

**DISTRIBUTED DENIAL OF SERVICE (DDoS) ATTACK ON
UNMANNED AERIAL VEHICLE**

A DISSERTATION

SUBMITTED IN PARTIAL FULFILLMENT OF THE
REQUIREMENTS FOR THE AWARD OF THE DEGREE

OF
MASTER OF TECHNOLOGY
IN
INFORMATION SYSTEMS

Submitted by:

Akshat Shrivastava

2K20/ISY/01

Under the supervision of

Dr. Kapil Sharma

Professor



DEPARTMENT OF INFORMATION TECHNOLOGY

DELHI TECHNOLOGICAL UNIVERSITY

(Formerly Delhi College of Engineering)

Bawana Road, Delhi

May, 2022

DEPARTMENT OF INFORMATION TECHNOLOGY**DELHI TECHNOLOGICAL UNIVERSITY**

(Formerly Delhi College of Engineering)

Bawana Road, Delhi

CANDIDATE'S DECLARATION

I, Akshat Shrivastava, Roll No. 2K20/ISY/01 of M.Tech. (Information Systems),
Hereby declare that the dissertation report titled “DISTRIBUTED DENIAL OF
SERVICE (DDoS) ATTACK ON UNMANNED AERIAL VEHICLE” which is
submitted by me to the Department of Information Technology, Delhi Technological
University, Delhi in partial fulfillment of the requirement for the award of the degree of
Master of Technology, is original and not copied from any source without proper
citation. This work has not previously formed the basis for the award of any Degree,
Diploma Associate ship, Fellowship or other similar title or recognition.

Place: Delhi

Date:

Akshat Shrivastava

DEPARTMENT OF INFORMATION TECHNOLOGY
DELHI TECHNOLOGICAL UNIVERSITY

(Formerly Delhi College of Engineering)

Bawana Road, Delhi

CERTIFICATE

I, hereby certify that the dissertation which is submitted by Akshat Shrivastava, Roll No. 2K20/ISY/01 (Information Systems), Delhi Technological University, Delhi in partial fulfillment of the requirement for the award of the degree of Master of Technology, is a record of the project work carried out by the student under my supervision. To the best of my knowledge this work has not been submitted in the part or full for any Degree or Diploma to this University or elsewhere.

Akshat Shrivastava

Prof. Kapil Sharma

(2K20/ISY/01)

SUPERVISOR

Place: Delhi

Date:

ACKNOWLEDGEMENT

I am grateful to Prof. Kapil Sharma, HOD (Department of Information and Technology), Delhi Technological University (Formerly Delhi College of Engineering), New Delhi and all other faculty members of our department for their astute guidance, constant encouragement and sincere support for this project work.

I would like to take this opportunity to express our profound gratitude and deep regard to our project mentor Dr. Kapil Sharma, for his exemplary guidance, valuable feedback and constant encouragement throughout the duration of the project. His valuable suggestions were of immense help throughout our project work. His perspective criticism kept us working to make this project in a much better way. Working under him was an extremely knowledgeable experience for us.

We would also like to give our sincere gratitude to all our friends for their help and support.

AKSHAT SHRIVASTAVA

Abstract

The Unmanned Aerial Vehicle aka Drones are the new devices which are evolving at great pace from last decade. Before that the drones found the application in military warfare only. But as the technology is evolving it is making impact on this device as well. Now days these drones are also called as Internet of Flying Things (IoFT) as they are getting inspiration from Internet of Things (IoT) devices. As these IoT devices are getting adapted in modern world these IoFT are also finding the application in various sectors like agriculture, medical emergencies, disaster prone areas, searching and surveillance industry, delivery industry etc. These IoFT devices can make use of internet for communication purposes between them as well as to ground station where they are controlled. So as these devices make use of internet it is also capable of getting attacked by different types of cyber-attacks. Distributed Denial of Service or DDoS attack is one the cyber-attack which can be disastrous in nature if not handled properly. This attack as if do nothing to device but it will eat all the resources of the network of drones which we can also refer to Internet of Drones (IoD). So as the resources like bandwidth of communication channel is full it can cause the drones to get blind such that it will not receive the correct signals as its bandwidth is full, So it can result in harm for public safety as the drone can crash and also for stealing the drone and its information. So DDoS detection for drones is one of the important task. Machine learning is evolving technique which is useful for many tasks and one of the task is prediction analysis. So in order to detect the DDoS attack on UAV machine learning models can be used. So this report discuss the experiment which is used in order to get our dataset by making a setup where drone is been DDoS attacked and data has been collected. Then this dataset is used to predict the attack and also it represent the feature extraction technique in order to improve the accuracies of the machine learning models and making them more efficient to use.

CONTENTS

Candidate's Declaration	i
Certificate	ii
Acknowledgement	iii
Abstract	iv
Contents	v
List of Figures	viii
List of Tables	xi
CHAPTER 1 INTRODUCTION	1
1.1 Motivation	1
1.2 DOS AND DDoS ATTACK	1
1.2.1 What is DOS Attack	1
1.2.2 What is DDoS Attack	2
1.3 INTRODUCTION TO UNMANNED AERIAL VEHICLES	3
1.4 INTERNET OF DRONES (IoD)	3
1.5 INTERNET OF DRONES (IoD) PART IN SMART CITY ENVIRONMENT	5
1.6 THESIS OBJECTIVE	6
1.7 SCOPE	6
1.8 THESIS STRUCTURE	6
CHAPTER 2 LITERATURE REVIEW	8
2.1 HOW DDoS ATTACK OCCURS	8
2.2 CLASSIFICATION OF DDoS ATTACK	10
2.3 DIFFERENT TYPES OF CYBER ATTACKS ON DRONES	13
2.3.1 GPS Spoofing attack	13
2.3.2 GPS Jamming attack	13
2.3.3 GNSS Spoofing and Jamming attack	13
2.3.4 Data Injection attack	14

2.3.5 Snoopy attack	14
2.3.6 Skyjet attack	14
2.3.7 Maldrone attack	14
2.3.8 Eavesdropping attack	14
2.3.9 DDoS attack	14
2.3.10 Acoustic Attack	14
2.4 AFFECTS OF CYBER ATTACKS ON UAV	15
2.4.1 Vulnerability on Availability	15
2.4.2 Vulnerability on Confidentiality	15
2.4.3 Vulnerability on Privacy	15
2.4.4 Vulnerability on Integrity	15
2.4.5 Vulnerability on Authenticity	15
2.5 DDoS DETECTION METHODS	16
2.6 BRIEF OVERVIEW OF DDoS DETECTION TECHNIQUES	16
2.6.1 DDoS attack using wavelet Analysis	16
2.6.2 DDoS attack detection by covariance model	17
2.6.3 Empherical Evaluation of information metrics for low and high rate DDoS detection	17
2.6.4 DDoS detection using Machine Learning on Internet of things devices	17
2.6.5 DDoS attack detection using Statistical and Measurement	18
2.6.6 DDoS attack detection using fuzzy estimators	18
2.6.7 DDoS Detection for drones using deep learning model	18
2.6.8 DDoS Detection for drones using block chain technology	18
2.6.9 DDoS detection for drones on GPS technology	18
CHAPTER 3 RESEARCH METHODOLOGY	19
3.1 INTRODUCTION	19
3.2 WORKFLOW	19
3.3 IMPLEMENTATION OF EXPERIMENT	20
3.3.1 Hardware Components of experiment	20

3.3.2 Software Components of experiment	24
3.3.3 Architecture of experiment	26
3.3.4 Attacks during experiment	28
3.3.5 Data Segregation and ML model building	30
3.4 OPTIMIZATION	32
CHAPTER 4 RESULT	34
4.1 PERFORMANCE EVALUATION	34
4.1.1 Accuracy of the Machine Learning Models	34
4.1.2 Confusion Matrix	35
4.1.3 AUC-ROC Curve	41
4.1.4 Precision, Recall and F-Score	47
4.1.5 Graphical Visualization on Victim	51
CHAPTER 5 CONCLUSION AND FUTURE WORK	53
References	54

List of Figures

Figure Number	Figure Name	Page Number
Fig. 1.1	Internet of Drones Architecture overview	4
Fig. 1.2	Smart City Architecture	5
Fig. 2.1	Working of block diagram of DDoS attack	10
Fig. 3.1	Workflow	20
Fig. 3.2	Customized Drone used for experiment	22
Fig. 3.3	Raspberry pi version 3 used for experiment	23
Fig. 3.4	Hping3 Tool used for attacking in experiment	24
Fig. 3.5	Wireshark tool used for packet analysis in experiment	25
Fig. 3.6	Nmap tool used for port scanning	25
Fig. 3.7	Architecture of experiment	26
Fig. 3.8	UDP flooding through Hping3 in the experiment	27
Fig. 3.9	Ping of Death attack with Hping3 in the experiment	27
Fig. 3.10	TCP flooding with Hping3 in the experiment	28
Fig. 3.11	Snip of normal packet flow before the attack in wireshark tool	28
Fig. 3.12	Snip of Wireshark tool when UDP flooding is going on in experiment	29
Fig. 3.13	Snip of Wireshark tool when ICMP flooding is going on in experiment	29

Fig. 3.14	Snip of Wireshark tool when TCP flooding is going on in experiment	30
Fig. 3.15	Distribution of data	31
Fig. 3.16	Graphical distribution of feature scores with respect to features	33
Fig. 4.1	Confusion Matrix for Logistic Regression before feature selection	36
Fig. 4.2	Confusion Matrix for Decision Tree before feature selection	37
Fig. 4.3	Confusion Matrix for Naïve Bayes before feature selection	37
Fig. 4.4	Confusion Matrix for K-Nearest Neighbor before feature selection	38
Fig. 4.5	Confusion Matrix for XGBoost before feature selection	38
Fig. 4.6	Confusion Matrix for Logistic Regression after feature selection	39
Fig. 4.7	Confusion Matrix for Decision Tree after feature selection	39
Fig. 4.8	Confusion Matrix for Naïve Bayes after feature selection	40
Fig. 4.9	Confusion Matrix for K-Nearest Neighbor after feature selection	40
Fig. 4.10	Confusion Matrix for XGBoost after feature selection	41
Fig. 4.11	AUC-ROC Curve for Logistic Regression before feature selection	42

Fig. 4.12	AUC-ROC Curve for Decision Tree before feature selection	42
Fig. 4.13	AUC-ROC Curve for Naïve Bayes before feature selection	43
Fig. 4.14	AUC-ROC Curve for K-Nearest Neighbor before feature selection	43
Fig. 4.15	AUC-ROC Curve for XGBoost before feature selection	44
Fig. 4.16	AUC-ROC Curve for Logistic Regression after feature selection	44
Fig. 4.17	AUC-ROC Curve for Decision Tree after feature selection	45
Fig. 4.18	AUC-ROC Curve for Naïve Bayes after feature selection	45
Fig. 4.19	AUC-ROC Curve for K-Nearest Neighbor after feature selection	46
Fig. 4.20	AUC-ROC Curve for XGBoost after feature selection	46
Fig. 4.21	Ping of Death attack packet transmitted graph	51
Fig. 4.22	UDP flooding attack packet transmitted graph	52
Fig. 4.23	TCP flooding attack packet transmitted graph	52

List of Tables

Table Number	Table Name	Page Number
Table 4.1	Accuracy of models before feature extraction techniques are applied	34
Table 4.2	Accuracy of models after feature extraction techniques are applied	35
Table 4.3	Precision, Recall and F-Score for Logistic Regression before feature extraction	48
Table 4.4	Precision, Recall and F-Score for Decision Tree before feature extraction	48
Table 4.5	Precision, Recall and F-Score for K-Nearest Neighbor before feature extraction	48
Table 4.6	Precision, Recall and F-Score for Naïve Bayes before feature extraction	49
Table 4.7	Precision, Recall and F-Score for XGBoost before feature extraction	49
Table 4.8	Precision, Recall and F-Score for Logistic Regression after feature extraction	49
Table 4.9	Precision, Recall and F-Score for Decision Tree after feature extraction	50
Table 4.10	Precision, Recall and F-Score for K-Nearest Neighbor after feature	50
Table 4.11	Precision, Recall and F-Score for Naïve Bayes after feature extraction	50
Table 4.12	Precision, Recall and F-Score for XGBoost before feature extraction	51

CHAPTER 1

INTRODUCTION

1.1 MOTIVATION

In 2016, a cyber-attack occurs called Mirai Dyn DDoS attack which was one of the largest attack and this attack was none other than DDoS attack. Then in 2017, DDoS attack has captivate Google which is one of the well-recognized IT Company and recently Amazon AWS in February, 2020 this attack happened. So if such giants company which has large network and also have top securities even they can get caught in such attacks then small firms are so easy to take down with this type of attack. This gives me a fascination to know more about this attack. DDoS attack has become more powerful over the years yet many detection techniques have been evolved then also every time the attack becomes more powerful than previous attack and this is the loophole that every detection scheme gets old for that attack. Also every time it is seen that new type of DDoS attack was done so it become difficult to make a particular classification of this type of attack. And as UAVs are new vehicles which is used in various sector. I got motivate that why not research on this topic to search how this attack occurs on drones. What will be the effects of this attack on the drones? And in order to stop the attack it needs to be identified first so AI and machine learning are evolving technology which can be good methods for attack prediction. So this dissertation will discuss about DDoS attack, UAV technologies and detection techniques for this type of cyber-attack.

1.2 DOS AND DDoS ATTACK

1.2.1 What is DOS Attack?

DOS attack or Denial of Service attack is an attempt by an attacker such that it hampers the normal user service of any network or any other internet application. This attack can cause corruption in data but its main target is to block the resources of any server or any

application. DOS attacks normally attack on a network causing entire usage of bandwidth which result in large amounts of traffic on the network such that it causes complete utilization of operating system resources of server or any application making it difficult to access the system by any normal user. The victim of this attack can be a single router or can be the entire network of any organization. The attacker will supply such a huge number of baseless packets so that it can make a service unavailable for a few hours to a few days.

This DOS attack can be in many forms. Some of them are:

1. In one form it can attack on networking devices such that making use of its hardware resources completely.
2. The other form can be flooding the machine with ICMP echo requests causing failure on the targeted machine.
3. One other form is by finding a loophole in the algorithm of any internet application causing the application to exhaust all the resources of the network on which it is hosted.
4. Another form is by exhausting the whole of the bandwidth of a network or device by bombarding a lot of useless packets such that it prevents normal flow of legitimate users.
5. One more form can be attacked on several protocols like DNS by spoofing and causing normal disruption.

1.2.2 What is DDoS Attack?

WWW Security FAQ [1] describes DDoS attack or Distributed Denial of Service attack as “A DDoS attack uses many computers to launch a coordinated DOS attack against one or more targets. Using client/server technology, the perpetrator is able to multiply the effectiveness of the DOS significantly by harnessing the resources of multiple unwitting accomplice computers, which serve as attack platforms”. This attack becomes more powerful by its property of distributing over internet and causing massive traffic on network. This attack takes advantage of open internet architecture. Due to its open design it becomes more vulnerable for DDOS attack. It can be understood by following points:

1. Every internet host is occupied by limited resources which can serve only limited number of users but this attack takes all the resources in its use.

2. Even though we can make our system protected but still it will always depend on global internet. Therefore becoming vulnerable to attack.

1.3 INTRODUCTION TO UNMANNED AERIAL VEHICLES

Unmanned Aerial Vehicles, UAVs, more popularly known as Drones are becoming one of the important aspects of human life making many things easy. A drone can be defined as machine which is controlled by a computer or controller in order to complete different types of task. UAVs are being used in a wide range of applications like military, agriculture, ecommerce etc. These UAVs are well sufficient such that many big companies are developing systems which involve these machines in order to complete their different tasks. For example Amazon has started delivering their orders using UAVs. As with the development of technology these UAVs are getting cheaper day by day making them useful in various other applications like surveillance, research etc. But as these drones are also vulnerable in security. As these UAVs have their own computational unit and being computer controlled makes them good victim for any cyber-attack.

1.4 INTERNET OF DRONES (IoD)

Internet of drones (IoD) [2] can be defined as framework which do management and connects the different drones in restricted airspace in order to perform different services to complete their tasks. Since the connection between the drones forming the network is through Internet of Things (IoT) so this IoD also faces the same vulnerability issues related to its security as those faced by IoT. IoD architecture is such a versatile way which can be helpful in various sectors like industrial investigation, delivery systems, search and rescue operations in disaster prone areas etc. This IoD will be the part of smart city in future but as its security is vulnerable it is difficult to implement for different tasks. This IoD holds various responsibility such as 1. By following this IoD architecture it will be responsible for its safety such that drones in air doesn't get collided. 2. It will be responsible for communication between the drones and ground station. 3. It will be responsible for secured communication of the data which the drone's sensors collects and it should be delivered at proper location. Thus it is clear that a proper

IoD architecture is important for drone communication in smart cities. The Fig. 1.1 shows overview of the Internet of Drones (IoD).

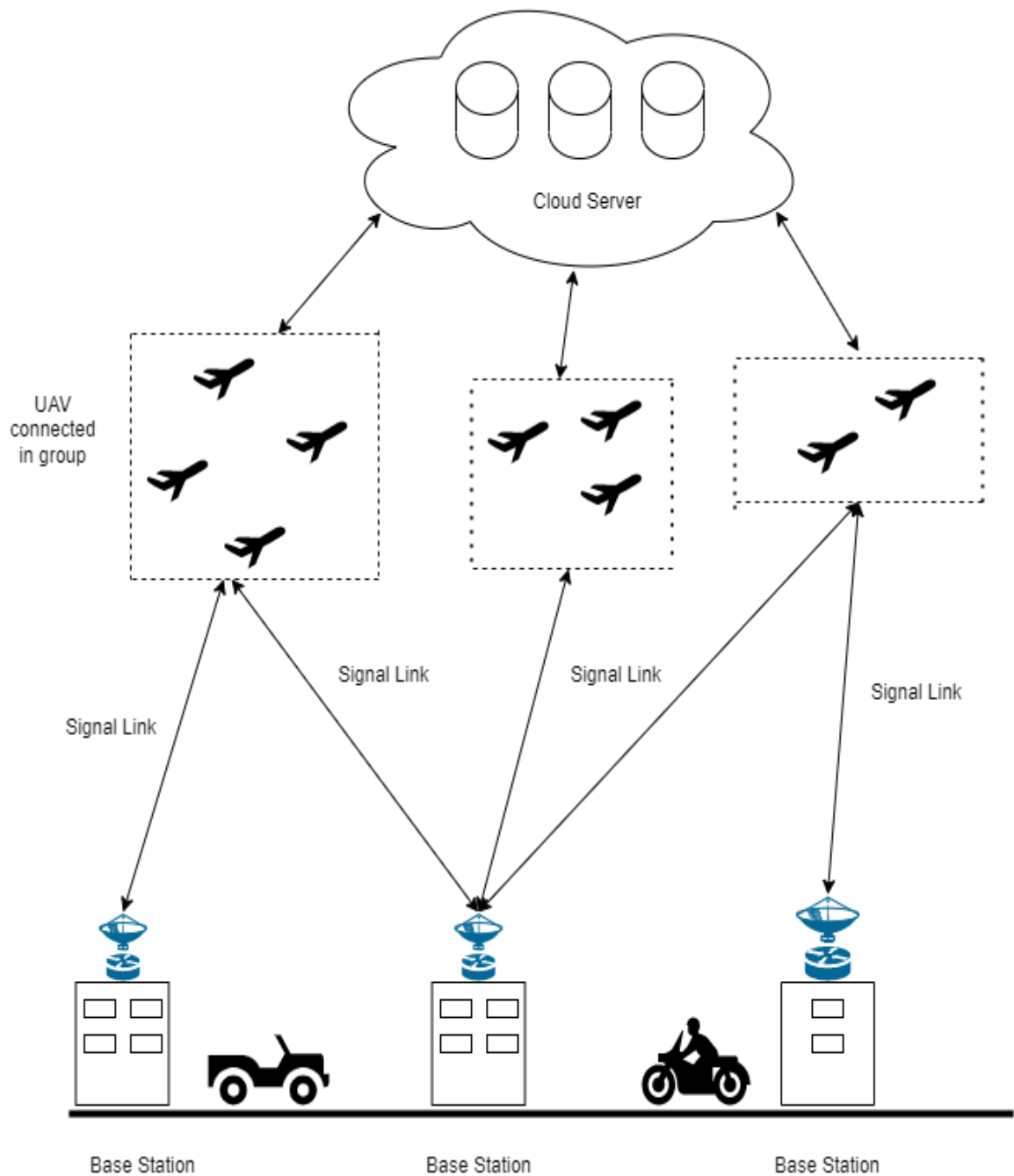


Fig. 1.1 Internet of Drones Architecture overview

1.5 INTERNET OF DRONES (IoD) PART IN SMART CITY ENVIRONMENT

Smart city can be defined as city which is having representation of Information Communication and technologies (ICT). The smart city are getting designed by keeping the future aspects in mind. It will be consists of very intelligent systems which are capable of performing smart decisions in order to complete its tasks and share information to the required places. The Internet of Drones will be the part of smart city. As these drones also comes under smart intelligent devices making them a part of this city. These IoD architecture will be integrated with it in order to perform different operations. These drones can be used in various sectors like military, agriculture, health sector, disaster affected areas etc. They can collect the information using smart sensors and can perform in smart city environment by manipulating and transferring information to various other devices which are also part of smart city. These drones in smart city will be having there restricted airspace where they needs to perform the tasks and connected to other systems for data manipulation which is been collected by drones sensors and can be stored in cloud or central repository. The Smart city architecture can be seen in Fig. 1.2

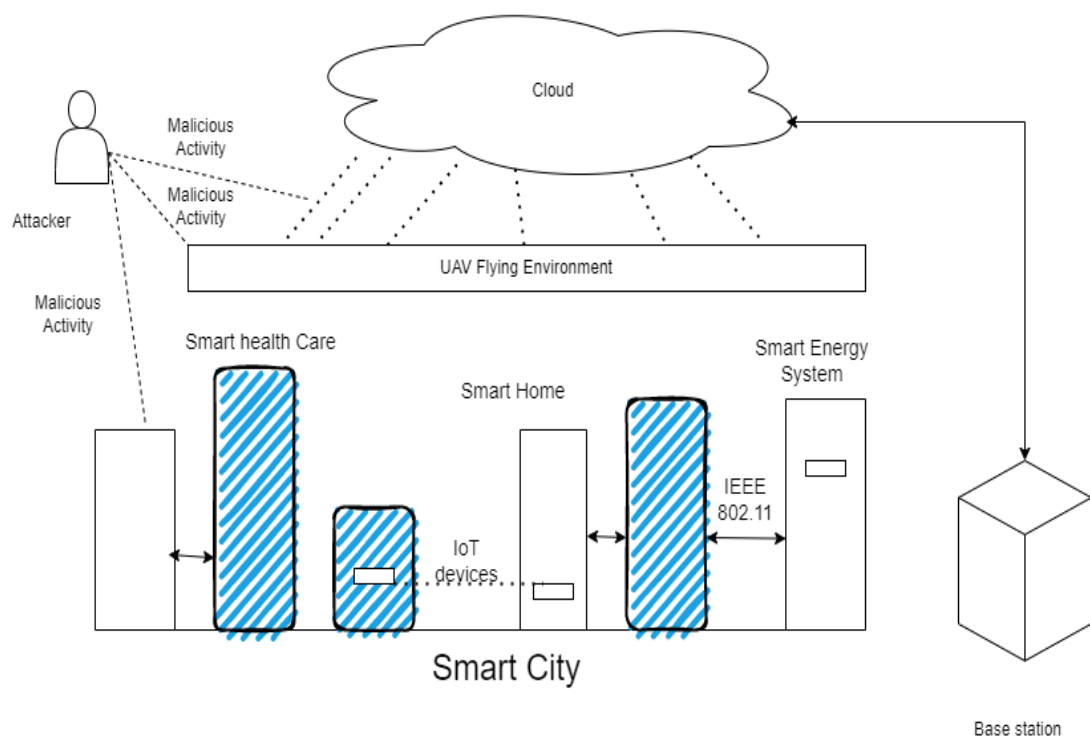


Fig. 1.2 Smart City Architecture

1.6 THESIS OBJECTIVE

From last two decades Unmanned Aerial Vehicle (UAVs) are making their contribution not only for military purposes but they are also making their way into the commercial services like agriculture, delivery services, medical fields etc. These drones use communication medium for transmitting information to each other as well as to ground stations. These communication medium can be Wireless Sensor Networks, Satellite networks or radio signals. But as the use for these drones are becoming common many network for commercial purposes use wireless sensor networks like 3G, 4G internet medium in order to transmit the information. As the internet is very vulnerable target for cyber-attack resulting the drones to become the part of attack. DDoS or DoS attack can be targeted for drone's network making them threat for information stealing or public safety. Following are the main objectives of this thesis:

1. To study literature for DDoS attack, its various detection techniques and about Unmanned Aerial Vehicle (UAV).
2. To analyze and implement machine learning models for detecting DDoS attack on UAV communication network.
3. To improve the accuracy of our ML models by implementing feature selection algorithm.

1.7 SCOPE

This thesis studies the DDoS attack and UAV technology. And how these UAV are having threat issues with this attack. It also give understandings for various types of DDoS detection techniques. It also gives understanding to detect the DDoS attack on UAV network in local area network with the help of machine learning models. And also improving the accuracy of models using feature extraction techniques.

1.8 THESIS STRUCTURE

The chapter 2 in this thesis will put light on the literature survey part for this thesis. It will give the understanding related to how the DDoS attack works and also how this attack has been classified into different types according to various measures. It will give

the understanding for various types of cyber-attacks on UAVs. And what are the effects of cyber-attack on UAV. This chapter will also give insights for what are the various types of DDoS detection techniques.

The chapter 3 in this thesis will give details about research methodologies. It will give understanding for how the attack scenario have been created in order to collect the data and then apply the machine learning models on the data. It will also put light on the methods used for improving the accuracy of the models by using feature extraction techniques. The chapter 4 will discuss the results of our experiments on the basis of various performance metrics. And chapter 5 will conclude the thesis with future scope for this project.

CHAPTER 2

LITERATURE REVIEW

The understanding of our research methodology can become better if we fully understand the concepts of DDoS attack and detection schemes related to it. The chapter 2 gives us the full insights of DDoS attack how this attack works. This chapter will also give the information regarding the classification of DDoS attack. This chapter will also talk about different types of cyber-attacks on drone networks and what effects they propagates. It also discuss the different types of DDoS detection techniques which are related to different domains and can be used to understand the most feasible technique.

2.1 HOW DDoS ATTACK OCCURS

Following are the steps for DDoS attack to occur:

1. Preparation of Agents: The attacker is one who is responsible for the whole attack. So in order to complete its goal the first step is to set up the agents. This can be done either in active mode or in passive mode. In active mode the attacker scans the whole system (tools such as Nmap) if there is any possibility of weakness in any system, by identifying that weakness the attacker runs its malicious script to break into the system and install its software thus making that system compromise. And in passive mode attackers generally use corrupted files through browsers such that when a user clicks these files he will scan its vulnerable point and do its job of installing malicious software. And these software are kept in such a way that the original user is not able to find them. So a user does not know that his machine has been compromised.
2. Calling Agent: Now after the preparation of agents, now the attacker is ready with its setup and he will use different handlers which are available all over the internet to communicate with these agents. These handlers then can easily instruct agents about attack like when to attack, for how much duration this attack will last etc. This communication can be done by using any protocol like TCP, UDP, and ICMP.

3. Attack: This is the final step of attack when the attacker will command all agents to attack the system.

We can understand this whole process by diagram Fig. 2.1:

1. Attackers are one which is responsible for attack and he is the one who will do all preparations for attack.
2. Then the attacker communicates with handlers through TCP,UDP or ICMP such that these handlers will be responsible to communicate with agents under them and when the attacker communicates to the handler about the attack then these handlers communicate this information to agents for attack.
3. Then, when handlers order the agents which are having the code which will be responsible for attack, agents get active and they start flooding the victim's machine.

And in this way when there are thousands or more agents at same time attacking the target machine it will cause a slowdown of the machine or complete shutdown of the system. And hence DDoS attacks become successful.

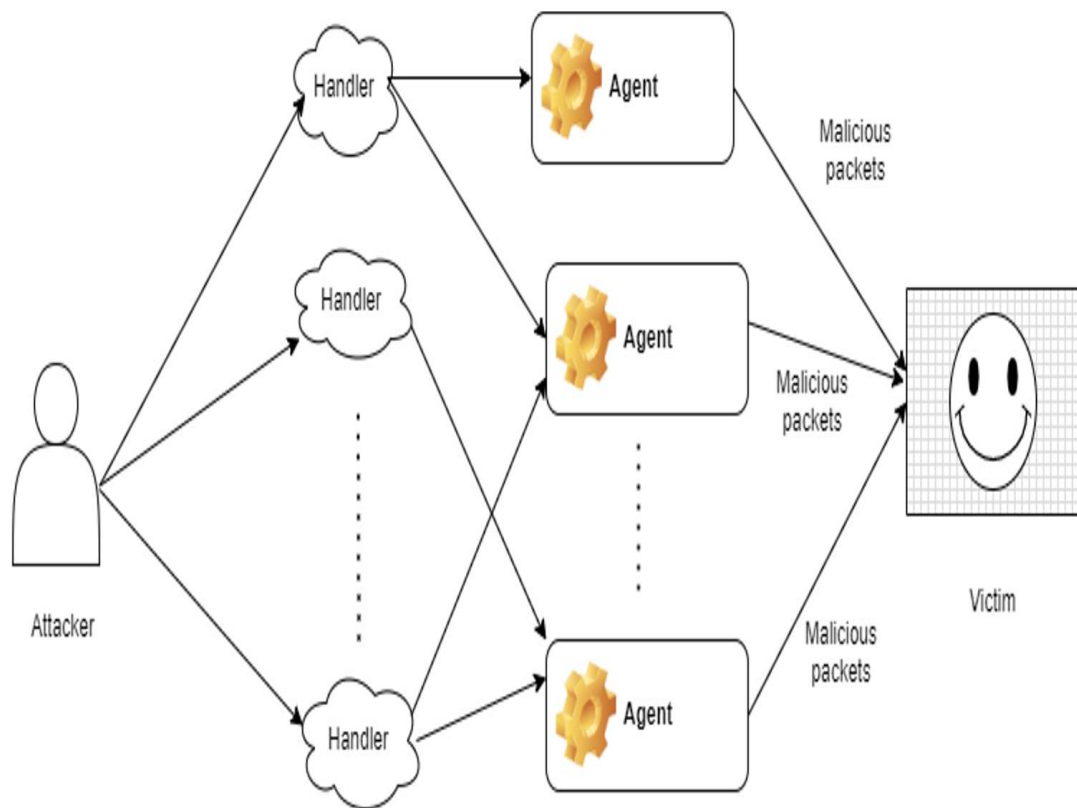


Fig. 2.1 Working of block diagram of DDoS attack

2.2 CLASSIFICATION OF DDoS ATTACK

There is no particular fixed classification of DDOS attacks. Some research papers [3][4][5][6] have included some types of DDOS attack in one category some have included them in other categories. I have tried to generalize and cover most of the classification of DDOS attack. Following are classification of DDOS Attack:

1. Agent Handler Model:

In this type of model we have some categories called as Attacker, Agents, Handlers and Victim. So Attacker is one who plans to attack a target network. Then Handlers are software bundles on the internet which are used to communicate with agents distributive, then Agents are host machines which are compromised and will be responsible for attack on target and target is one on which attack is going to happen. Generally the target machine and host machine

which is acting as agent doesn't know that their machine will be involved in a DDoS attack.

2. Reflector Model:

This model consists of attacker, handler, agents and reflectors. Attacker will be playing its role of attacking then handlers are used for communicating with agents and agents are one who attacks the victim but in this model agents send the packets with the victim's IP address as source IP address to other targeted machines. These reflectors can also be responsible for amplifying packet distribution by broadcasting it and making problem worse.

3. IRC Based Model:

It stands for Internet Relay Chat and it is used for online chatting. There are IRC servers all over the internet that allows two or multiple connection to create a channel where user can chat. There are Public channels which are open and their messages and name can be seen by everyone. Then there are private and secret channels where messages and names are not visible to person who doesn't belong to that channel. The attacker uses this secret channel which are difficult to trace. So it also uses same agent handler model type concept but with difference that here IRC servers are used for communication with agents and it will be easy task for attacker to identify all the list of agents and when the attacker commands it run through IRC channel and causes attack on victim's machine. These agents in IRC model are known as "Zombie Bots".

4. Degree of Automation Base: This can again be classified as

1. Manual: In this vulnerable machines are identified and then code is installed on that machine and then used for attacks. It was before when the manual process was there.
2. Semi-Automatic: In this attack attackers usually run automatic scripts which identify machines which are capable of becoming the handlers and agents. Although the attack can be done in one of the two ways first is by using an agent handler model in which the attacker attacks the victim using a handler and another one is using an IRC based model in which the attacker attacks the victim using IRC servers and using IRC communication channels.
3. Automatic: In this type of attack there is no communication between attacker and agents instead the attacker automates the attack by defining

the start of attack timing to that of duration of attack and victim's IP address.

5. Classification by Impact: On the basis of impact it can be divided into two types:
 1. Disruptive: This attack will lead to complete use of bandwidth.
 2. Degrading: If attack uses only partial bandwidth then it will be of degrading type.

6. Classification on basis of vulnerability: On the basis of vulnerability it can be divided into many categories:
 1. Flood Attack: This attack basically targets the victim's machine by sending a large amount of packet stream to the network thus blocking the bandwidth which is done by zombie bots making the machine slower or completely shutting it off from the network. It can attack in the form of either UDP packets or ICMP packets flooding the bandwidth.
 2. Amplification Attack: In this generally attacker uses IP address for broadcasting feature on all routers and it amplifies and broadcasts the packet to each IP address in its range. In this way when several routers broadcast the packets it will cause enormous packets on bandwidth thus blocking it. These types of attack are Smurf and Fraggle attacks. Smurf attack amplification method by broadcasting ICMP packet to all other machines and Fraggle attack uses UDP packet for broadcasting.
 3. Protocol exploit attack: This attack usually targets the weakness of several protocols and using them against the user for attacking purposes. For example In TCP protocol the machine needs to perform three way handshake for that client need to send SYN packet to receiver and it waits for receiver's acknowledgement packet i.e. SYN/ACK packet. The attacker uses this weakness of TCP protocol sending a large amount of SYN packet continuously to receiver making buffer overflow and in result it causes crashing of receiver server or machine.
 4. Malformed Packet attack: This attack targets the machine by making a malformed packet. This can be done by changing the different fields of the packet such that when received by the victim and as some of the fields which are changed can cause the victim's machine to take more

computation time. So if a large number of such packets are bombarded at same time then the victim's machine can crash at that time.

7. Attack Rate Dynamics base: On the basis of attack rate dynamics it can be classified further:
 1. Continuous: In this attack when agents are ordered they attack with full force.
 2. Variable Rate: In this attack it is not continuous it varies from time and due to fluctuation in attacking rate they are somewhat difficult to capture.
8. Propagation Strategy base: On the basis of propagation strategy it can be further classified as:
 1. Central: In this strategy the code which is responsible for attack lies on the central server and from there it is downloaded to agent machines which can further attack on victims.

Back-Chaining: In this strategy code is retrieved from a machine which was used to infect all servers. Then this new machine becomes a source for spreading the code.

2.3 DIFFERENT TYPES OF CYBER ATTACKS ON DRONES

The drones are connected in such a way that they can communicate with each other and also to different other applications in order to perform different types of tasks. This communication medium plays important part and it is vulnerable for cyber-attacks. Different types of possible attacks [2][7] are:

2.3.1 GPS Spoofing attack

In this type of attack the attacker use to tampered Global Positioning System (GPS) signal to UAV and thus forcing the drone to land to the position specified by the attacker.

2.3.2 GPS Jamming attack

In this type of attack the attacker tries to block all the signal for GPS thus making it difficult for drones to get navigational signals. This jamming of signal will lead to compromising of drone or even crashing of drone making it vulnerable to public safety.

2.3.3 GNSS Spoofing and Jamming attack

It is also the type of GPS spoofing and jamming with only difference that here the tampered Global Navigational Satellite System (GNSS) is send to the UAV such that in

GNSS spoofing it gets wrong direction to get land and in jamming attack all of the navigational signals get blocked making it vulnerable to crash.

2.3.4 Data Injection attack

The attacker manipulates the UAV direction estimation by tampering with directional measurement data so that it will not be able to detect the correct directions.

2.3.5 Snoopy attack

In this type of attack the attacker inject some malicious program to get its information and control it using wireless sensor network.

2.3.6 Skyjet attack

In this attack the attacker installs the malicious program to tamper navigational system.

2.3.7 Maldrone attack

The attacker inject the maldrone malware on a drone as a result it acts like a proxy between the drone and the communication medium as a result it can be hijacked.

2.3.8 Eavesdropping attack

During the real time scenario if any intruder can eaves drop a communication link then it can have access to real time data.

2.3.9 DDoS attack

If the communication medium between the drones is vulnerable and exposed making it good position for attacker to get into the network and make compromise different ground station machine and making them ready to make a DDoS attack on the drones. As a result its network bandwidth will get blocked and important communication can get blocked making it blind and vulnerable to public safety.

2.3.10 Acoustic Attack

In this type of attack the attacker deploy a compromised drone with different sound frequency resulting in distorting the targeted drone's gyroscope resonant frequency leading it to crash.

2.4 AFFECTS OF CYBER ATTACKS ON UAV

These different types of attacks on UAV causes various affects. It can be in many forms:

2.4.1 Vulnerability on Availability

When we say about availability we means that the drone will be always in communication within its Internet of drones network. But due to these physical attack or DDoS attack or Jamming attack the UAV becomes unavailable. These attack can block the resources or completely make the drone vulnerable such that it will be unavailable for use. This can cause the UAV to become dangerous for public safety.

2.4.2 Vulnerability on Confidentiality

These attacks can make the confidentiality of the machine to compromise. Attacks like replay attack or spoofing attack can make it to loose. These attacks will steal the data and corrupt it and forward it to targeted machine.

2.4.3 Vulnerability on Privacy

The cyber-attacks on UAV can cause privacy breach. As we know the UAVs consists of various sensors which are used for getting the data for various operations. The attacks like traffic analysis attack, reconnaissance and malware attacks can be responsible for breaching the privacy. These malware are made to install on the drones and with the help of these compromised software important information gets collected by attacker.

2.4.4 Vulnerability on Integrity

If the information is transmitted from ground station then it should reach to destination UAV without any changes. But various cyber-attacks like wormhole attack, eavesdropping attack, man-in-the-middle attack can disturb the integrity of messages. These attacks will be acting like message is reaching to target from authenticate source but it may have changed.

2.4.5 Vulnerability on Authenticity

Authenticity is important as it implies that the information is coming from trusted source. But the cyber-attacks like key-loggers, DE-authentication attack can be

responsible for breaching authenticity. The attacker will be able to disconnect the original target and taking it overpower with infected entity.

2.5 DDoS DETECTION METHODS

DDoS detection has become one of the important research area in the field of computer science. From the point when DDoS attack occurs first time researchers have proposed several methods based on various theories and models. These theories are not only motivated from computer science world but also they are inspired by other area like entropy based model, energy distribution based model etc. they are also motivated from statistical world and many researchers have proposed good detection methods which are based on this method, other models are also on AI/ML. As with the evolution of artificial intelligence (AI), it has been utilized for detecting this attack using various machine learning models like Support Vector model, Random Forest model, Decision tree model and many others. Below mentioned are few detection methods and later given introduction to UAVs.

2.6 BRIEF OVERVIEW OF DDoS DETECTION TECHNIQUES

Below mentioned are few techniques:

2.6.1 DDoS attack using wavelet Analysis

In this detection scheme [8] wavelet analysis is used for getting temporal correlation for various time scales. And in this method they have mentioned that it will require minimum computation for detection. Also they have used the Energy prediction model on wavelet analysis for detecting the DDoS attack in the network. According to this model during the normal circumstances when there is regular flow of data packets over internet there will be almost constant flow i.e. the projection which we will see in graph will not vary daily there can be some variation although, So when we see it using energy prediction model it will show slight variation in graph but when there is attack then there will be sudden and more variation in graph such that it can be identified as there is some attack on system.

2.6.2 DDoS attack detection by covariance model

This [9] method of detection uses covariance model for detecting SYN flooding DDoS attack. The researcher of this method claims that as comparison to other statistical methods their methods give more accurate results and in less computation time. There are many methods which are based on statistical analysis and there are also methods which are clustering based. The statistical method needs prior information for predicting its result. But clustering method does not need any prior information it has various other parameters which can be used to predict the result.

2.6.3 Empirical Evaluation of information metrics for low and high rate DDoS detection

The researchers of this [10] literature tried to empirically evaluate many information metrics like Renyi's entropy, generalized entropy, Shannon entropy, Hartley entropy, KullbackLeibler divergence. By using these metrics they tried to evaluate a metrics which can help in detecting the low as well as high rate DDoS attack. Metrics based on Information theory is a very good method of differentiating between legitimate traffic and malicious traffic. And low computation requirement is one of the major advantages of this method.

2.6.4 DDoS detection using Machine Learning on Internet of things devices

With the growing Internet of things devices in the world as it is making life all easier at the same time it is producing more vulnerability for DDoS attack. There was a massive DDoS attack in October 2016 by using Mirai botnets which mostly targeted CCTV cameras. But for IoT devices there are many advantages in capturing the attack since IoT devices do not use a large number of servers as other devices use rather it uses limited resources and IoT devices generally perform tasks which are generally repetitive in nature making the traffic pattern repetitive in nature so it becomes an advantage for identifying the changes in traffic. So using these principles, the researchers have tried to use machine learning for detecting the DDoS attack. Here they have utilized protocol, packet length etc. as features for predicting model [11].

2.6.5 DDoS attack detection using Statistical and Measurement

This [12] method of detecting DDoS attack is based on statistical mechanism called as continuous ranked probability score and exponentially smoothing scheme for better detection of DDoS attack. There are several statistical methods and also other methods developed before for detection of DDoS attack like a rank correlation method for DDoS attack but it is based on the fact that reflectors when tend go close to victim it is linearly auto correlated.

2.6.6 DDoS attack detection using fuzzy estimators

One of the method of detecting the DDoS attack is by using the fuzzy estimators. In this [13] method they have taken mean packet arrival time and applied on fuzzy estimators so that attack can be detected.

2.6.7 DDoS Detection for drones using deep learning model and machine learning model

In [14][15] the DDoS detection method is used for drones. This method uses deep learning models and machine learning models for detecting the attack in order to prevent it before it gets intense.

2.6.8 DDoS Detection for drones using block chain technology

In [16] DDoS attack has been identified using block chain technology. When the drone uses peer to peer network between them so in order to secure them block chain is being used and this technology is able to detect the attack and respond in early stage.

2.6.9 DDoS detection for drones on GPS technology

GPS Jamming and spoofing are on the dangerous threat for drones which can make it blind and as result it can get crash and can cause mass destruction. So in order to tackle this GPS spoofing and jamming various tools can be used which are capable of tackling these types of attack [17].

CHAPTER 3

RESEARCH METHODOLOGY

3.1 INTRODUCTION

DoS or DDoS attacks are both cyber-attack which can easily be targeted on these UAVs computational units and their important information can be extracted if security measures are not followed. These UAVs or drones contains computation part which can be any small processing unit like Raspberry Pi, Nano Pi, Banana Pi etc. which are used differently for different purpose, like a camera connected to raspberry pi over drone used for monitoring or surveillance purpose if got attacked then whole drone can get ruined. Various literatures [18][19][20][21] give insights for these types of attacks. Also these attacks can make drones unstable leading it to falling down which can cause damage to anyone. Also getting some important information compromised by security threats can be a cause of national security. So detection of these attacks at initial rate is important so that necessary steps can be taken to save these UAVs. The research methodology is targeting on making an experimental setup of DoS/DDoS attack on the computational part (Raspberry Pi) which will be mounted on a customized drone. To study the attack's behavior on the UAV and collect the data from this experimental setup and using it to detect attack using Machine Learning.

3.2 WORKFLOW

The workflow is representing a brief overview of how this research methodology will work in various phases. In Fig. 3.1 we can see that first experiment will be performed then on attacking the victim (drone) will be analyzed and its data will be collected and then various machine learning algorithm will be applied to it in order to detect the attack.

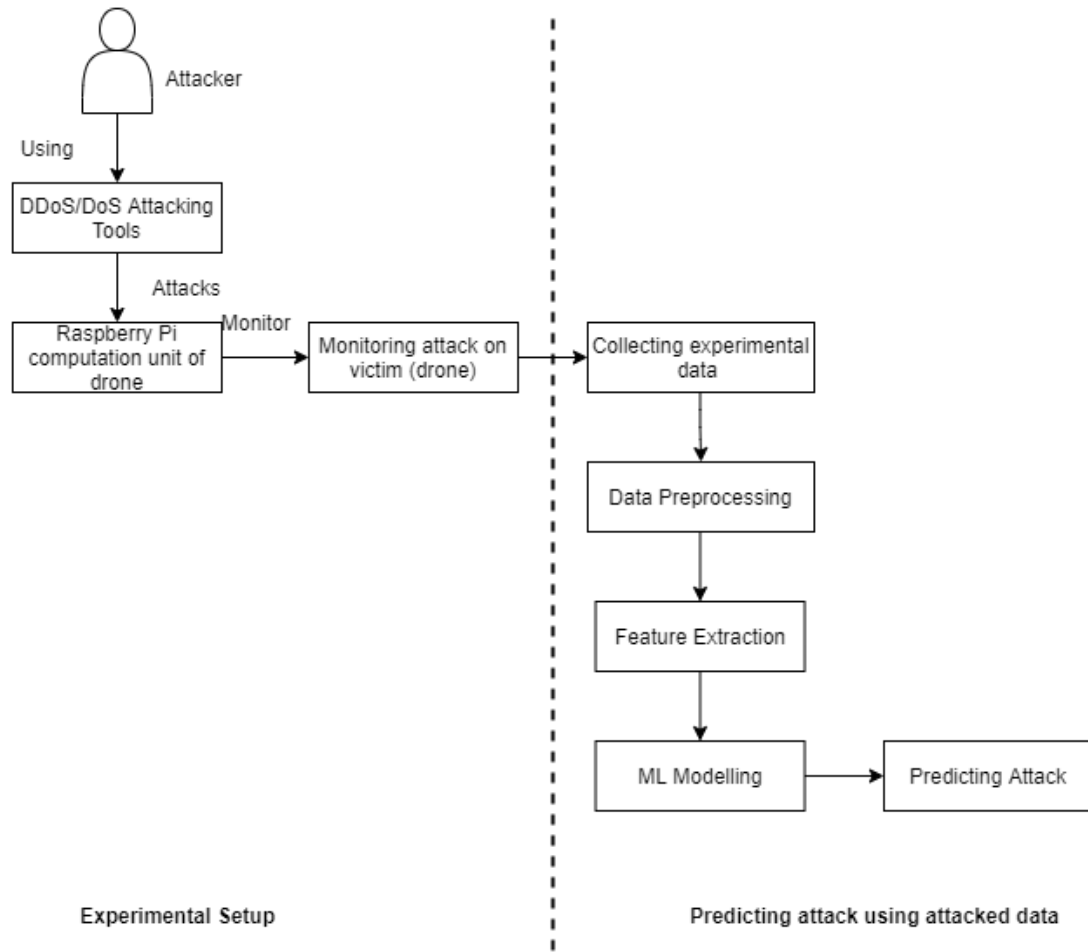


Fig. 3.1 Workflow

3.3 IMPLEMENTATION OF EXPERIMENT

In order to get this attack predicted either DoS or DDoS we need to perform a experiment from where we actually attacked the drone by creating such a scenario and then taking out data so that we can apply different machine learning model to predict the attack. Details of this experiments are presented below

3.3.1 Hardware Components of experiment

Various components used for performing this experiments are:

3.3.1.1 Unmanned Aerial Vehicle (UAV)

In order to perform this experiment on of the important component was UAV. So I have made my own customized drone which can be act as target for attacking. Various components of this drones are:

3.3.1.1.1 Frame of drone

Frame of drone is the basic structure which is needed in order to make the drone. On this frame only all the parts of drone are installed.

3.3.1.1.2 Motors

As we are using Quad copter so 4 motors are required for making this drone. These motors are responsible for making a drone fly with the help of propeller.

3.3.1.1.3 Battery

A battery is required in order to give power to drone which help it to fly and perform all other operation.

3.3.1.1.4 Flight Controller

A flight controller is also installed on the drone which contains of all the instructions regarding its flight and all other modules which can be tried out using the drone.

3.3.1.1.5 Transmitter

A remote transmitter is needed in order to control the movements of drone.

3.3.1.1.6 Raspberry pi

This raspberry pi is along with its camera module is installed on the drone which help in performing the visualization operations.

On combining all these equipment a drone is formed which is used for making it as victim of DDoS attack.



Fig. 3.2 Customized Drone used for experiment

3.3.1.2 Raspberry Pi

Raspberry Pi is small CPU having its own memory, NIC etc. all the important parts which are needed for making a computer. We can say that it is a small computer which can be used for various purposes. It can be used for home automation or any industrial application in various products it can be installed and used a small size computer and also for educational purposes it can be used. It can be operated with the help of mouse, keyboard and a monitor used for displaying and controlling the application. It can also be run in headless manner where no monitor is required. As drone is getting more and more application nowadays. So raspberry pi can be a good selection for installing in it and used for various purposes although many companies has started using their own built in small CPU for their drone but raspberry pi can also be a good option for this purpose.

In our experiment we have used Raspberry pi version 3 Model B.



Fig. 3.3 Raspberry pi version 3 used for experiment

3.3.1.3 Attacker and user laptops

For this experiment we have used 2 laptops one for attacking and other for user.

Attacker laptop has specification as i5 processor with 4GB RAM and UBUNTU as operating System.

User laptop has specification as i7 processor with 1GB RAM and Windows as operating system.

3.3.1.4 Router

A standard router is used for making the Local Area Network in which the drone, user laptop and attacker laptop was connected and all the sharing is done on this network and this router is used to handle all the network related configurations.

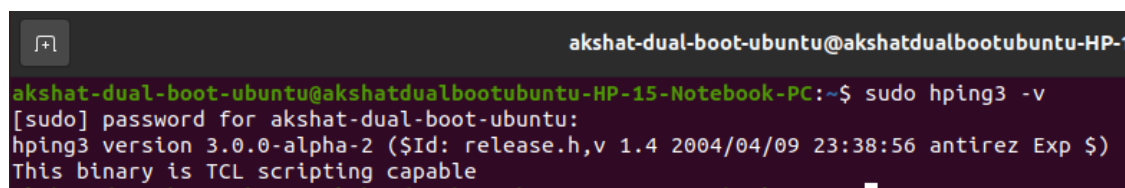
3.3.2 Software Components of experiment

3.3.2.1 Raspbian OS

For this experiment for raspberry pi I have installed Raspbian OS for it and performed all the experiments on it only.

3.3.2.2 Hping3

Hping3 is basically a network tool which is used for sending UDP/TCP/ICMP packets and displays the result. I have installed this software on attacking machine from where I will cause DoS/DDoS attack on the victim using this tool.

A terminal window with a dark background. The title bar shows 'akshat-dual-boot-ubuntu@akshatdualbootubuntu-HP-15-Notebook-PC'. The terminal text shows a user running 'sudo hping3 -v'. The output displays the version '3.0.0-alpha-2', release information, and a note about TCL scripting capability.

```
akshat-dual-boot-ubuntu@akshatdualbootubuntu-HP-15-Notebook-PC:~$ sudo hping3 -v
[sudo] password for akshat-dual-boot-ubuntu:
hping3 version 3.0.0-alpha-2 ($Id: release.h,v 1.4 2004/04/09 23:38:56 antirez Exp $)
This binary is TCL scripting capable
```

Fig. 3.4 Hping3 Tool used for attacking in experiment

3.3.2.3 Wireshark

Wireshark is an open source packet analyzer. It is used all over world for many purposes including troubleshooting network, analysis, forensic analysis and also for education purpose. It runs on Windows, Linux, IOS, raspbian OS etc. it is available as both its GUI version which can used for network analysis purpose as well as it is available as command line version which can be used for same. In the experiment I have used this tool for analysis of normal packets as well as for malicious packets on the local area network setup by me.

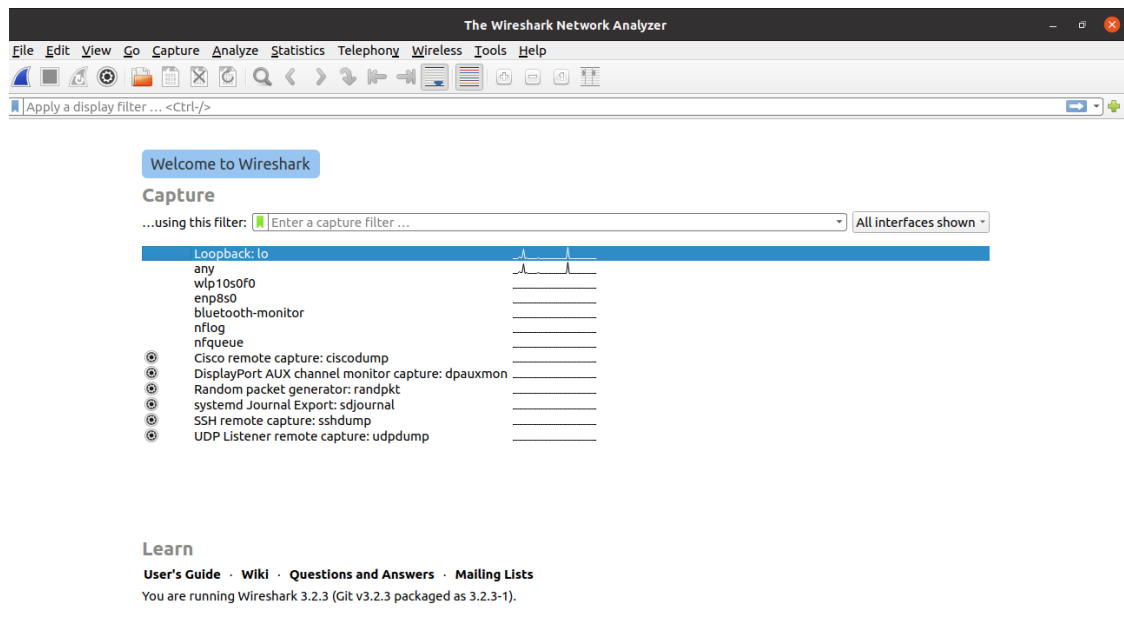


Fig. 3.5 Wireshark tool used for packet analysis in experiment

3.3.2.4 Nmap

Nmap is the network tool which is used in analyzing the network and is used by various organization for different purposes. In our experiment we have used Nmap for scanning the open port of the victim machine. So that the attacker can use this port to attack it with different types using Hping3 tool.

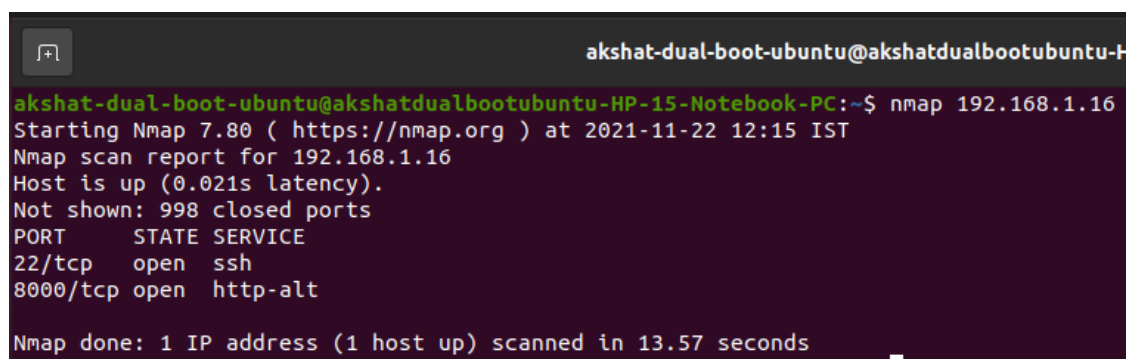


Fig. 3.6 Nmap tool used for port scanning

3.3.2.4 Programming Languages

For the experiment after the data is collected from the experiment I have used Python scripting language to preprocess the data and also to make machine learning models.

3.3.3 Architecture of experiment

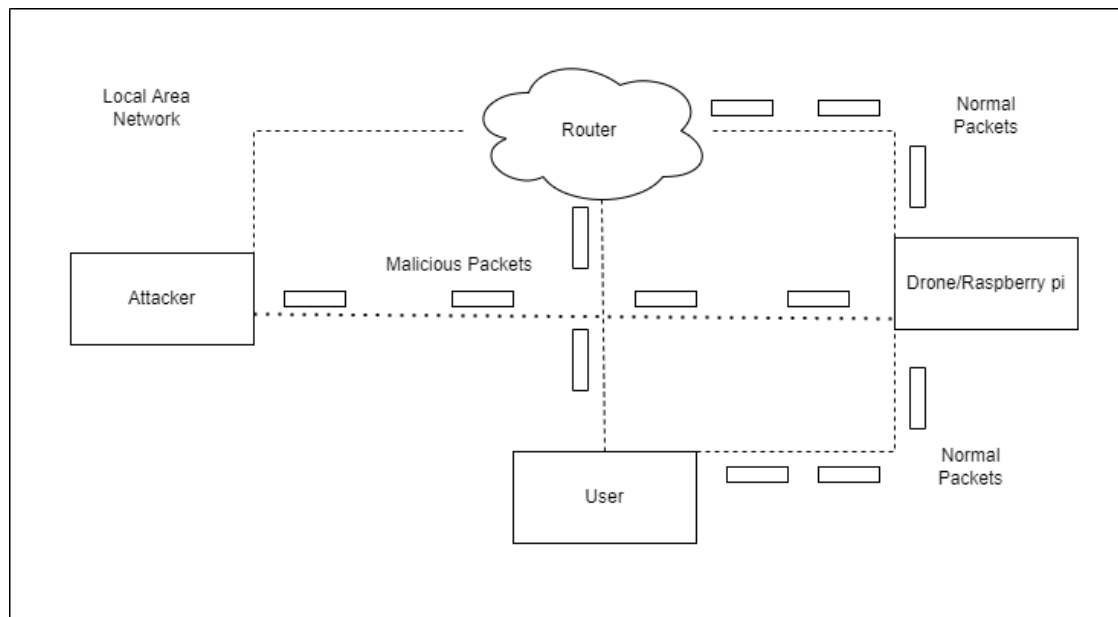


Fig. 3.7 Architecture of experiment

So in this experiment I have created a Local Area Network in which the router is connected with Drone having the raspberry pi, a user is connected which is able to see the streaming from drone and the attacker is also in the same network. A drone is flying which is installed with raspberry pi on it with a camera module fitted on the raspberry pi. The video is streaming on user laptop with a python script i.e. running on raspberry pi and as the attacker is in the network so with the help of Hping3 tool the drone is been attacked as DDoS attack. And the data using the Wireshark is analyzed and its CSV files are taken out.

3.3.3.1 Types of attacks

The experiment have targeted 3 types of DDoS attacks and collected their data on which the machine learning model is built. These attacks are:

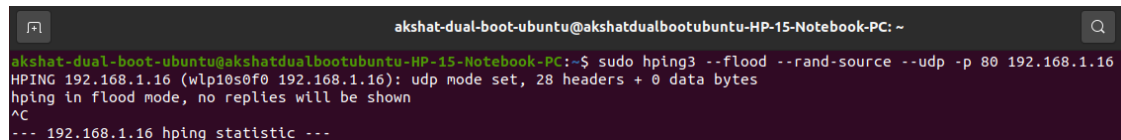
3.3.3.1.1 UDP flooding

A UDP DDoS attack is attack in which enormous amount of UDP data packets are sent to the machine whose IP is targeted with the aim of blocking it's all bandwidth making it machine which is incapable of performing communication which it was doing earlier. In this attack when the attacker send the UDP packet to a port which is open at the time of attack, in the normal situation the application which is expecting the packet absorbs

the packet but in attacked condition as no application is expecting the UDP then the machine will respond with the ICMP packet back to give information to sender that destination is unreachable. Now as number of packets are very large so in that case the machine started doing in that flow and all of its bandwidth is in that use only.

Command used for UDP attack using Hping3:

```
'hping3 --flood --rand-source --udp -p 80 192.168.1.16'
```



```
akshat-dual-boot-ubuntu@akshatdualbootubuntu-HP-15-Notebook-PC: ~
akshat-dual-boot-ubuntu@akshatdualbootubuntu-HP-15-Notebook-PC:~$ sudo hping3 --flood --rand-source --udp -p 80 192.168.1.16
HPING 192.168.1.16 (wlp10s0f0 192.168.1.16): udp mode set, 28 headers + 0 data bytes
hping in flood mode, no replies will be shown
^C
--- 192.168.1.16 hping statistic ---
```

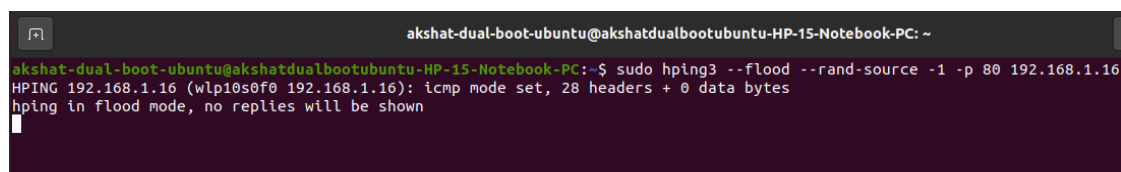
Fig. 3.8 UDP flooding through Hping3 in the experiment

3.3.3.1.2 Ping of Death

Ping of Death is the type of DDoS attack in which attacker attacks with malicious packets by using the network command 'ping'. And in this attack the frequency of packets caused by ping command is very large and as a result it blocks the bandwidth of the victim computer. Packet with length more than 65,535 bytes it violates the IP so attacker will plan to send malformed packets in fragments. And when the target machine try to reassembles the different fragments of a packet it will lead to oversized packet and as a result it will cause the buffer to overflow and it will lead to crash the system.

Command used for Ping of Death using Hping3:

```
'hping3 --flood --rand-source -1 -p 80 192.168.1.16'
```



```
akshat-dual-boot-ubuntu@akshatdualbootubuntu-HP-15-Notebook-PC: ~
akshat-dual-boot-ubuntu@akshatdualbootubuntu-HP-15-Notebook-PC:~$ sudo hping3 --flood --rand-source -1 -p 80 192.168.1.16
HPING 192.168.1.16 (wlp10s0f0 192.168.1.16): icmp mode set, 28 headers + 0 data bytes
hping in flood mode, no replies will be shown
```

Fig. 3.9 Ping of Death attack with Hping3 in the experiment

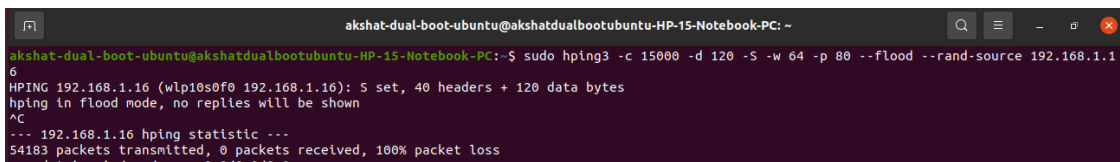
3.3.3.1.3 TCP flooding

TCP flood attack is a type of DoS attack which uses TCP protocol in order to target the attack. It exploits the normal three way handshake of the TCP protocol mechanism such that it starts consuming the resources available at victim side and try to consume all of its bandwidth leaving it to not communicate properly with original system. In normal

TCP three way handshake it performs as by sending the SYN packet initially by client which is then received by the server which sends the SYN-ACK back in order to acknowledge it and then client sends ACK packet in order to form the TCP connection but when attacker sends it, he sends it with multiple Ips with repeated SYN packet and as the victim is unaware of attack it continuously started sending the SYN-ACK packet, so as the IP address is spoofed then that IP never receives the packet as a result it causes complete blockage of the bandwidth causing the system to not communicate with original system.

Command used for TCP flood using Hping3:

```
'hping3 -c 20000 -d 120 -S -w 64 -p 80 --flood --rand-source 192.168.1.16'
```



```

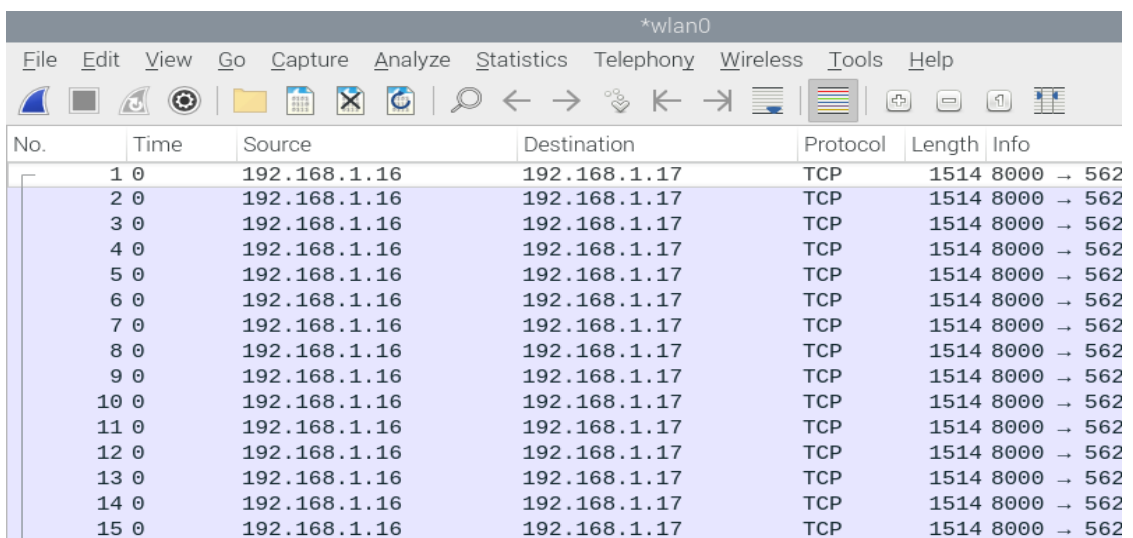
akshat-dual-boot-ubuntu@akshatdualbootubuntu-HP-15-Notebook-PC: ~
akshat-dual-boot-ubuntu@akshatdualbootubuntu-HP-15-Notebook-PC:~$ sudo hping3 -c 15000 -d 120 -S -w 64 -p 80 --flood --rand-source 192.168.1.16
6
HPING 192.168.1.16 (wlp10s0f0 192.168.1.16): S set, 40 headers + 120 data bytes
hping in flood mode, no replies will be shown
^C
--- 192.168.1.16 hping statistic ---
54183 packets transmitted, 0 packets received, 100% packet loss

```

Fig. 3.10 TCP flooding with Hping3 in the experiment

3.3.4 Attacks during experiment

So when the attack is happening it has blocked whole of the bandwidth such that the streaming which was normally happening to the user computer started getting blocked because of the attack. And in the wireshark tool we can continuously watch how the packets are receiving at the victim end.



No.	Time	Source	Destination	Protocol	Length	Info
1	0	192.168.1.16	192.168.1.17	TCP	1514	8000 → 562
2	0	192.168.1.16	192.168.1.17	TCP	1514	8000 → 562
3	0	192.168.1.16	192.168.1.17	TCP	1514	8000 → 562
4	0	192.168.1.16	192.168.1.17	TCP	1514	8000 → 562
5	0	192.168.1.16	192.168.1.17	TCP	1514	8000 → 562
6	0	192.168.1.16	192.168.1.17	TCP	1514	8000 → 562
7	0	192.168.1.16	192.168.1.17	TCP	1514	8000 → 562
8	0	192.168.1.16	192.168.1.17	TCP	1514	8000 → 562
9	0	192.168.1.16	192.168.1.17	TCP	1514	8000 → 562
10	0	192.168.1.16	192.168.1.17	TCP	1514	8000 → 562
11	0	192.168.1.16	192.168.1.17	TCP	1514	8000 → 562
12	0	192.168.1.16	192.168.1.17	TCP	1514	8000 → 562
13	0	192.168.1.16	192.168.1.17	TCP	1514	8000 → 562
14	0	192.168.1.16	192.168.1.17	TCP	1514	8000 → 562
15	0	192.168.1.16	192.168.1.17	TCP	1514	8000 → 562

Fig. 3.11 Snip of normal packet flow before the attack in wireshark tool

No.	Time	Source	Destination	Protocol	Length	Info
31151	15	192.168.1.16	219.152.98.175	ICMP	70	Destination unreachable
31152	15	119.32.82.41	192.168.1.16	UDP	42	29916 → 80
31153	15	192.168.1.16	119.32.82.41	ICMP	70	Destination unreachable
31154	15	56.125.232.143	192.168.1.16	UDP	42	29917 → 80
31155	15	192.168.1.16	56.125.232.143	ICMP	70	Destination unreachable
31156	15	0.7.17.27	192.168.1.16	UDP	42	29919 → 80
31157	15	192.168.1.16	0.7.17.27	ICMP	70	Destination unreachable
31158	15	208.194.214.239	192.168.1.16	UDP	42	29985 → 80
31159	15	192.168.1.16	208.194.214.239	ICMP	70	Destination unreachable
31160	15	131.21.62.180	192.168.1.16	UDP	42	29986 → 80
31161	15	192.168.1.16	131.21.62.180	ICMP	70	Destination unreachable
31162	15	239.151.144.125	192.168.1.16	UDP	42	29987 → 80
31163	15	129.28.41.154	192.168.1.16	UDP	42	29988 → 80
31164	15	192.168.1.16	129.28.41.154	ICMP	70	Destination unreachable
31165	15	58.117.201.162	192.168.1.16	UDP	42	29989 → 80

Fig. 3.12 Snip of Wireshark tool when UDP flooding is going on in experiment

No.	Time	Source	Destination	Protocol	Length	Info
12564	10	192.168.1.16	65.113.217.226	ICMP	42	Echo (ping)
12565	10	152.7.78.81	192.168.1.16	ICMP	42	Echo (ping)
12566	10	192.168.1.16	152.7.78.81	ICMP	42	Echo (ping)
12567	10	135.178.208.57	192.168.1.16	ICMP	42	Echo (ping)
12568	10	192.168.1.16	135.178.208.57	ICMP	42	Echo (ping)
12569	10	24.137.134.121	192.168.1.16	ICMP	42	Echo (ping)
12570	10	192.168.1.16	24.137.134.121	ICMP	42	Echo (ping)
12571	10	235.248.113.21	192.168.1.16	ICMP	42	Echo (ping)
12572	10	139.65.195.208	192.168.1.16	ICMP	42	Echo (ping)
12573	10	192.168.1.16	139.65.195.208	ICMP	42	Echo (ping)
12574	10	137.241.50.81	192.168.1.16	ICMP	42	Echo (ping)
12575	10	192.168.1.16	137.241.50.81	ICMP	42	Echo (ping)
12576	10	166.115.29.69	192.168.1.16	ICMP	42	Echo (ping)
12577	10	192.168.1.16	166.115.29.69	ICMP	42	Echo (ping)
12578	10	132.64.72.108	192.168.1.16	ICMP	42	Echo (ping)

Fig. 3.13 Snip of Wireshark tool when ICMP flooding is going on in experiment



No.	Time	Source	Destination	Protocol	Length	Info
32348	18	255.179.162.26	192.168.1.16	TCP	54	80 → 11821
32349	18	192.168.1.16	255.179.162.26	TCP	54	80 → 11821
32350	18	249.255.107.28	192.168.1.16	TCP	174	11822 → 8
32351	18	192.168.1.16	249.255.107.28	TCP	54	80 → 11821
32352	18	210.5.107.92	192.168.1.16	TCP	174	11823 → 8
32353	18	192.168.1.16	210.5.107.92	TCP	54	80 → 11821
32354	18	223.195.222.160	192.168.1.16	TCP	174	11824 → 8
32355	18	192.168.1.16	223.195.222.160	TCP	54	80 → 11821
32356	18	143.148.180.178	192.168.1.16	TCP	174	11825 → 8
32357	18	192.168.1.16	143.148.180.178	TCP	54	80 → 11821
32358	18	201.156.65.56	192.168.1.16	TCP	174	11827 → 8
32359	18	192.168.1.16	201.156.65.56	TCP	54	80 → 11821
32360	18	6.106.132.163	192.168.1.16	TCP	174	11828 → 8
32361	18	192.168.1.16	6.106.132.163	TCP	54	80 → 11821
32362	18	2.201.60.53	192.168.1.16	TCP	174	11829 → 8

Fig. 3.14 Snip of Wireshark tool when TCP flooding is going on in experiment

3.3.5 Data Segregation and ML model building

3.3.5.1 Data Collection

As the attack continues it was continuously analyzed using the Network tool called as Wireshark. So every attack TCP, UDP or ping of death is attacked and there all packets information is continuously sniffed using the wireshark. For each attack I have taken out data from Wireshark as CSV file. And then I preprocess the data and then merged this data and collectively formed a single CSV file with all the data.

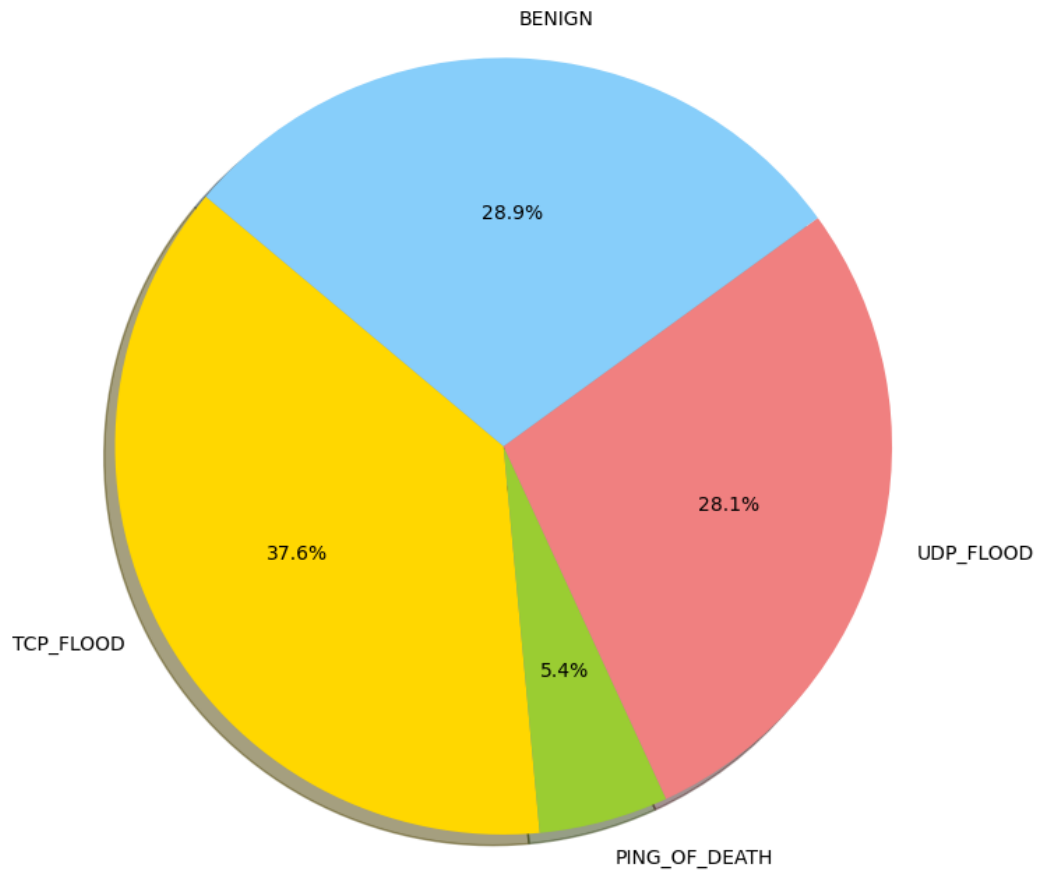


Fig. 3.15 Distribution of data

3.3.5.2 Machine Learning Models

This project have used various types of ML models in order to predict the attack. As this project involves 3 types of attack so there are four classes which are used for classification purpose namely TCP_FLOOD, UDP_FLOOD, BENIGN, PING_OF_DEATH. So following classifier are used:

3.3.5.2.1 Logistic Regression

It is a supervised machine learning algorithm used to classify the data on the basis of either one or multiple independent features. And predicting the dependent value. If only

one independent feature is there then it is called as logistic regression and if there are more than one independent features then it is called as multiple regression.

3.3.5.2.2 Decision Tree Classifier

This is supervised learning algorithm for classification. With the help of this model we can predict class of target variable by learning rules which can be derived from previous data. We start from root node of tree then we start splitting the data downwards till it reaches to leaf node having single value.

3.3.5.2.3 Naïve Bayes Classifier

It is a classification technique based on Bayes' Theorem. In simple terms, a Naive Bayes classifier assumes that the presence of a particular feature in a class is unrelated to the presence of any other feature. It is very useful model for prediction and it is very useful when dataset is very large.

3.3.5.2.4 K-Nearest Neighbor Classifier

K-Nearest Neighbor is a supervised machine learning algorithm. It is used for solving the classification problems. The number of nearest neighbor to an unknown variable is what we termed as K in this. Generally its value is taken as odd only. It is basically a distance based approach which focuses on classifying a class on the basis of distance as a class with similar attributes are generally close to each other.

3.3.5.2.5 XGBoost Classifier

The XGBoost which is called as Extreme Gradient Boosting is the machine learning algorithm which uses concept of boosting to implement. This algorithm provides parallel tree boosting technique and can be used for regression, classification. This algorithm outperform other ML algorithm like Logistic Regression, decision tree, SVM etc.

3.4 OPTIMIZATION

In order to increase the accuracy and also to reduce the space and time complexity we have used feature extraction techniques. In this experiment after applying machine learning model we have calculated accuracy then we have used statistical filter selection

algorithm for categorical classification. We have used information gain for selecting our features. The feature scores of all the features can be seen in Fig. 3.16. Out of all the features we have selected features which are having feature scores greater than 0.15. So at last 13 features have been selected. And using these extracted features machine learning models are again trained and tested and then their accuracies have been calculated.

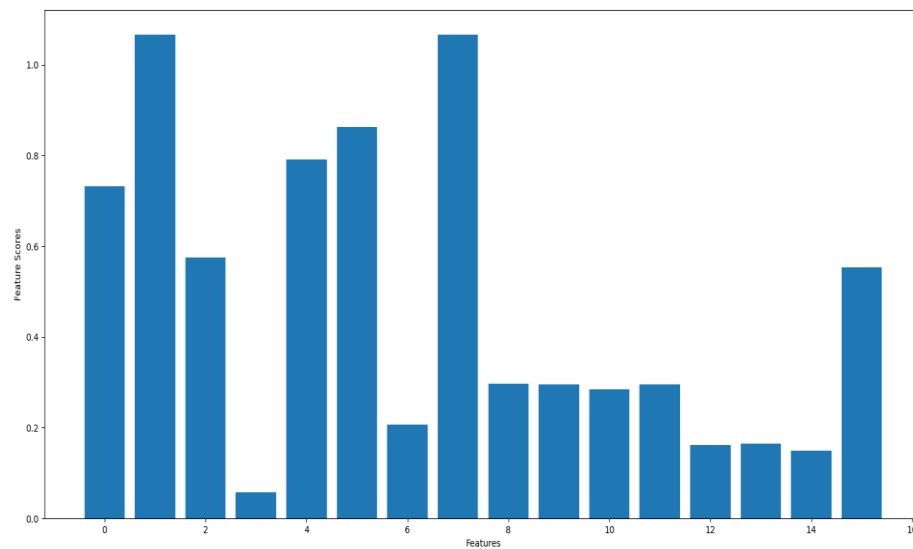


Fig. 3.16 Graphical distribution of feature scores with respect to features

CHAPTER 4

RESULT

4.1 PERFORMANCE EVALUATION

The performance of the machine learning models have been calculated using various metrics like accuracy of model, confusion matrix, ROC and F-score of the models. As we have applied the optimization on the machine learning models so the accuracies and the other performance evaluation metrics can be compared. The model accuracy and confusion matrix, AUC-ROC and F-Score evaluation is done before applying feature extraction methods as well as after the feature extraction.

4.1.1 Accuracy of the Machine Learning Models

Accuracy of classifier can be calculated using True Positive, True Negative and Total of all he dataset.

$$Accuracy = \frac{True\ Positive\ (TP) + True\ Negative\ (TN)}{Total}$$

We can see in Table 4.1 the accuracy of machine learning models before feature extraction is applied and the accuracy of machine learning models after the features are extracted in Table 4.2. We can observe that the accuracy of the models have been improved. And also as the features are extracted so its space and time complexity have been improved.

Serial No.	Model	Accuracy
1	Logistic Regression	0.954
2	Decision Tree Classifier	1.0
3	Naive Bayes Classifier	0.5365
4	K-Nearest Neighbor	0.9842
5	XGBoost Classifier	1.0

Table 4.1 Accuracy of models before feature extraction techniques are applied

Serial No.	Model	Accuracy
1	Logistic Regression	0.9707
2	Decision Tree Classifier	1.0
3	Naive Bayes Classifier	0.5105
4	K-Nearest Neighbor	0.9863
5	XGBoost Classifier	1.0

Table 4.2 Accuracy of models after feature extraction techniques are applied

We can see the improved accuracies by comparing the aforementioned accuracies tables. But there are other parameters as well which can be helpful in knowing the performance of the machine learning models.

4.1.2 Confusion Matrix

Confusion matrix is one of the important performance evaluation parameter for different machine learning classifiers. Classification accuracy alone cannot be a good parameter for performance evaluation in the cases if the dataset have more than two classes. So we need other parameter like confusion matrix. The confusion matrix have following terms which are used to get the information for ML model performance.

True Positive (TP): These are the cases which we have predicted correct as yes and they are yes.

True Negative (TN): These are the cases which we have predicted correct as no and they are no.

False Positive (FP): These are the cases which we have predicted incorrect as yes but they are no.

False Negative (FN): These are the cases which we have predicted incorrect as no but they are yes.

The confusion matrix for all the machine learning models applied before and after the feature selection algorithm have been applied can be seen from figures 4.1 to 4.10. And from the matrix we can observe that all the machine learning models are performing

well except the Naïve Bayes machine learning model which has accuracy also below 80%.

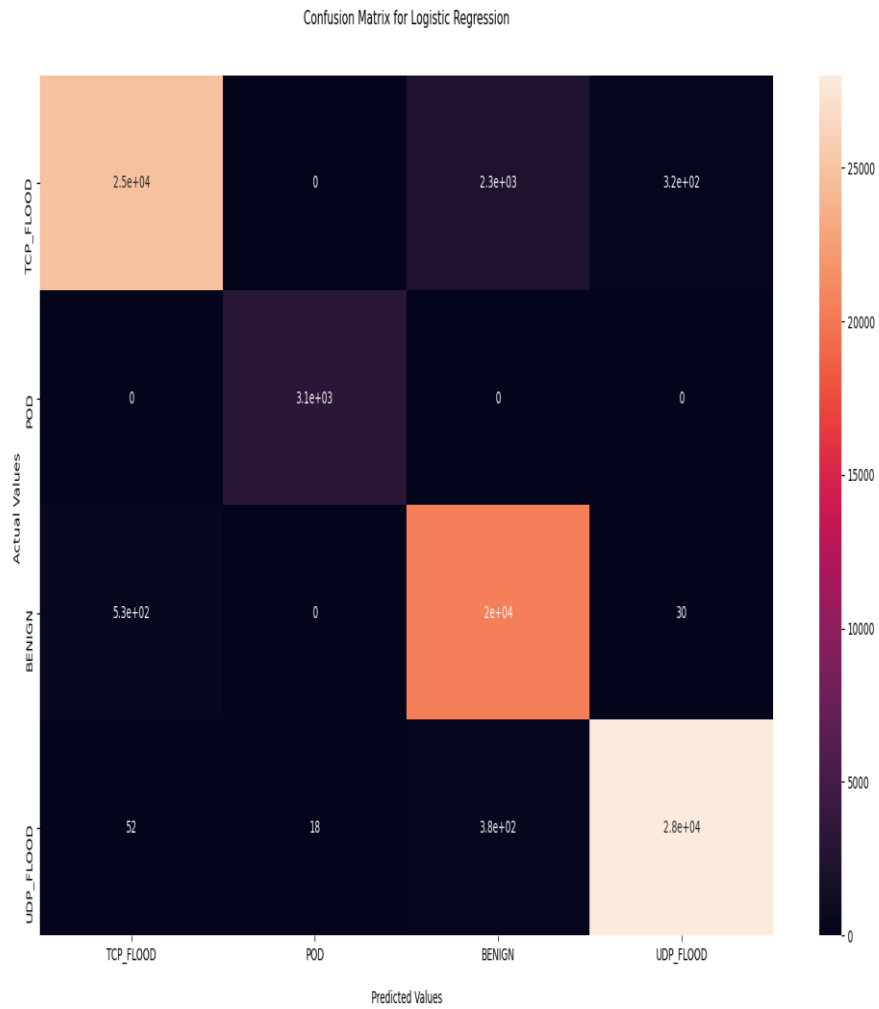


Fig. 4.1 Confusion Matrix for Logistic Regression before feature selection

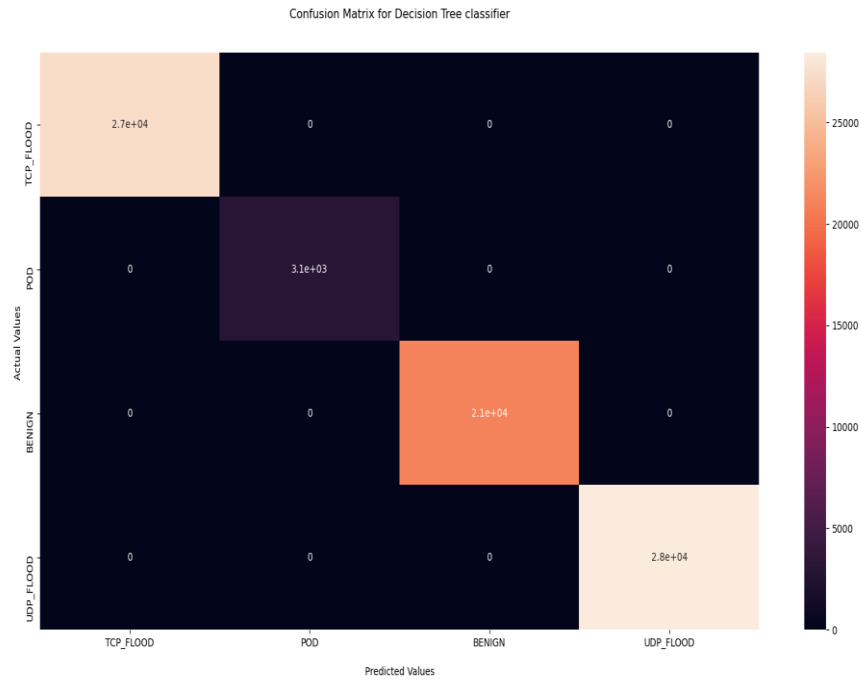


Fig. 4.2 Confusion Matrix for Decision Tree before feature selection

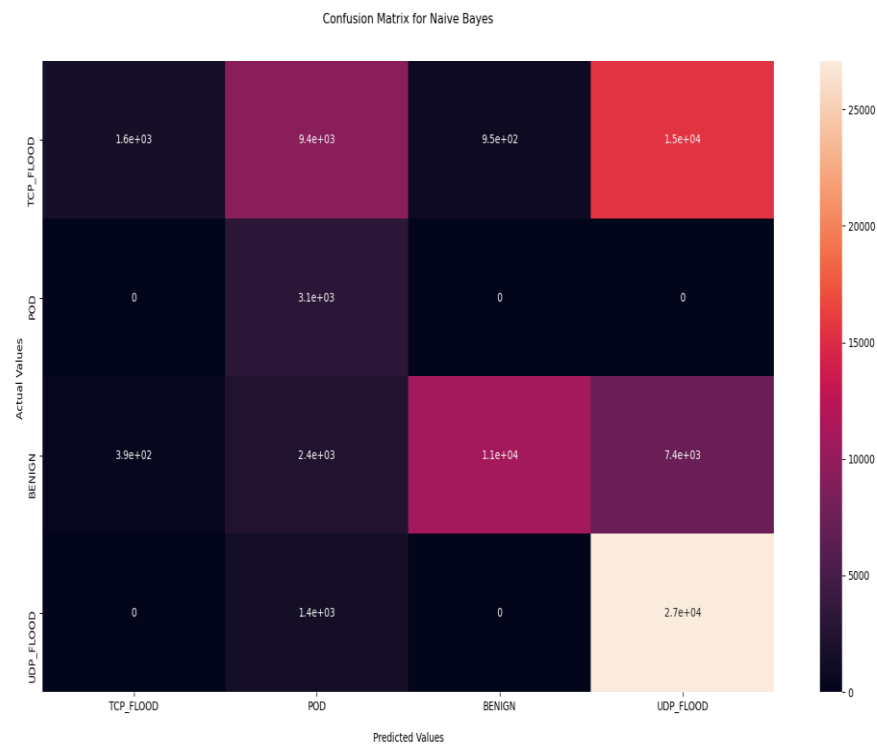


Fig. 4.3 Confusion Matrix for Naïve Bayes before feature selection

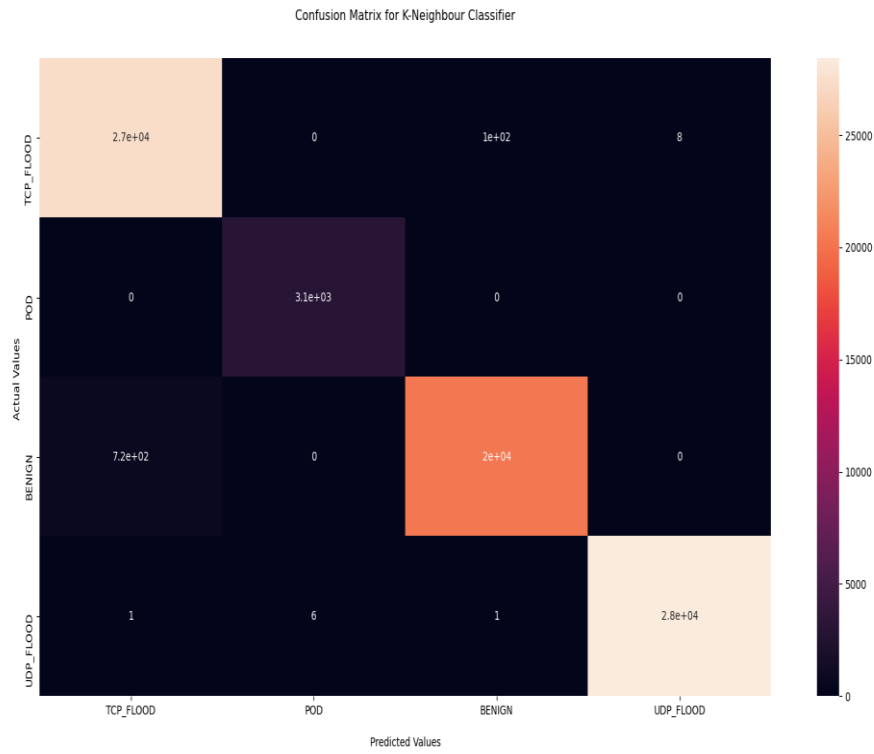


Fig. 4.4 Confusion Matrix for K-Nearest Neighbor before feature selection

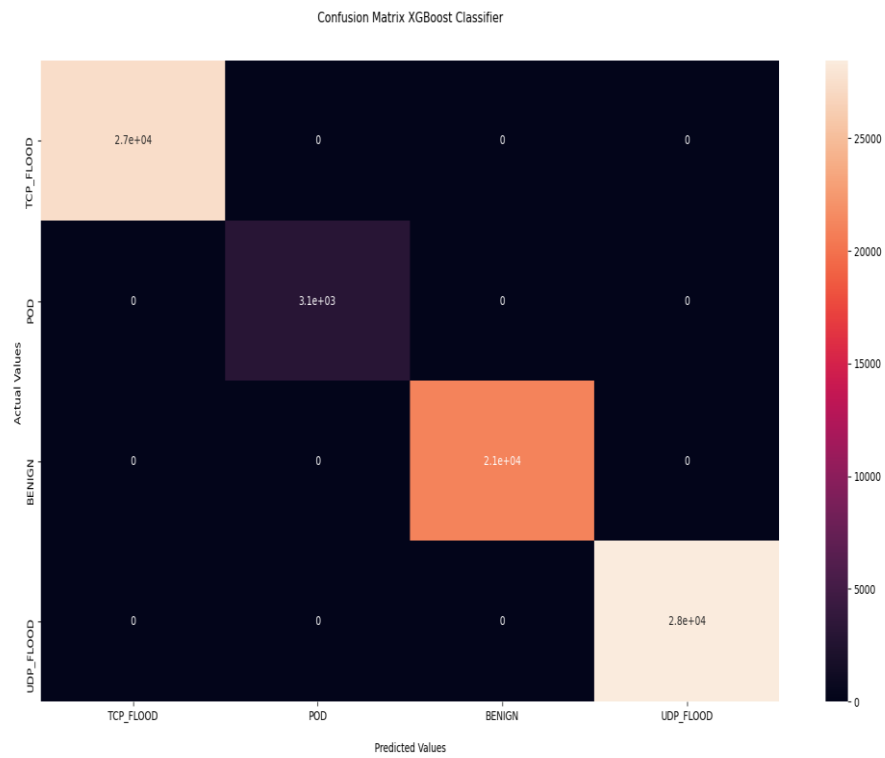


Fig. 4.5 Confusion Matrix for XGBoost before feature selection

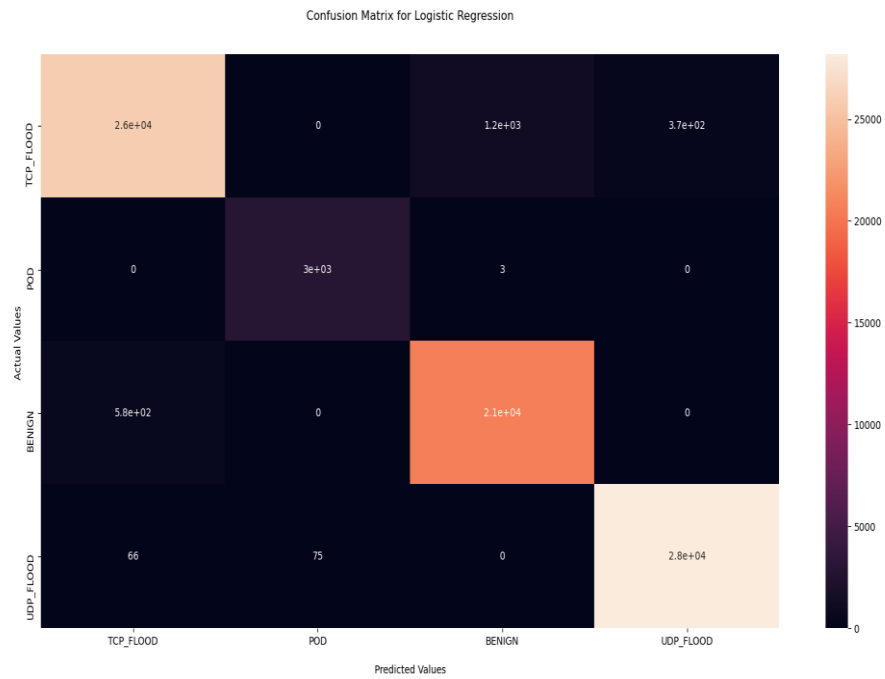


Fig. 4.6 Confusion Matrix for Logistic Regression after feature selection

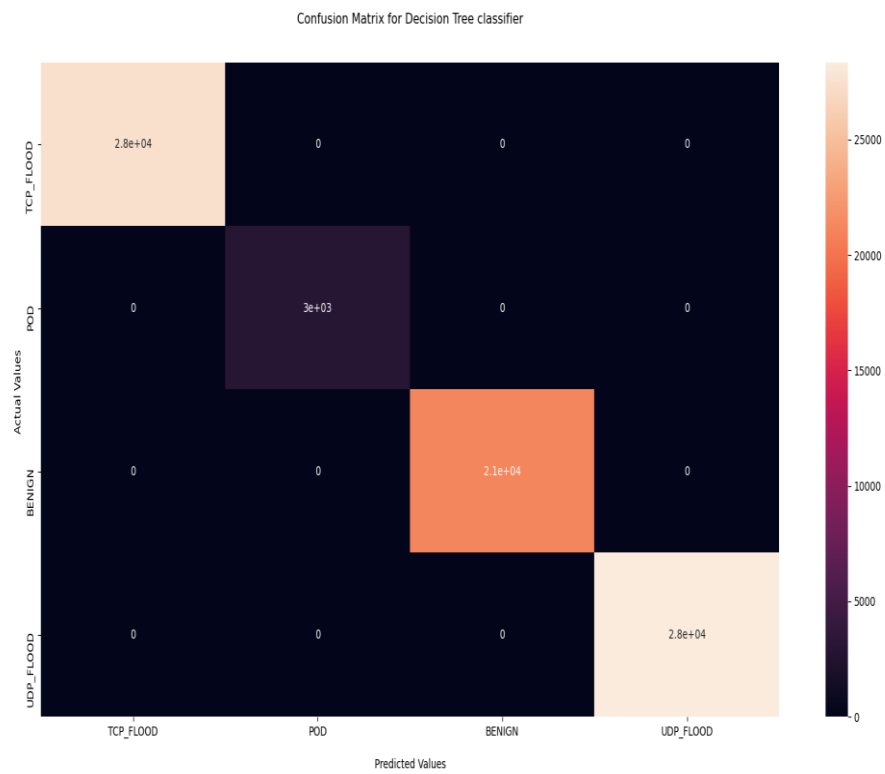


Fig. 4.7 Confusion Matrix for Decision Tree after feature selection

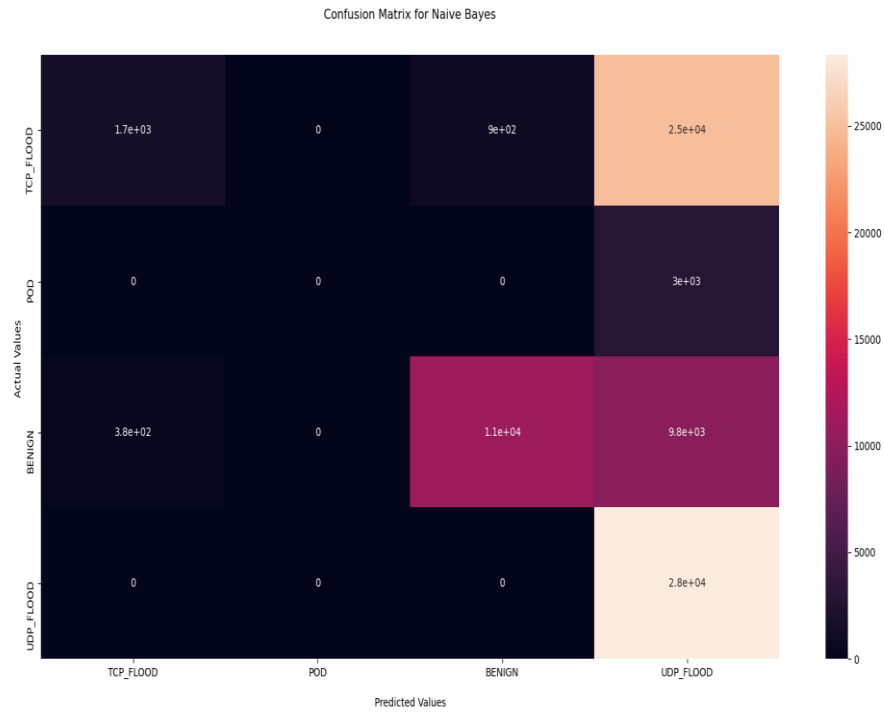


Fig. 4.8 Confusion Matrix for Naïve Bayes after feature selection

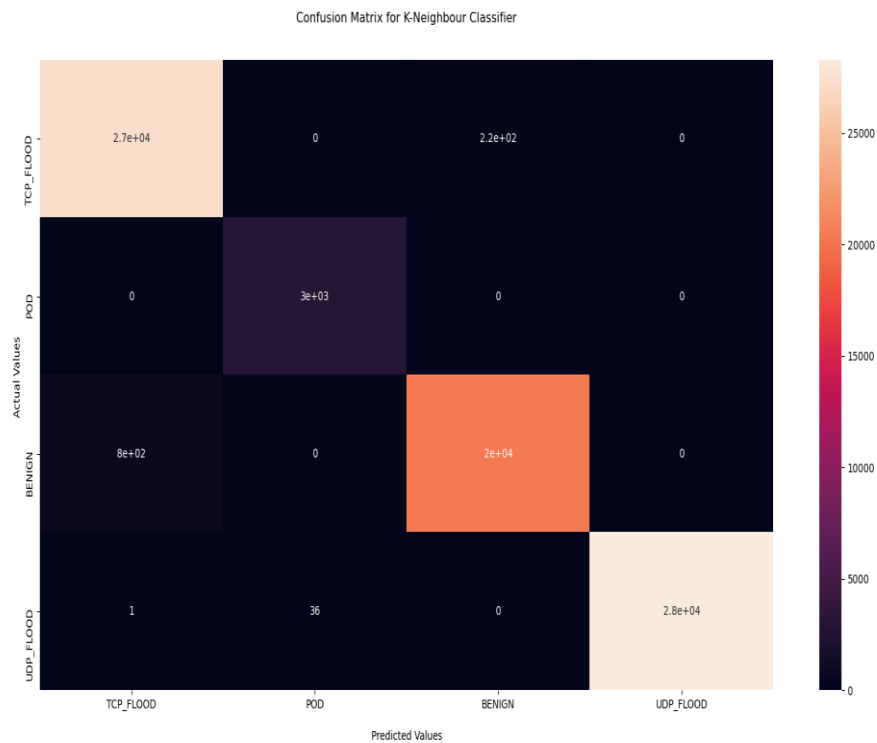


Fig. 4.9 Confusion Matrix for K-Nearest Neighbor after feature selection

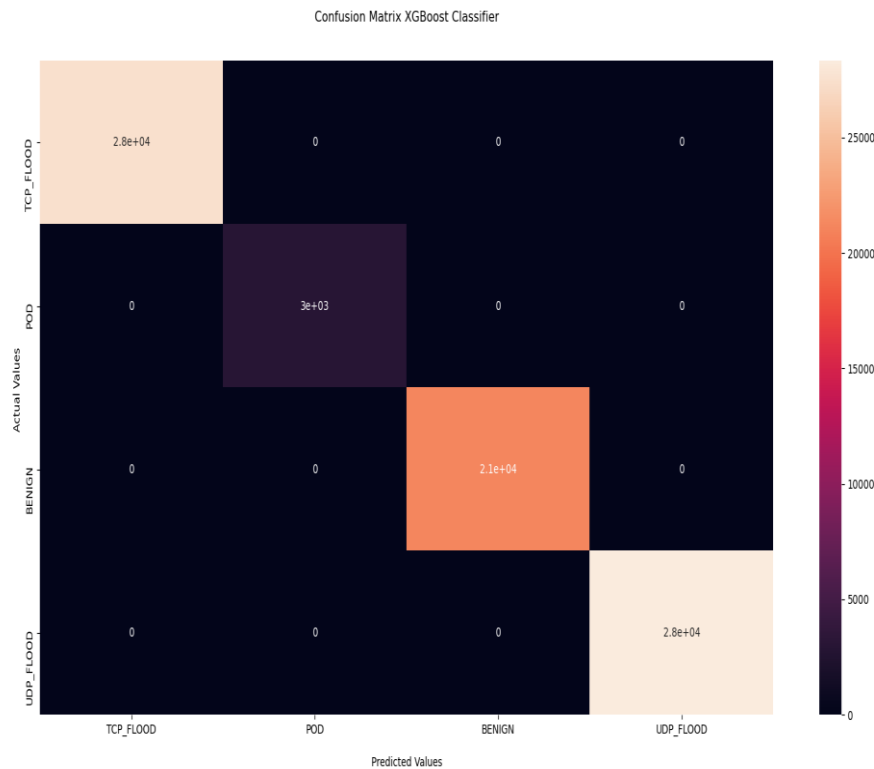


Fig. 4.10 Confusion Matrix for XGBoost after feature selection

4.1.3 AUC-ROC Curve

The Receiver Operator Characteristic (ROC) curve is a performance evaluation parameter for classification which plots the True Positive Rate (TPR) against False Positive Rate (FPR) for different threshold values. The Area Under Curve (AUC) is a parameter to tell how well classifier can distinguish different classes. When the value of AUC is 1 it means the classifier is completely able to distinguish between positive and negative classes, when its value is 0 the classifier is just opposite and it will distinguish all positive as negative and all negative as positive. And when its value is between 0.5 and 1 it will be able to distinguish positive class value from negative class values.

The AUC-ROC curves have been plotted for all the machine learning models before and after the feature selection algorithm have been applied. And we can observe the ROC curve for all models in figures having number from 4.11 to 4.20. And all the curve shows that all our model have been performing well.

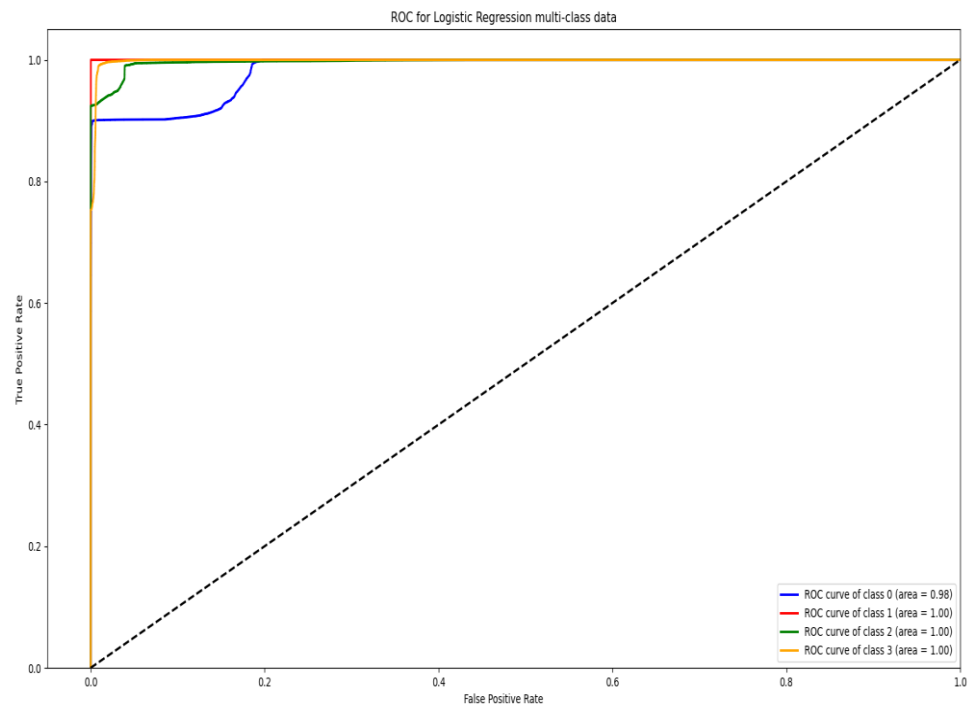


Fig. 4.11 AUC-ROC Curve for Logistic Regression before feature selection

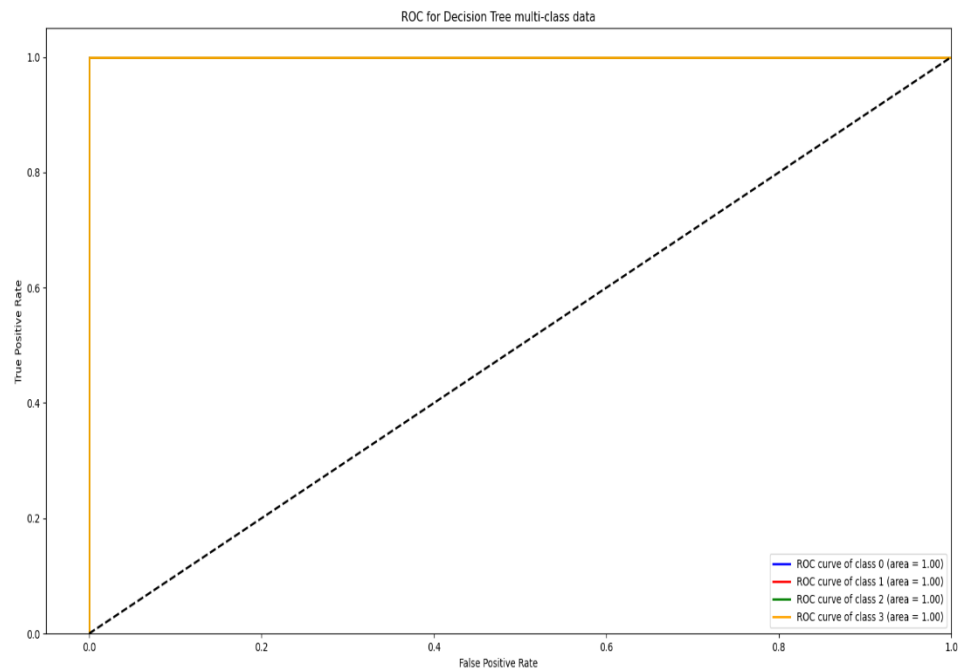


Fig. 4.12 AUC-ROC Curve for Decision Tree before feature selection

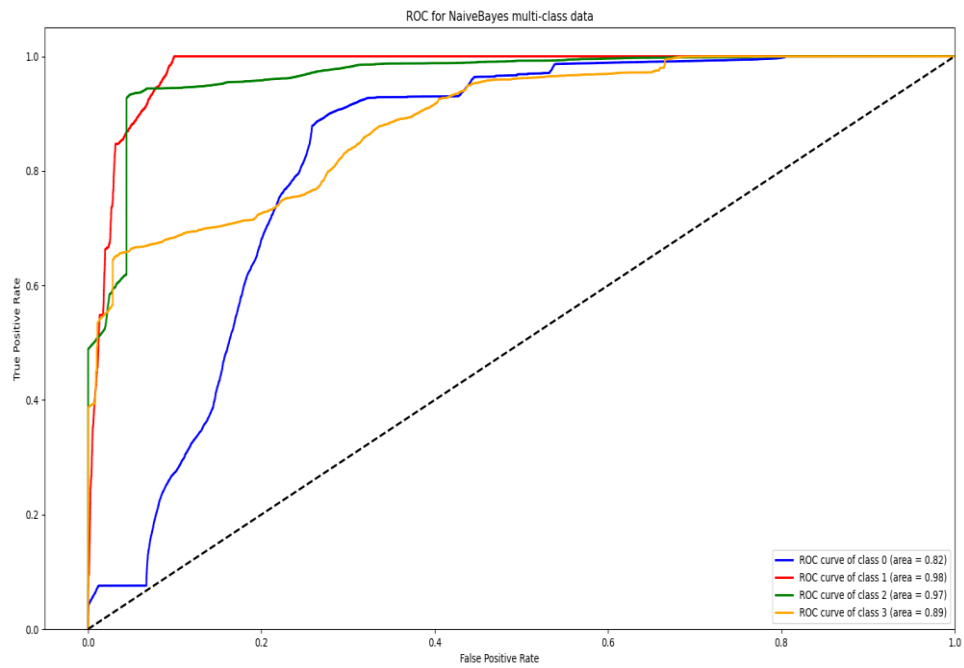


Fig. 4.13 AUC-ROC Curve for Naïve Bayes before feature selection

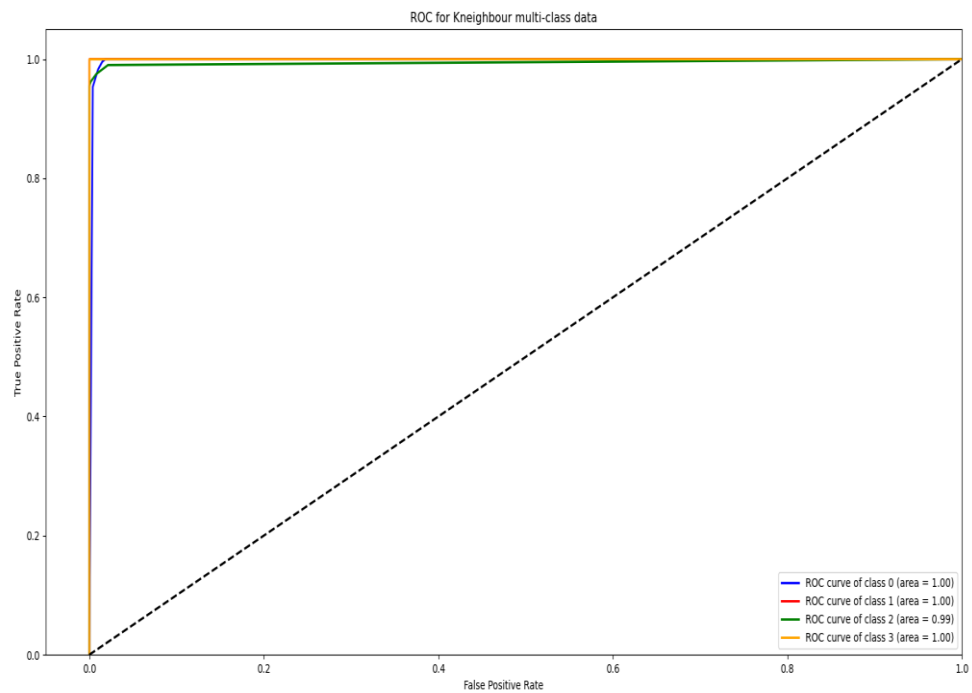


Fig. 4.14 AUC-ROC Curve for K-Nearest Neighbor before feature selection

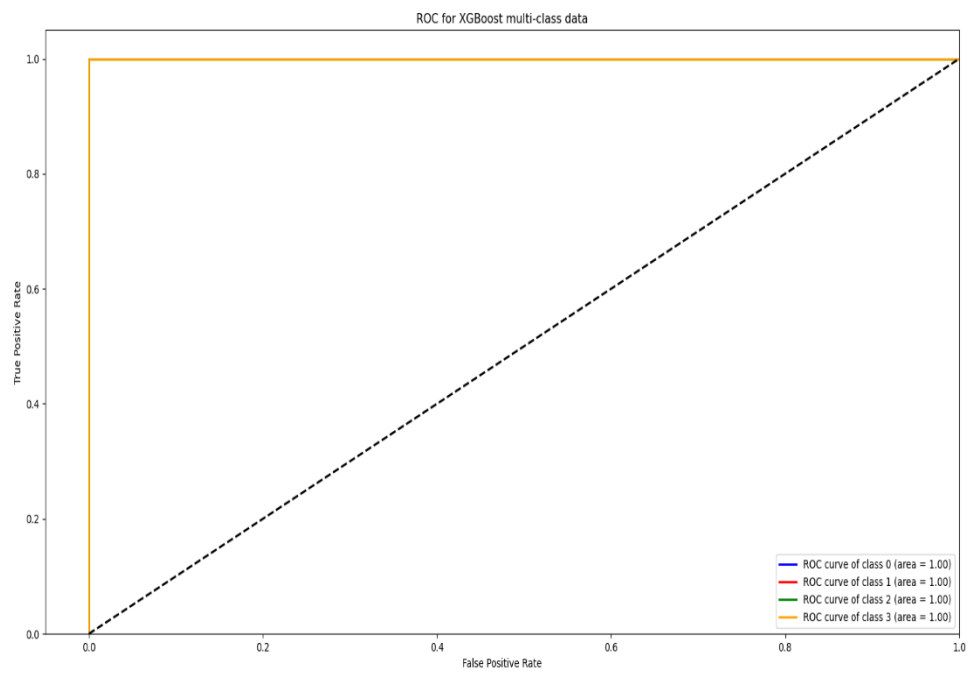


Fig. 4.15 AUC-ROC Curve for XGBoost before feature selection

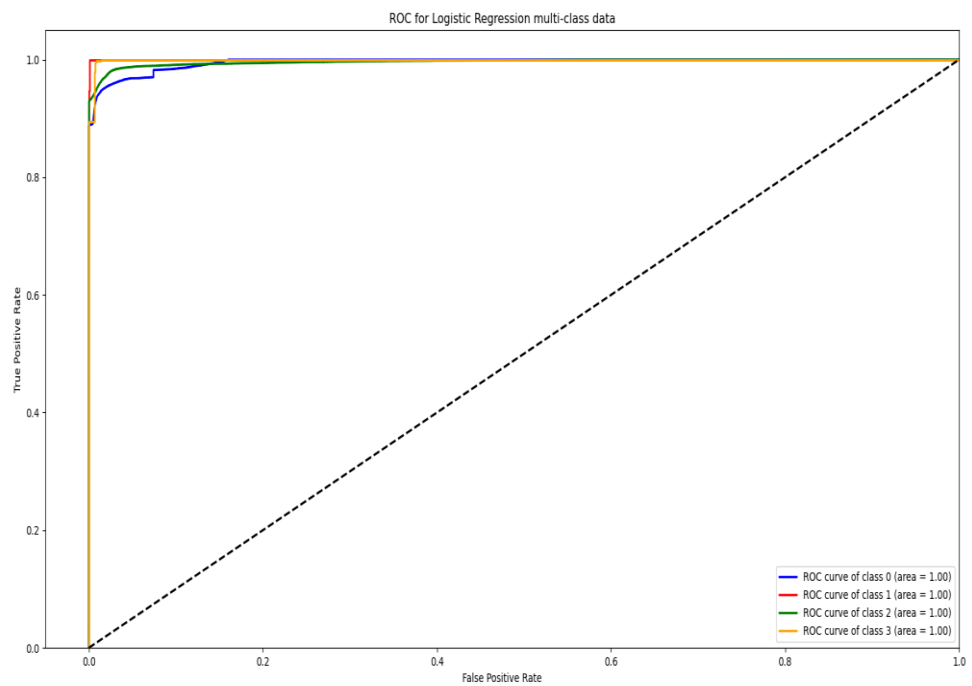


Fig. 4.16 AUC-ROC Curve for Logistic Regression after feature selection

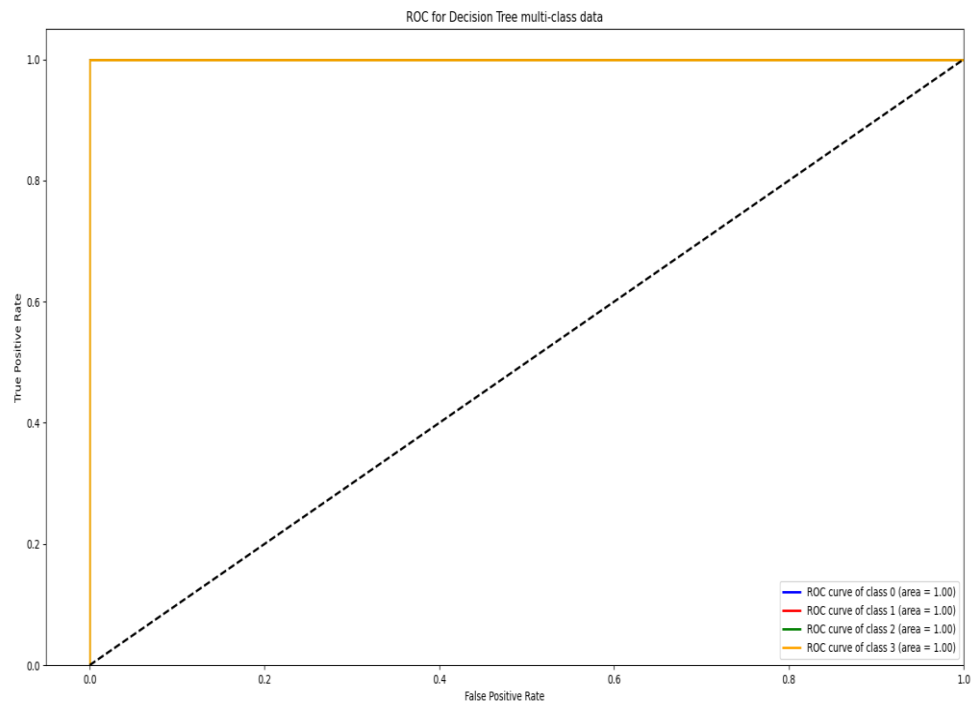


Fig. 4.17 AUC-ROC Curve for Decision Tree after feature selection

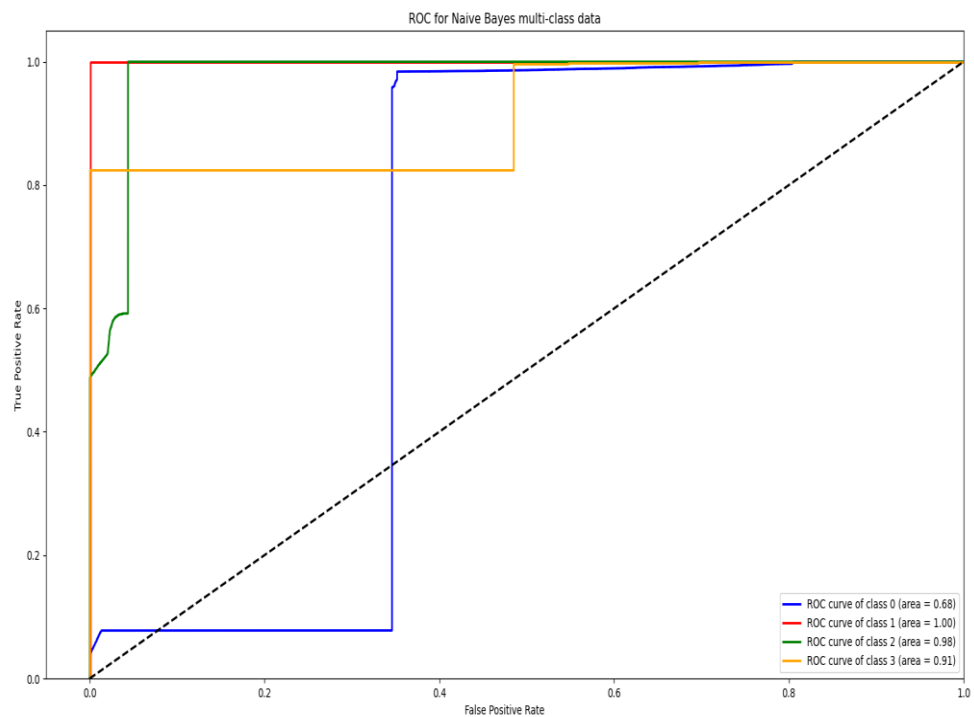


Fig. 4.18 AUC-ROC Curve for Naïve Bayes after feature selection

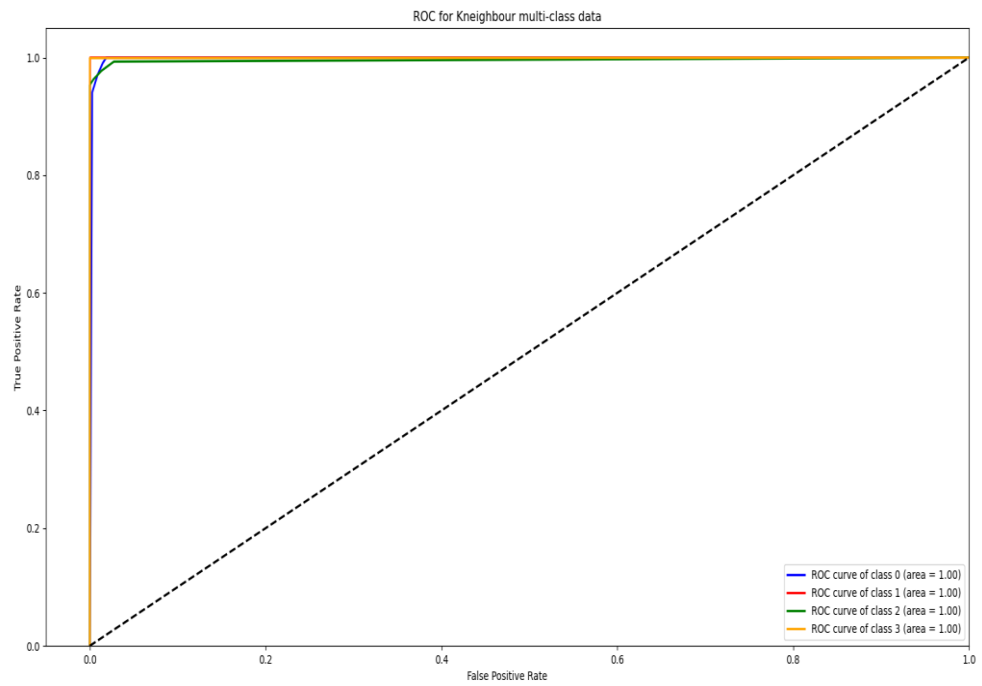


Fig. 4.19 AUC-ROC Curve for K-Nearest Neighbor after feature selection

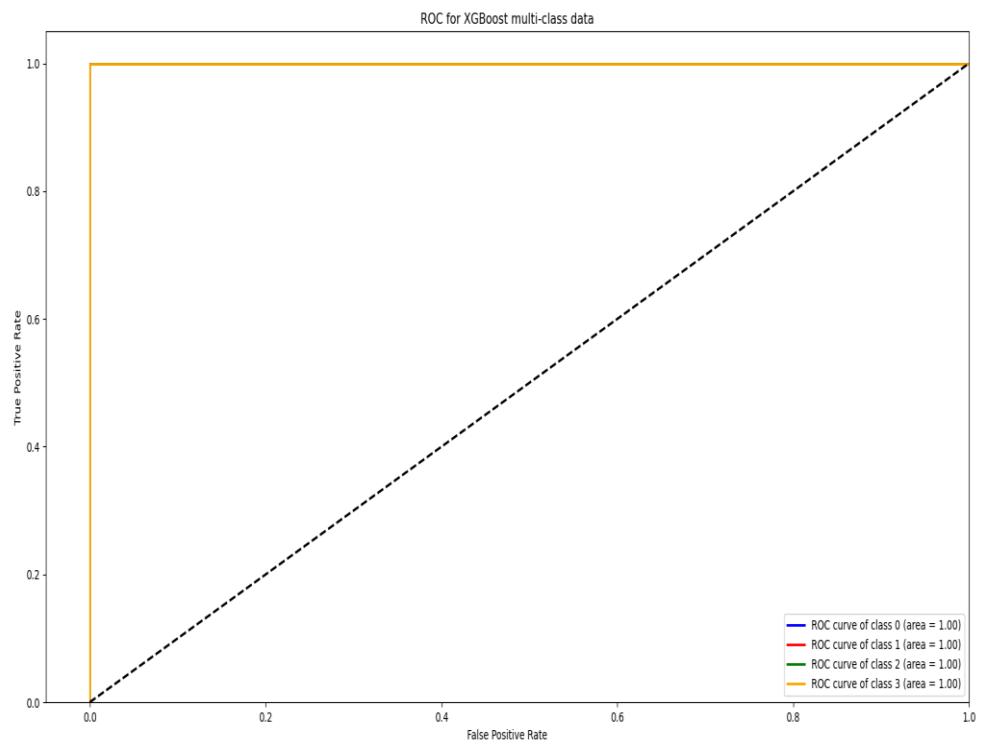


Fig. 4.20 AUC-ROC Curve for XGBoost after feature selection

4.1.4 Precision, Recall and F-Score

Precision is performance metric that calculates the number of correct positive prediction made by machine learning models. For multiclass classification problems it is calculated as total sum of all the positive classes divided by the total of true positives and false positive for all the different classes.

$$Precision = \frac{\text{Sum of all the true Positive}}{\text{Sum of all true positive} + \text{Sum of all false positive}}$$

Recall is performance metric that calculates number of correct positive prediction made out of total positive predictions that could be made from all the machine learning models. It signifies the missing positive predictions. It is calculated as sum of true positive for all classes divided by total of true positive and false negative for all classes.

$$Recall = \frac{\text{Sum of all True Positive}}{\text{Sum of true positive} + \text{Sum of false negative}}$$

F-Score is used to measure the performance of classifiers. It is the combination of both precision and recall such that it combines the properties of both the parameters. F-score can be calculated as:

$$F - Score = \frac{2 * Precision * Recall}{Precision + Recall}$$

For our dataset the ML models which we have applied we have calculated the Precision, Recall and F-Score for them and all the models have performed well except naïve Bayes model. We can see the table number from 4.3 to 4. 12 for all the values for our models.

Classes	Precision	Recall	F-Score
TCP Class	0.98	0.90	0.94
ICMP Class	0.99	1.00	1.00
UDP Class	0.89	0.97	0.93
Normal Class	0.99	0.98	0.99

Table 4.3 Precision, Recall and F-Score for Logistic Regression before feature extraction

Classes	Precision	Recall	F-Score
TCP Class	1.00	1.00	1.00
ICMP Class	1.00	1.00	1.00
UDP Class	1.00	1.00	1.00
Normal Class	1.00	1.00	1.00

Table 4.4 Precision, Recall and F-Score for Decision Tree before feature extraction

Classes	Precision	Recall	F-Score
TCP Class	0.97	1.00	0.98
ICMP Class	1.00	1.00	1.00
UDP Class	1.00	0.96	0.98
Normal Class	1.00	1.00	1.00

Table 4.5 Precision, Recall and F-Score for K-Nearest Neighbor before feature extraction

Classes	Precision	Recall	F-Score
TCP Class	0.81	0.06	0.11
ICMP Class	0.19	1.00	0.32
UDP Class	0.92	0.52	0.67
Normal Class	0.54	0.95	0.69

Table 4.6 Precision, Recall and F-Score for Naïve Bayes before feature extraction

Classes	Precision	Recall	F-Score
TCP Class	1.00	1.00	1.00
ICMP Class	1.00	1.00	1.00
UDP Class	1.00	1.00	1.00
Normal Class	1.00	1.00	1.00

Table 4.7 Precision, Recall and F-Score for XGBoost before feature extraction

Classes	Precision	Recall	F-Score
TCP Class	0.98	0.94	0.96
ICMP Class	0.99	1.00	0.99
UDP Class	0.94	0.97	0.96
Normal Class	0.99	1.00	0.99

Table 4.8 Precision, Recall and F-Score for Logistic Regression after feature extraction

Classes	Precision	Recall	F-Score
TCP Class	1.00	1.00	1.00
ICMP Class	1.00	1.00	1.00
UDP Class	1.00	1.00	1.00
Normal Class	1.00	1.00	1.00

Table 4.9 Precision, Recall and F-Score for Decision Tree after feature extraction

Classes	Precision	Recall	F-Score
TCP Class	0.97	0.99	0.98
ICMP Class	0.99	1.00	0.99
UDP Class	0.99	0.96	0.97
Normal Class	1.00	1.00	1.00

Table 4.10 Precision, Recall and F-Score for K-Nearest Neighbor after feature extraction

Classes	Precision	Recall	F-Score
TCP Class	0.81	0.06	0.11
ICMP Class	0.02	0.02	0.02
UDP Class	0.92	0.52	0.67
Normal Class	0.43	1.00	0.60

Table 4.11 Precision, Recall and F-Score for Naïve Bayes after feature extraction

Classes	Precision	Recall	F-Score
TCP Class	1.00	1.00	1.00
ICMP Class	1.00	1.00	1.00
UDP Class	1.00	1.00	1.00
Normal Class	1.00	1.00	1.00

Table 4.12 Precision, Recall and F-Score for XGBoost before feature extraction

4.1.5 Graphical Visualization on Victim

We can see from the graphs which are observed during the attack there is sudden rise and fall in the packets as the constant flow is broken due to the attack.

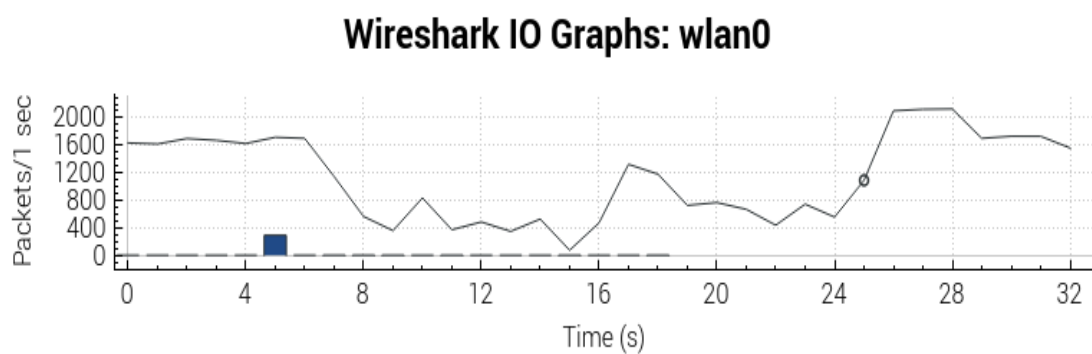


Fig. 4.21 Ping of Death attack packet transmitted graph

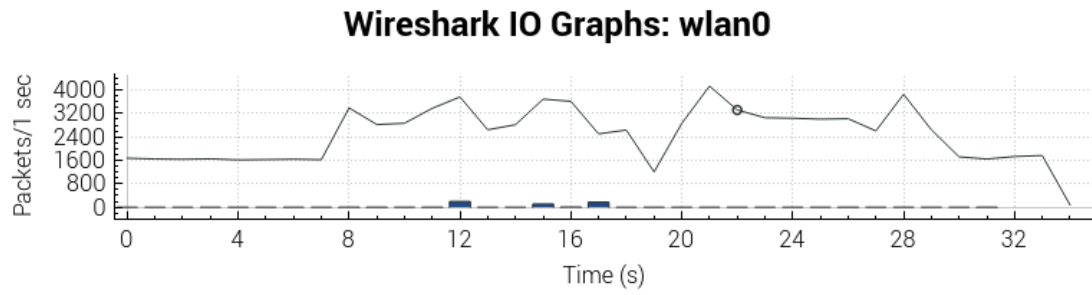


Fig. 4.22 UDP flooding attack packet transmitted graph

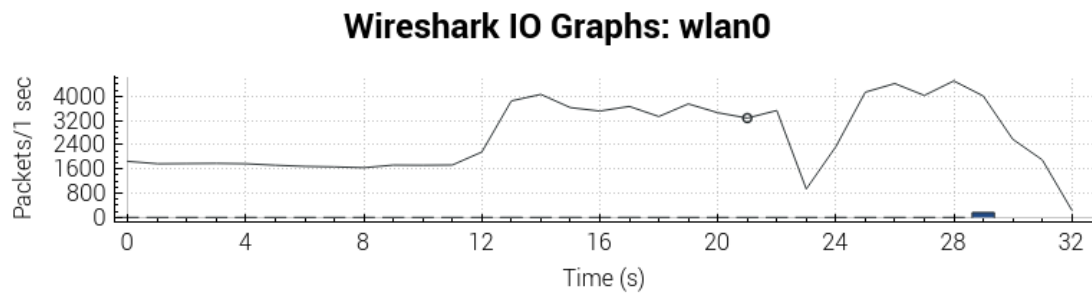


Fig. 4.23 TCP flooding attack packet transmitted graph

CHAPTER 5

CONCLUSION AND FUTURE WORK

Distributed Denial of Service or DDoS attack is one of the most powerful and disastrous attack of cyber world which can put a complete shutdown to network of any institute, organization or even whole region. DoS/DDoS attack are mentioned in various literature with many aspects like cloud, any organization, government etc. But as we know the UAVs are new technology that is evolving and taking a further steps. But these UAVs are very prone to cyber-attacks because of the use of open communication medium which is easily applicable for local drones. The internet used for communication is prone to DDoS attack. So UAV can get attacked by this attack. The machine learning is evolving and promising technique to detect these types of cyber-attacks. With the growth of different machine models it is become stronger in prediction analysis. In this project we have used five different machine learning models and majority of these models have performed very well with good accuracy of more than 95%. The machine learning models if performed in pipeline will be a good detection method for this attack. As the future scope for this project we can make our dataset more refined and can also involve new machine learning and deep learning models for its detection. And this machine learning model can be combined with web application such that it can be like web app which is more user friendly for technical and non-technical users. So it has good scope for improvement in many sectors.

References

- [1] Stein, L. D. "The World Wide Web Security FAQ, version 3.1. 2." [http://www. w3. org/Security/Faq/](http://www.w3.org/Security/Faq/) (2002).
- [2] Abdelmaboud, Abdelzahir. "The Internet of Drones: Requirements, Taxonomy, Recent Advances, and Challenges of Research Trends." *Sensors* 21, no. 17 (2021): 5718.
- [3] Srivastava, A., et al. "A recent survey on DDoS attacks and defense mechanisms." *International Conference on Parallel Distributed Computing Technologies and Applications*. Springer, Berlin, Heidelberg, 2011.
- [4] Asosheh, Abbass, and Naghmeh Ramezani. "A comprehensive taxonomy of DDOS attacks and defense mechanism applying in a smart classification." *WSEAS Transactions on Computers* 7.4 (2008): 281-290.
- [5] Douligeris, Christos, and Aikaterini Mitrokotsa. "DDoS attacks and defense mechanisms: classification and state-of-the-art." *Computer Networks* 44.5 (2004): 643-666.
- [6] Specht, Stephen, and Ruby Lee. "Taxonomies of distributed denial of service networks, attacks, tools and countermeasures." *CEL2003-03, Princeton University, Princeton, NJ, USA* (2003).
- [7] Yahuza, Muktar, Mohd Yamani Idna Idris, Ismail Bin Ahmedy, Ainuddin Wahid Abdul Wahab, Tarak Nandy, Noorzaily Mohamed Noor, and Abubakar Bala. "Internet of drones security and privacy issues: Taxonomy and open challenges." *IEEE Access* 9 (2021): 57243-57270.
- [8] Li, Lan, and Gyungho Lee. "DDoS attack detection and wavelets." *Telecommunication Systems* 28.3-4 (2005): 435-451.
- [9] Jin, Shuyuan, and Daniel S. Yeung. "A covariance analysis model for DDoS attack detection." *2004 IEEE International Conference on Communications (IEEE Cat. No. 04CH37577)*. Vol. 4. IEEE, 2004.
- [10] Bhuyan, Monowar H., D. K. Bhattacharyya, and Jugal K. Kalita. "An empirical evaluation of information metrics for low-rate and high-rate DDoS attack detection." *Pattern Recognition Letters* 51 (2015): 1-7.

- [11] Doshi, Rohan, Noah Apthorpe, and Nick Feamster. "Machine learning ddos detection for consumer internet of things devices." *2018 IEEE Security and Privacy Workshops (SPW)*. IEEE, 2018.
- [12] Bouyeddou, Benamar, et al. "DDoS-attacks detection using an efficient measurement-based statistical mechanism." *Engineering Science and Technology, an International Journal* (2020).
- [13] Shiaeles, Stavros N., et al. "Real time DDoS detection using fuzzy estimators." *computers & security* 31.6 (2012): 782-790.
- [14] Khan, Inam Ullah, Arsin Abdollahi, Muhammad Asghar Khan, Irfan Uddin, and Insaf Ullah. "Securing Against DoS/DDoS Attacks in Internet of Flying Things using Experience-based Deep Learning Algorithm." (2021).
- [15] Shrestha, Rakesh, Atefeh Omidkar, Sajjad Ahmadi Roudi, Robert Abbas, and Shiho Kim. "Machine-learning-enabled intrusion detection system for cellular connected UAV networks." *Electronics* 10, no. 13 (2021): 1549.
- [16] Yazdinejad, Abbas, Reza M. Parizi, Ali Dehghantanha, Hadis Karimipour, Gautam Srivastava, and Mohammed Aledhari. "Enabling drones in the internet of things with decentralized blockchain-based security." *IEEE Internet of Things Journal* 8, no. 8 (2020): 6406-6415.
- [17] He, Daojing, Sammy Chan, and Mohsen Guizani. "Communication security of unmanned aerial vehicles." *IEEE Wireless Communications* 24, no. 4 (2016): 134-139.
- [18] Vasconcelos, Gabriel, et al. "Evaluation of dos attacks on commercial wi-fi-based uavs." *International Journal of Communication Networks and Information Security* 11.1 (2019): 212-223.
- [19] Sahi, Aqeel, et al. "An efficient DDoS TCP flood attack detection and prevention system in a cloud environment." *IEEE Access* 5 (2017): 6036-6048.
- [20] Nagpal, Bharti, et al. "DDoS tools: Classification, analysis and comparison." *2015 2nd International Conference on Computing for Sustainable Global Development (INDIACom)*. IEEE, 2015.
- [21] Bogdanoski, Mitko, Tomislav Suminoski, and Aleksandar Risteski. "Analysis of the SYN flood DoS attack." *International Journal of Computer Network and Information Security (IJCNIS)* 5.8 (2013): 1-11.