate inside the SDN controller to perform real-time classification tasks.

Random Forest (RF): The Random Forest algorithm uses ensemble learning to create numerous decision trees which make predictions through random selection of their feature sets. The Random Forest method demonstrates resistance against noisy data while successfully processing high-dimensional datasets and delivering accurate results in new data situations.

Support Vector Machine (SVM): Support vector machines create their optimal hyperplanes which separate different classes by maximizing the distance between the two classes. The system achieves successful results through its ability to handle both linear and non-linear classification tasks because of its kernel functions and its capacity to handle complex decision boundaries.

K-Nearest Neighbor (KNN): The KNN distance-based classifier determines the sample's class by identifying the most common class among its closest neighboring samples. The system uses a straightforward method that effectively detects local data patterns.

Gradient Boosting Algorithm (GBA): Gradient Boosting creates its model through a sequence of weak learners, which build on the mistakes from preceding models. The method successfully handles complicated non-linear relationship modeling. The selected models demonstrate successful results in intrusion detection while providing mutual learning benefits.

Neural Network(NN): A neural network is a machine learning model inspired by the structure of the human brain, made up of layers of connected nodes called neurons. It learns patterns from data by adjusting weights through a process called training, often using backpropagation and gradient descent. Neural networks are widely used in applications like image recognition, language translation, speech processing, and recommendation systems.

4.8 Information Gain Based Mitigation Mechanism

The Software Defined Networks (SDN) based mitigation mechanism which we propose uses an Information Gain (IG) decision model to create automated DDoS attack responses which

track threat levels. The system uses SDN's central control and programming capabilities to implement mitigation procedures which adapt to current data traffic patterns monitored by the controller. The SDN controller receives continuous traffic data which OpenFlow-enabled switches transmit to it. The system collects packet statistics during its observation period, especially for tracing how often each source MAC address appears. The studies utilized the collected statistics to measure traffic source distribution patterns by applying entropy analysis. The DDoS attack detection system shows a strong probability of detecting malicious activity because its entropy values decrease when many packets come from few sources.The global entropy of source traffic distribution is computed as:

$$H(X) = -\sum_{j} P_j \log_2 P_j \tag{10}$$

where $P_j$represents the probability of occurrence of packets from the j^{th}source. High entropy values indicate normal and random traffic behaviour, whereas low entropy values suggest malicious traffic and possible attack conditions.

To further isolate suspicious traffic contributors, a subset of sources having very low occurrence probability is selected. Sources satisfying $P_j < 0.2$ are considered suspicious and grouped into a set A:

$$A = \{j | P_j < 0.2\}, \quad A_{count} = |A| \tag{11}$$

For the selected suspicious source subset A, a normalized entropy measure is computed to quantify the uncertainty associated with suspicious traffic contributors. Lower entropy values indicate a higher concentration of traffic among a few suspicious sources, which is a characteristic behaviour of DDoS attacks.

$$H\left(\frac{X}{Y}\right) = -\sum_{j \in A} \frac{P_j}{A_{Count}} \log_2 \left(\frac{P_j}{A_{Count}}\right) \tag{12}$$

The Information Gain (IG) is then calculated as the difference between global entropy and conditional entropy:

$$IG = H(X) - H\left(\frac{X}{Y}\right) \tag{13}$$

The IG value reflects the degree of uncertainty reduction between the global traffic distribution and the suspicious traffic subset. Under normal network conditions, traffic is distributed across multiple sources, resulting in relatively high IG values. During DDoS

attacks, traffic becomes concentrated among a limited number of sources, causing entropy patterns to change and reducing the IG value. Therefore, lower IG values indicate greater deviation from normal traffic behaviour and a higher likelihood of DDoS activity. Based on IG, traffic is classified into three severity levels using two adaptive thresholds, α(upper) and β(lower):

$$DDoS\ Level = \begin{cases} Normal\ , if\ IG \geq \alpha \\ Low\ DDoS\ , if\ \beta < IG < \alpha \\ High\ DDoS\ , if\ IG \leq \beta \end{cases} \quad (14)$$

Thresholds $\alpha$and β are dynamically derived from the training data using the mean Information Gain values of normal, low-severity, and high-severity traffic classes.

Let μ_N, μ_L, and μ_H denote the mean IG values of normal, low-severity, and high-severity traffic, respectively, where $\mu_N > \mu_L > \mu_H$. The adaptive thresholds are computed as:

$$\alpha = (\mu_N + \mu_L)/2 \quad (15)$$

$$\beta = (\mu_L + \mu_H)/2 \quad (16)$$

Therefore, $\alpha > \beta$, ensuring that the classification regions are mutually exclusive and collectively exhaustive. Consequently, each traffic instance is assigned to exactly one severity level. Based on the determined severity level, the SDN controller applies proportional mitigation actions according to the following decision rule. This severity-aware strategy minimizes unnecessary blocking of legitimate traffic while ensuring rapid containment of high-impact attacks.

$$DDoS\ Mitigation\ Rule = \begin{cases} Allow\ Traffic\ , & Normal \\ Redirect\ to\ Honeypot\ , & Low\ DDoS \\ Drop\ Packet(Block\ Port), & HighDDoS \end{cases} \quad (17)$$

The mitigation policy is severity-aware, ensuring that mitigation actions become progressively stronger as the estimated attack severity increases.

For normal traffic, packets are forwarded without intervention. For low-severity DDoS attacks, suspicious flows are redirected to a honeypot through OpenFlow rules, enabling attack observation while preserving legitimate services. For high-severity DDoS attacks, the SDN controller installs drop rules to block malicious flows and protect network resources. Mitigation rules are automatically removed after the timeout period to prevent unnecessary service disruption.

CHAPTER 5

EXPERIMENTAL SETUP & IMPLEMENTATION

This chapter presents the experimental environment and implementation details used to validate the proposed Information Gain driven multi-level DDoS detection and mitigation framework. It describes the dataset, SDN testbed configuration, controller implementation, attack generation procedures, training and testing strategy, and evaluation metrics employed for performance assessment.

5.1 Dataset Description and Traffic Sources

This section describes the data sources used for developing and evaluating the proposed framework. Although multiple benchmark datasets are discussed in Chapter 2, the proposed methodology primarily relies on the CICDDoS2019 dataset and live traffic generated in an SDN testbed. These two sources together enable both offline model training and real-time validation in a realistic SDN environment.

5.1.1 CICDDoS2019 Dataset Description

The CICDDoS2019 dataset serves as the main benchmark and will be used for both training and offline assessment in this study. This dataset contains a comprehensive collection of modern DDoS attack traffic and benign flows, spanning multiple reflection-based and flooding attacks and featuring realistic traffic patterns. The CICDDoS2019 dataset outperforms previous datasets because it provides more detailed flow-level data and captures different attack patterns, enabling researchers to examine multiple levels of attack intensity.

The research work does not use publicly available datasets, including ISCX2012, UNSW-NB15, and CAIDA DDoS 2007, because they contain outdated attack types and provide limited labelling options while lacking severity-related annotations. Therefore,

CICDDoS2019 is chosen as the dataset that best supports the goals of detecting DDoS attacks at multiple severity levels.

5.1.2 Live Traffic Generation

The SDN environment uses live traffic to test the proposed framework which operates under actual network conditions that exhibit changing conditions. Live traffic generation simulates legitimate user activities together with DDoS attack simulations which allow for testing of detection and mitigation systems in actual operational conditions.

Legitimate traffic is produced by benign hosts using standard network utilities such as ICMP ping and TCP/UDP communication with default configurations. This traffic represents routine network communication which established a baseline for researchers to study typical network traffic patterns. The ping3 tool creates malicious traffic because it provides users with complete control over their packet traffic. The system creates two distinct types of DDoS traffic.

Normal Traffic: The system generates legitimate traffic through regular network operations which use default ICMP ping network tools from harmless host entities. The traffic which represents normal communication behaviour functions as the baseline for identifying typical network patterns.

Low-Severity DDoS Attack: Low-rate DDoS attacks create attacks that appear to operate at hidden attack conditions which they use to slowly deteriorate network performance while remaining undetected. The testbed can demonstrate this through execution of the following command.

h1 ping3 -c 500 -d 120 -S -w 64 --rand-source h8

The command sends data packets to the target host h8 with a limited transmission speed that uses random source addresses. The network traffic generates extreme disturbance to data flow patterns after it reaches the point of full network capacity. The framework testing requires evaluation of how common low-severity attacks affect its performance because these attacks represent typical attack patterns.

High-Severity DDoS Attack: The system creates DDoS attacks through its ability to generate high-rate flooding attacks which will simulate attacks that lead to immediate system failure for the targeted system. The following command is used:

h1 ping3 -c 10000 -d 120 -S -w 64 -p 80 --flood --rand-source h8

The system achieves packet transmission rates above 1,00,000 packets per second which creates essential network disruptions because it affects both traffic distribution and network performance. DDoS attacks create severe traffic patterns which cause entropy and Information Gain values to reach zero under these conditions.

The proposed framework achieves evaluation through its testing across multiple attack scenarios which include various attack conditions. The system needs to be tested through its capacity to classify attack severity at multiple levels while activating SDN-based defense systems for all attack intensities.

5.2 SDN Testbed Design

The proposed Information Gain driven multi-level DDoS detection and mitigation framework evaluation tests its performance in real-world situations through a Software Defined Networks testbed which uses the Mininet network emulator and the Ryu SDN controller for testing purposes. The testbed enables researchers to create controlled environments which allow them to generate authentic traffic while testing different DDoS attack scenarios and tracking network flow data and implementing real-time mitigation strategies.

The SDN testbed systematizes its operations through six OpenFlow switches and eight end hosts which create a hierarchical network that mimics a small-to-medium enterprise network. Among the eight hosts, selected nodes act as benign users, attacker nodes, victim server, and a dedicated honeypot system. The OpenFlow protocol enables all switches to function, while a Ryu controller system controls their operational management.

The primary objectives of the testbed design are:

- To enable continuous collection of flow-level statistics from switches
- To support real-time execution of machine learning based detection at the controller

- To facilitate dynamic installation of OpenFlow rules for mitigation
- To validate the framework against both low-rate and high-rate DDoS attacks

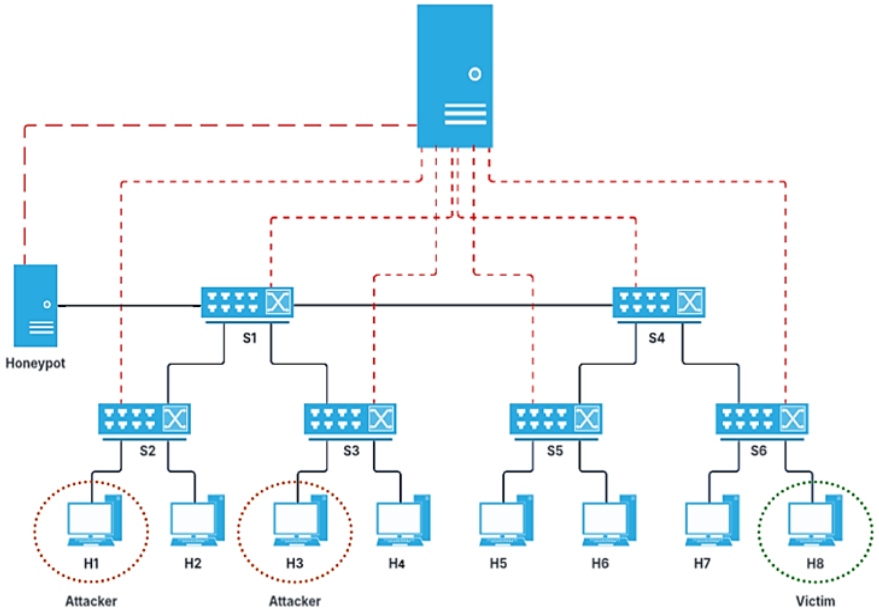


FIGURE 5.1 DARTNet: DDoS Attack Response Topology Network

FIGURE 5.1. illustrates the SDN testbed topology employed in the proposed work. The victim host represents a protected service or server, while attacker hosts generate malicious traffic toward the victim. The legitimate user activity was simulated through the normal user behaviour which the benign hosts generated. The honeypot node serves as a destination for low-severity DDoS traffic while it enables the detection of suspicious flows which do not interfere with authentic communication.

The controller maintains a secure control channel which connects all switches to its system. The controller requests flow statistics from switches at regular intervals, which include information about packet counts and byte counts and source address details. The proposed detection module processes these statistics to calculate entropy and Information Gain values, which it uses to assess traffic severity. The controller implements automatic mitigation actions based on the detected severity level.

- Normal traffic is forwarded without restriction
- Low-severity DDoS traffic is redirected to the honeypot

- High-severity DDoS traffic is blocked at the ingress switch

The testbed modular design enables users to change topology specifications and host quantities and attack settings without difficulty. The system provides multiple network operating conditions to test network performance under different traffic patterns. The SDN testbed functions as a testing platform which enables to assess the real-time capabilities and system capacity and operational performance of their multi-level DDoS protection system.

5.3 Ryu Controller Implementation

The proposed framework is implemented within the Ryu SDN controller to enable real-time monitoring, analysis, and enforcement of security policies. The selection of Ryu as the appropriate controller solution relies on its lightweight design which includes built-in OpenFlow support and allows developers to extend its functionality through Python-based applications.

The controller implementation is developed as a modular Ryu application composed of multiple functional components which each handle a different responsibility within the detection and mitigation pipeline. The system components work together to gather network traffic data which they use to extract features and calculate entropy and Information Gain to determine traffic severity and deploy corresponding OpenFlow rules.

5.4 Training & Testing Strategy

This section describes the strategy adopted for training and testing the machine learning models used in the proposed Information Gain driven multi-level DDoS detection framework. The strategy aims to achieve three goals which include enabling reliable model learning and enabling fair performance evaluation and enabling generalization testing across different network traffic conditions.

The preprocessed data with its optimized features from the CICDDoS2019 dataset. The data distribution includes 70% of the data for training purposes and 30% of the data for testing purposes. The training set is used to build machine learning models, while the testing set is reserved exclusively for performance evaluation. The data split provides enough information for the model to learn from while creating an independent test set that allows for genuine evaluation without bias. The dataset uses stratified sampling to maintain the traffic

distribution between Normal, Low-severity DDoS and High-severity DDoS. The system guarantees that every subset maintains correct class distribution which protects against learning biases that favor majority classes.

The training process requires all numeric features to undergo min-max scaling which transforms their values into the [0,1] range. The proposed Mutual Information and Joint Entropy-based sequential approach perform feature selection on the training set while the same selected feature subset is used for testing to protect against information leakage. The research utilizes Random Forest, Support Vector Machine, K-Nearest Neighbors, Gradient Boosting Algorithm and Neural Network as supervised machine learning classifiers to train on the optimized feature set.

The controller environment uses models which were trained offline with the CICDDoS2019 dataset for testing purposes in real-time SDN testbed evaluation. The system verifies its operational performance through real-time classification of incoming live traffic flows which do not require additional training.

5.5 Evaluation Metrics

The proposed framework evaluation process uses classification performance metrics together with time-based performance metrics to measure its performance. The framework tests two types of metrics which include attack detection accuracy and severity classification reliability and its ability to respond in real time during offline dataset tests and live SDN tests.

5.5.1 Confusion Matrix Parameters

The confusion matrix forms the basis for evaluating classification performance by comparing predicted labels with actual traffic classes. The following parameters are used:

- True Positive (TP): Number of DDoS attack flows correctly classified as attacks.
- True Negative (TN): Number of benign flows correctly classified as normal.
- False Positive (FP): Number of benign flows incorrectly classified as attacks, leading to false alarms.

- False Negative (FN): Number of attacks flows incorrectly classified as normal, representing missed detections.

These parameters are computed for each traffic class (Normal, Low-severity DDoS, and High-severity DDoS) in the multi-class classification setting.

5.5.2 Classification Performance Metrics

- **Accuracy:** Which measures the correct classification ratio of attack and benign flows against all traffic instances.

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

- **Precision:** The precise measurement of attack detection effectiveness establishes the relationship between correctly identified attack patterns and all flows which were classified as attacks.

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

- **Recall:** Recall measures the detection system's ability to correctly identify real attack traffic. This is very critical in preventing service damage from undetected DDoS flows.

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

- **F1-Score:** The F1-Score provides an equal evaluation method which combines precision and recall, making it suitable for DDoS detection situations that show unequal distribution of classes.

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

5.5.3 Time-Based Performance Metric

- $T_{\text{flow arrival}}$**:** The time when a traffic flow initially arrives at the SDN controller for observation and evaluation.

- $T_{\text{classification}}$**:** The time 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 of the processing time confirm the framework's suitability for real-time SDN deployment.

$$Processing\ Time = T_{Classification} - T_{Flow\ Arrival} \tag{16}$$

The proposed DDoS detection and mitigation framework is comprehensive SDN based framework which uses sequential feature selection and multi-level machine learning classification and threat level-based SDN mitigation to enhance existing DDoS detection methods. The system architecture provides modern high-speed SDN environments with its combination of low computational requirements and immediate response capabilities and its dynamic security control system.

CHAPTER 6

RESULTS & DISCUSSION

This chapter presents a comprehensive analysis of experimental results obtained from offline dataset experiments and live SDN testbed evaluation. The Information Gain based multi-level DDoS detection and mitigation framework performance evaluation depends on its ability to select features and machine learning classification accuracy and processing speed and real-time detection performance and mitigation capacity. Results are reported using standard evaluation metrics defined in Chapter 5, and comparisons are made across different classifiers and attack types to demonstrate the robustness of the proposed approach.

6.1 Feature Selection Results on Dataset

The proposed sequential feature selection method which uses Mutual Information and Joint Entropy together with its effectiveness will be evaluated in this section. The framework demonstrates its ability to reduce feature dimensionality while maintaining its ability to differentiate between various DrDoS attack types.

Table 6.1 Feature Reduction Results Using Sequential Feature Selection Approach on the Dataset

Type	Total Feature	After MI	After Joint Entropy	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

Table 6.1 displays the results of testing the sequential feature selection method which uses Mutual Information (MI) and Joint Entropy on various DrDoS attack styles from the CICDDoS2019 dataset. The original dataset for all attack types includes 84 flow-level features. The MI-based filtering process reduced features between 74 to 81 because the method successfully eliminated most low-relevance attributes while maintaining crucial features that link to attack behaviour. The Joint Entropy based refinement process reduces the feature set to approximately 54–57 features which applies to most attack categories. The Joint Entropy method demonstrates its ability to remove unnecessary features which showed high correlation during the MI phase while maintaining essential feature groups that assist in distinguishing different traffic patterns. In the DNS and NTP attack categories, the feature count reduces from 84 to 79 and 77 after MI and then decreases to 57 after Joint Entropy. LDAP exhibits a similar pattern with its feature count decreasing from 84 to 74 and then to 54. MSSQL shows a similar pattern because its feature count decreases from 84 to 78 and then to 55. SSDP shows a similar pattern because its feature count decreases from 84 to 75 and then to 55. The research shows consistent decreases across different protocols because the proposed sequential selection method functions equally well against all attacks.

The results from Table 6.1 validate that the proposed Mutual Information and Joint Entropy based sequential feature selection method achieves substantial dimensionality reduction which typically reaches 30 to 35 percent while maintaining power to represent data. The reduction results in decreased computational costs and quicker model training and enhanced detection framework performance for actual SDN systems.

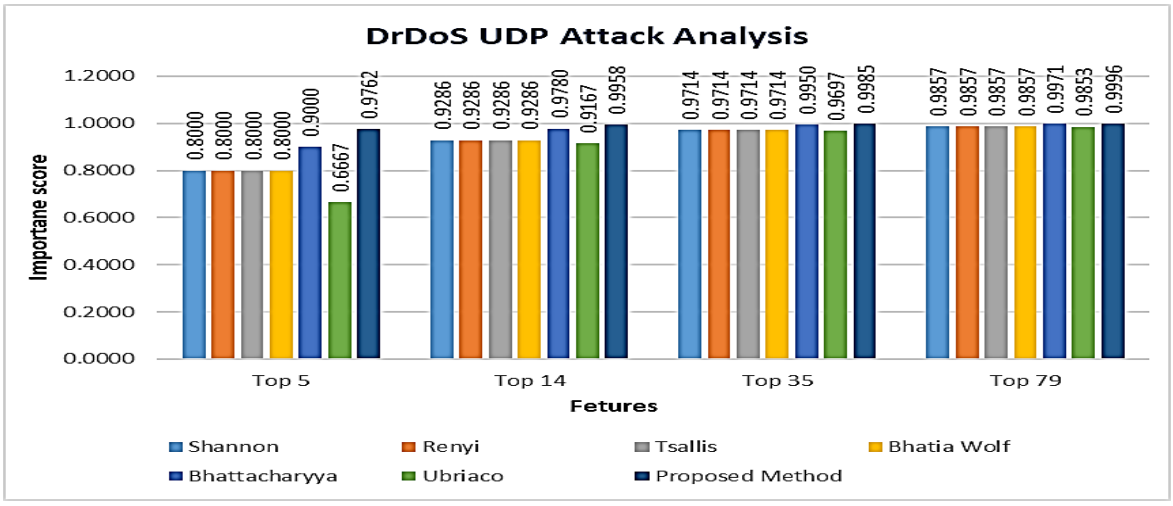


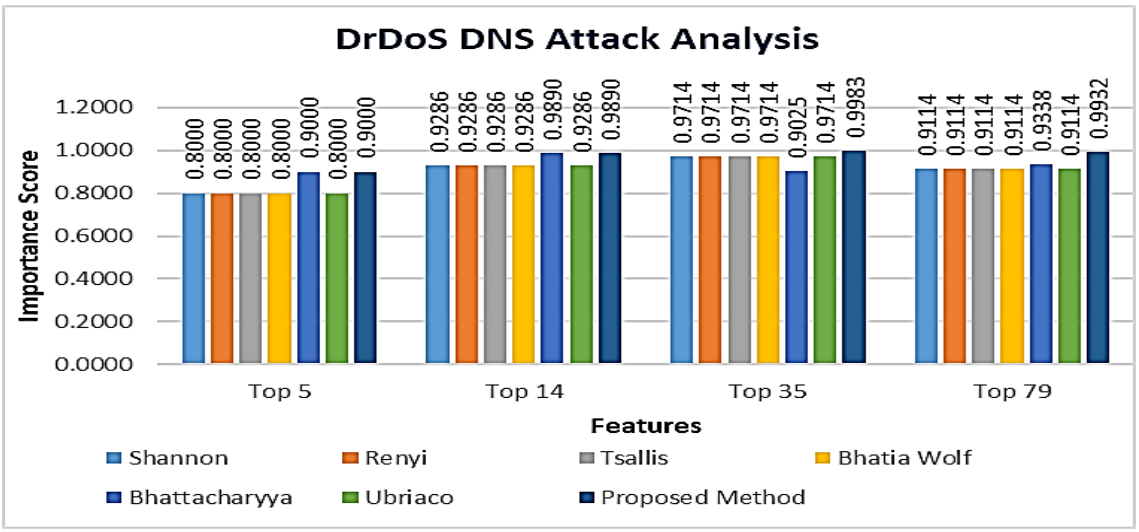
FIGURE 6.1 Entropy-Based Feature Importance for DrDoS UDP

FIGURE 6.1 provides a comparison of the importance scores achieved on DrDoS_UDP attack by various entropy-based feature selection techniques, for instance, Shannon entropy, Rényi entropy, Tsallis entropy, Bhatia-Wolf entropy, Bhattacharyya coefficient, the Ubriaco method, and the proposed Joint Entropy based approach. Such an analysis must be done for the feature subset sizes that differ slightly in this area, such as Top 5, Top 14, Top 35, and Top 79.

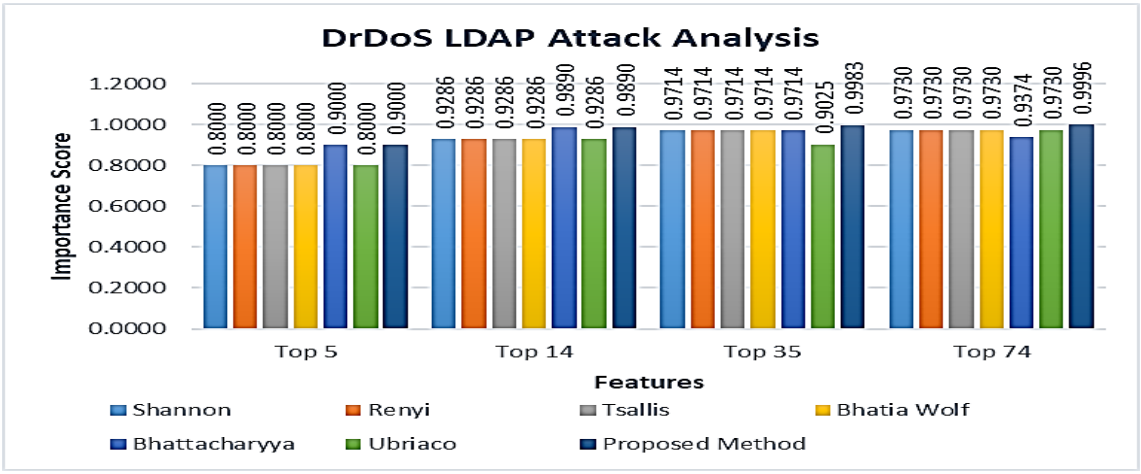
Typically, classical entropy measures such as Shannon, Rényi, Tsallis, and Bhatia-Wolf produce almost the same set of scores for importance of around 0.80 for the topmost leading 5 feature subset. They are used to identify highly discriminative features in a moderate way. It is quite lower in the Ubriaco method because it fetches weaker capability in capturing the characteristics of features that are relevant. However, the newly introduced approach has managed to obtain a significantly higher score of 0.98, which indicates that the approach performs superbly in identifying informative and complementary feature interactions even from highly limited subset sizes. If Top 14 and Top 35 were the numbers of features chosen, the score is highest of all in every feature. However, the joint entropy-based method still offers higher scores, always approaching 0.99. This suggests that it can discover important features as individuals, and this method is preserving interaction with other features that helps in increasing the power of distinction. In connection with the entire set of features , all the measures have resulted in respectably high importance scores indeed, while the method outruns the other methods, which shows that it is robust and can be dependent on in differences in the most dimensional features.

Specifically, as demonstrated by the performance results in FIGURE 6.1, the proposed joint entropy-based feature selection on DrDoS_UDP attacks surpasses classical entropy-based techniques by providing detailed and reduced subsets of features for efficient detection. The resulting improvements can be summarized as follows.

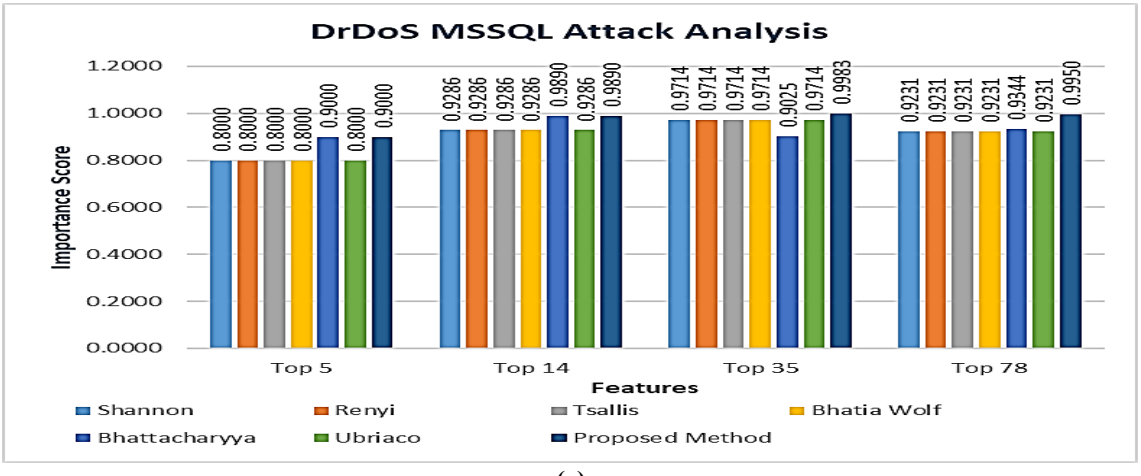
The figure in FIGURE 6.2 (a-c) gives the varying comparison of feature ranking created by different entropy notions for DrDoS DNS, LDAP, and MSSQL attacks across distributed numbers of feature subspace features under divergent entropy-based selection approaches. Smaller numbers of features, incorporating among them the likes of Shannon, Rényi, Tsallis, and Bhatia-Wolf, typically produce more moderate importance values for these conventional measures of entropy in contrast to the Ubriaco technique showing slightly lower disbursement in measurements.



(a)

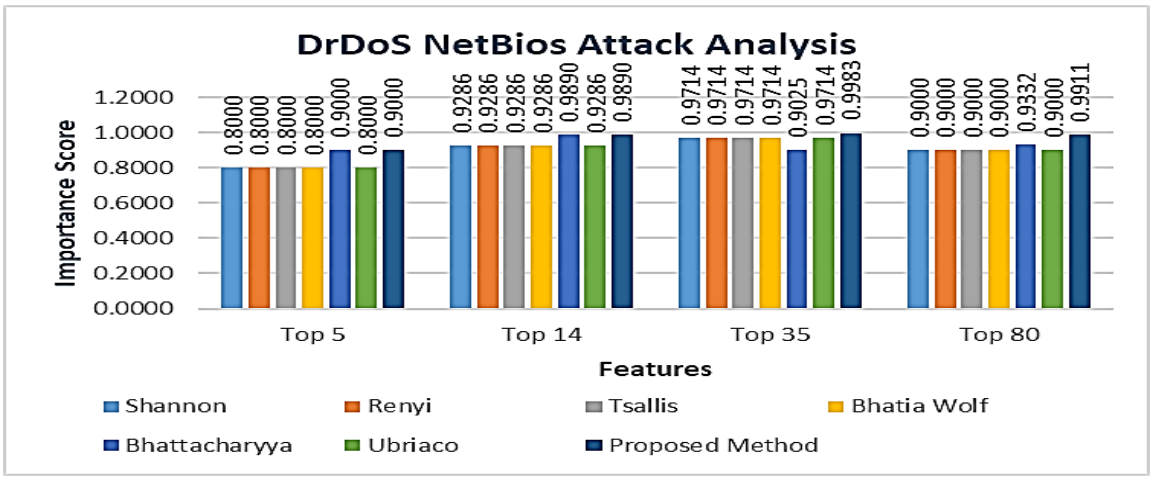


(b)

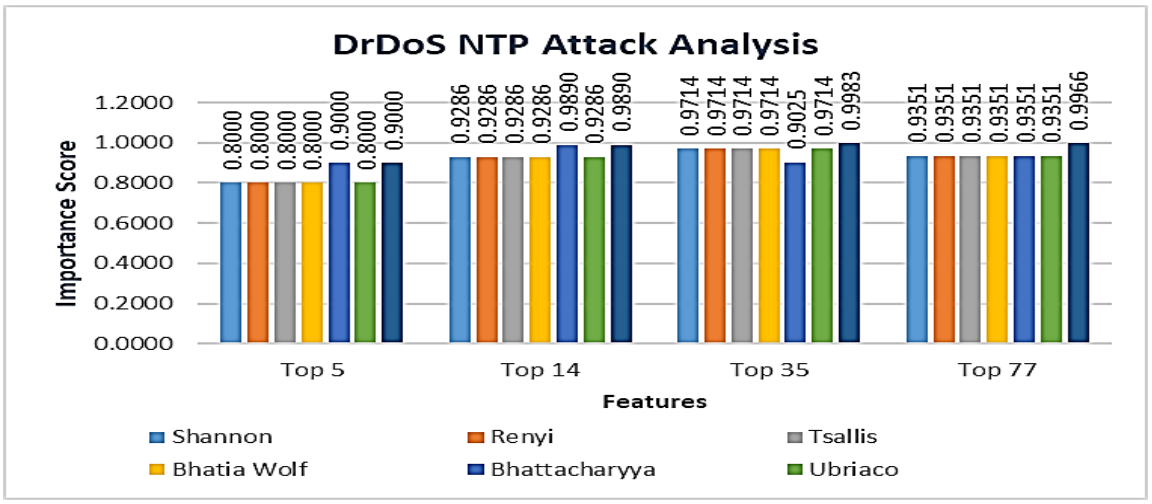


(c)

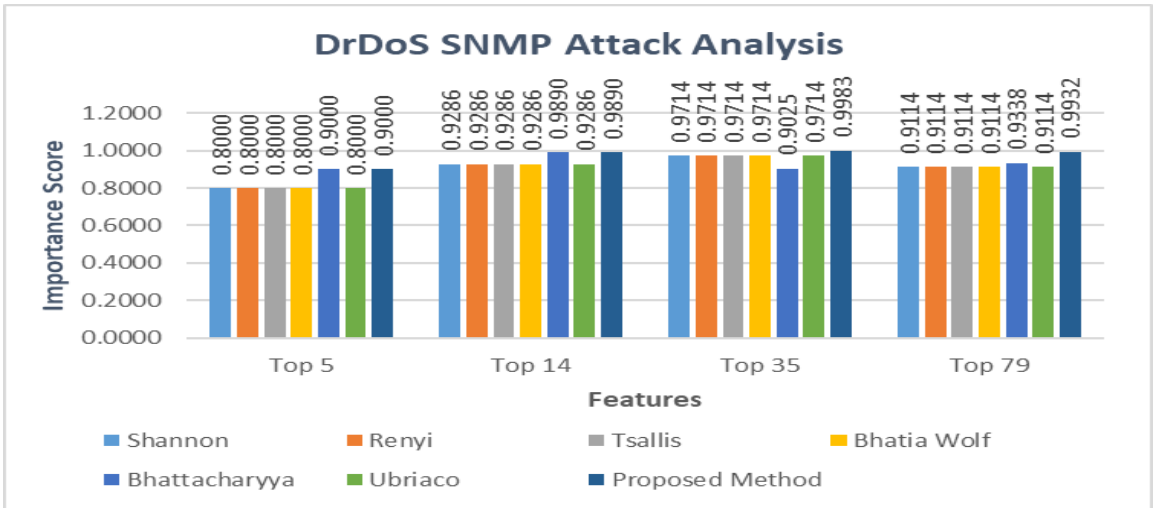
FIGURE 6.2 (a-c) Entropy-Based Feature Importance Analysis for DrDoS_DNS, DrDoS_LDAP, and DrDoS_MSSQL Attacks



(d)



(e)

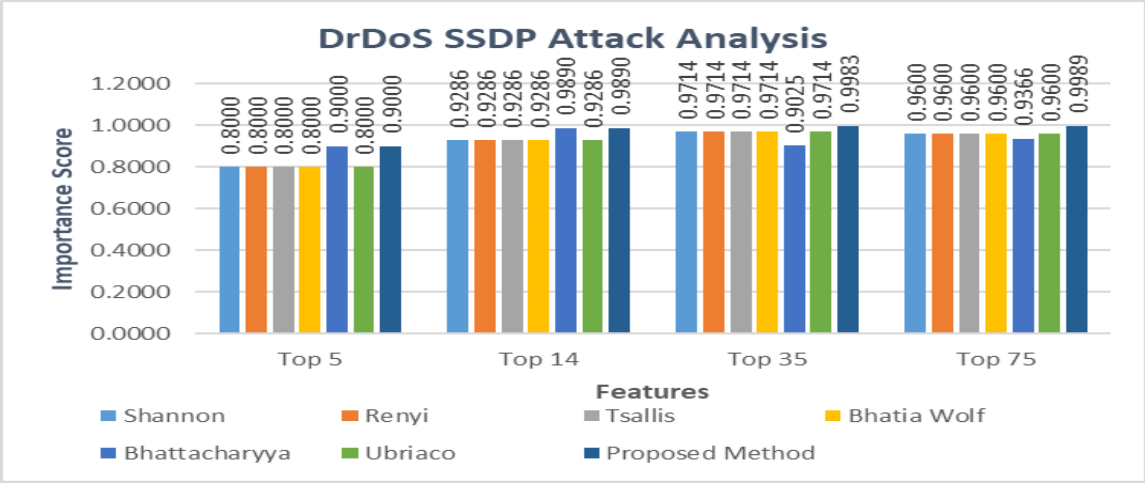


(f)

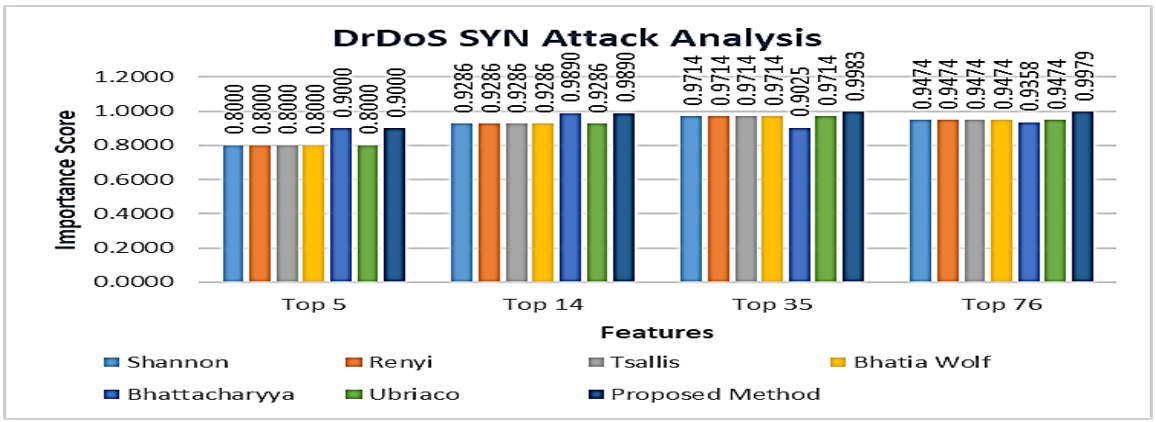
FIGURE 6.3 (d-f) Entropy-Based Feature Importance Analysis for DrDoS_NetBIOS, DrDoS_NTP, and DrDoS_SNMP Attacks

On the other hand, the proposed method traces all three attack rates positively toward higher mean importance rates, even when only a few selected features are used. An increase in the number of features that are chosen naturally leads to a higher importance score in almost all methods; the proposed approach has still maintained a solid edge, approaching values from about 0.98–0.99 across various attacks using DNS, LDAP, and MSSQL. This would show that the approach proposed is not just a hit machine when it comes to single identifiable features; it further shows that it can maintain meaningful relationships to bring about a stronger performance.

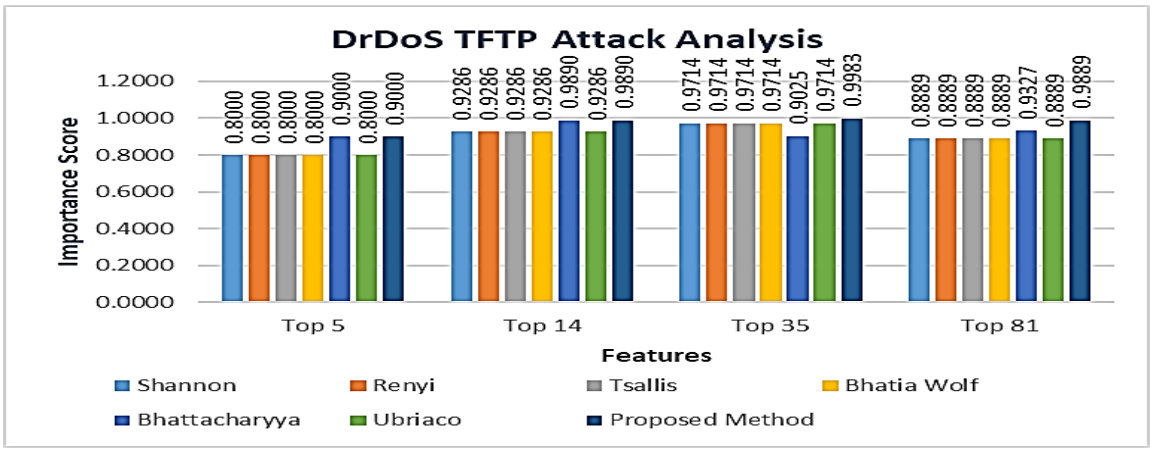
FIGURE 6.3 (d-f) above compares the importance scores of features as obtained through different entropy-based selection for DrDoS NetBIOS, NTP and SNMP attacks across multiple scales of feature subsets. For smaller feature subsets Shannon, Renyi, Tsallis and Bhatia-Wolf provide average importances while Ubriaco generally provides slightly lower values. On the other hand, Joint Entropy-Based is receiving less marks than any of the features even if less in numbers. As numbers of selected features increase, scores from all the techniques show an upward trend, but the proposed approach has clear superiority with values ranging to 0.98-0.99 for NetBIOS, NTP, and SNMP attacks. It is noteworthy that the proposed method can grasp the essence of individual feature relevance and more importantly, dependencies between features, which is crucial for a proper demarcation between different traffic patterns.



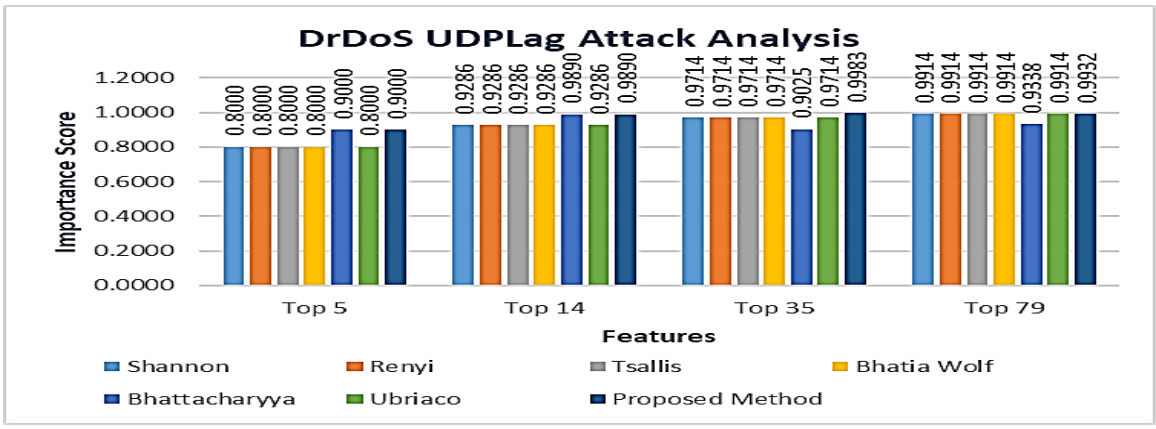
(g)



(h)



(i)



(j)

FIGURE 6. 4 (g-j) Entropy-Based Feature Importance Analysis for DrDoS DrDoS _SSDP, DrDoS _SYN, DrDoS _TFTP, DrDoS UDPLag Attacks

This was carried out using several entropy-based selection methods illustrated in FIGURE 6. 4 (g-j) for all four attack data sets. According to the graph, generally, all conventional entropy-based methods like Shannon, Rényi, Tsallis, and Hirschman-Wolf have been able to provide moderate importance in feature selection for the various subset sizes, but Ubriaco fell short in a few samples. In contrast, joint entropy -based proposed novel method consistently turned out to have a very high importance score with very few selected features.

The findings, which still leave enough meaning for inter-feature relationships, will point out the proper selection of the most influential features through protocol-based attack propagation. The greater number of selected features, the higher importance scores feature each of these methods; reasonably every time, and select the most commended proposed method, which does not go below 0.98 or 0.99 in terms of subsequent importance for SSDP, SYN, TFTP, and UDPLag attacks. Indeed, this seed has aged well since a rather stable performance across a fully different category of attacks will be witnessing the robustness and attack-agnostic characteristics of the proposed feature selection strategy. In general, all of the eleven different types of DrDoS attacks being observed in the study display the fact that the implementation of the sequential architecture of Mutual Information and Joint Entropy feature selector extracts significantly larger and more informative subsets of features when compared to those traditionally extracted by entropy methods, thereby supporting greater accuracy in detection while significantly reducing computational overhead in the machine learning-based classification which follows.

6.2 Machine Learning Model Performance Analysis on Dataset

The section evaluated the performance of classification using the feature selection optimized using the presented sequential mutual information and joint entropy-based approach. It analyses different classifiers' performances in differentiating Normal, Low Severity DDoS, and High Severity DDoS traffic.

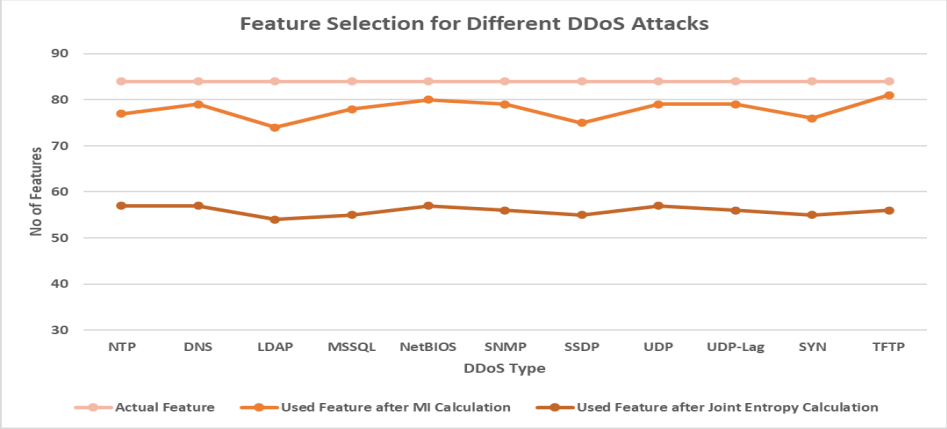


FIGURE 6.5 Selected Features of Different DrDoS Attack on Dataset

FIGURE 6.5 reveals the number of features in several DrDoS attack types with the sequential selected feature process. In all the forms of attacks, the original dataset, therefore, has 84 functionalities. The number of features retained is decreased from approximately 74 to 81

by MI filtering, indicating that an insignificant value is being dismissed. Subsequently, Joint Entropy, for example, further narrows the composed feature set to within around 54-57 during almost all types of attacks. With the optimized feature sub construction through the proposed sequential feature selection strategy, detailed performance results of these machine learning models concerning all maximum accuracies, precision, recall, and F-1 scores across each DDoS attack type will be presented in subsequent sections.

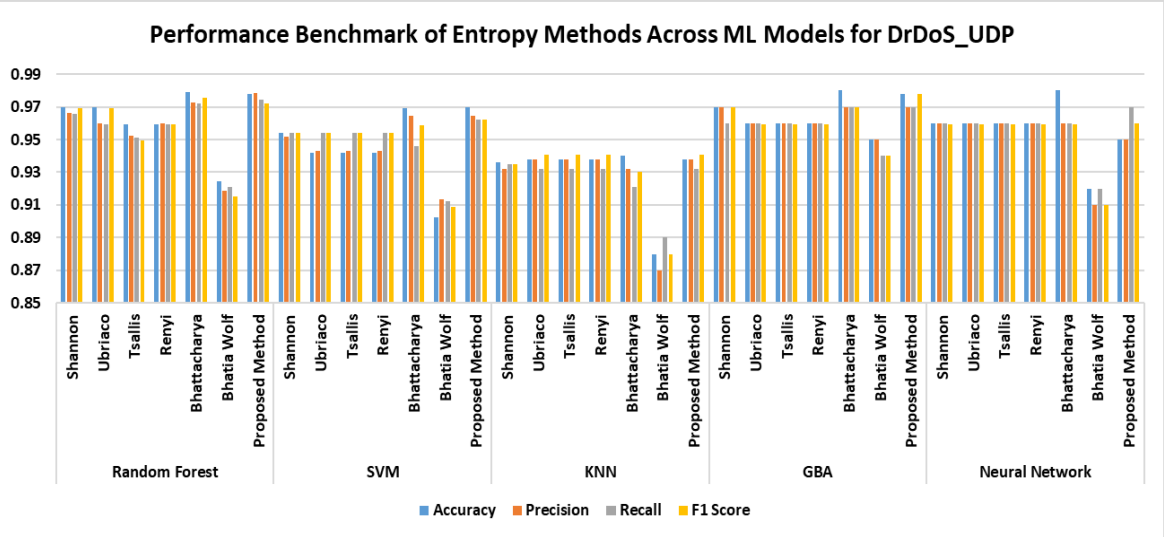
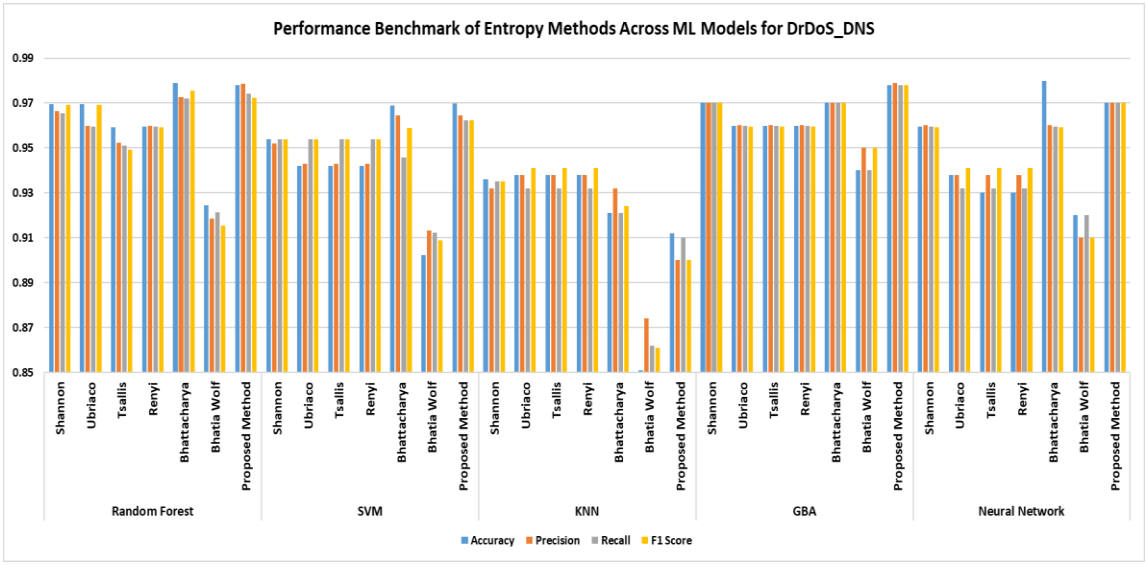
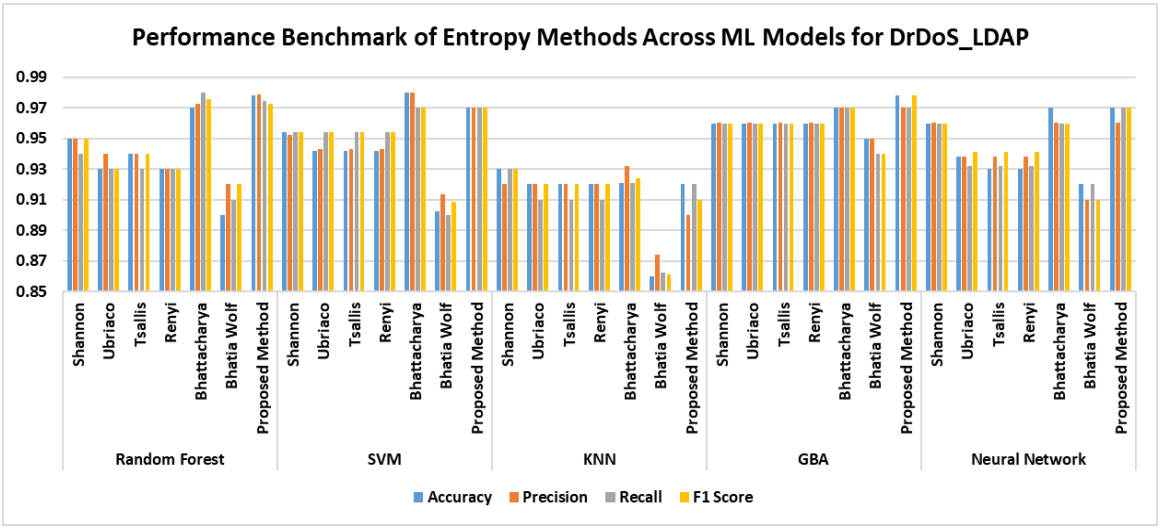


FIGURE 6.6 Performance Benchmark of Entropy Methods Across ML Models for DrDoS_UDP

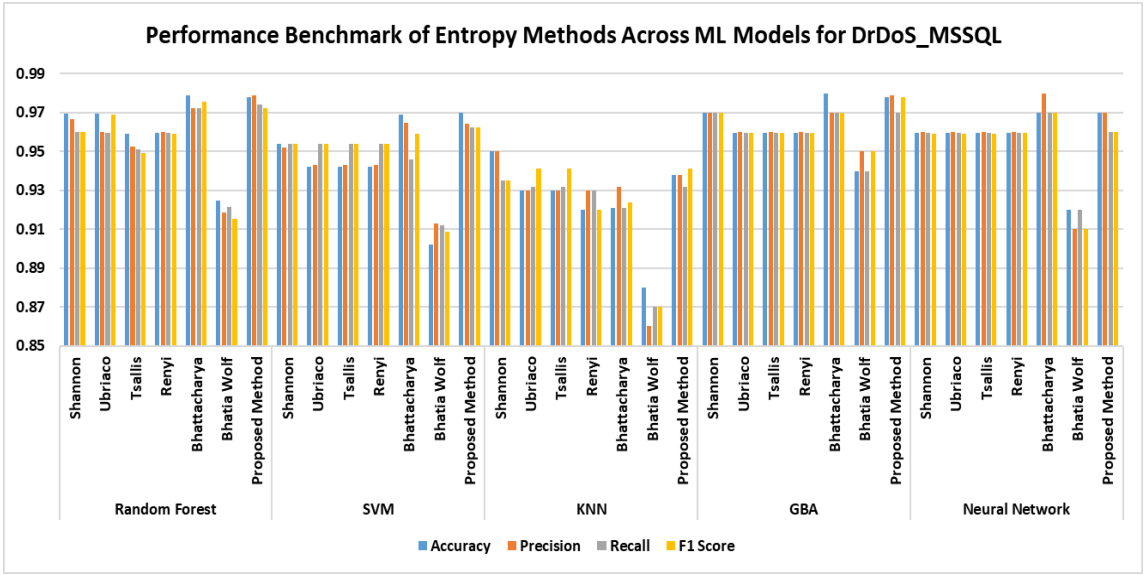
As can be seen in FIGURE 6.6, a comparative report of various entropy-based feature selection methods on various machine learning models is provided for DrDoS UDP attack. The figure shows the Accuracy, Precision, Recall, and F1-score for Random Forest, SVM, KNN, GBA, and Neural Network classifiers as trained with Shannon entropy, Ubriaco, Tsallis, Rényi, Bhatia-Wolf, Bhattacharyya and the proposed Joint Entropy-based feature selection methods. The only difference rests in the fact that in all classifiers, the proposed method generates higher or near-highest values when compared with all performance attributes. This only reveals the effectiveness of the new technique in providing more informative and discriminatory subsets of features that can be learned along several learning models. In terms of the classifiers that are considered, Random Forest, along with Gradient Boosting, demonstrate the highest performance for a wide range of performance parameters. Using proposed feature selection, one can achieve nearly 0.98 accuracy and F1 with both. Despite that, Neural Network models still show commendable high performance, relatively even less is seen in both SVM and KNN because of concerns regarding sensitivity to overlapping feature distribution and class.


Performance Benchmark of Entropy Methods Across ML Models for DrDoS_DNS
0.99
0.97
0.95
0.93
0.91
0.89
0.87
0.85
Shannon
Ubriaco
Tsallis
Renyi
Bhattacharya
Bhatia Wolf
Proposed Method
Random Forest
SVM
KNN
GBA
Neural Network
Accuracy
Precision
Recall
F1 Score

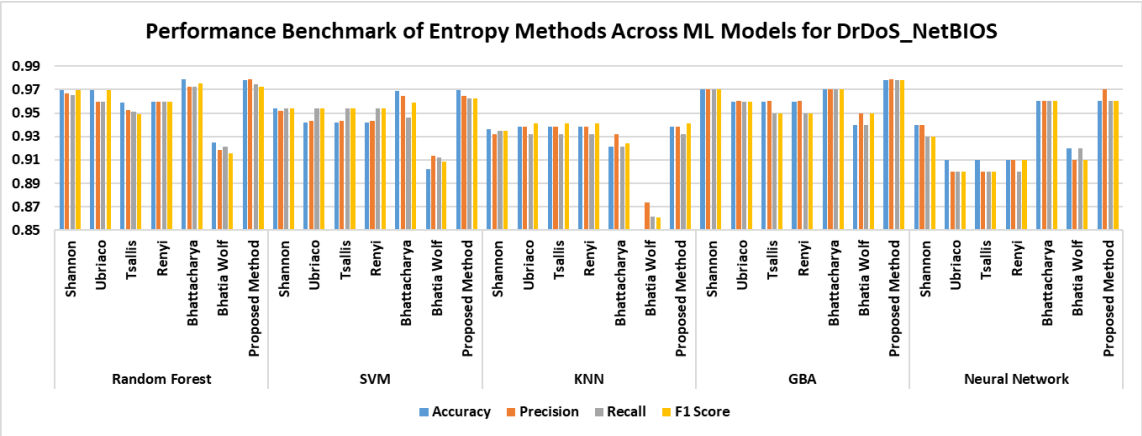
(a)


Performance Benchmark of Entropy Methods Across ML Models for DrDoS_LDAP
0.99
0.97
0.95
0.93
0.91
0.89
0.87
0.85
Shannon
Ubriaco
Tsallis
Renyi
Bhattacharya
Bhatia Wolf
Proposed Method
Random Forest
SVM
KNN
GBA
Neural Network
Accuracy
Precision
Recall
F1 Score

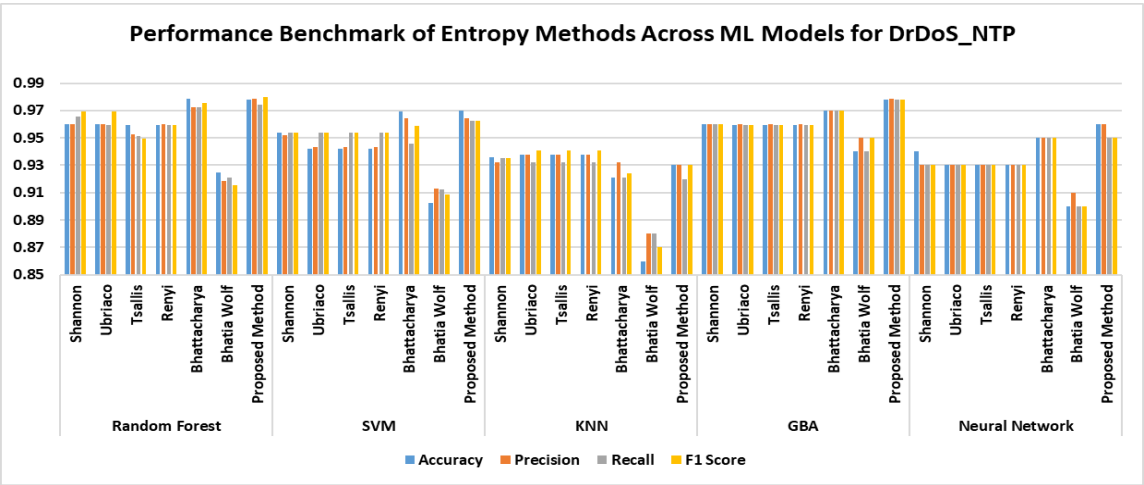
(b)


Performance Benchmark of Entropy Methods Across ML Models for DrDoS_MSSQL
0.99
0.97
0.95
0.93
0.91
0.89
0.87
0.85
Shannon
Ubriaco
Tsallis
Renyi
Bhattacharya
Bhatia Wolf
Proposed Method
Random Forest
SVM
KNN
GBA
Neural Network
Accuracy
Precision
Recall
F1 Score

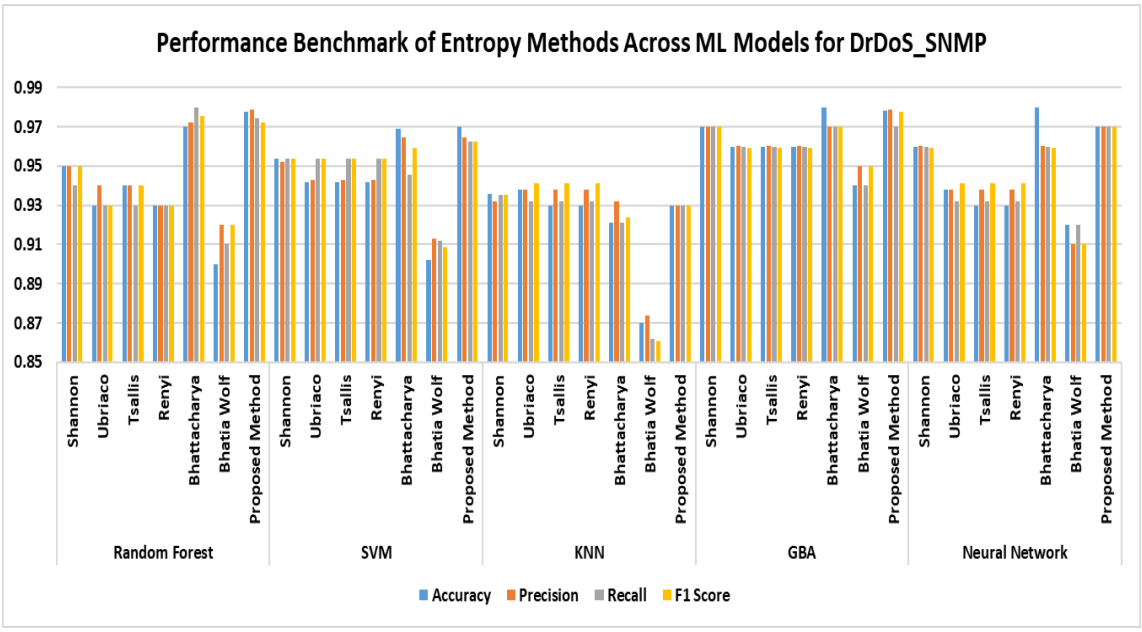
(c)


Performance Benchmark of Entropy Methods Across ML Models for DrDoS_NetBIOS
0.99
0.97
0.95
0.93
0.91
0.89
0.87
0.85
Shannon
Ubriaco
Tsallis
Renyi
Bhattacharya
Bhatia Wolf
Proposed Method
Random Forest
SVM
KNN
GBA
Neural Network
Accuracy
Precision
Recall
F1 Score

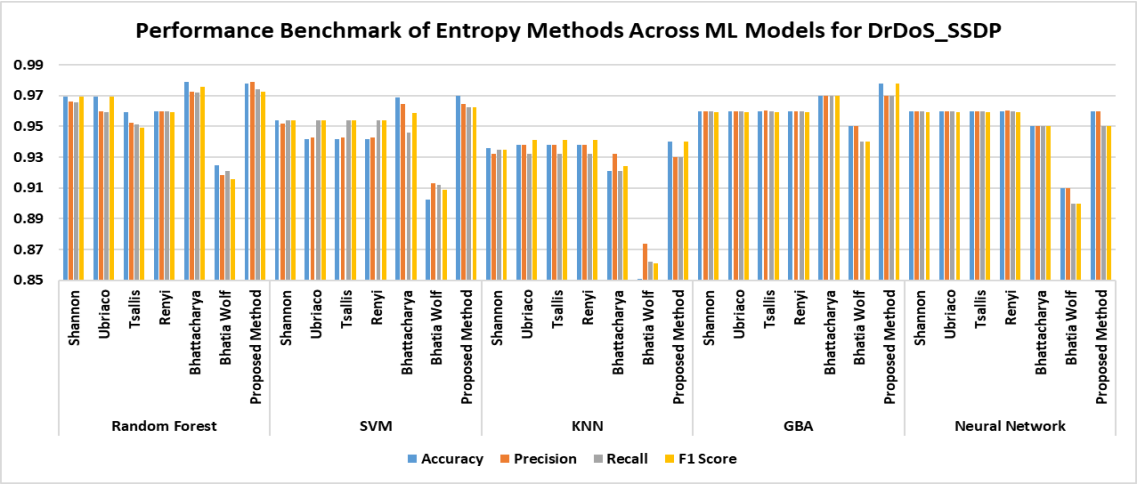
(d)


Performance Benchmark of Entropy Methods Across ML Models for DrDoS_NTP
0.99
0.97
0.95
0.93
0.91
0.89
0.87
0.85
Shannon
Ubriaco
Tsallis
Renyi
Bhattacharya
Bhatia Wolf
Proposed Method
Random Forest
SVM
KNN
GBA
Neural Network
Accuracy
Precision
Recall
F1 Score

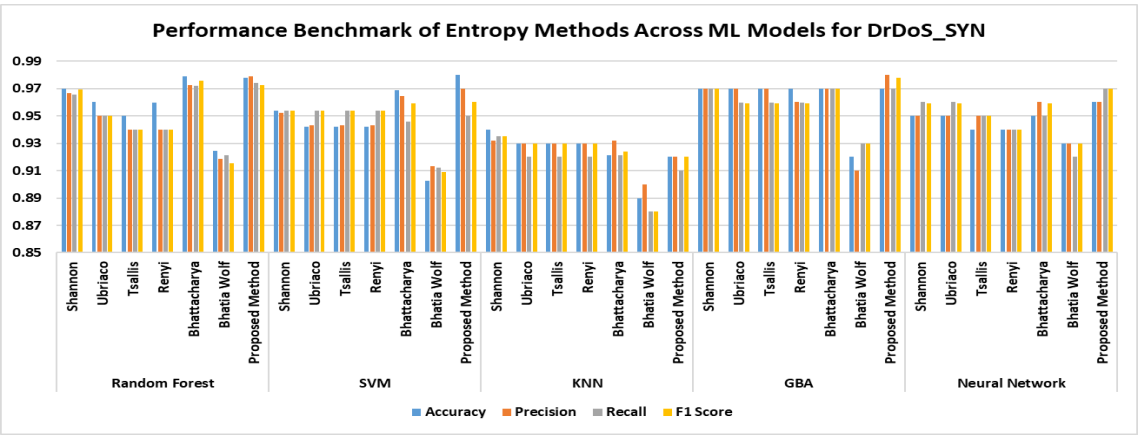
(e)


Performance Benchmark of Entropy Methods Across ML Models for DrDoS_SNMP
0.99
0.97
0.95
0.93
0.91
0.89
0.87
0.85
Shannon
Ubriaco
Tsallis
Renyi
Bhattacharya
Bhatia Wolf
Proposed Method
Random Forest
SVM
KNN
GBA
Neural Network
Accuracy
Precision
Recall
F1 Score

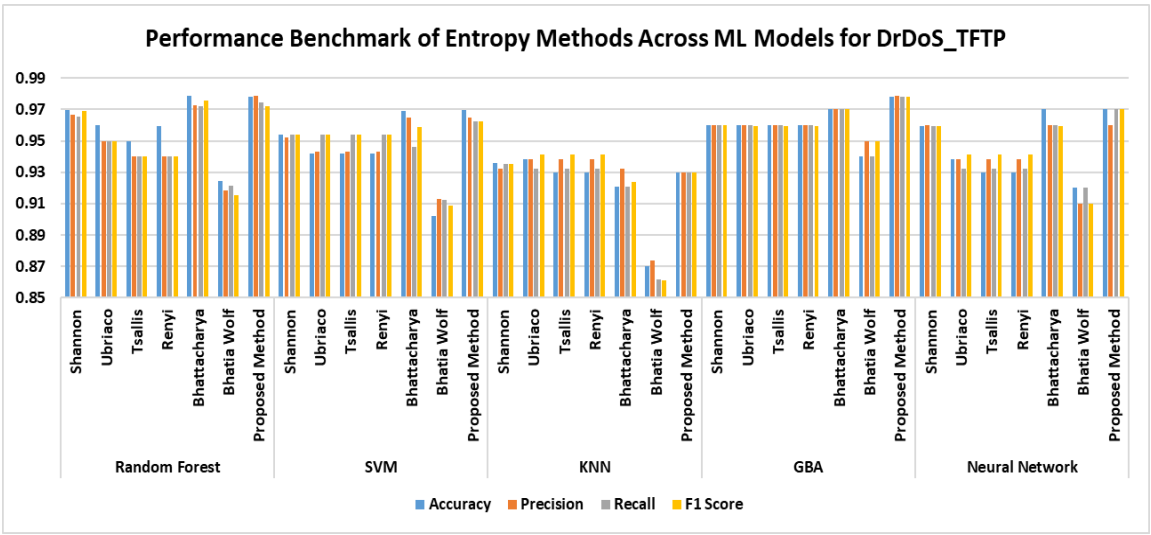
(f)


Performance Benchmark of Entropy Methods Across ML Models for DrDoS_SSDP
0.99
0.97
0.95
0.93
0.91
0.89
0.87
0.85
Shannon
Ubriaco
Tsallis
Renyi
Bhattacharya
Bhatia Wolf
Proposed Method
Random Forest
SVM
KNN
GBA
Neural Network
Accuracy
Precision
Recall
F1 Score

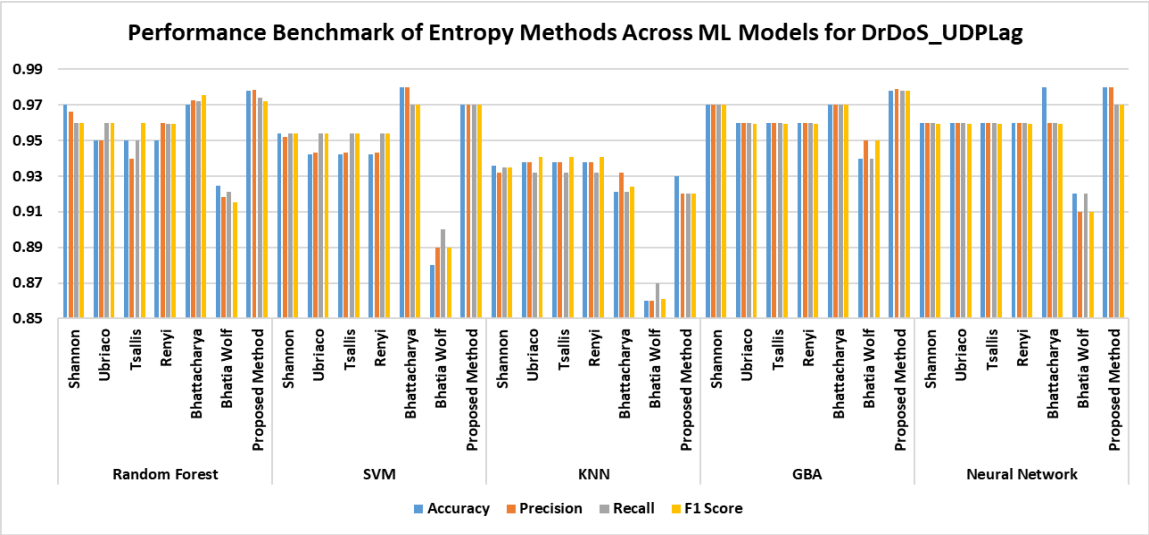
(g)


Performance Benchmark of Entropy Methods Across ML Models for DrDoS_SYN
0.99
0.97
0.95
0.93
0.91
0.89
0.87
0.85
Shannon
Ubriaco
Tsallis
Renyi
Bhattacharya
Bhatia Wolf
Proposed Method
Random Forest
SVM
KNN
GBA
Neural Network
Accuracy
Precision
Recall
F1 Score

(h)


Performance Benchmark of Entropy Methods Across ML Models for DrDoS_TFTP
0.99
0.97
0.95
0.93
0.91
0.89
0.87
0.85
Shannon
Ubriaco
Tsallis
Renyi
Bhattacharya
Bhatia Wolf
Proposed Method
Random Forest
SVM
KNN
GBA
Neural Network
Accuracy
Precision
Recall
F1 Score

(i)



(j)

FIGURE 6.7 (a-j) Performance Benchmark of Entropy Methods Across ML Models for Various DrDoS Attack

In FIGURE 6.7 (a-j) to exhibit the comparison between various entropy-based feature selection methods and their performance with different machine learning models (Random Forest, SVM, KNN, Gradient Boosting algorithm, and Neural Network) over multiple DDoS attacks, it appears that the proposed Joint Entropy among others performs well in various DDoS attacks. For a particular category attack, there is one of the four standard performance metrics, which are Accuracy, Precision, Recall, and F1-score, shown. In over almost all attack scenarios, the Joint entropy method was utilized for feature selection, computed higher, or the best close values for the corresponding metric classical entropy measures like Shannon, Renyi, Tsallis, Bhattacharyya, Bhattacharyya, and Ubriaco. It means that it is better in selecting statistically better and more informative and discriminative feature sets that are available for DDoS detection in machine learning.

Ensemble-based models tend to perform best among all classifier types under consideration: usually, Random Forest and Gradient Boosting classifiers demonstrate the highest overall performance over different types of attacks. Such classifiers average between 0.98 and 0.99 in terms of recall and false negatives (F1-score) at the feature selection level proposed. Neural network models tend to do well, too- SVM and KNN, in contrast, tend to lag somewhat in terms of recall, especially with respect to some attacks showing similar network characteristics. However, the feature selection approach generally benefits all models, meaning that it can generally be applied across diverse learning paradigms. The letdown rate of performance is comparable for different categories of DDoS attacks DrDOS-reflection-based (like, for instance DNS, NTP, SNMP, SSDP) or flooding-based (like SYN, TFTP,

UDPLag)-high metric values are maintained by the method throughout. This corresponds to attack-agnostic feature selection and greatly helps multi-layered DDoS classification strategies within very heterogeneous SDN environments.

Results from all performance benchmark graphs mentioned that effectiveness in getting classifiers of machine learning for detection of multilevel DDoS can be significantly improved through the sequential loading of select-features depending on the mutual information and joint entropy. Improvement in every measure-accuracy, precision, recall, and F1-score-across various attack types and classifiers provided evidence that the framework works effectively and should be generalizable. The next subsection is about operational efficiency time and latency in detections of the proposed models for real-time deployment in SDN.

6.3 Processing Time Analysis on Dataset

To detect distributed denial of service (DDoS) attacks within software defined networks efficiently and accurately, machine learning models mechanized should be configured to operate with low processing overhead for a fast response and of course damage mitigation. It will reflect the success of deploying the model in real-time environments with swift classification and decision-making. This section evaluates and compares the processing time of different machine learning algorithms using optimized feature subsets generated by the proposed feature selection approach.

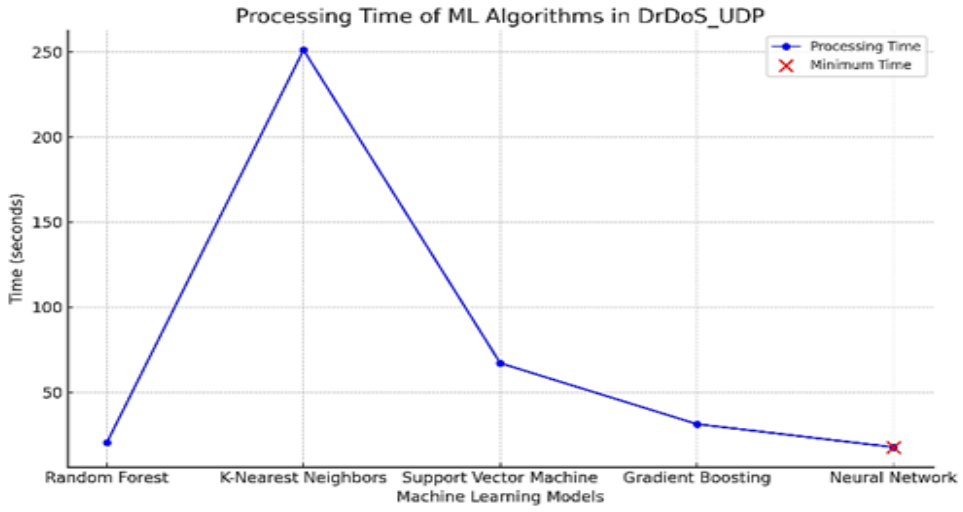
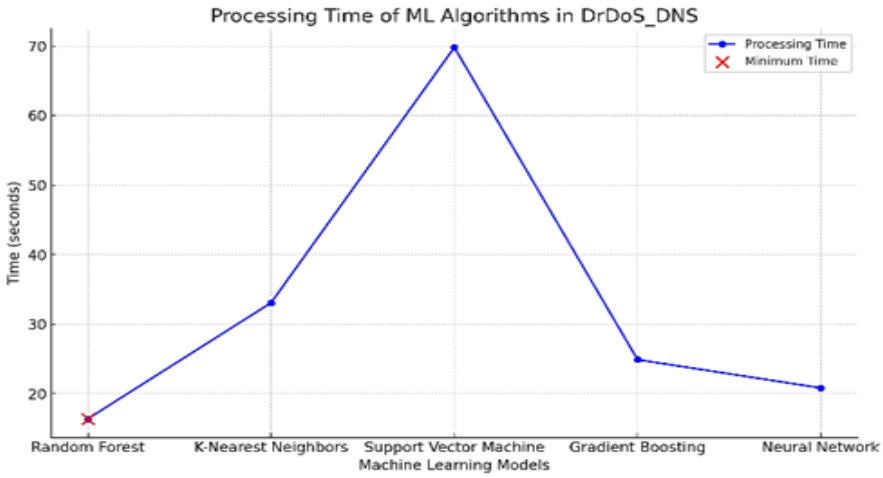


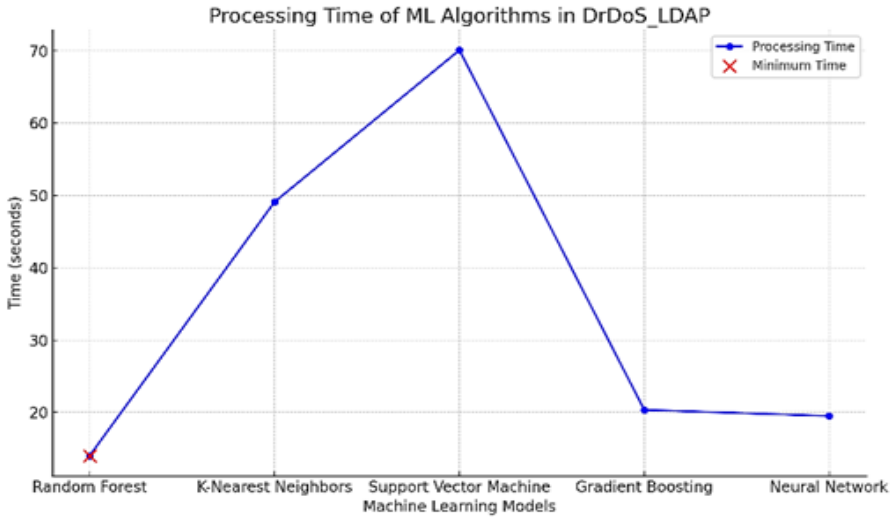
FIGURE 6.8 Processing Time of Various Machine Learning Models for the DrDoS_UDP attack.

Processing times for various machine learning models against the DrDoS Normal Rules are given in FIGURE 6.8 Among the examined models, the Random Forest classifier is quite low, showing good performance for execution along with reduced feature selection. Among the models, the Neural Network model exhibits the least processing time, demonstrating suitability with low latency and fast real-time implementation. The Gradient Boosting model includes a balance between classifying performance and computational cost, evident in a moderate processing time. KNN generally demands the most processing time because it is instance-based and must estimate instances against all training set instances, i.e., compute all elementary distances when classifying. The processing time is also significantly higher for those learning algorithms that are closer to SVMs; this is mainly due to the overhead associated with kernel-based computations.

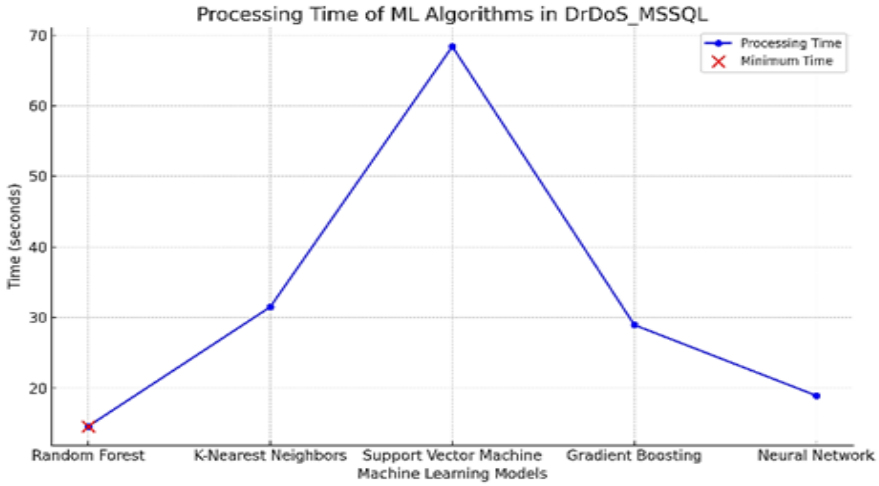
FIGURE 6.9 (a-j) illustrated are optimized times of machine learning algorithms against different DrDoS attack types for their optimized feature subsets. Clearly, in comparison with the other attack scenarios, there were some constant trends observable. RF and NN classifiers continued to demonstrate the least processing time for the better suitability for real-time application. By contrast, SVM invariably exhibits a higher processing time because kernel-based learning is inherently still regarded as overhead. KNN typically outweighs all attacks owing to its instance-based division, which involves the calculation of distances across the training set in cases such as SSDP and UDPLag. In every scenario, time for GBA is quite moderate, which is a nice balance between computation costs and detection performance.



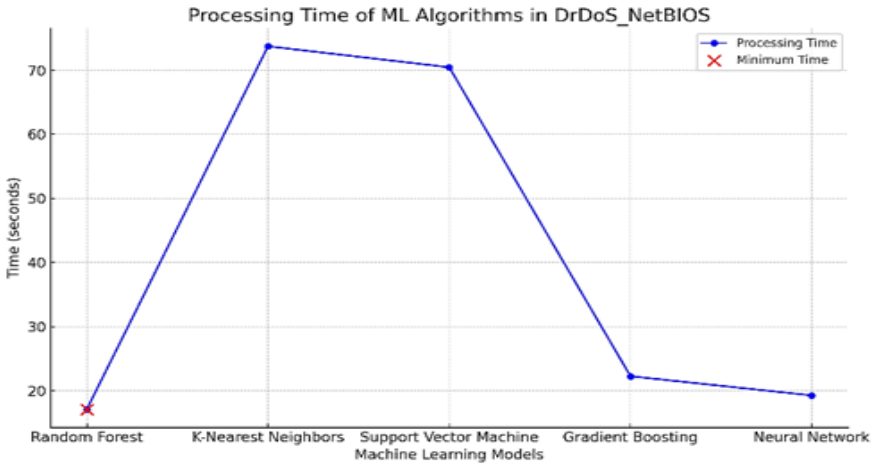
(a)


Processing Time of ML Algorithms in DrDoS_LDAP
Processing Time
Minimum Time
Time (seconds)
70
60
50
40
30
20
Random Forest
K-Nearest Neighbors
Support Vector Machine
Gradient Boosting
Neural Network
Machine Learning Models

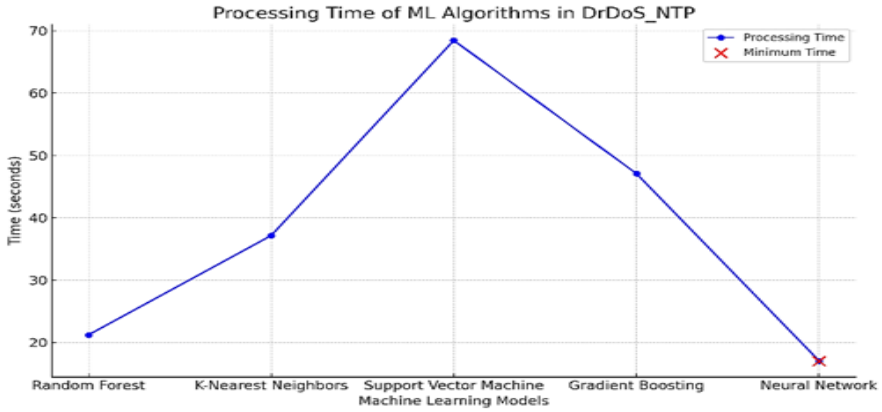
(b)


Processing Time of ML Algorithms in DrDoS_MSSQL
Processing Time
Minimum Time
Time (seconds)
70
60
50
40
30
20
Random Forest
K-Nearest Neighbors
Support Vector Machine
Gradient Boosting
Neural Network
Machine Learning Models

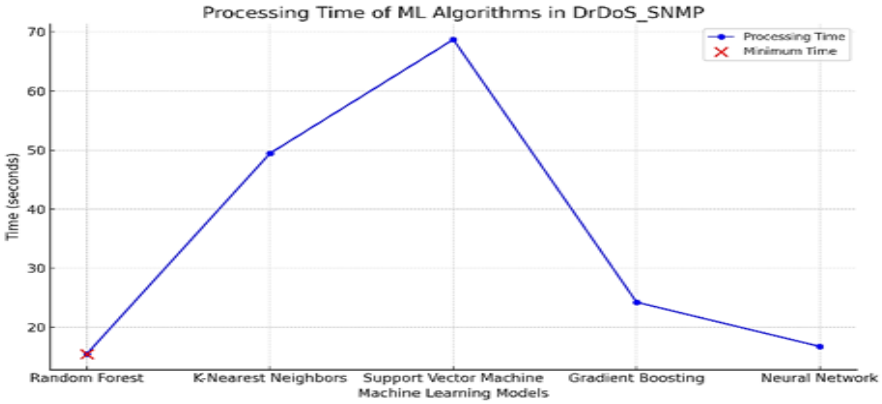
(c)


Processing Time of ML Algorithms in DrDoS_NetBIOS
Processing Time
Minimum Time
Time (seconds)
70
60
50
40
30
20
Random Forest
K-Nearest Neighbors
Support Vector Machine
Gradient Boosting
Neural Network
Machine Learning Models

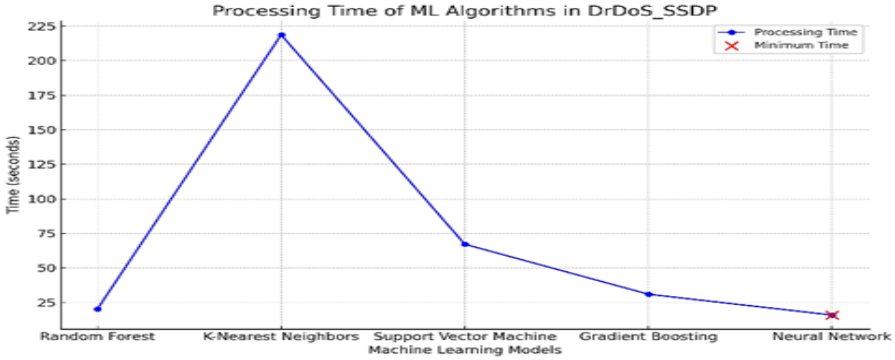
(d)


Processing Time of ML Algorithms in DrDoS_NTP
Processing Time
Minimum Time
Time (seconds)
70
60
50
40
30
20
Random Forest
K-Nearest Neighbors
Support Vector Machine
Gradient Boosting
Neural Network
Machine Learning Models

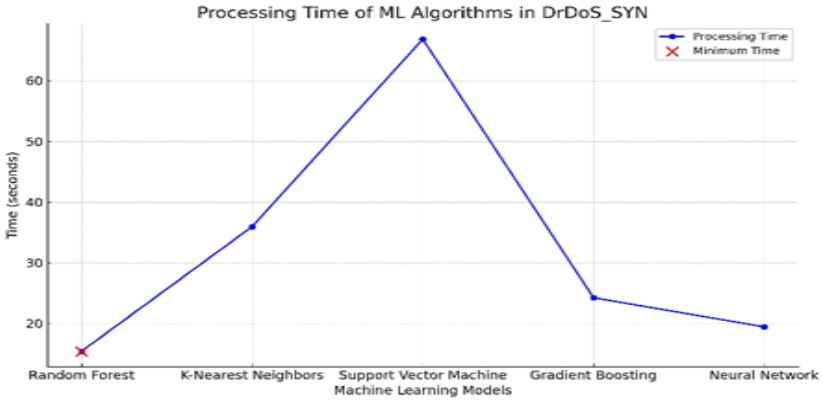
(e)


Processing Time of ML Algorithms in DrDoS_SNMP
Processing Time
Minimum Time
Time (seconds)
70
60
50
40
30
20
Random Forest
K-Nearest Neighbors
Support Vector Machine
Gradient Boosting
Neural Network
Machine Learning Models

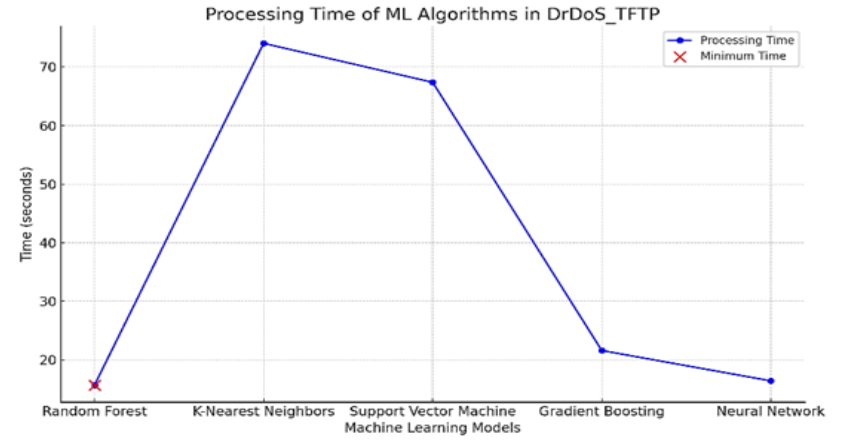
(f)


Processing Time of ML Algorithms in DrDoS_SSDP
Processing Time
Minimum Time
Time (seconds)
225
200
175
150
125
100
75
50
25
Random Forest
K-Nearest Neighbors
Support Vector Machine
Gradient Boosting
Neural Network
Machine Learning Models

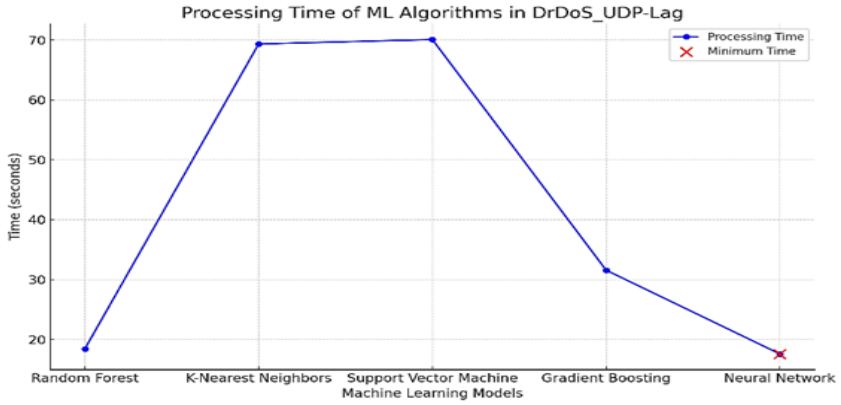
(g)


Processing Time of ML Algorithms in DrDoS_SYN
Processing Time
Minimum Time
Time (seconds)
60
50
40
30
20
Random Forest
K-Nearest Neighbors
Support Vector Machine
Gradient Boosting
Neural Network
Machine Learning Models

(h)



(i)



(j)

FIGURE 6.9 (a-j) Processing Time of Various DrDoS Attacks on Dataset

At first, the processing performance times differ slightly among modes of attack, but the ranking of algorithms also remains mostly consistent. For reflection-based attacks (DNS, NTP, SNMP, SSDP) and flooding-based attacks (SYN, TFTP, UDPLag), Random Forest and Neural Network keep showing low latency across the board, whereas SVM and KNN remains computationally heavier. This substantiates that feature selection strategy proposed compact and efficient feature subset is beneficial to all classifiers or even particularly all ensemble-based and neural model classifiers. In fact, running all the 11 DrDoS attacks proved that this scheme led to the smaller detection latencies during Random Forest, Gradient Boosting, and Neural Network modules.

Table 6.2 represents the relative processing-time behaviour while using various machine learning models in the context of different DrDoS attack types. The observed trends can be generalized for all the categories of attacks. Majority of the RF and NN model categories are moderately classified as Fast or Moderate (about 75%) and can thus easily detect an attack with minimal load on computational machinery. These make this category of models fit for real time SDN-based detection and mitigation of DDoS.

Table 6.2 Qualitative Processing Time Comparison of Machine Learning Models on Dataset

DrDoS Type	RF	NN	SVM	KNN	GB
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

However, SVM is classified more frequently as the Slowest moving or Slow because kernel-based learning is expensive in terms of computation. KNN also turns out to be relatively very slow for most of the attacks, owing to its instance-based classification process. GBA, in general, has a moderate to slow processing time, and is a moderate trade-off in protection due to computation and accuracy.

6.4 Live Traffic Based Detection Performance

In this part, the evaluation of detection capability of the developed framework is presented on live traffic generated within the SDN test bed. A case turns up in other sections that the previous sections focused on offline evaluation using benchmark datasets, and eventually the live traffic-based analysis is necessary to prove its practical applicability of the proposed

method under real-time network condition. This section's performance goal was to gauge if the two were complementary when they were addressing real-time traffic streams.

6.4.1 Feature Selection Results on Live Traffic

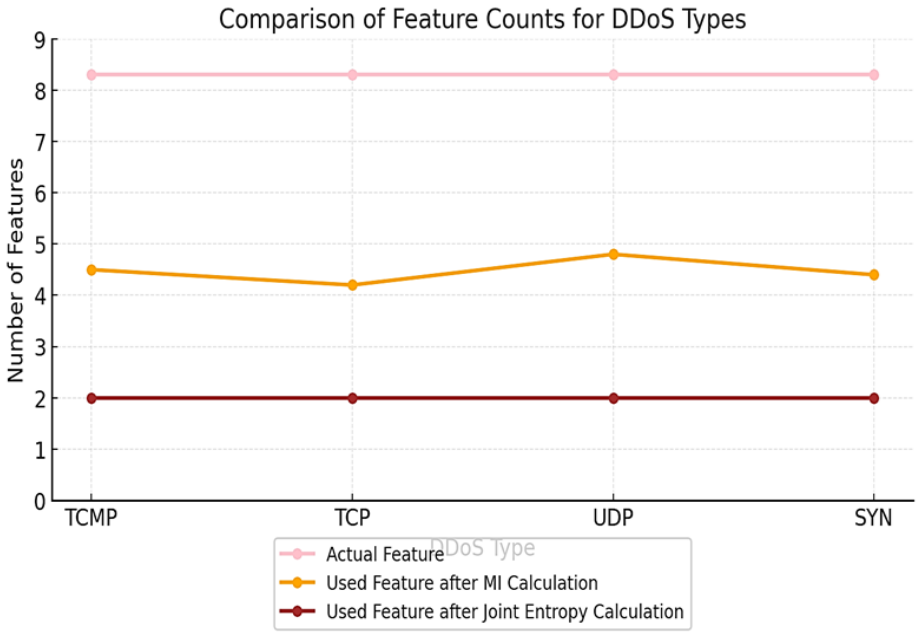


FIGURE 6.10 Selected features of different DrDoS attack on Live traffic

FIGURE 6.10 illustrate live traffic DDoS detection after successive times of reducing features. Despite the original information plotted about those traffic types (ICMP, TCP, UDP, and SYN), in the eight main information source lists, when applying Mutual Information-based filtering, that drops down to some four to five features each, leaving lesser insightful details for removing irrelevant attributes; the next Joint Entropy-based refinement would greatly shrink these information sets in all traffic types to only two features.

The results of the selection process using the proposed method demonstrate its effectiveness in selecting non-redundant and meaningful features, even in complex and dynamic traffic environments. The ability to achieve substantial dimensionality reduction while preserving discriminative information confirms that the proposed method is lightweight and suitable for real-time deployment in SDN environments.

6.4.2 Entropy-Based Threshold Validation

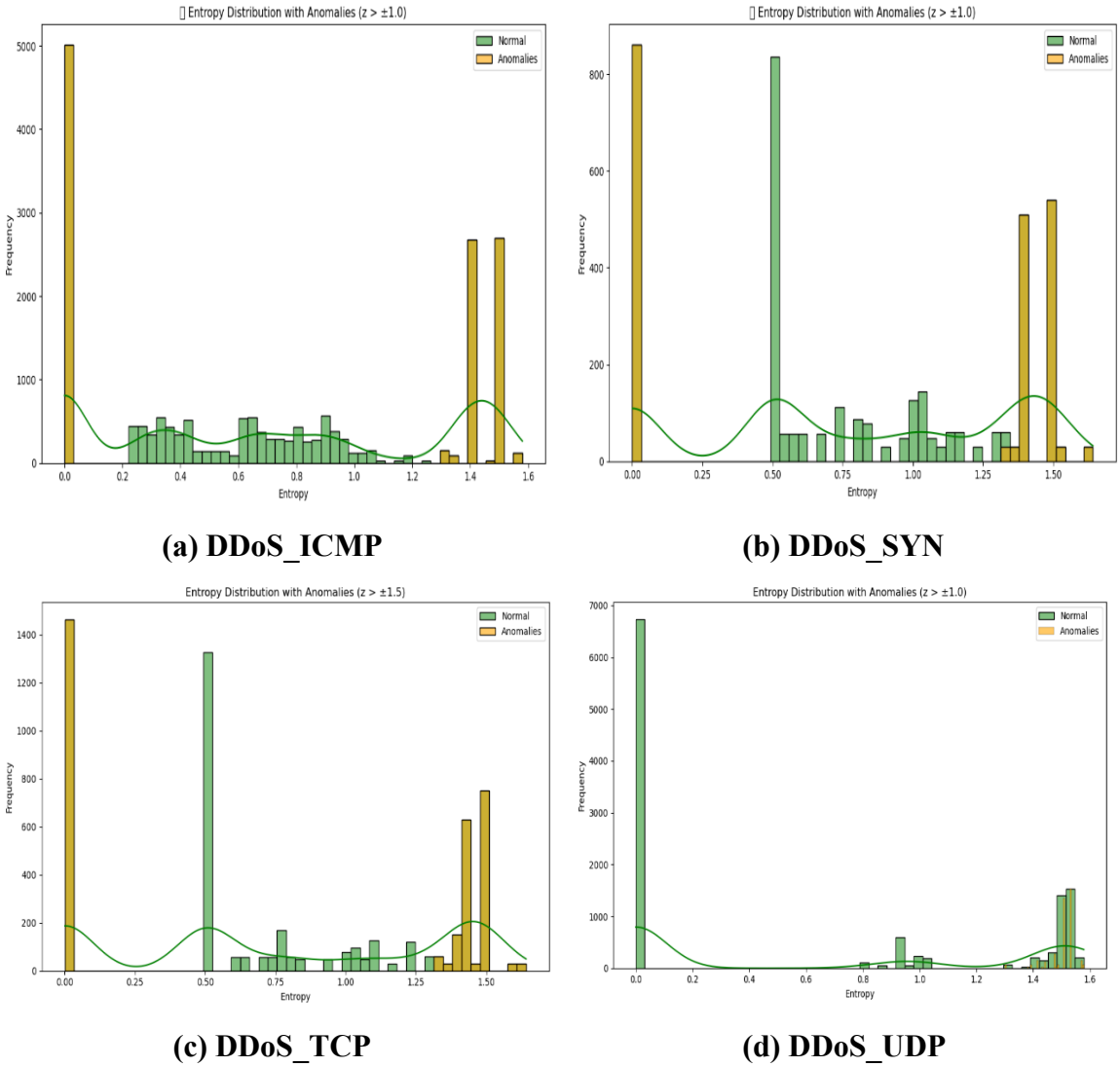
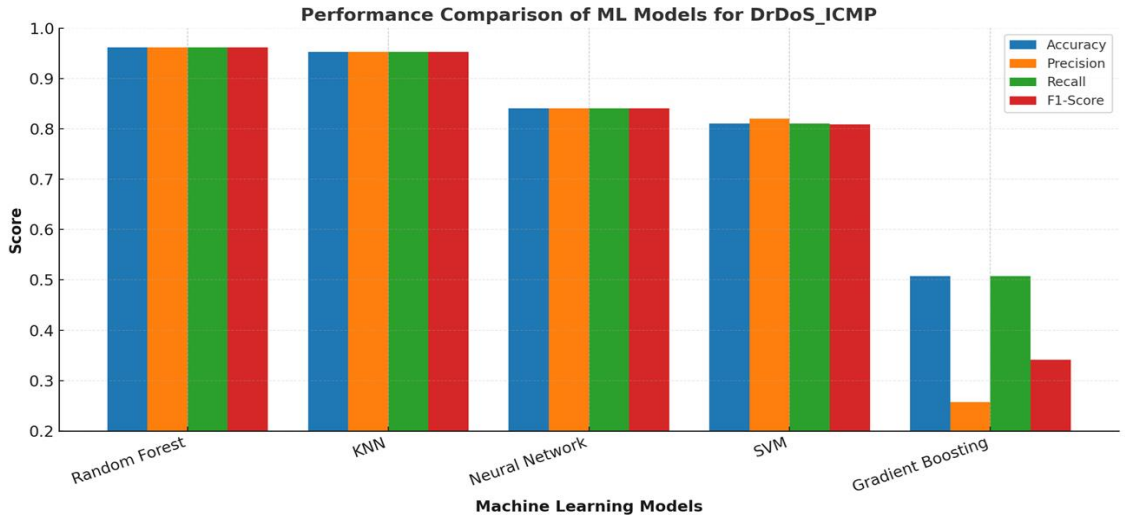
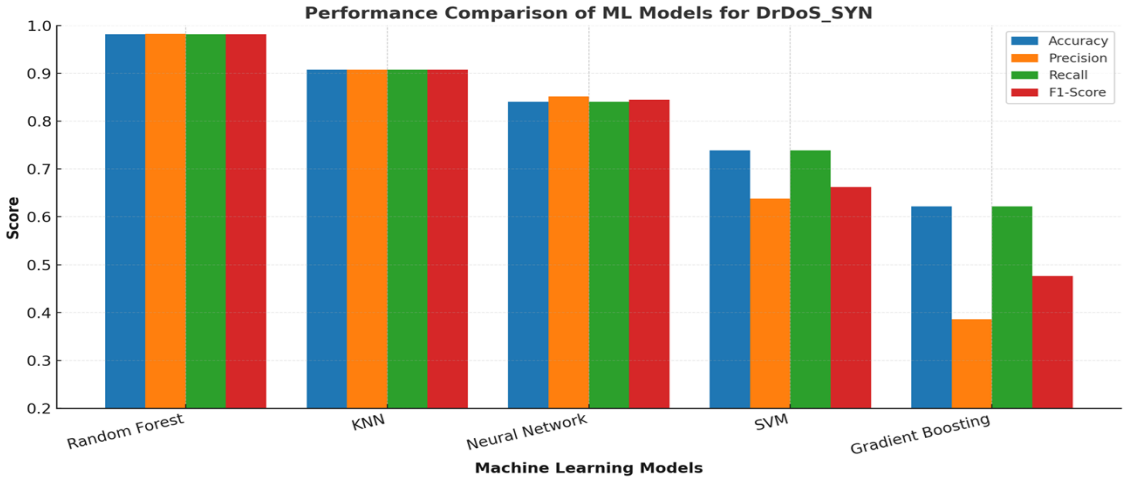


FIGURE 6.11 (a-d) Entropy Distribution of Normal and Anomalous Traffic Under Different Thresholds

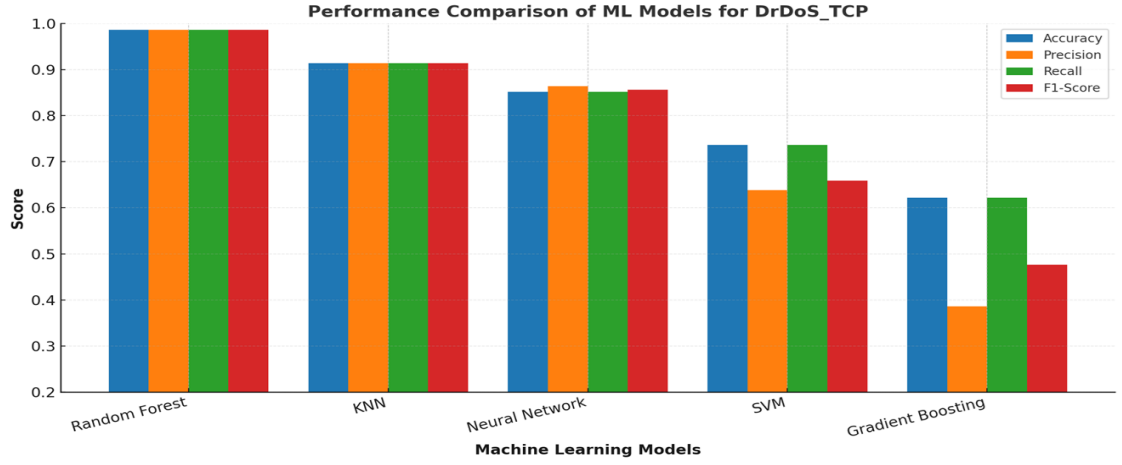
The FIGURE 6.11 (a-d) illustrates entropy distributions for ICMP, SYN, TCP, and UDP DDoS attacks, showing clear separation between normal and anomalous traffic. Normal traffic is mainly concentrated in the moderate entropy range (≈0.3-1.0), indicating diverse and legitimate communication patterns. In contrast, anomalous traffic appears at very low entropy (~0) due to repetitive flooding behaviour and at high entropy (≈1.3-1.6) due to distributed attack sources. The ICMP and SYN attacks show stronger low-entropy spikes, while TCP and UDP exhibit more high-entropy distributions. Applying Z-score thresholds (±1.0 and ±1.5) helps control anomaly sensitivity, where ±1.0 detects more deviations and ±1.5 focuses on stronger anomalies. Overall, the graphs validate entropy as an effective feature for distinguishing different types of DDoS attack behaviours.


Performance Comparison of ML Models for DrDoS_ICMP
Accuracy
Precision
Recall
F1-Score
Score
1.0
0.9
0.8
0.7
0.6
0.5
0.4
0.3
0.2
Random Forest
KNN
Neural Network
SVM
Gradient Boosting
Machine Learning Models

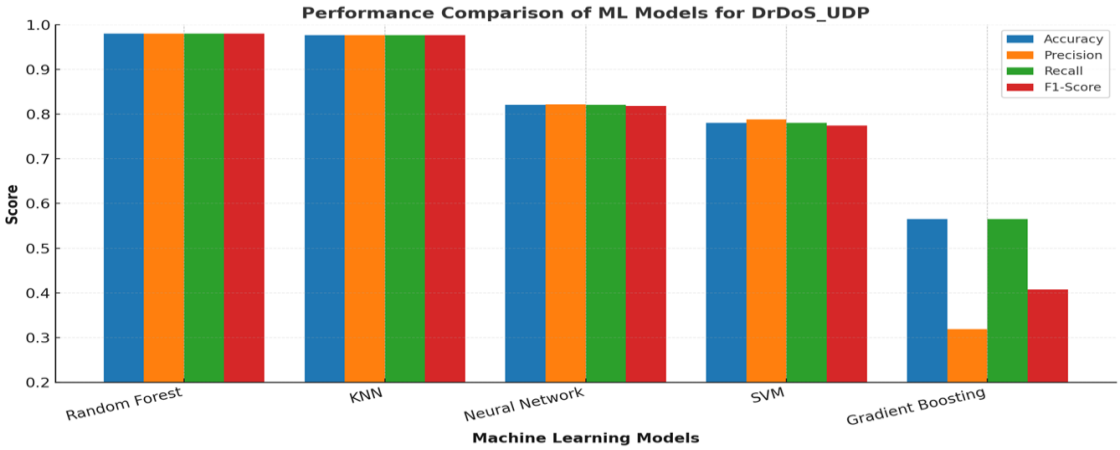
(a)


Performance Comparison of ML Models for DrDoS_SYN
Accuracy
Precision
Recall
F1-Score
Score
1.0
0.9
0.8
0.7
0.6
0.5
0.4
0.3
0.2
Random Forest
KNN
Neural Network
SVM
Gradient Boosting
Machine Learning Models

(b)


Performance Comparison of ML Models for DrDoS_TCP
Accuracy
Precision
Recall
F1-Score
Score
1.0
0.9
0.8
0.7
0.6
0.5
0.4
0.3
0.2
Random Forest
KNN
Neural Network
SVM
Gradient Boosting
Machine Learning Models

(c)



(d)

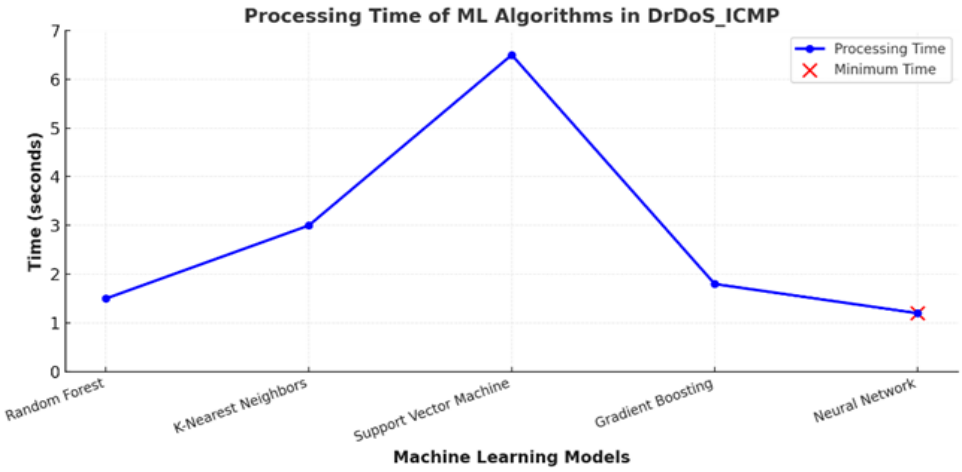
FIGURE 6.12 (a-d) Performance Comparison of Different ML Models on various Live Traffic

The results, which are based on the live DrDoS ICMP, SYN, TCP, and UDP traffic, are as shown below in FIGURE 6.12 (a-d). The proposed method and real-time traffic applications are thus maintaining strong detection performance, as the design characteristics can be seen with the database-based evaluations.

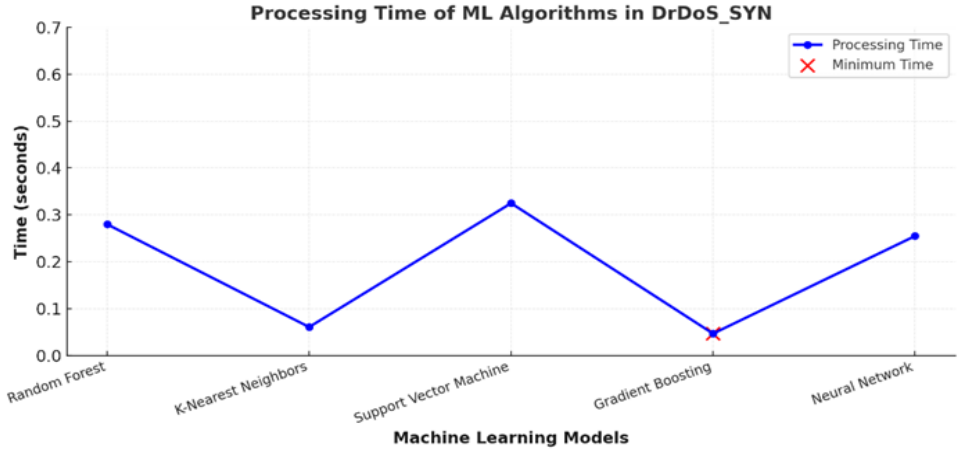
The Random Forest classifier is the best in performance for all four types of traffic with an average accuracy and F1 score higher than 0.98–0.99. KNN had competitive scores too, particularly for ICMP and UDP traffic, wherein the accuracy achieved is over 0.95. The Neural Network models perform well in the mid-range, with an average accuracy over 0.82–0.86 across all live traffic scenarios. SVM shows inferior results-especially for SYN and TCP attacks-because the higher-level sampling display lower performance, indicative of sensitivity to overlapping feature distributions in real-time traffic. Of all the models evaluated, Gradient Boosting shows the lowest impact, particularly in precision and F1-score. In comparison with the Random Forest model, almost all the traffic types show a decreasing line on precision and recall ratings compared to elevated accuracy trends in accuracy. The consistently high recall score of Random Forest further confirms its goodness in detecting attacker traffic with minimal false negatives that are required for real-time DDoS defense purposes. In general, these results verify that the suggested feature selection and multi-tier detection structure effectively generalizes to live SDN traffic. The alignment between offline dataset outcomes and live traffic performance further supports the robustness and real-world applicability of the proposed system. Random Forest stands out as the best classifier for deployment in the live SDN environment due to its high accuracy, stability, and reliability.

6.4.3 Processing Time Analysis on Live Traffic

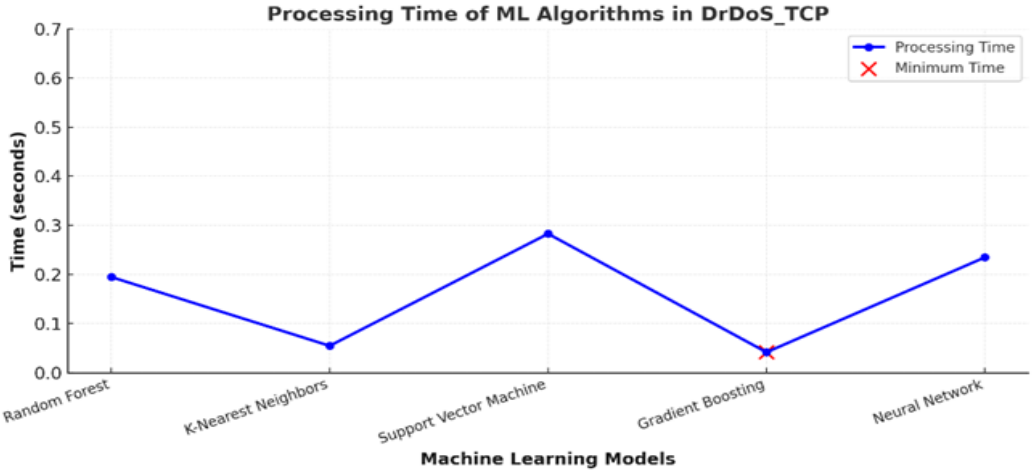
FIGURE 6.13 illustrates the processing times for various machine-learning models on real-time DrDoS ICMP, SYN, TCP, and UDP traffic data by employing optimally selected subsets of features. Results indicated that performances of all models investigated were in the lowest possible classification period, thus showcasing the suitability for real-time deployment of the proposed framework. The RF and NN traffic types are two types of traffic that are fast, less than one second, and therefore have short inference time and are likely to be efficient in utilizing selected features. KNN has a fast edge till it hits the case of a limited number of selected features in live scenarios. Compared to other models, SVM consistently takes higher processing time, reflecting overhead incurred because of kernel-related operations. GBA brings a minimum time to conduct SYN, TCP, and UDP traffic, whereas latency remains competitive for ICMP traffic.



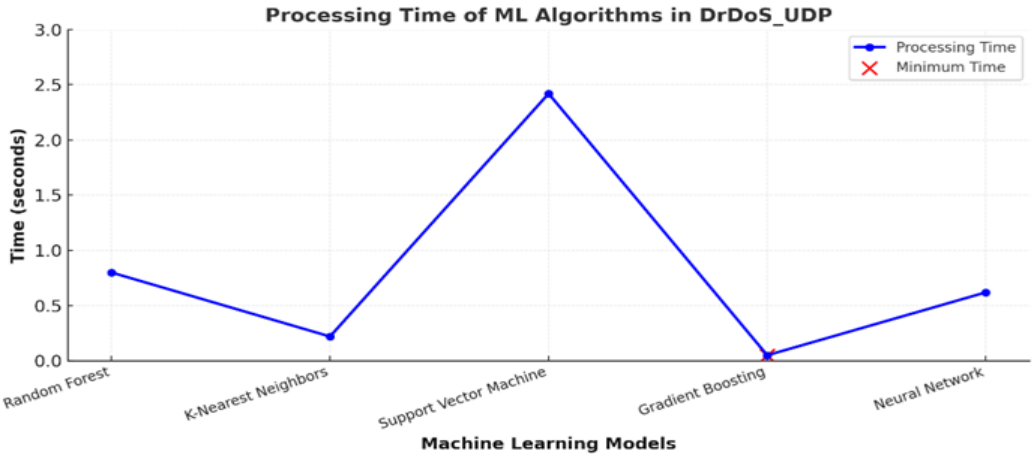
(a)



(b)



(c)



(d)

FIGURE 6.13 (a-d) Processing Time of Various DrDoS Attacks on Live Traffic

Therefore, these results were observed in using the proposed feature selection approach which allowed a lighter and faster model execution on live traffic. Moreover, with the robust detection feature observed earlier, further evidence was proven about the practical possibility of implementing the framework in online SDN-based DDoS detection and mitigation.

In Table 6.3 the processing-time model qualitative form for live traffic going through DDoS using various machine learning models is presented. In general, Random Forest, Neural Network, KNN, and Gradient Boosting gave the optimal speeds for data of most types of attack, making them be good candidates for real-time implementation. SVM, as discussed, invariably registered the lowest processing times on moderate values due to lags in computation. Overall, these results tend to point out that Random Forest, Neural Network, and Gradient Boosting represented the most recommended algorithms for effective traffic detection in real time.

Table 6.3 Qualitative Processing Time Comparison of Machine Learning Models 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

6.5 Live Testbed Results

This section presents a discussion of outcomes and analysis resulting from the experiments conducted on the live SDN testbed that was set up using Mininet and the Ryu controller. Aim to test the viability of Information Gain driven multi-level DDoS detection and mitigation framework using a real-world network scenario. Evaluation based on offline datasets does not apply here since live testbed allows demonstration of traffic patterns, their gravity evaluation, offers mitigation of the attacks as they take place in the system.

FIGURE 6.14 depicts the Ryu controller terminal output while the live testbed is running. The logs continuously report entropy values, IG scores, and traffic classifications for packets received at various switches. For most packets, the controller provides entropy and IG values within the normal range, and the traffic is classified as Normal, signifying legitimate network behaviour. the calculated IG value falls under the set low-severity limit, and the controller labels the traffic as Low DDoS. Immediately after this classification, the controller triggers a mitigation action and installs an OpenFlow rule to redirect the suspicious traffic to the honeypot node (IP: 10.0. 0.100) via switch S3, port 1.

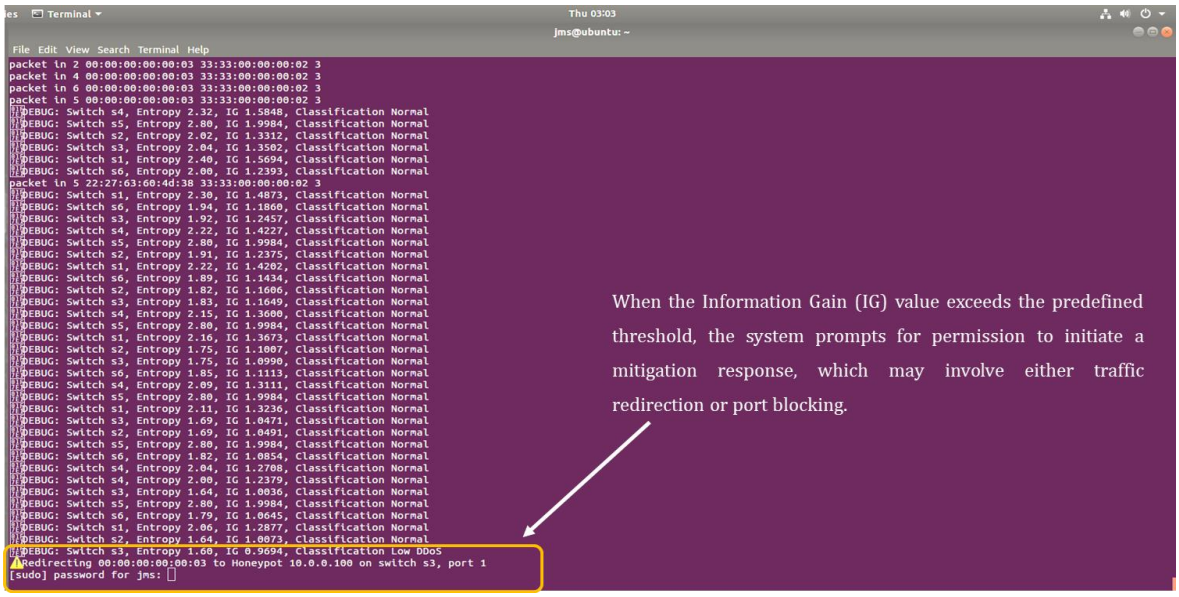


FIGURE 6.14 RYU-Mininet Simulation Environment Normal Traffic

This action demonstrates that the proposed framework can identify low-rate attacks instantly and enforce severity-aware mitigation automatically.

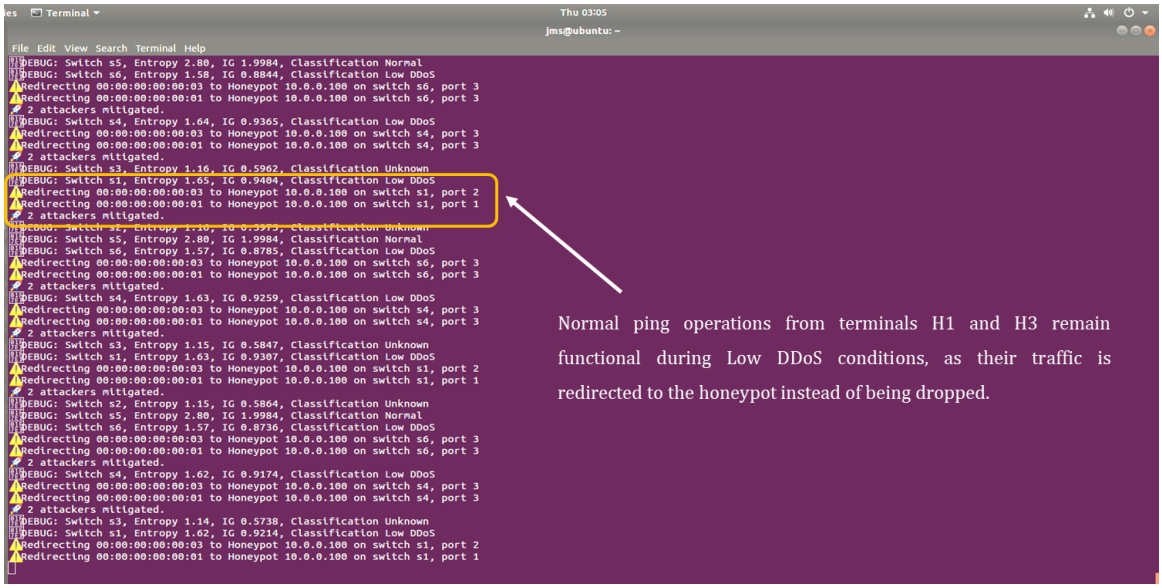


FIGURE 6.15 Low-Severity DDoS Mitigation via Honeypot Redirection

Ryu controller outputs during experiments are shown in FIGURE 6.15. A continuous detection and mitigation of low-severity DDoS attacks have been ensured. In a real-time basis, the logs of the controller will help you to know the entropy and Information Gain published and their corresponding classification as far as different switches are concerned. When the IG value falls within the low-severity threshold range, the controller labels traffic as Low DDoS. The controller then immediately installs a set of OpenFlow rules to redirect flows of concern on suspicious traffic seen onto the honeypot (10.0. 0.100) switching it on

the correct switch and port. This assists to remove malicious data for further analysis, rather than stop it abruptly. An important observation is that normal ping operations from legitimate hosts (e.g., H1 and H3) continue to function correctly during low-severity attack conditions. This confirms that the proposed framework applies proportional mitigation, preserving normal network services while containing malicious activity.

The output from both the H1 and H3 host terminals during a low-assault DDoS attack could be seen from FIGURE 6.16 On the Live SDN testbed. ICMP echo reply messages would continue, so it would still be able to ping well continuously on behalf of a legitimate host while attack traffic crosses the network. Instead of completely interrupting the traffic, the proposed framework tends to perform honeypot redirection for any traffic suspected of participating in very mild DDoS conditions. Consequently, malicious flows will find their way into isolation, with legitimate traffic experiencing no visible degradation while reaching its destination.

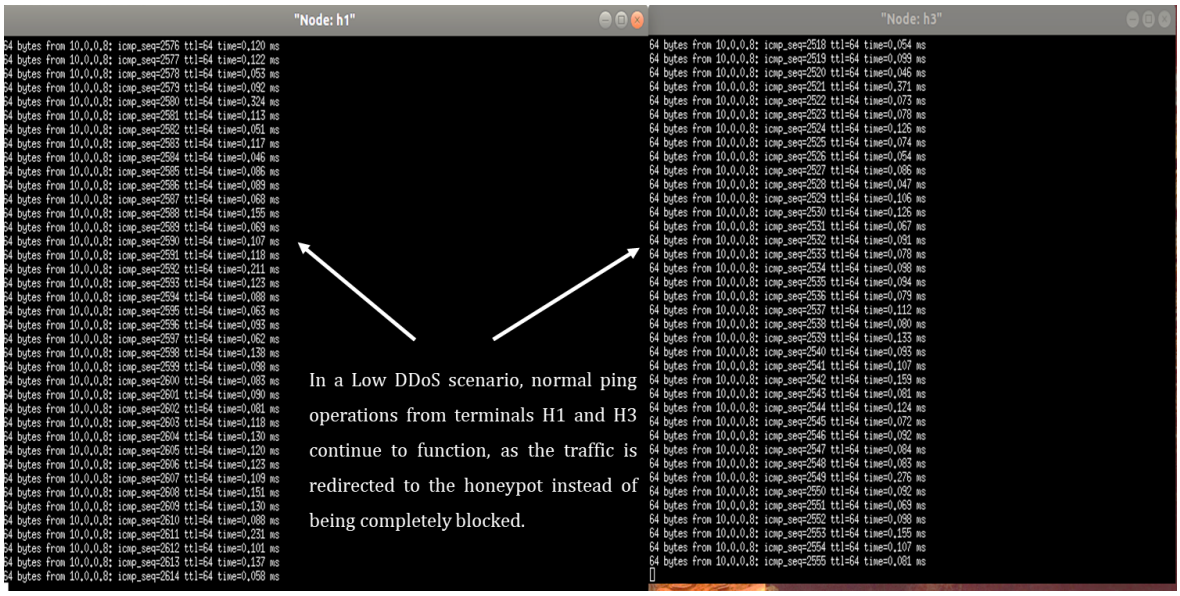


FIGURE 6.16 Normal Ping Connectivity from Legitimate Hosts During Low-Severity DDoS Attack

Illustrations were shown in the form of screenshots illustrating the proportionality and non-interference features of the proposed mitigation strategy. Instead of a hard drop, the system guarantees continued network availability for regular users while still managing to minimize low-rate undesirable traffic that will account for the successful operation of the severity-aware mitigation mechanism in real-time.

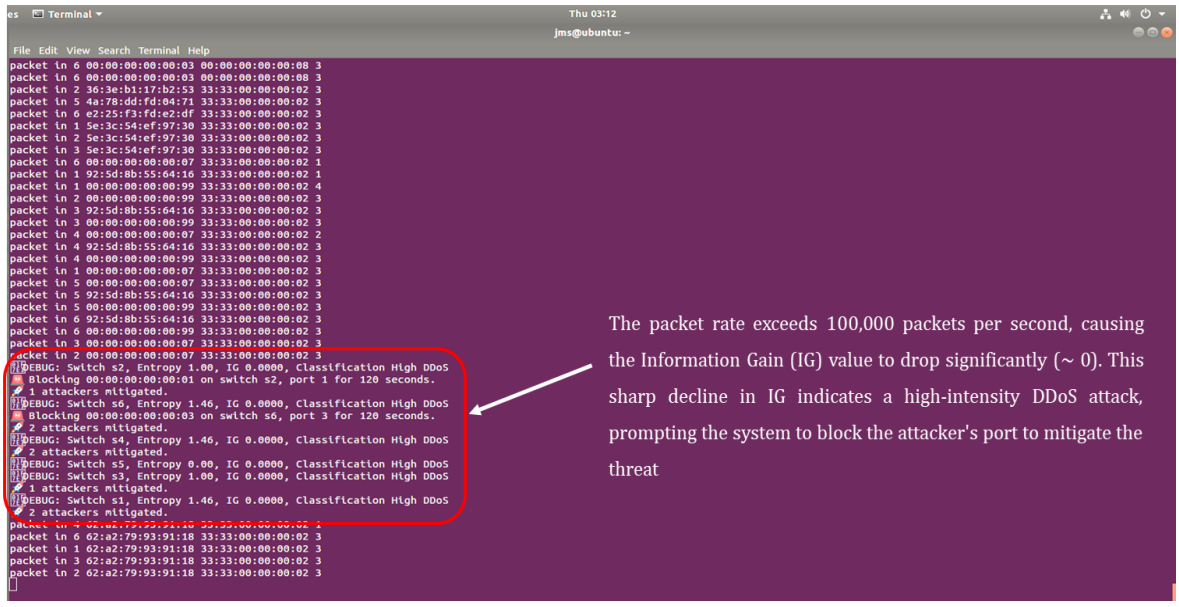


FIGURE 6.17 High-Severity DDoS Detection and Port Blocking

The snapshot gets illustrated in FIGURE 6.17, showing the Ryu controller terminal during the live SDN test bed DDoS attack sector of high severity. The graph shows an initial rise in incoming packets' rate, which is followed by a sharp drop towards very near zero of the Information Gain value.

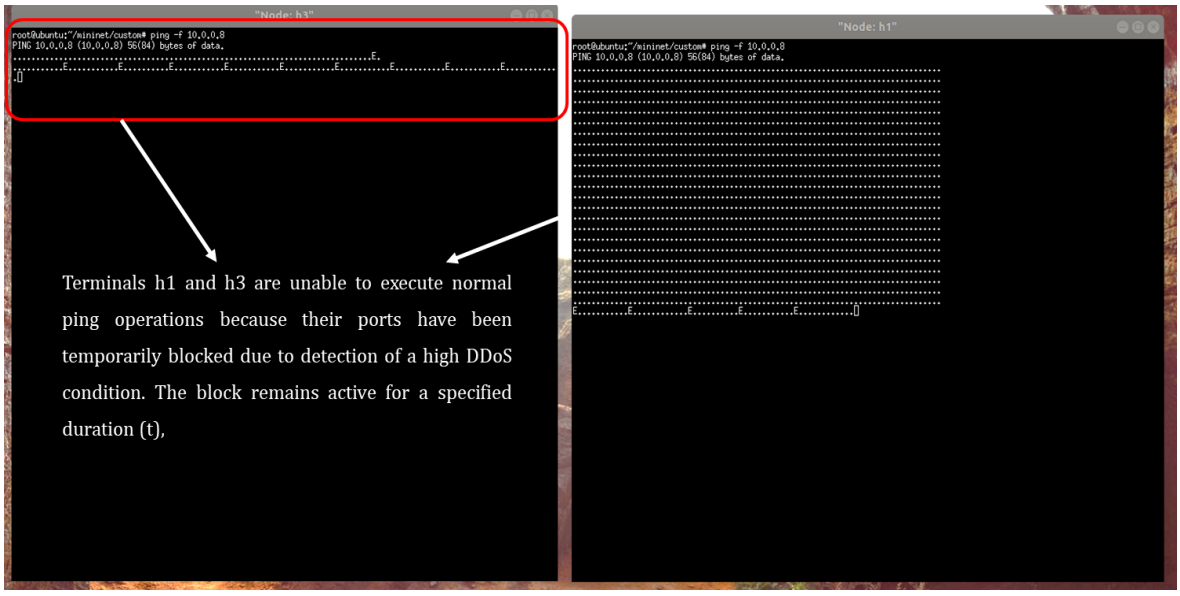


FIGURE 6.18 Ping Failure at Legitimate Hosts Due to Port Blocking During High-Severity DDoS Attack

This behaviour confirms that the traffic is very concentrated and comes mainly from a few source characteristics of the high-intensity DDoS flooding attacks. FIGURE 6.17, demonstrates that the proposed framework can rapidly detect high-severity attacks and apply aggressive mitigation actions when required, thereby protecting network resources and

preventing controller overload. Together with the low-severity redirection results, these observations validate the effectiveness of the severity-aware mitigation mechanism in real-time SDN environments.

FIGURE 6.18, illustrates the terminal results of hosts H1 and H3 under a high-intensity DDoS attack within a real SDN testbed. It is evident that normal ping operations are unsuccessful, as ICMP echo requests remain unanswered. This behaviour confirms that the traffic has been identified as high-severity DDoS, triggering mitigation mechanisms that block the corresponding ingress switch ports to prevent further network disruption.

In FIGURE 6.19 the termination message of the host when a major DDoS outbreak and mitigation event is expected. Several ICMP echo requests sent come back with a "Destination Host Unreachable" message which means that SDN controller, as part of the high-severity mitigation action strategy, has managed to take care of blocking ports. Things should return to normal shortly after this time as normal package forwarding will now be re-enabled and security policy deployed in such a way as to resume the propagation of illegal traffic.

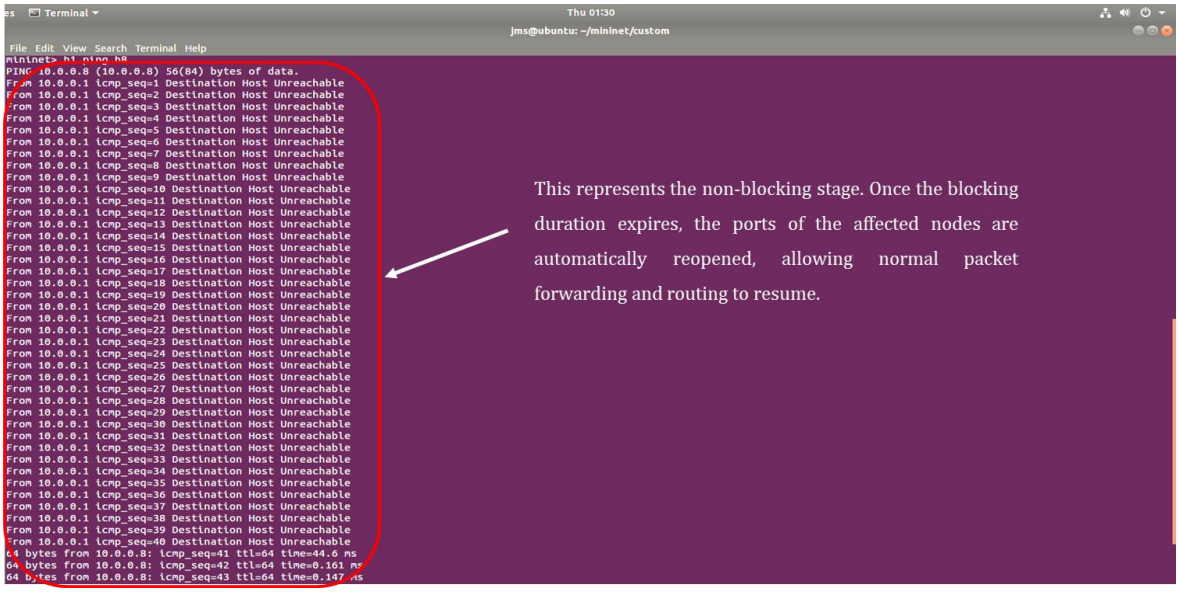


FIGURE 6.19 Automatic Recovery and Restoration of Connectivity After High-Severity DDoS Mitigation

After the pre-determined blocking duration has lapsed, the ICMP echo replies are duly received. Hence, this is indicative of the automated removal of the mitigation rules by the controller that ultimately opens the ports which were earlier affected and stranded; hence, normal communication resumes without requiring any intervention. This screen makes it

easy to secure that self-healing feature has been integrated into the framework to ensure temporary mitigation actions do not have any lasting impact on the system. This function is crucial in the automatic restoration of connectivity once the attack conditions pass away, ensuring network availability and operational flow or continuity in real-time SDN operation mode. In summary, the live SDN testbed experiments demonstrate that the proposed framework functions reliably under real-time conditions. The controller can constantly observe traffic, precisely distinguish normal, low-severity, and high-severity DDoS flows, and apply appropriate mitigation measures using SDN-native techniques. Low-severity attacks are effectively isolated via honeypot redirection without impacting legitimate users, while high-severity attacks prompt immediate port-level blocking to safeguard network resources. Additionally, the automated recovery mechanism guarantees restoration of normal connectivity once attack conditions ease. These findings confirm the practical feasibility and effectiveness of the proposed framework for real-world SDN deployment.

6.6 Mitigation Performance

This section assesses how well the proposed severity-aware SDN mitigation mechanism can translate detection decisions into right, partly right, or compensating response actions. So far, the previous sections have focused on detection accuracy, processing time, and real-time feasibility. After detection performance analysis, mitigation performance is focused quite much on how dependably the framework applies right actions or the failure to stop legitimate traffic, the redirection of low-severity attack flows to a honeypot, and immediate blocking of attack sources having severe severity. This evaluation set includes benchmark dataset outcomes with similar live SDN testbed observations in clarifying the consistency and quite perfect reliability of the proposed mitigation strategy.

6.6.1 Mitigation Performance on Dataset

CICDDoS2019 has been utilized to analyse mitigation efficiency by labelling predicted severity values and linking them to their respective mitigation actions. The output discovered that many normal traffic samples were classified correctly under the "Allow" action, while only low severity attack samples were classified largely under "Honeypot Redirection," and high severity attacks are "Blocking," respectively. The few false mitigations usually are the results of correct classifications and misalignments, as true-positive are very much higher and the false-dismissed mitigation outcomes are also very low in magnitude. Moreover, the

proportion of false negative mitigation instances have been very small, reinforcing the belief that only a few attack flows are likely to escape from a response-an element critical to maintaining network security. Such findings conclude that, once turned against an offline giant dataset, the proposed framework will make objective and exact decisions for mitigation purposes.

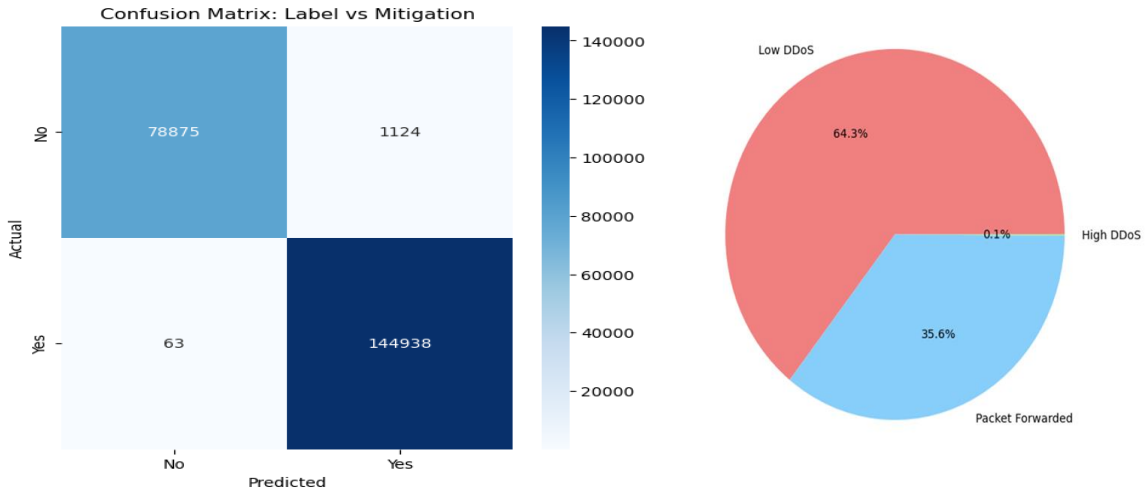
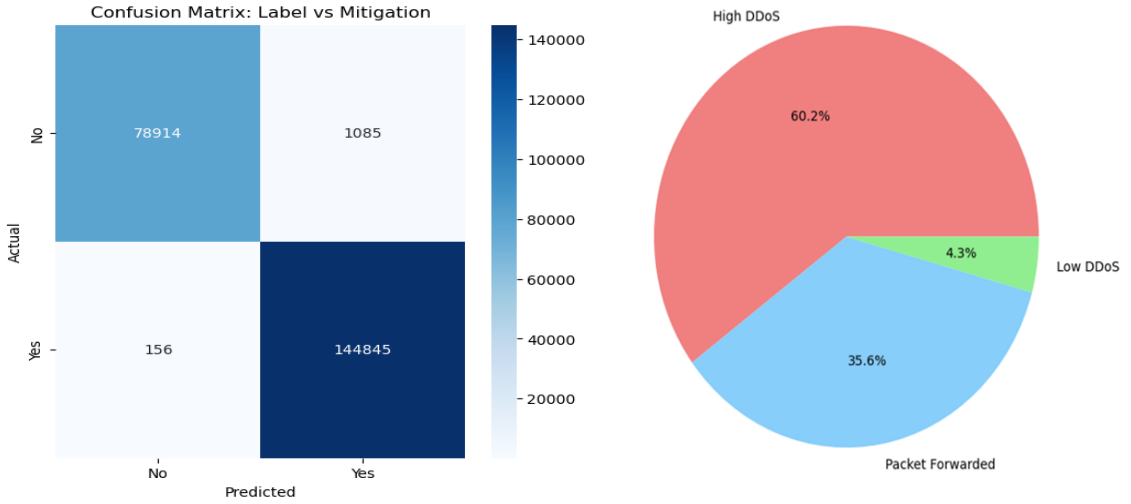


FIGURE 6.20 Severity-Aware Mitigation Performance for DrDoS_UDP on Dataset

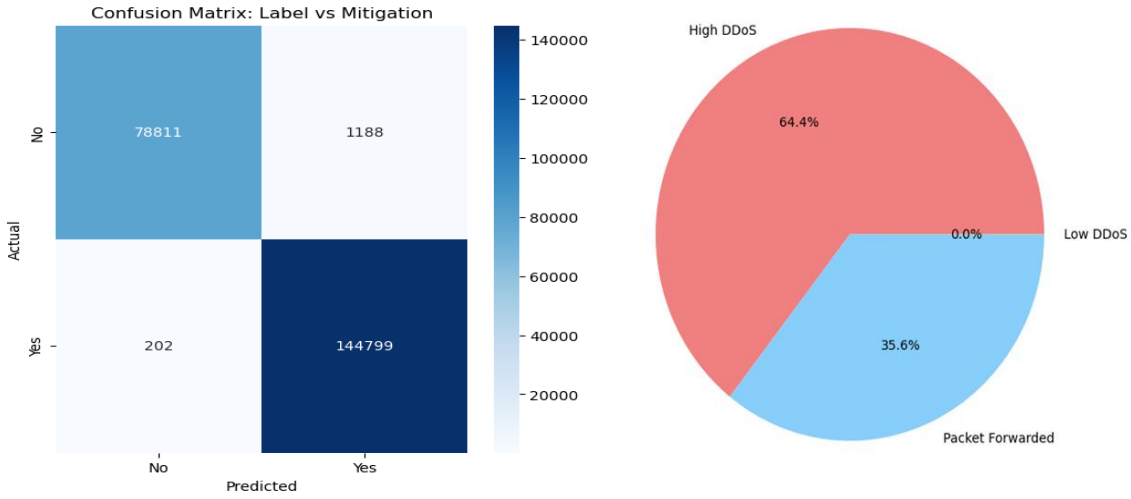
In FIGURE 6.20 the image of the proposed framework is shown with the beneficiary performance over the CICDDoS2019 dataset using the complementary visualizations, like displayed immediately above. The distribution of mitigation treatments applied after detection has been depicted using a pie chart, while the correctness of such mitigations acquires a precision score when judged in a confusion matrix. There are approximately 35.6% of legitimate flows on the normal path forwarded from the pie chart. The high proportion of flows has 64.3% tagged with low-severity DDoS and then redirected towards a honeypot for further isolation and analysis. Less with only 0.1% reaches the level of blocking, which corresponds to clear situational compliance, demonstrating an application of aggressive mitigation only when necessary. Therefore, the skewness explains the existence of scale for proportionate levels of mitigation, staying away from wholesale actions of blocking.

The Label vs Mitigation confusion matrix, in addition, emphasizes the validity of the steps taken. Out of this, 78,875 normal sample is rightly left without mitigation – True Negatives, while 144,938 attack samples rightly activate the mitigation – True Positives. On the other hand, only about 1,124 normal samples receive unnecessary mitigation which is the False Positive and about 63 attack samples are avoided which is equivalent to the False Negative.

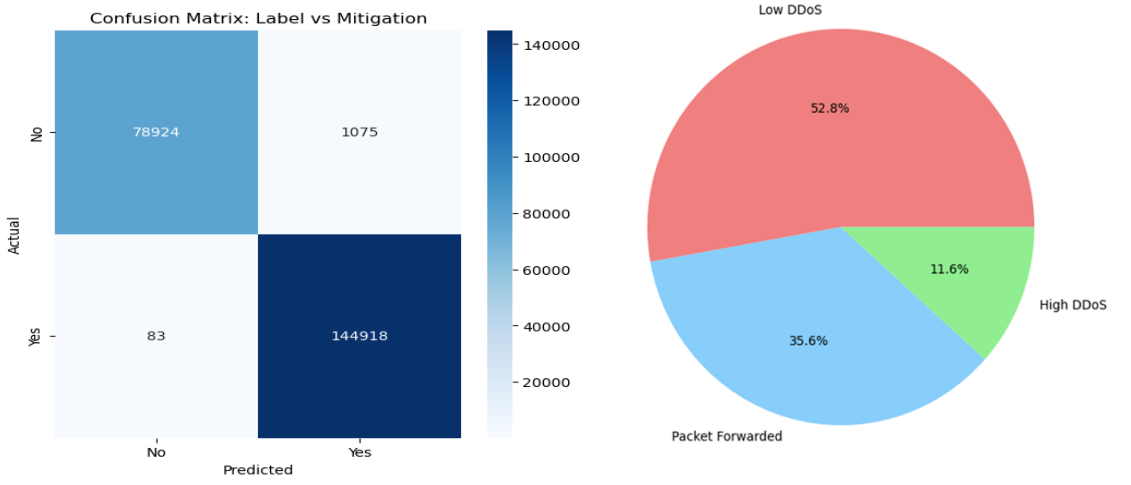
It is also critical that this count is so low on false negatives because it means that very few attacks evade mitigation.



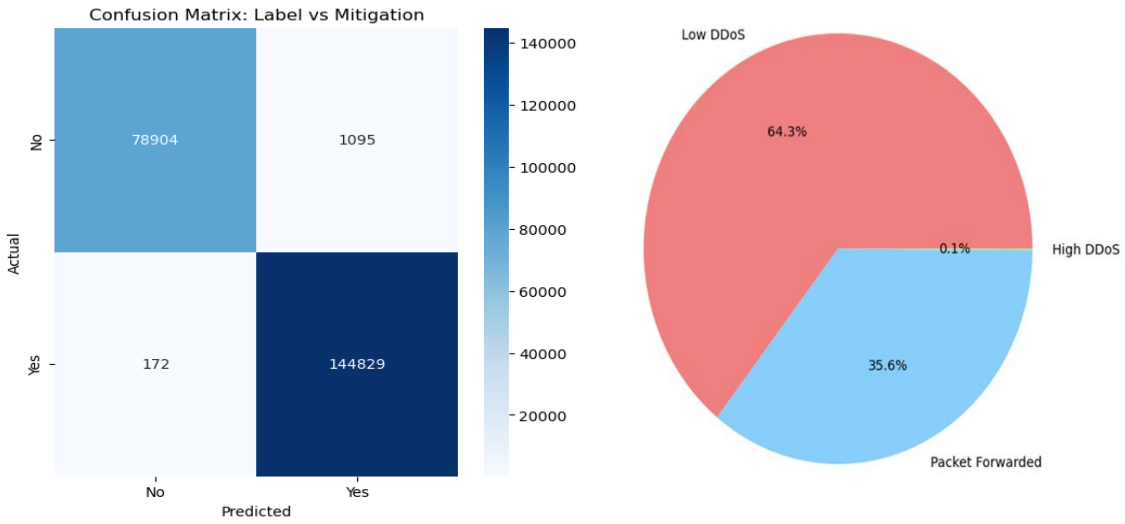
(a) DrDoS_DNS



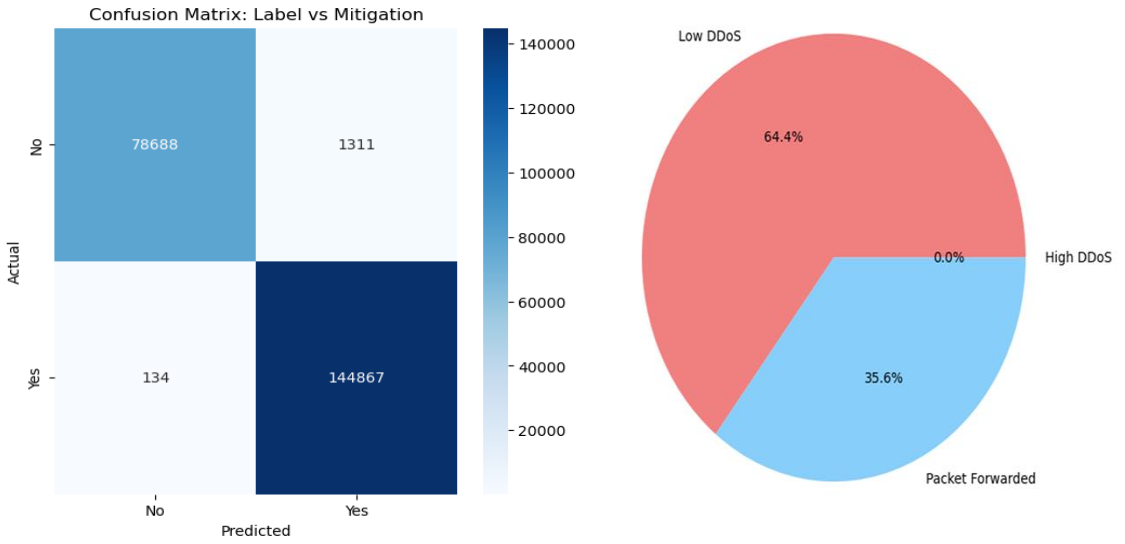
(b) DrDoS_LDAP



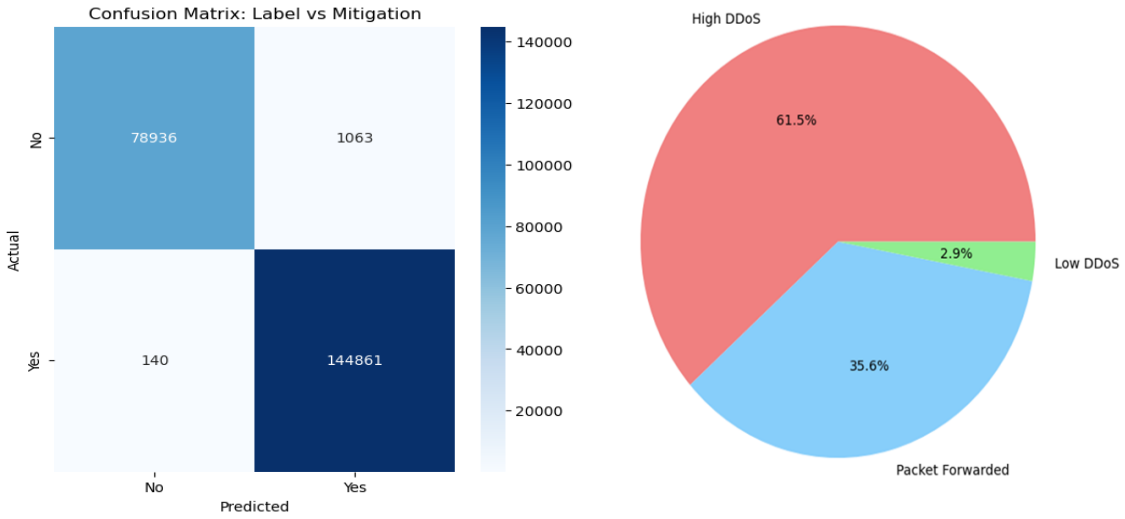
(c) DrDoS_MSSQL



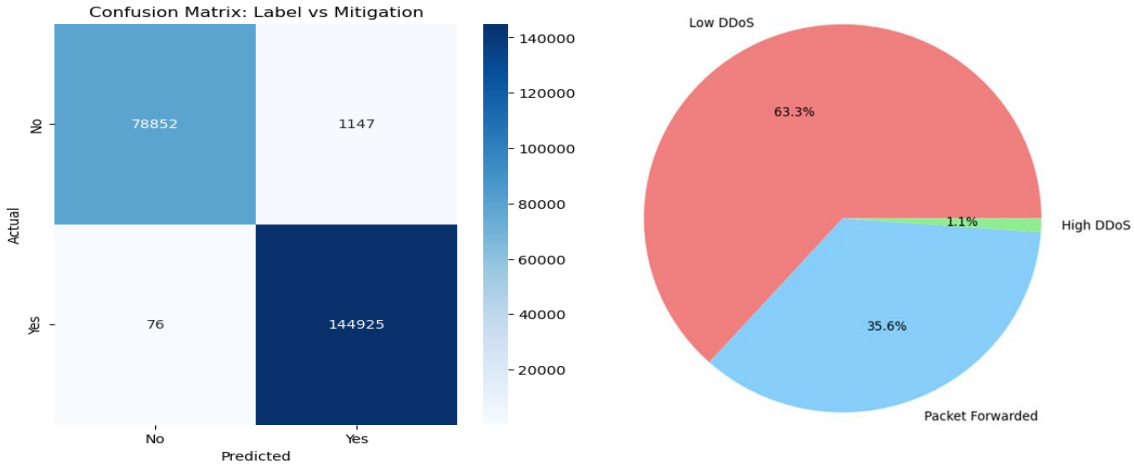
(d) DrDoS_NetBIOS



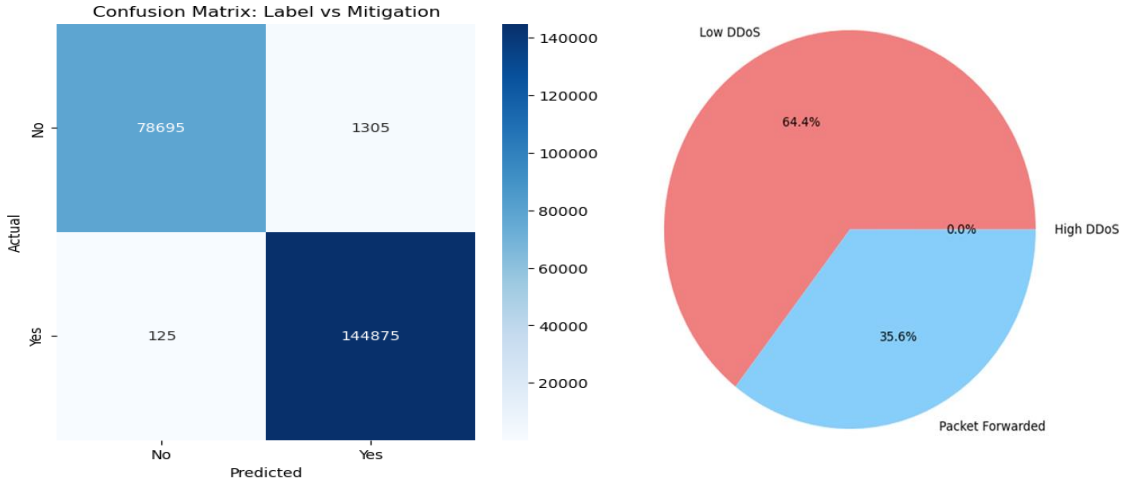
(e) DrDoS_NTP



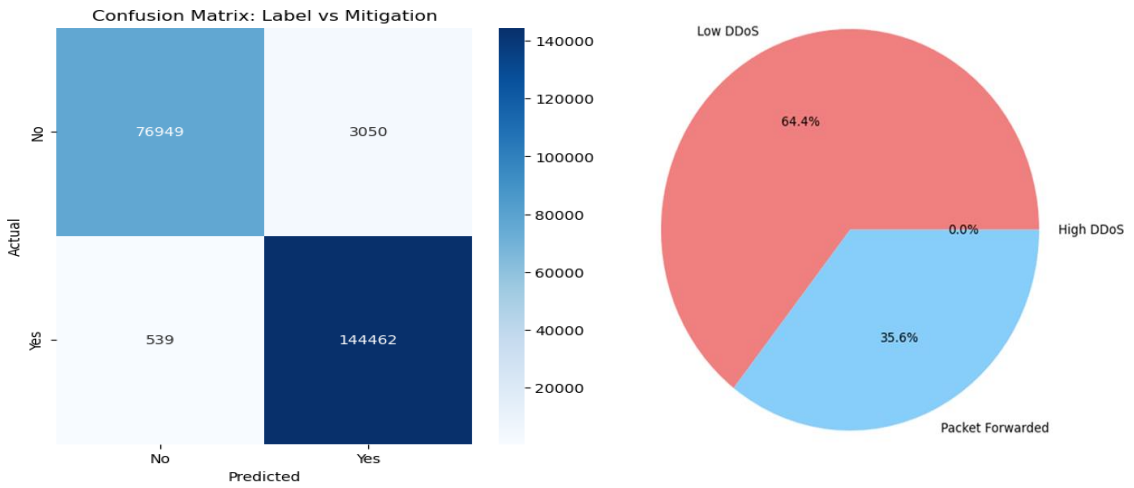
(f) DrDoS_SNMP



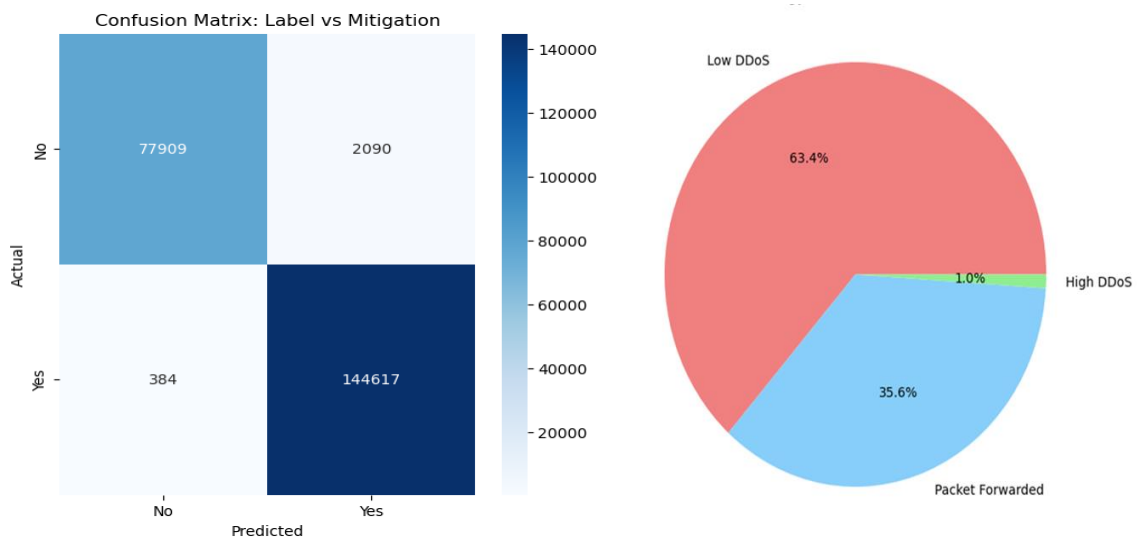
(g) DrDoS_SSDP



(h) DrDoS_SYN



(i) DrDoS_TFTP



(j) DrDoS_UDPLag

FIGURE 6.21(a-j) Severity-Aware Mitigation Performance for various DDoS attacks on Dataset

The FIGURE 6.21(a-j) illustrate the mitigation performance of the framework with paired visualize a Label vs Mitigation confusion matrix along with its corresponding distribution of mitigation actions. It consistently shows that most of the case is handled correctly, such that a normal traffic is not passed through the mitigation-True negatives with the attack traffic passing through them as True Positives, triggering actions towards mitigation. Only a small percentage of false positives-prompting the need for mitigation for benign traffic-and even a tiny number of false negatives, which points toward missed mitigations of attacks, can be noted. Moreover, pie charts exhibit an overlap with the distribution of the implemented mitigating measures. A specific share of the traffic (approximately 1/3) escapes properly as normal traffic, while most malicious flows run into low-severity redirection or high-severity blocking as applicable-which throttles everything depending on the severity of the attack. In numerous cases, the low-severity DDoS traffic group forms a large part of the mitigated flows, followed by nonintrusive honeypot redirection as a preferred alternative for the system design. This selective responsiveness to blocking on high severity indicates that intensive attack flooding should be greeted with aggressive mitigation. In all the eleven types of DrDoS attacks, the mitigation performance results demonstrate high correctness and reliability over time. The present framework aligns significantly with the outcomes of detection that are subsequently mitigated through next actions and maintains an extremely low false-negative rate using blocking techniques that are less resolute. The confusion matrices, along with the distribution plots for mitigation, all stand in agreement in showing that the proposed framework successfully balances security and service availability by isolating low-severity attacks and aggressively blocking only high-severity threats.

6.6.2 Mitigation Performance on Live Traffic

This subsection evaluates the attack mitigation mechanism is proposed, which is severity-aware from the generated live traffic on the actual SDN testbed. The purpose is to ensure that results are identified through detection are effectively translated into real-time mitigation actions or responses to include allowing legitimate types of traffic flow through, redirecting the lesser severity types of attacks to a honeypot, and blocking the high severity source of an attack.

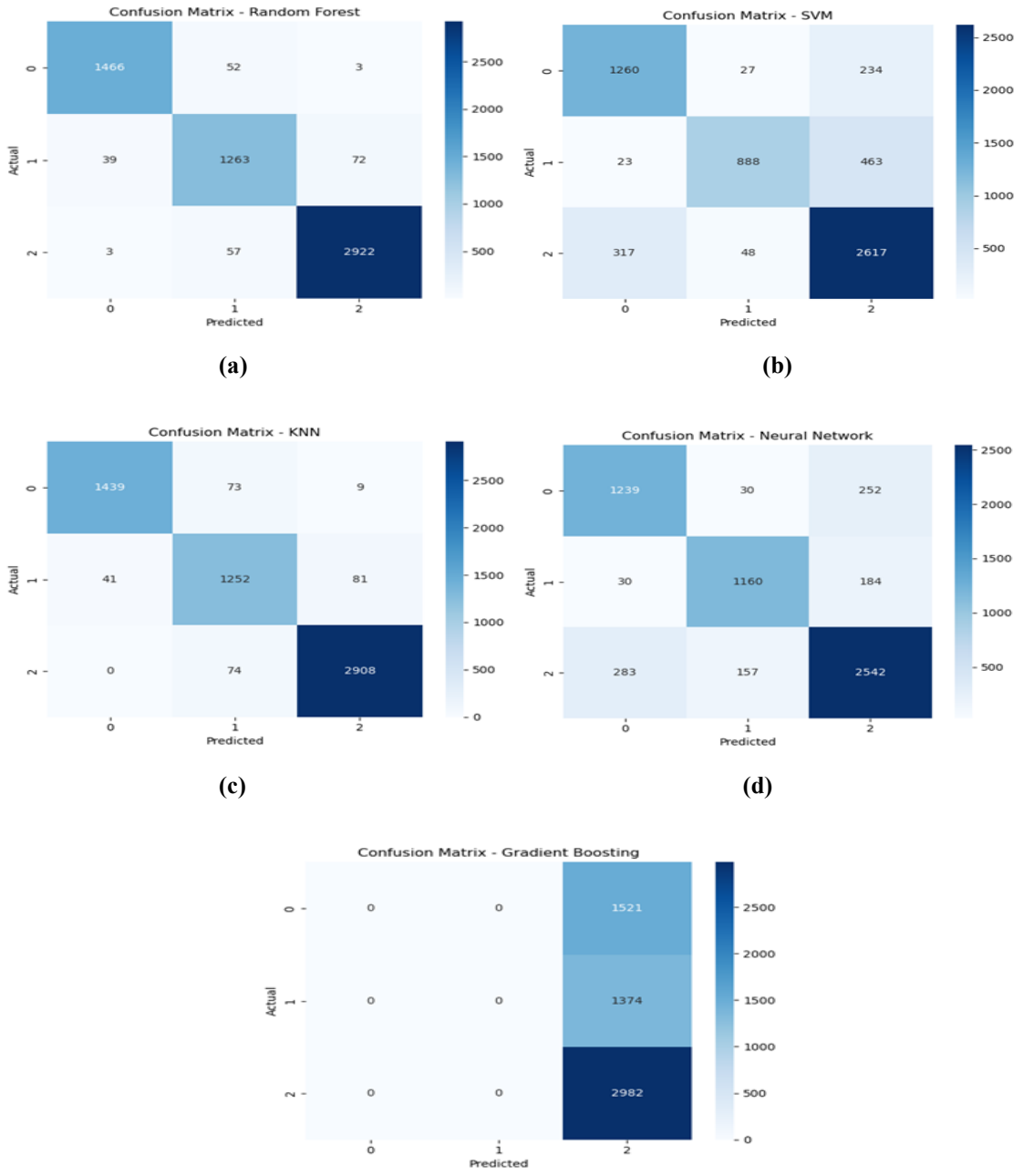


FIGURE 6.22 (a-e) Confusion Matrices of different ML Models for Live DrDoS_ICMP Traffic

FIGURE 6.22 (a-e) display five confusion matrices that represent the multi-class performance of Random Forest, SVM, KNN, Neural Network, and Gradient Boosting for normal (class 0), low severity (class 1), and high severity (class 2) DDoS traffic. The Random Forest and KNN, both appear to have a dominance of the diagonal, indicating high correct classification with very-well-minimal misclassification, especially at best, high severity attacks. Neural Network does well but shows a slightly more confusion between low and high severity classes. An SVM is distinguished by apparent confusion between the Normal and High-severity classes in traffic. However, Gradient Boosting seems to have the greatest number of false large severity classes.

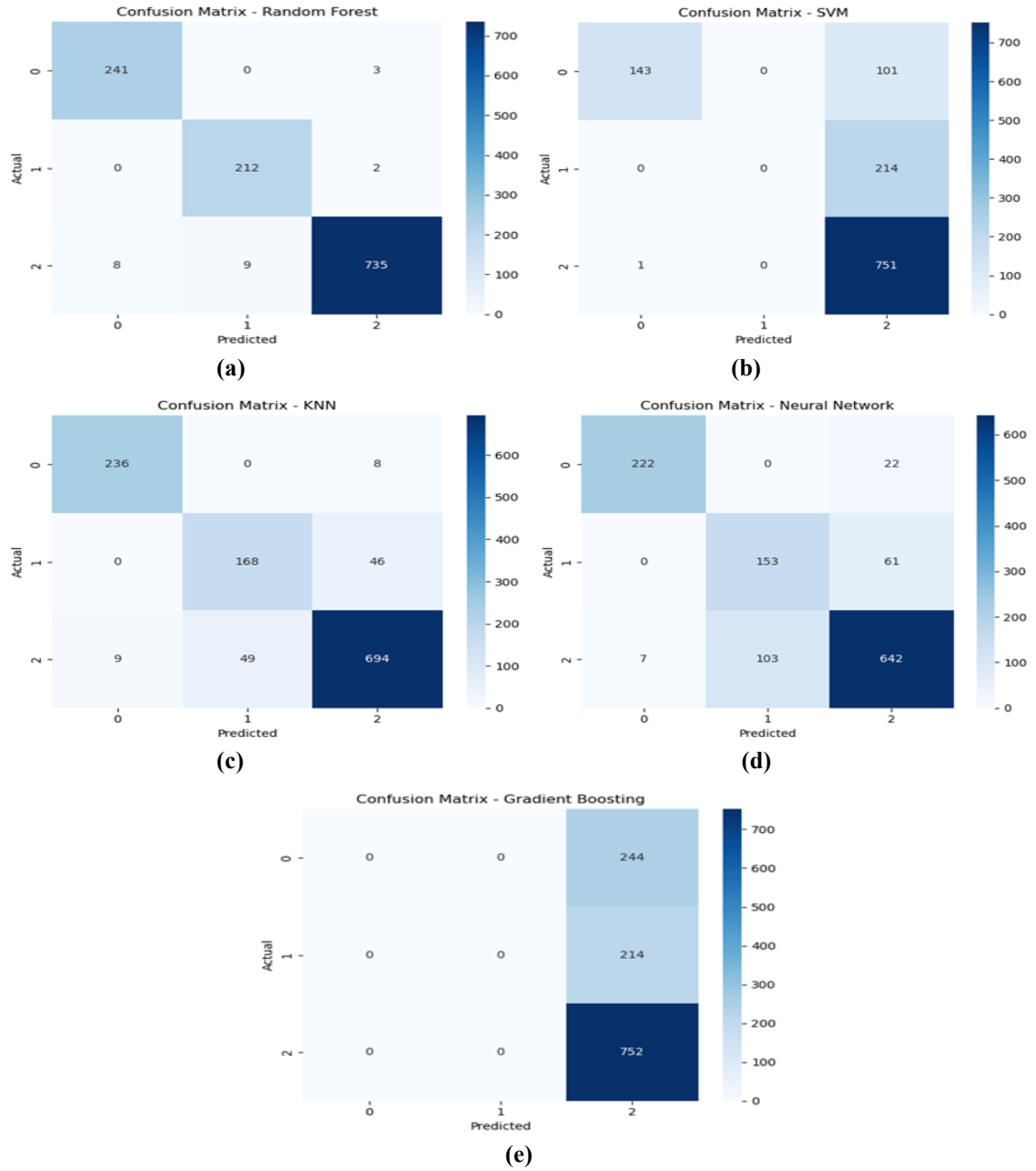
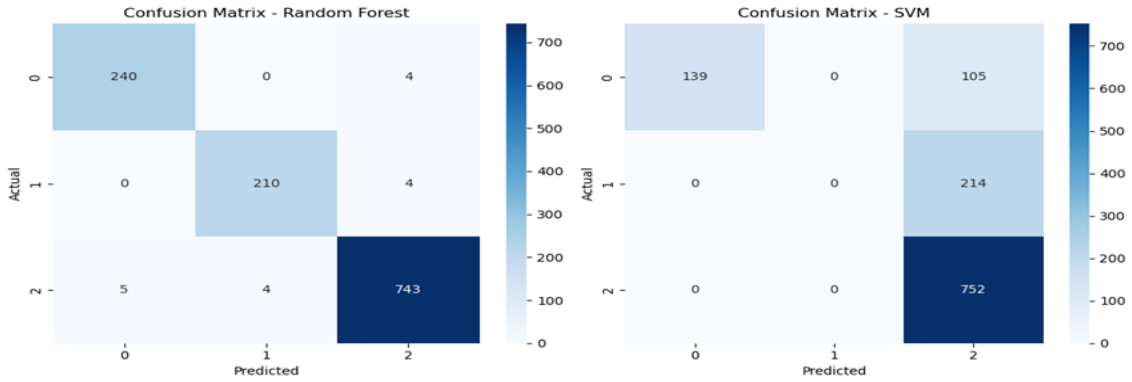


FIGURE 6.23 (a-e) Confusion Matrices of different ML Models for Live DrDoS_SYN Traffic

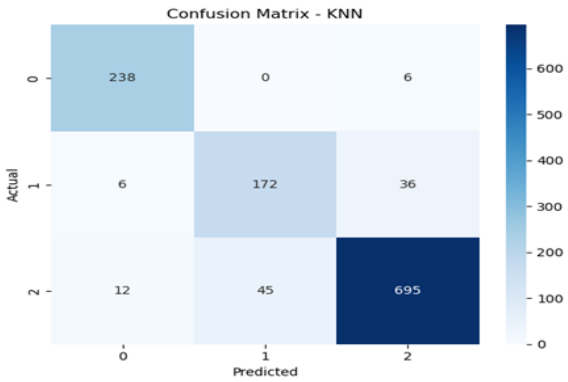
The live traffic confusion matrices shown in FIGURE 6.23 (a-e) reveal that Random Forest and KNN have a high degree of dominance along the diagonal line, displaying an accurate and balanced classification of Normal, Low-severity, and High-severity DDoS traffic along the x-axis. Whereas the neural network gives equivalent results, it did experience notably higher confusion between low and high severity. The SVM and Gradient Boosting results were skewed toward predicting high-severity DDoS attack traffic, which led to a poor separation of other classes. In general, Random Forest and KNN exhibit maximum liability for real-time DDoS detection based on severity levels.

FIGURE 6.24 (a-e) depicts five confusion matrices according to which for Random Forest and KNN strong diagonals have been shown, which means that Normal (0) and Low-severity (1) and High-severity (2) are almost correct classification with only very little cross-class confusion. The Neural Network is performing its job as it exhibits just a little bit higher confusion between low and high severity. But the SVM, on the other hand, is having a very hard time turning Normal traffic into High-severity by showing a simple lack of difference among the classes and Gradient Boosting is very much inclined to predict class-2 for most samples, leading to very low discrimination in the multi-class situation.

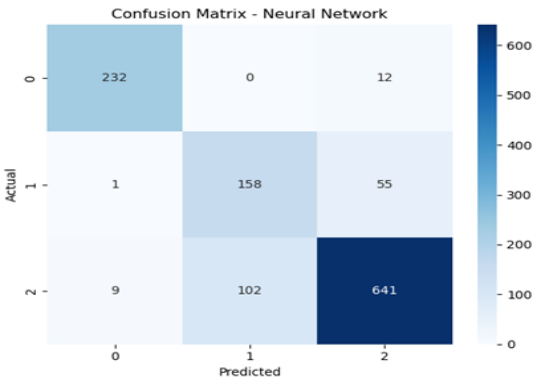


(a)

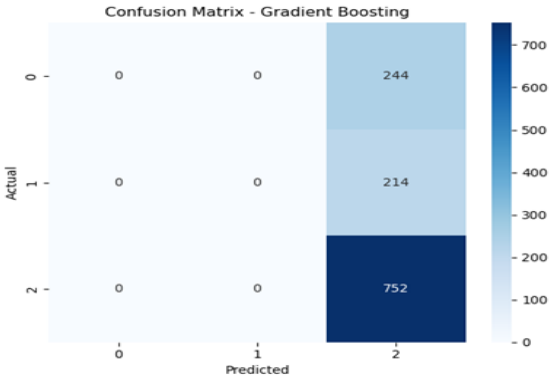
(b)



(c)



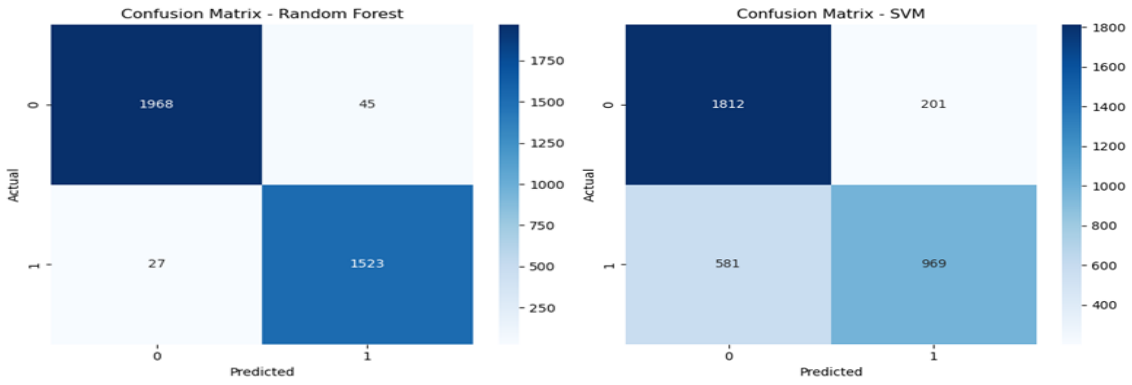
(d)



(e)

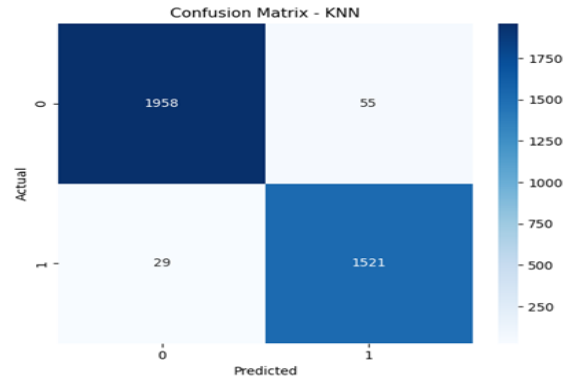
FIGURE 6.24 (a-e) Confusion Matrices of different ML Models for Live DrDoS_TCP Traffic

In FIGURE 6.25 (a-e) Both Random Forest and the nearest neighbors are the most reliable binary classification in true positives and true negatives and only have a few misclassifications supporting a high-performance capability in distinguishing normal and attack traffic in live conditions. NN is somewhere in the middle with significantly higher numbers of false positive and false negative as opposed to SVM, which shows separation between classes as weaker. Gradient Boosting, however, always leads to predicting the majority of Normal, most of the time failing to catch the attacks. Of all the techniques, Random Forest and KNN are still the best ones to detect DDoS attacks in live traffic.

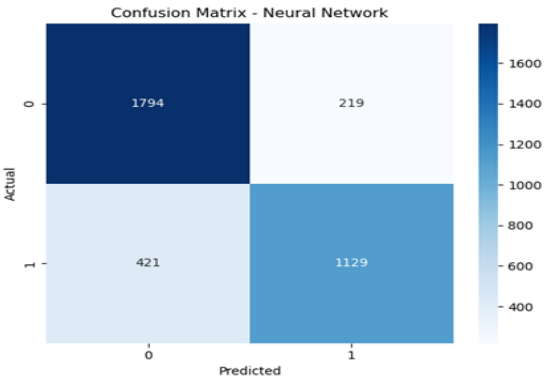


(a)

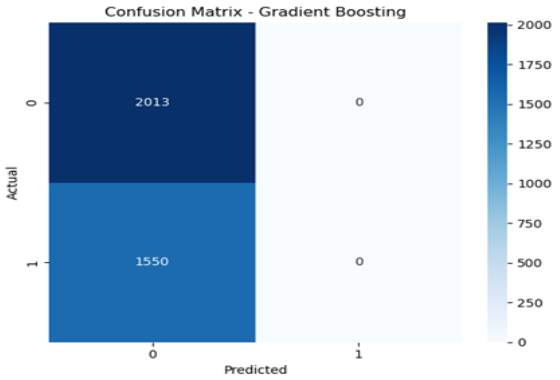
(b)



(c)



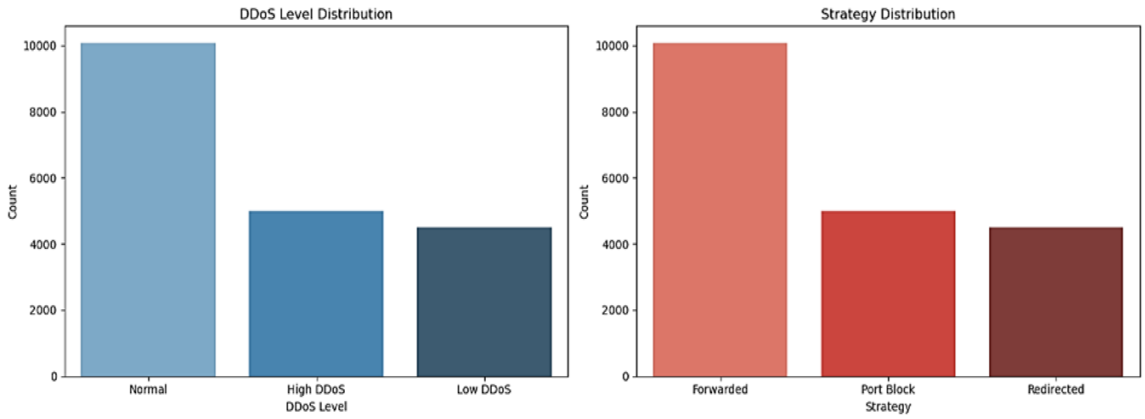
(d)



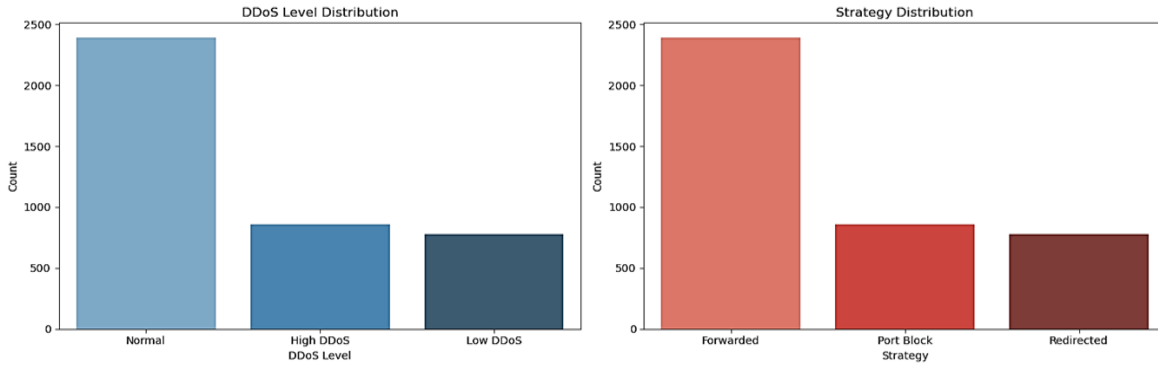
(e)

FIGURE 6.25 (a-e) Confusion Matrices of different ML Models for Live DDoS_UDP Traffic

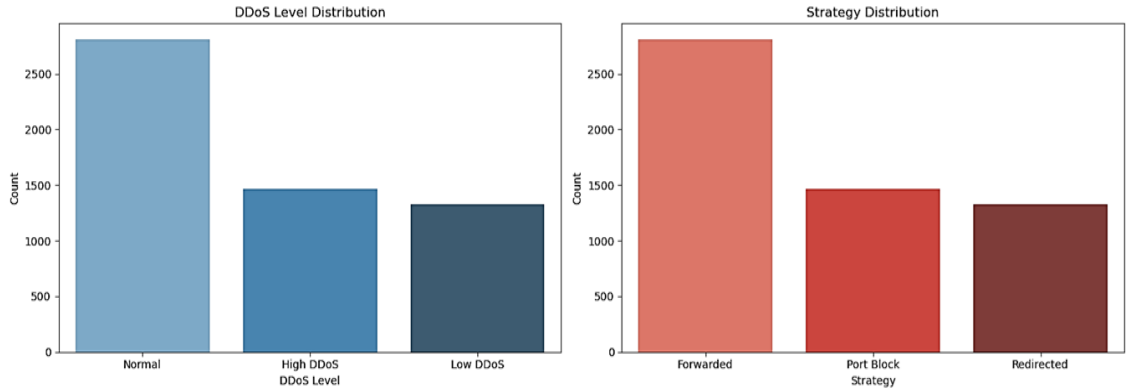
The outcomes derived from confusion matrices, whether in multi-class or binary scenarios, have consistently demonstrated that RF and KNN are the most well-balanced and reliable, they provide strong true positive and true negative rates and exhibit low rates of misclassification. Neural networks deliver usually competitive results but show moderate confusion between severity labels, whereas among all models, SVM generally excels at detecting overlapping features but mislabels more samples.



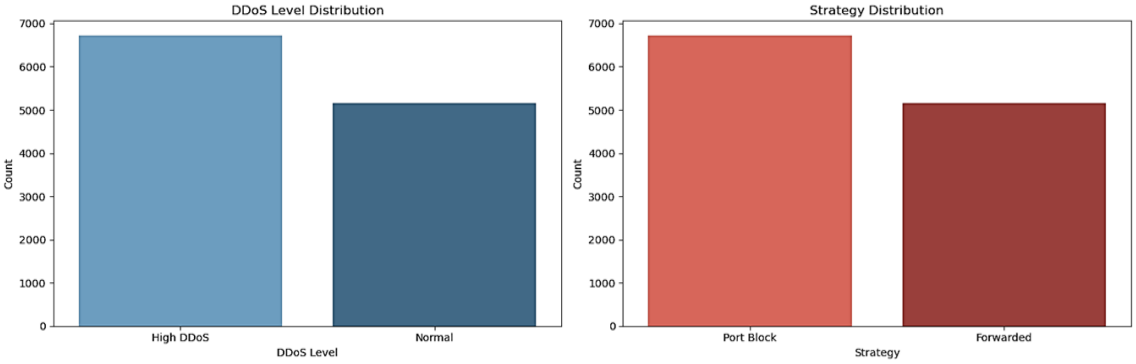
(a) DrDoS_ICMP



(b) DrDoS_SYN



(c) DrDoS_TCP



(d) DrDoS_UDP

FIGURE 6.26 (a-d) DrDoS level and Strategy Distribution of Live Traffic

Ensemble-based GBA often predict bias. it either clearly favors one class or struggles to separate severity levels. Nonetheless, common trends validate that ensemble RF and instance-based KNN remain the preferred choices for application-aware DDoS mitigation within the proposed SDN framework. The FIGURE 6.26 (a-d) depicts the detected degree of DrDoS-positive relationships and its systematic responses over varied traffic patterns through the mitigation actions selected automatically by the proposed scheme. In this case, the greatest proportion of traffic is represented by normal event flows. This is followed by high-severity and low-severity DrDoS traffic distributions monitored by the system. A clear separation of benign and malevolent traffic is achieved along with identification of the intensity of attack. It outlines normal traffic views are forwarded without any limitations, high severity usually gets restrictions to port-levels, and low severity are all redirected to honey pots. From the distribution of the strategies included in this setup, the system is tightly coupled to the severity classification output.

6.7 Discussion

A detailed attack-wise evaluation was conducted using the CICDDoS2019 dataset to assess the effectiveness of the proposed model across multiple DrDoS attack types, including DNS, LDAP, MSSQL, NetBIOS, SNMP, SSDP, UDP, UDP-Lag, SYN, TFTP, and NTP. The proposed sequential feature selection method significantly reduced the feature space from 84 to approximately 54–57 features, achieving nearly 71% dimensionality reduction while preserving discriminative capability. This reduction contributed to faster processing and improved model stability without compromising detection performance.

In terms of classification, the Random Forest model consistently outperformed other machine learning models across all attack categories. For high-volume reflection-based attacks such as DNS, LDAP, and SSDP, the model achieved accuracy, precision, recall, and F1-scores exceeding 97.5%, with detection latency remaining below 1 second per flow. Similarly, NTP attacks exhibited slightly higher detection performance (approximately 98%) due to their distinctive traffic characteristics and entropy variations.

For UDP and UDP-Lag attacks, the model achieved accuracy in the range of 96.8%–97.5%, with minor variations due to their highly distributed behaviour. SYN and MSSQL attacks also demonstrated strong performance, maintaining F1-scores above 97%, although SYN traffic incurred slightly higher processing time due to semi-random spoofing patterns. NetBIOS and SNMP attacks showed comparatively lower performance (approximately 96.5%–97%) due to partial overlap between normal and attack traffic distributions.

The proposed Joint Entropy-based feature selection enhanced feature relevance, with top-ranked features achieving importance scores close to 0.99, ensuring minimal redundancy. In the live SDN testbed, the system achieved over 85% reduction in network downtime during attacks. The Information Gain-based multi-level mitigation strategy effectively classified traffic into normal, low, and high severity levels, enabling adaptive responses such as honeypot redirection for low-severity attacks and temporary port blocking (e.g., 60 seconds) for high-severity attacks, followed by automatic recovery to maintain service continuity

CHAPTER 7

CONCLUSION & FUTURE WORK

7.1 Conclusion

This research presents an advanced and comprehensive multi-level Distributed Denial of Service (DDoS) detection and mitigation framework for Software Defined Networks (SDN), integrating sequential feature optimization, machine learning-based severity classification, and automated mitigation mechanisms. The proposed approach was extensively evaluated using the CICDDoS2019 dataset, which represents diverse and realistic DDoS attack scenarios. The primary objective was to significantly reduce feature dimensionality while preserving discriminative capability. To achieve this, a novel Sequential Feature Selection strategy combining Mutual Information (MI) and Joint Entropy was introduced. Experimental results demonstrate that approximately 71% of the original features can be eliminated without degrading detection performance, thereby improving computational efficiency and model stability.

Multiple machine learning models, including Random Forest, Neural Networks, Gradient Boosting Algorithm, K-Nearest Neighbors, and Support Vector Machine, were trained and tested on the optimized CICDDoS2019 dataset. Among these, the Random Forest model consistently outperformed others, achieving approximately 97.8% accuracy and nearly 98% recall across various DDoS attack types. The results confirm that feature optimization significantly enhances the performance, robustness, and scalability of learning models, making them suitable for real-time SDN based environments. Furthermore, the proposed framework was validated in a live SDN testbed implemented using Mininet and the Ryu controller, demonstrating its practical applicability beyond dataset-based evaluation. The system successfully enforced mitigation actions through OpenFlow rules, where high-severity attacks triggered immediate port blocking, while low-severity attacks were redirected to a honeypot for further analysis. This adaptive mitigation strategy ensured minimal disruption to legitimate traffic and maintained network service continuity. The

system achieved over 85% reduction in network downtime during attack scenarios, highlighting its effectiveness in real-world conditions.

In addition, performance analysis indicated that Random Forest and Gradient Boosting models provided low inference time, supporting real-time detection requirements. Overall, the integration of entropy-driven feature selection, multi-level machine learning-based classification using the CICDDoS2019 benchmark dataset, and SDN-native automated mitigation forms a robust and efficient defense mechanism against DDoS attacks.

7.2 Key Findings

- Sequential feature selection using Mutual Information and Joint Entropy reduced feature dimensionality by approximately 71% while maintaining high detection accuracy.
- Random Forest achieved the best overall performance among evaluated models, with high accuracy, recall, and robustness across attack types.
- Multi-level classification successfully differentiated Normal, Low-severity, and High-severity DDoS traffic.
- Severity-aware mitigation avoided unnecessary blocking by redirecting low-severity traffic to honeypot and aggressively blocking high-severity attacks.
- Live testbed experiments verified that legitimate traffic remains accessible during low-severity attacks and is restored after mitigation timeout.
- All models demonstrated real-time feasibility with sub-second detection latency.

7.3 Contributions Revisited

This thesis makes the following major contributions:

1. Proposed an Information Gain-driven multi-level DDoS detection framework for SDN, capable of classifying traffic into normal, low-severity, and high-severity attacks, enabling adaptive and proportional response mechanisms.

2. Developed a sequential feature reduction technique combining Mutual Information and Joint Entropy, achieving approximately 71% dimensionality reduction (from 84 to ~54–57 features) while maintaining high detection accuracy and improving computational efficiency.

3. Designed and implemented a severity-aware SDN mitigation mechanism, integrating honeypot redirection for low-severity attacks and OpenFlow-based dynamic port blocking for high-severity attacks, ensuring real-time and automated network defense.

4. Performed extensive experimental validation using the CICDDoS2019 dataset and a real-time SDN testbed (Mininet with Ryu controller), demonstrating practical applicability and robustness under realistic network conditions.

5. Conducted a comprehensive comparative analysis of machine learning models, where the Random Forest classifier achieved superior performance (~97.8% accuracy, ~98% recall, and low detection latency), validating its suitability for real-time SDN-based DDoS detection.

6. Demonstrated real-time effectiveness of the proposed framework, achieving over 85% reduction in network downtime and maintaining service continuity through adaptive mitigation and automatic recovery mechanisms.

7.4 Future Research Directions

This research can be further expanded by numerous research opportunities. Extensive research might analyse deep-learning systems including CNN and RNN architectures and combined models to capture spatiotemporal patterns of traffic in innovative ways. Validation involves identifying spatial and high-dimensional traffic patterns using multi-protocol real SDN traffic and IoT-generated DDoS scenarios. It may also encompass distributed or multi-controller SDN architectures to enhance scalability and redundancy. Future research will focus on reinforcement learning for adaptive threshold selection and dynamic OpenFlow rule management, allowing mitigation strategies to adjust to evolving attack behaviours. Hence, further studies should validate on diverse datasets, larger networks, and live environments to improve applicability for large-scale SDN deployments.

References

1. Zhang H, Cai Z, Liu Q, et al (2018) A Survey on Security-Aware Measurement in SDN. Security and Communication Networks 2018:. https://doi.org/10.1155/2018/2459154
2. Alnaim AK (2024) Securing 5G virtual networks: a critical analysis of SDN, NFV, and network slicing security. Int J Inf Secur 23:3569–3589. https://doi.org/10.1007/s10207-024-00900-5
3. Dayal N, Maity P, Srivastava S, Khondoker R (2016) Research Trends in Security and DDoS in SDN. Security and Communication Networks 9:6386–6411. https://doi.org/10.1002/sec.1759
4. Shah AFMS, Karabulut MA, Kamruzzaman A, et al (2025) A Survey on Artificial Intelligence and Blockchain Clustering for Enhanced Security in 6G Wireless Networks. Computers, Materials and Continua 84:1981–2013. https://doi.org/10.32604/cmc.2025.064028
5. Mirkovic J, Reiher P, Hall B (2004) A Taxonomy of DDoS Attack and DDoS Defense Mechanisms. In: ACM SIGCOMM Computer Communications Review. pp 39–53. https://doi.org/10.1145/997150.997156
6. Chaudhary S, Mishra PK (2023) DDoS attacks in Industrial IoT: A survey. Computer Networks 236:. https://doi.org/10.1016/j.comnet.2023.110015
7. Singh MP, Bhandari A (2020) New-flow based DDoS attacks in SDN: Taxonomy, rationales, and research challenges. Comput Commun 154:509–527.https://doi.org/10.1016/j.comcom.2020.02.085
8. Li Q, Huang H, Li R, et al (2023) A comprehensive survey on DDoS defense systems: New trends and challenges. Computer Networks 233:. https://doi.org/10.1016/j.comnet.2023.109895
9. Swami R, Dave M, Ranga V (2021) Detection and Analysis of TCP-SYN DDoS Attack in Software-Defined Networking. Wirel Pers Commun 118:2295–2317. https://doi.org/10.1007/s11277-021-08127-6
10. Huang Y-F, Chang S-W, Lin C-B, et al (2023) An Improved Light Weight Countermeasure Scheme to Efficiently Mitigate TCP Attacks in SDN. In: Communications in Computer and Information Science. Springer, Singapore, pp 501–511.https://doi.org/10.1007/978-981-19-9582-8_44

11. Cil AE, Yildiz K, Buldu A (2021) Detection of DDoS attacks with feed forward based deep neural network model. Expert Syst Appl 169:. https://doi.org/10.1016/j.eswa.2020.114520
12. MacFarland DC, Shue CA, Kalafut AJ (2017) The best bang for the byte: Characterizing the potential of DNS amplification attacks. Computer Networks 116:12–21.https://doi.org/10.1016/j.comnet.2017.02.007
13. Zheng J, Li Q, Gu G, et al (2018) Realtime DDoS Defense Using COTS SDN Switches via Adaptive Correlation Analysis. IEEE Transactions on Information Forensics and Security 13:1838–1853. https://doi.org/10.1109/TIFS.2018.2805600
14. Sinha M (2025) A comprehensive survey of DDoS attack defense systems for different SDN architectures. Computer Networks 272:. https://doi.org/10.1016/j.comnet.2025.111711
15. Kurniawan MT, Yazid S (2019) A systematic literature review of security software defined network: Research trends, threat, attack, detect, mitigate, and countermeasure. In: ACM International Conference Proceeding Series. Association for Computing Machinery, pp 39–45. https://doi.org/10.1145/3369555.3369567
16. Nisharani Meti, D G Narayan, V. P. Baligar (2017) Detection of Distributed Denial of Service Attacks using Machine Learning Algorithms in Software Defined Networks. In: 2017 International Conference on Advances in Computing, Communications and Informatics (ICACCI). https://doi.org/10.1109/ICACCI.2017.8126031
17. Foschini L, Mignardi V, Montanari R, Scotece D (2021) An SDN-Enabled architecture for IT/OT converged networks: A Proposal and Qualitative Analysis under DDoS Attacks. Future Internet 13:. https://doi.org/10.3390/fi13100258
18. Deb R, Roy S (2019) DDOS Attack on Software-Defined Networks and Its Mitigation Techniques. In: Communications in Computer and Information Science. Springer Verlag, pp 280–292. https://doi.org/10.1007/978-981-13-8578-0_22
19. Vizváry M, Vykopal J (2014) Future of DDoS Attacks Mitigation in Software Defined Networks. In: International Conference on Autonomous Infrastructure, Management and Security. AIMS 2014, pp 123–127.https://doi.org/10.1007/978-3-662-43862-6_15

20. Chauhan P, Atulkar M (2023) An efficient centralized DDoS attack detection approach for Software Defined Internet of Things. Journal of Supercomputing 79:10386–10422. https://doi.org/10.1007/s11227-023-05072-y
21. Ram A, Dutta MP, Chakraborty SK (2024) A Flow-Based Performance Evaluation on RYU SDN Controller. Journal of The Institution of Engineers (India): Series B 105:203–215. https://doi.org/10.1007/s40031-023-00982-0
22. David J, Thomas C (2019) Efficient DDoS flood attack detection using dynamic thresholding on flow-based network traffic. Comput Secur 82:284–295. https://doi.org/10.1016/j.cose.2019.01.002
23. 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
24. Rodriguez-Gomez RA, Macia-Fernandez G, Garcia-Teodoro P (2014) Survey and taxonomy of botnet research through life cycle. ACM Comput Surv 45:. https://doi.org/10.1145/2501654.2501659
25. Valdovinos IA, Pérez-Díaz JA, Choo KKR, Botero JF (2021) Emerging DDoS attack detection and mitigation strategies in software-defined networks: Taxonomy, challenges and future directions. Journal of Network and Computer Applications 187:. https://doi.org/10.1016/j.jnca.2021.103093
26. Kaur S, Kumar K, Aggarwal N, Singh G (2021) A comprehensive survey of DDoS defense solutions in SDN: Taxonomy, research challenges, and future directions. Comput. Secur. 110. https://doi.org/10.1016/j.cose.2021.102423
27. Rathore S, Bhandari A, Maini R (2026) A multi-dimensional study of IoT DDoS in smart environments: SDN integration, taxonomy, security gaps, and emerging defenses. Comput Sci Rev 60:100903. https://doi.org/10.1016/j.cosrev.2026.100903
28. Walfish M, Vutukuru M, Balakrishnan H, et al (2010) DDoS defense by offense. ACM Transactions on Computer Systems 28:. https://doi.org/10.1145/1731060.1731063
29. Bouyeddou B, Kadri B, Harrou F, Sun Y (2020) DDOS-attacks detection using an efficient measurement-based statistical mechanism. Engineering Science and Technology, an International Journal 23:870–878. https://doi.org/10.1016/j.jestch.2020.05.002

30. Basicevic I, Ocovaj S (2019) Application of entropy formulas in detection of denial-of-service attacks. International Journal of Communication Systems 32:.https://doi.org/10.1002/dac.4067
31. Basicevic I, Blazic N, Ocovaj S (2021) On the use of generalized entropy formulas in detection of denial-of-service attacks. Security and Privacy 4:. https://doi.org/10.1002/spy2.134
32. Tsobdjou LD, Pierre S, Quintero A (2022) An Online Entropy-Based DDoS Flooding Attack Detection System with Dynamic Threshold. IEEE Transactions on Network and Service Management 19:1679–1689.https://doi.org/10.1109/TNSM.2022.3142254
33. 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
34. AbdelAzim NM, Fahmy SF, Sobh MA, Bahaa Eldin AM (2021) A hybrid entropy-based DoS attacks detection system for software defined networks (SDN): A proposed trust mechanism. Egyptian Informatics Journal 22:85–90. https://doi.org/10.1016/j.eij.2020.04.005
35. Sinha M, Mukherjee JC, Bera P, Satpathy M (2025) SynFloWatch: An Entropy-Based Live Defense System against SYN Spoofing DDoS Attacks in Hybrid SDN. Journal of Network and Systems Management 33:.https://doi.org/10.1007/s10922-025-09934-z
36. 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
37. 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
38. 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

39. 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. https://doi.org/10.1007/978-981-15-0324-5_30
40. 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. https://doi.org/10.1016/j.procs.2015.04.007
41. Leu Y, Lin I-L (2010) A DoS/DDoS Attack Detection System Using Chi-Square Statistic Approach. In: J. Syst. Cybern. Inform 8. pp 41–51. https://doi.org/10.1109/IAS.2009.292
42. Loukas G (2007) Likelihood Ratios and Recurrent Random Neural Networks in Detection of Denial-of-Service Attacks. In: International Symposium on Performance Evaluation of Computer and Telecommunication Systems. SPECTS 2007, San Diego, CA, USA.
43. Oshima S, Nakashima T, Sueyoshi T (2010) Early DoS/DDoS detection method using short-term statistics. In: CISIS 2010 - The 4th International Conference on Complex, Intelligent and Software Intensive Systems. pp 168–173. https://doi.org/10.1109/CISIS.2010.53
44. Nosrati E, kashi AS, Yashar D (2011) Register Flooding Attacks Detection in IP Multimedia Subsystems by Using Adaptive z-score CUSUM Algorithm. In: Proceedings of the 5th international Conference on Information Technology and Multimedia. IEEE, Malaysia, https://doi.org/10.1109/ICIMU.2011.6122765
45. Shalini P V., Radha V, Sanjeevi SG (2022) DOCUS-DDoS detection in SDN using modified CUSUM with flash traffic discrimination and mitigation. Computer Networks 217:. https://doi.org/10.1016/j.comnet.2022.109361
46. Melo LH, De Carvalho Bertoli G, Saotome O, et al (2022) Combination of Models for Denial-Of-Service Classification over Different Networks. In: ACM International Conference Proceeding Series. Association for Computing Machinery, pp 137–142. https://doi.org/10.1145/3569902.3570176
47. Prakongsin S, Kanjanasurat I (2025) A Comparison of Machine Learning Models Based on Feature Variations for Phishing URL Detection. In: Association for Computing Machinery (ACM). Association for Computing Machinery (ACM), pp 51–57. https://doi.org/10.1145/3760622.3760637
48. Xu Z, Ramanathan S, Rush A, et al (2022) Xatu: Boosting Existing DDoS Detection Systems Using Auxiliary Signals. In: CoNEXT 2022 - Proceedings of

the 18th International Conference on emerging Networking EXperiments and Technologies. Association for Computing Machinery, Inc, pp 1–17. https://doi.org/10.1145/3555050.3569121

49. Al-Eryani AM, Omara FA, Hossny E (2025) A Deep Learning GRU-BiLSTM for DDoS Attack Detection. SN Comput Sci 6:. https://doi.org/10.1007/s42979-025-04110-1
50. Jayakrishna N, Prasanth NN (2025) A hybrid deep learning model for detection and mitigation of DDoS attacks in VANETs. Sci Rep 15:. https://doi.org/10.1038/s41598-025-15215-1
51. Najar AA, Naik SM, Lone FR, Nazir A (2025) A novel CNN-enhanced detection and mitigation of DDoS attacks in SDN. Cluster Comput 28:. https://doi.org/10.1007/s10586-024-05003-3
52. 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
53. 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
54. 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. https://doi.org/10.1016/j.procs.2025.01.008
55. Hossain MA, Islam MS (2024) Enhancing DDoS attack detection with hybrid feature selection and ensemble-based classifier: A promising solution for robust cybersecurity. Measurement: Sensors 32:. https://doi.org/10.1016/j.measen.2024.101037
56. Coscia A, Dentamaro V, Galantucci S, et al (2024) Automatic decision tree-based NIDPS ruleset generation for DoS/DDoS attacks. Journal of Information Security and Applications 82:. https://doi.org/10.1016/j.jisa.2024.103736
57. Chen L, Zhang Y, Zhao Q, et al (2018) Detection of DNS DDoS Attacks with Random Forest Algorithm on Spark. In: Procedia Computer Science. Elsevier B.V., pp 310–315. https://doi.org/10.1016/j.procs.2018.07.177

58. Hill W, Mason J, Aldrich B, et al (2025) Enhancing DDoS Detection in Software-Defined Networking: A Machine Learning and Deep Learning Approach. In: icABCD 2025 - Proceedings of the 2025 International Conference on Ai, Big Data, Computing and Data Communication Systems. Association for Computing Machinery, Inc. https://doi.org/10.1145/3759023.3759101
59. Hekmati A, Zhang J, Sarkar T, et al (2024) Correlation-Aware Neural Networks for DDoS Attack Detection in IoT Systems. IEEE/ACM Transactions on Networking 32:3929–3944. https://doi.org/10.1109/TNET.2024.3408675
60. 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
61. Madathi M, Gowthami N (2022) Detection of DDoS attack in SDN environment using KNN algorithm. International Journal of Research and Analytical Reviews 9: http://ijrar.org/viewfull.php?&p_id=IJRAR1COP044
62. Rajakumaran G, Venkataraman N, Mukkamala RR (2020) Denial of Service Attack Prediction Using Gradient Descent Algorithm. SN Comput Sci 1:. https://doi.org/10.1007/s42979-019-0043-7
63. Shen G, Zhang Y, Zhong G, Gong Z (2026) DDoS attack detection using deep transfer learning and FFT-based data transformation. Journal of Supercomputing 82:. https://doi.org/10.1007/s11227-026-08253-7
64. Kalafy SAA, Pashazadeh S, Salehpour P (2025) Dynamic graph neural network-based framework to increase detection accuracy in SDN under DDOS. Sci Rep 16:. https://doi.org/10.1038/s41598-025-32102-x
65. Sumadi FDS, Alsubhi K (2026) DDoS attack detection using semi-supervised hyperparameter optimized federated learning in software defined internet of drones. International Journal of Machine Learning and Cybernetics 17:. https://doi.org/10.1007/s13042-026-03108-2
66. Sbai O, Allaert B, Sondi P, Meddahi A (2026) SIP-DDoS framework based on federated learning for collaborative anomaly detection. Cybersecurity 9:. https://doi.org/10.1186/s42400-025-00527-6
67. Komarchesqui M, Silva Ruffo VG da, Carvalho LF, Proença ML (2026) eXplainable Artificial Intelligence for Transparent Optimization of Deep Learning-Based Intrusion Detection Systems. Journal of Network and Systems Management 34:. https://doi.org/10.1007/s10922-026-10084-z

68. S. Niktabe, D. P. Sharma, and A. H. Lashkari, (2026) Unveiling intruders' behaviours: Explainable AI-based profiling of malicious bot activities in IoT networks, The Journal of Supercomputing, vol. 82, no. 5, p. 352, Apr. 2026, https://doi: 10.1007/s11227-026-08494-6.
69. Lee C, Lee GG (2006) Information gain and divergence-based feature selection for machine learning-based text categorization. Inf Process Manag 42:155–165. https://doi.org/10.1016/j.ipm.2004.08.006
70. Ramasamy M, Meena Kowshalya A (2022) Information Gain Based Feature Selection for Improved Textual Sentiment Analysis. Wirel Pers Commun 125:1203–1219. https://doi.org/10.1007/s11277-022-09597-y
71. Lei S (2012) A feature selection method based on information gain and genetic algorithm. In: Proceedings - 2012 International Conference on Computer Science and Electronics Engineering, ICCSEE 2012. pp 355–358. https://doi.org/10.1109/ICCSEE.2012.97
72. Huang L, Zhou X, Shi L, Gong L (2024) Time Series Feature Selection Method Based on Mutual Information. Applied Sciences (Switzerland) 14:. https://doi.org/10.3390/app14051960
73. Liu S, Motani M (2022) Improving Mutual Information based Feature Selection by Boosting Unique Relevance, arXiv:2212.06143v2 https://doi.org/10.48550/arXiv.2212.06143
74. Khan S, Gani A, Wahab AWA, Singh PK (2018) Feature Selection of Denial-of-Service Attacks Using Entropy and Granular Computing. Arab J Sci Eng 43:499–508. https://doi.org/10.1007/s13369-017-2634-8
75. Hamidreza Lotfalizadeh, Dongso S. Kim (2020) Investigating Real-Time Entropy Features of DDoS Attack Based on Categorized Partial-Flows. In: 14th International Conference on Ubiquitous Information Management and Communication (IMCOM): 03-05 January 2020, Taichung, Taiwan. https://doi.org/10.1109/IMCOM48794.2020.9001690
76. Kachavimath A V., Narayan DG (2025) An Efficient DDoS Attack Detection in SDN using Multi-Feature Selection and Ensemble Learning. In: Procedia Computer Science. Elsevier B.V., pp 241–250. https://doi.org/10.1016/j.procs.2024.12.026

77. Razzaque A, Badholia DA (2024) PCA based feature extraction and MPSO based feature selection for gene expression microarray medical data classification. Measurement: Sensors 31:. https://doi.org/10.1016/j.measen.2023.100945
78. Basicevic I, Blazic N, Ocovaj S (2022) On the use of principal component analysis in the entropy-based detection of denial-of-service attacks. SECURITY AND PRIVACY 5:. https://doi.org/10.1002/spy2.193
79. Wang M, Zhou H, Chen J (2018) A moving window principal components analysis-based anomaly detection and mitigation approach in SDN network. KSII Transactions on Internet and Information Systems 12:3946–3965. https://doi.org/10.3837/tiis.2018.08.022
80. Kumavat KS, Gomes J (2025) Multi-layer DDoS attacks detection with mitigation in IoT-enabled sensor network. Cybersecurity 8:. https://doi.org/10.1186/s42400-025-00378-1
81. Pradeesh S, Jeyakarthic M, Thirumalairaj A (2025) Enhanced Hybrid Approach for Multi-Class DDoS Attack Detection and Classification in Software-Defined Networks Using Remote Sensing and Data Analytics. Remote Sens Earth Syst Sci 8:530–544. https://doi.org/10.1007/s41976-025-00204-9
82. Zhou L, Liao M, Yuan C, Zhang H (2017) Low-Rate DDoS Attack Detection Using Expectation of Packet Size. Security and Communication Networks 2017:. https://doi.org/10.1155/2017/3691629
83. Bhuyan MH, Bhattacharyya DK, Kalita JK (2015) An empirical evaluation of information metrics for low-rate and high-rate DDoS attack detection. Pattern Recognit Lett 51:1–7. https://doi.org/10.1016/j.patrec.2014.07.019
84. Na S, Chen L, Lin M (2026) Detecting low-rate DDoS attacks using Rényi entropy and trans-KAN hybrid model in SDN. Digital Signal Processing: A Review Journal 172:. https://doi.org/10.1016/j.dsp.2025.105859
85. Abu Al-Haija Q, Droos A (2025) Resilient intrusion detection system for adversarial attacks on Low-Rate DDoS. International Journal of Machine Learning and Cybernetics 16:8473–8502. https://doi.org/10.1007/s13042-025-02734-6
86. Feraudo A, Popescu DA, Yadav P, et al (2024) Mitigating IoT Botnet DDoS Attacks through MUD and eBPF based Traffic Filtering. In: ACM International Conference Proceeding Series. Association for Computing Machinery, pp 164–173. https://doi.org/10.1145/3631461.3631549

87. El Kamel A, Eltaief H, Youssef H (2022) On-the-fly (D)DoS attack mitigation in SDN using Deep Neural Network-based rate limiting. Comput Commun 182:153–169. https://doi.org/10.1016/j.comcom.2021.11.003
88. Rouf MA, Silvia AR, Roy MK, et al (2025) Proposing a framework to prevent Distributed Denial of Service (DDoS) attacks on IoT Devices. In: ICCA 2024 - 3rd International Conference on Computing Advancements, 2024. Association for Computing Machinery, Inc, pp 1066–1073. https://doi.org/10.1145/3723178.3723319
89. Mölsä JVE (2004) EFFECTIVENESS OF RATE-LIMITING IN MITIGATING FLOODING DOS ATTACKS. In: International Conference on Communications, Internet, and Information Technology. IASTED, St. Thomas, US Virgin Islands
90. Wang H, Xu L, Gu G (2015) FloodGuard: A DoS Attack Prevention Extension in Software-Defined Networks. In: 45th Annual IEEE/IFIP International Conference on Dependable Systems and Networks. IEEE, Rio de Janeiro, Brazil. https://doi.org/10.1109/DSN.2015.27
91. Srivastava S, Pokharna R, Shafiq S, Kanavalli A (2018) Mitigation of DDoS attack instigated by compromised switches on SDN controller by analyzing the flow rule request traffic. International Journal of Engineering & Technology 7:46–49. https://doi.org/10.14419/ijet.v7i2.6.10065
92. 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. https://doi.org/10.1109/CloudNet.2016.9
93. Shin S, Yegneswaran V, Porras P, Gu G (2013) AVANT-GUARD: Scalable and vigilant switch flow management in software-defined networks. In: Proceedings of the ACM Conference on Computer and Communications Security. pp 413–424. https://doi.org/10.1145/2508859.2516684
94. Duy PT, An LD, Pham VH (2019) Mitigating flow table overloading attack with controller-based flow filtering strategy in SDN. In: ACM International Conference Proceeding Series. Association for Computing Machinery, pp 154–158. https://doi.org/10.1145/3371676.3371706
95. Rabah MAO, Drid H, Medjadba Y, Rahouti M (2024) Detection and Mitigation of Distributed Denial of Service Attacks Using Ensemble Learning and

Honeypots in a Novel SDN-UAV Network Architecture. IEEE Access 12:128929–128940. https://doi.org/10.1109/ACCESS.2024.3443142.

96. Han W, Zhao Z, Doupé A, Ahn GJ (2016) HoneyMix: Toward SDN-based intelligent honeynet. In: SDN-NFV Security 2016 - Proceedings of the 2016 ACM International Workshop on Security in Software Defined Networks and Network Function Virtualization, co-located with CODASPY 2016. Association for Computing Machinery, Inc, pp 1–6. https://doi.org/10.1145/2876019.2876022
97. Dwi Setiawan Sumadi F, Rakhmat Widagdo A, Faishal Reza A (2022) SD-Honeypot Integration for Mitigating DDoS Attack Using Machine Learning Approaches. INTERNATIONAL JOURNAL ON INFORMATICS VISUALIZATION 6:39–44. https://doi.org/10.30630/joiv.6.1.853
98. Du M, Wang K (2020) An SDN-Enabled pseudo-honeypot strategy for distributed denial of service attacks in industrial internet of things. IEEE Trans Industr Inform 16:648–657. https://doi.org/10.1109/TII.2019.2917912
99. Kumar P, Tripathi M, Nehra A, et al (2018) SAFETY: Early Detection and Mitigation of TCP SYN Flood Utilizing Entropy in SDN. IEEE Transactions on Network and Service Management 15:1545–1559. https://doi.org/10.1109/TNSM.2018.2861741
100. Ishtiaq HU, Bhutta AA, Mian AN (2024) DHCP DoS and starvation attacks on SDN controllers and their mitigation. Journal of Computer Virology and Hacking Techniques 20:15–25. https://doi.org/10.1007/s11416-023-00483-0
101. Iman Sharafaldin AHL (2019) Developing Realistic Distributed Denial of Service (DDoS) Attack Dataset and Taxonomy. In: International Carnahan Conference on Security Technology (ICCST). https://doi.org/10.1109/CCST.2019.8888419
102. 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
103. Moustafa N, Slay J UNSW-NB15: A Comprehensive Data set for Network Intrusion Detection systems. https://doi.org/10.1109/MilCIS.2015.7348942
104. Shirsath V (2023) CAIDA UCSD DDoS 2007 Attack Dataset. https://dx.doi.org/10.21227/dvp9-s124

Publications

✓ Published Papers.

1. Shroff J M., & Shah S M. (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 (Scopus & WoS Indexed)
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 (Scopus Indexed).

✓ Paper Under Review.

3. Shroff, J. M., & Shah, S. M. Impact of Feature Selection on the Performance of Machine Learning Models for DDoS Detection.
   Submitted to IAES International Journal of Artificial Intelligence, (under review).

✓ Patent Filed.

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