Republic of Iraq

Ministry of Higher Education and Scientific Research

University of Babylon

College of Information Technology

Department of Information Networks

DDOS Attack Detection and Mitigation in Wireless Network Based on Maximum Data Rate

A Thesis

Submitted to the Council of the College of Information Technology for Postgraduate Studies of the University of Babylon in Partial Fulfillment of the Requirements for the Degree of Master in Information Technology - Information Networks

By

Noor Hassanin Hashim Tarish

Supervised by

Prof.Dr. Sattar B. Sadkhan

2023 A.D **1444 A.H**

بسم الله الرحمن الرحيم

﴿وَفَوْقَ كُلِّ ذِي عِلْمٍ عَلِيمٌ﴾

صدق الله العلي العظيم

سورة يوسف: اية ٧٦

Supervisor Certification

I certify that this thesis was prepared under my supervision at the Department of Information Networks / College of Information Technology / University of Babylon, **Noor Hassanin Hashim Tarish** as a partial fulfillment of the requirements for the degree of **Master in Information Technology**.

Signature:

Name:**Dr. Sattar B. Sadkhan**

Title: **Professor**

Date: / / 2023

The Head of the Department Certification

In view of the available recommendation, we forward this thesis for debate by the examining committee.

Signature:

Name:**Dr. Saad Talib Hasson**

Title: **Professor**

Date: / / 2023

Certification Of The Examination Committee

We, the undersigned, certify that (**Noor Hassanin Hashim Tarish**) candidate for the degree of Master in Information Technology - Information Networks, has presented his thesis of the following title (**DDoS Attack Detection and Mitigation in Wireless Network based on Maximum Data Rate**) as it appears on the title page and front cover of the thesis that the said thesis is acceptable in form and content and displays a satisfactory knowledge of the field of study as demonstrated by the candidate through an oral examination held on: (2023).

Signature:
Name: Bayan Mahdi Sabbar
Title: Prof. Dr.
Date: / / 2023
(**Chairman**)

Signature:
Name: Nawfal Turki Obeis
Title: Asst. Prof. Dr.
Date: / / 2023
(**Member**)

Signature:
Name: Aladdin Abbas Abdulhassan Al-sharifi
Title: Asst. Prof. Dr.
Date: / / 2023
(**Member**)

Signature:
Name: Sattar B. Sadkhan
Title: Prof. Dr.
Date: / / 2023
(**Member and Supervisor**)

Approved by the Dean of the College of Information Technology, University of Babylon.

Signature:
Name: Hussein Atiyah. Lafta
Title: Professor
Date: / / 2022
(**Dean of Collage of Information Technology**)

Declaration

Hereby declare that this dissertation entitled " **DDOS Attack Detection and Mitigation in Wireless Network Based on Maximum Data Rate** ", submitted to University of Babylon in partial fulfillment of requirements for the degree of Master in Information Technology \ Information Networks, has not been submitted as an exercise for a similar degree at any other University. I also certify that this work described here is entirely my own except for experts and summaries whose source are appropriately cited in the references.

Signature:

Name: **Noor Hassanin Hashim Tarish**

Date: / / 2023

Declaration Associated with This Thesis

(First Paper)

- **Name of journal /conference:** 3rd International Conference on Information Technology to enhance E-Learning and other Application.
- **Paper title: DDOS Attack Detection in Wireless Network Based on MDR**
- **Publication:** IEEE Xplore
- **Authors:**
  Noor Hassanin Hashim
  Sattar B. Sadkhan

Information Networks Department, College of Information Technology, Babylon University.

(Second Paper)

- **Name of journal /conference**: 5th International Conference on Engineering Technology and its Applications (IICETA).
- **Paper title: Information Theory Based Evaluation Method For Wireless IDS: Status, Open Problem And Future Trends**
- **Publication:** IEEE Xplore
- **Authors:**
  Noor Hassanin Hashim
  Sattar B. Sadkhan

Information Networks Department, College of Information Technology, Babylon University.

Dedication

To the last of prophets our, master Mohammed (God prays on him and his special family).

To my Imam (Al-Imam Al-Mahdi) God hasten his victory and release.

To my **dear father**, my biggest hero

To **my dear mother,** may God prolong her life

To those who encouraged me to continue my scientific career,

my **husband Dr. Karrar Salih**

and to **my sisters and my daughter Asawr** (the lights of my life)

To all **my family members** who were the best support and encouragement

And to **everyone** who encouraged and helped me complete this work.

Acknowledgments

I thank God Almighty and praise Him, for He is the Most Gracious and Most Merciful above all else. I thank Him for achieving what I aspire to. It enabled me to complete a master's degree in information technology to join the University of Babylon

I extend my great thanks and appreciation to **Prof.Dr. Sattar B. Sadkhan** for his good cooperation, as he provided me with what I needed to him from sources and inquiries and was present step by step in order to complete this study.

Grateful thankfulness and warm gratitude also extend to Information Technology College by its dean, it is head of the Information Networks department, its staff, and all my colleagues for their great potential in learning and encouraging me through my B.S.C and M.S.C studies.

Abstract

Intrusion detection systems (IDS) are the most efficient way of defending against network-based attacks on wireless system devices. These systems are used in almost all large-scale infrastructures components, and they are affected by different types of network attacks such as DDoS attacks.

Distributed Denial of Services (DDoS) attacks launched against several major network devices where security measures were in place, the protocols and systems that are designed to provide services such as servers are inherently subject to DDoS attacks. DDoS attack detection method can be used to protect network systems against DDoS attacks in the early stage of threat, response can be put into place to minimize damages, gather evidence for prosecution, and even launch counter-attacks.

The proposed system is based on an anomaly-based system (ABS) to build a log configuration model describing the normal network traffic as a whitelist, and any abnormal behavior as a blacklist that provides a detection rule against DDoS attacks. It identifies the source IP address, MAC address, and time stamp. The proposed methodology is based on the Maximum Data Rate (MDR) matching approach to matching the max traffic request with stored value to decide the behavior of the traffic as normal and abnormal traffic. Then, deny the abnormal traffic by filtering the model in the IDS firewall-rule based device. The results showed that the proposed method flooding attacks (DDoS attacks). The better results of DDoS detection of 16 nodes are 0.109 drop rate, 89.04% PDR, and throughput of 1778.346 KB.

List of Tables

III

VI

List of Algorithms

List of Abbreviations

Abbreviation	Description
AWGN	Additive white gaussian noise
ARP	Address resolution protocol
AODV	Ad-hoc on demand distance vector
ACC	aggregate congestion control
AIDS	Anomaly intrusion detection system
ANNs	Artificial neural networks
COMSEC	Communication security
DBN	Deep belief networks
DL	Deep learning
DNN	Deep neural networks
DOS	denial of services
DDoS	distributed denial of services
DDOSTB	distributed denial of services testbed
DHCP	Dynamic host configuration protocol
FPR	False positive rate
FEs	Flash events
GA	Genetic algorithm
GB	Gigabyte
HR-DDos	High rate distributed denial of services
ID	information distance
IP	Internet protocol
IPV6	Internet protocol version six
IDES	Intrusion detection expert system
IDS	intrusion detection system
kb	Kilo bytes
LCS	Learning classifier system
LIDS	Linux intrusion detection system

LSTM-RNN	Long short – term memory recurrent neural networks
LR-DDoS	Low rate distributed denial of services
MAC	Media access control
MBPS	Megabit per second
NAT	Network address translation
NIT	Network information theory
NIDS	Network intrusion detection system
PSO	particle swarm optimization
POD	Ping-of-death
PPP	Point-to-point protocol
RAM	Random access memory
ROC	Receiver operating characteristic
LR-DDoS	L IX ıte distributed denial of services
MAC	Media access control
MBPS	Megabit per second
MDR	Maximum Data Rate
NAT	Network address translation
NIT	Network information theory
NIDS	Network intrusion detection system
PSO	particle swarm optimization
POD	Ping-of-death
PPP	Point-to-point protocol
RAM	Random access memory
RAM	Random Access Memory
ROC	Receiver operating characteristic
SIEM	Security information and event management
SSID	Service set identifier
SNR	Signal-to-noise ratio
SRI	Stanford research institute
STA	static timing analysis
TCP/IP	Transmission control protocol / internet protocol
TPR	True positive rate
TIDS	trust intrusion detection system
VLAN	Virtual local area network
VPN	Virtual private network
WAFs	Web application firewalls
WPA	Wi-fi protected access
WLAN	Wireless local area network

Chapter One

General Introduction

1.1 Introduction

Intrusion Detection System (IDS) is a tool that recognizes an attack in the network. It takes immediate steps to evaluate such activities and restore them to normal. Thus, IDS in security is crucial in different wireless network. It can detect traffic as normal or abnormal . IDS will immediately send an alarm. This will help the IT team to take steps for such issues [1]. In addition, there is two types of IDS tools: Host-Based Intrusion Detection System(HBIDS), and Network-Based Intrusion Detection System [2].

The network is the interconnections of a set of devices capable of communicating with each other in a defined area. Several devices must be incorporated in the network classified as data terminal equipment and data communication equipment. There is a channel of communication between these devices categorized as guided channel and unguided channel. Guided channel media is a wired communication it transmits data either using twisted pair cable, coaxial cable or fiber optics; it requires maintenance charge. The unguided channel media is a wireless communication it transmits signal by broadcasting it through the air. Network components scramble for the control of the channel and with big bandwidth, every channel user will be able to transmit information without hustle, In a network several nodes try to get connection for access to a single communication channel and if that channel has a high enough bandwidth all of its users may send and receive data without much difficulty[3].

To avoid the issue of security primitive or objective being violated frequently, a detection criterion needs to be put in place and this is Intrusion Detection System (IDS). There are four major reasons to implement intrusion detection system: First, Current systems have security

flaws that make them exposed to attacks, but the attacks are very difficult to identify and eliminate due to technical and economic reasons. Second, these existing systems with security flaws cannot be replaced by more secure systems because of application and economic considerations (ideally not available). Third, the development of completely secure systems is probably impossible. Fourth, even highly secure systems are vulnerable to misuse by legitimate users (authorized) [4].

In general, the efficient intrusion detection system is based on max data rate, or information theory which provides an intuitive way to filter out the most important features in order to reduce the size of traffic data to be analyzed in real time. The intrusion detection process can be examined from an information-theoretic point of view [5].

The purpose of an IDS is to classify the input correctly as normal or intrusion. That is, the IDS output should faithfully reflect the "truth" about the input (or whether there is an intrusion or not). From an information-theoretic point of view, we should have less uncertainty about the input given the IDS output [6]. We illustrated the intrusion detection system in Figure (1.1) [6].

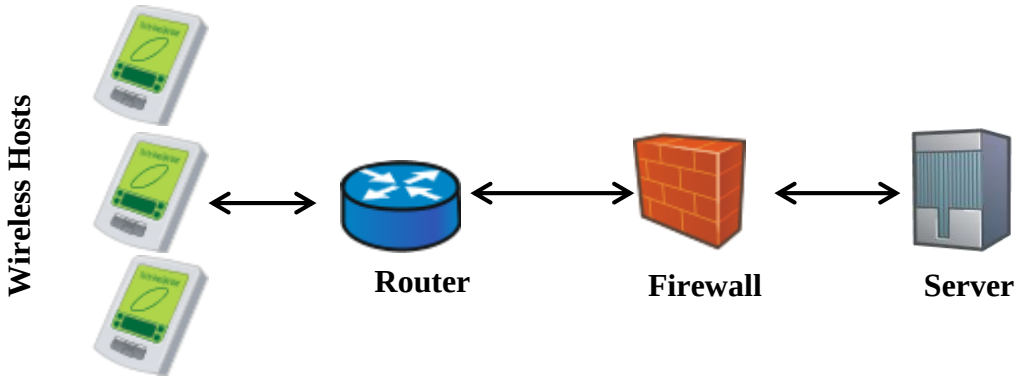


Figure (1.1): intrusion detection system [6]

1.2 Related Works

There are different related works dealt with the intrusion detection system (IDS) in wireless networks and applied to detect and decreased DDoS attack in these networks and the literature survey sorted as follow:

In (Behal, etal,2018), they have proposed a generalized detection system for the collective detection of low rate DDoS (LR-DDoS) and high rate DDoS (HR-DDoS) attacks along with flash events (FEs) for analyzing the behavior and performance of various information theory metrics. Divergence-based metrics produced greater information distance (ID) than entropy-based metrics, which led to the higher true positive rate (TPR) and classification rate of these metrics. ID-based detection systems also outperformed entropy-based detection systems [7].

In (Bala, etal,2019), they proposed a novel system network information based moderation model to identify and alleviate routing attacks. They used time variant snapshots to detect routing attacks. Each node learns network details using the network information theory (NIT) to get the knowledge about the nodes of network, the neighbor locations, energy details, displacement speed from the route discovery packets and reply packets. From the learned details each node constructs the network topology at each time window to perform intrusion detection. The use statistical method for information assessment, to identify interruptions based on the information of client activity deviation in the PC framework from learned profile representing standard user behavior[8].

In (Tang, etal,2020), they investigated the network traffic' characteristics, in which variance and entropy are used to evaluate the TCP traffic's characteristics, and the ratio of UDP traffic to TCP traffic (UTR) is also analyzed. Thus, a detection method combining two-step cluster analysis and UTR analysis is proposed. Through two-step cluster analysis

which is one of the machine learning algorithms, network traffic is divided into multiple clusters and then clusters subjected to LDoS attacks are determined using UTR analysis. NS2 simulation platform and test-bed network environment aim to evaluate the detection approach's performance. To better assess the effectiveness of the method, public dataset WIDE is also utilized. Experimental results with a good performance prove that the proposed detection approach can accurately detect LDoS attacks [9].

In (Riadul, etal,2020), they proposed a four-stage intrusion detection system that used the chi-squared method and can detect any kind of strong and weak cyber attacks in a CAN (controller area network). This work is the first-ever graph-based defense system proposed for the CAN. There experimental results showed that they have a very low 5.26% misclassification for denial of service (DoS) attack, 10% misclassification for fuzzy attack, 4.76% misclassification for replay attack, and no misclassification for spoofing attack. In addition, the proposed methodology exhibits up to 13.73% better accuracy compared to existing ID sequence-based methods. Also results showed it can detect simple impersonate-type attacks; however, it could not detect replay attacks. Analyzed the characteristics of all kinds of CAN monitoring-based attacks and proposed a four-stage (Intrusion Detection System) IDS with the help of graph theory, statistical analysis, and the chi-square method [10].

In (Bouyeddou, etal, 2020), they introduced a reliable detection mechanism based on the continuous ranked probability score (CRPS) statistical metric and exponentially smoothing (ES) scheme for enabling efficient detection of DOS and DDOS attacks. In this regard, the CRPS is used to quantify the dissimilarity between a new observation and the distribution of normal traffic. The ES scheme, which is sensitive in

detecting small changes, is applied to CRPS measurements for anomaly detection. Moreover, in CRPS-ES approach, a nonparametric decision threshold computed via kernel density estimation is used to suitably detect anomalies. Tests on three publically available datasets proclaim the efficiency of the proposed mechanism in detecting cyber-attacks [11].

In (Reza, etal, 2020), they proposed P_Secure approach detection algorithm is that attacks, for detecting DOS attacks used to commit time. This decreases the overhead for processing and securing the VANET is delayed. This approach has better special depending criteria removal rate, throughput, PDR and latency to , Therefore, this work proposes a self-managed VANET without any infrastructure, which will serve as an introduction to a more complex VANET, all this with better levels of security. They also proposed a approach in a vehicle network improves road safety, transport efficiency, but also reduces the impact of transport on the environment; all three of these applications are not perfectly perpendicular to each other. For example, reducing the number of accidents, in turn, can reduce the traffic congestion and this can lead to a reduction of the environmental impact [12].

In (Anand, etal,2021), an efficient trust-based attack detection module is presented to detect denial of service attacks such as selective forwarding and flooding attacks. Multi-dimensional trust parameters are extracted and estimated through the proposed approach to determine the packet forwarding activity from the sensor nodes. The proposed DoS attack detection model performance is verified through simulations and the results validate the better performance in terms of throughput, energy consumption, packet delay, and accuracy. Compared to conventional detection techniques proposed attack detection model outperforms well in all aspects[13].

In (Singh, etal,2021), a protocol is developed that can detect the Wireless Network Attack based on the reference of TCP/IP Model. In the proposed system the new feature is integrated in the IDS which are built in the router itself [14].

In (Pajila, etal, 2022), they aimed to identify the DDoS attack quickly and to recover sensors using the fuzzy logic mechanism. In the Fuzzy based DDoS attack Detection and Recovery mechanism (FBDR) method uses type fuzzy-logic to detect the occurrence of DDoS attack in a node. It is used for recovery DDoS attack. Both approaches used rule perform well in terms of identifying the DDoS attack and recover the DDoS attack. It also helps to reduce the energy consumption of each node and improves the lifetime of the network. The proposed FBDR scheme is compared with other related schemes. The experimental results represent that the FBDR method works better than other similar schemes [15].

There are many proposed enhancement system for DDoS attack detection in wireless network as within the following literature review from the past up to the latest directions:

Table (1.1) illustrates the aim of previous researchers trends and what the simulation tools are used to achieved the works.

Table (1.1): aim of researchers and the used simulation tools

Ref.No., Year	Aims of the work	Simulation tool	Challenges, evaluation metrics, still open problem
[7],2018	Detecting LR-DDoS attacks.	CAIDA dataset and DDoSTB dataset	The problem of discrimination becomes even more crucial and difficult when DDoS attacks are launched during FEs , with detection system evaluation metrics such as false positive rate,

			false negative rate, classification rate, and detection accuracy.
[8],2019	Distinguishing interruptions in versatile ad-hoc network.	NS2 and C++	Problem statement Most of the intrusion detection mechanism uses various metrics which are computed based on traffic flow, geographic information and so on. Still there are problems with the earlier approaches .
[9],2020	Evaluating the TCP traffic's characteristics, and the ratio of UDP traffic to TCP traffic (UTR)	NS2	It's hard to find the public dataset that contains LDoS attacks, build the test-bed including LDoS attacks in real network environment for further verification of the methods
[10],2020	Detecting attacks without any change in the CAN protocol and make it, applicable to any communication system that uses the CAN protocol.	Python language.	The still problem is apply different machine learning algorithms in place of the chi-square test to identify anomalies.
[11],2020	Efficient detection of DOS and DDOS attacks	Measurement and Analysis on the WIDE Internet) dataset	There is no assumption about the normality of data and a more realistic estimation of traffic distribution.

[12],2020	Supplying security and welfare for the travelers.	NS2 Simulation	The common networks problem is security challenges arise because of the unique characteristics of VANET such as high mobility, dynamic topology, short connection duration and frequent disconnections.
[13],2021	Detecting denial of service attacks such as selective forwarding and flooding attacks. Multi-dimensional trust parameters	NS2 Simulator	Providing better synchronization between user and host
[14],2021	Diving the facility to monitor the traffic of network, event or activities on network and finds out any malicious operation if present.	Network simulator (NS 2) and NAM (Network animator).	The mechanism can detect a false node in the network which is major threat in WSNs. Result has been evaluated the performance of IDS protocol by using Ad-hoc On Demand Distance Vector (AODV) Routing Protocol for routing.
[15],2022	Identifying the DDoS attack quickly and to recover sensors using the fuzzy logic mechanism	MATLAB	Dynamic with limited mobility, homogeneous or heterogeneous

1.3 Problem Statement

The proposed system applied to decreased these main problems:

1- How do identify the normal and abnormal traffic to make a decision by the firewall.
2- Attacks issues in the wireless network which effects the network behavior by increasing delay, and lost packets.
3- Increasing data rate traffic in the network due to increase number of wireless host devices.
4- Flooding traffic which effects on the network resources and consumes network resources.
5- How to evaluate intrusion detection system (IDS) traffic in wireless network?

1.4 Aim of study

This study is proposed to enhance the security of wireless network based on intrusion detection system by:

1. Recognizing data traffic using maximum data rate (MDR) as normal data traffic (allow), abnormal data traffic(deny).
2. Determining the maximum data rate to control data traffic in the network.
3. Building a flexibility approach to decrease flooding attack.
4. Increasing network performance with Firewall rule by increasing throughput, packet delivery ratio, and decreasing packet loss rate and delay by detect and prevent malicious users from redirect their traffic to the servers.

1.5 Thesis outline

Furthermore, this thesis contains four chapters in addition to chapter one:

Chapter Two: This chapter presents the introduction , Intrusion detection system architecture , ids layered network , advantage and disadvantage and technique ids algorithms , implementation tool , ids evaluation metrics(network evaluation , ids evaluation) .

Chapter Three: This chapter presents the proposed system and illustrates the practical stages of the system and explains the proposed methodology system.

Chapter Four: This chapter describes the results and evaluates proposed system.

Chapter Five: This chapter presents the results conclusion. Also, it describes future works suggestions.

Chapter two

Theoretical Background of intrusion detection system in wireless network

2.1 Introduction

A network consists of the links between all the devices in a certain region that can exchange data [16]. As with any kind of networked transmission, wireless communications adhere to a set of strict criteria [17]. Performance metrics are used to evaluate networks. Time spent waiting for a reply to an enquiry is called "response time," whereas "transit time" refers to the time it takes for a message to go from sender to receiver [18].

The effectiveness of the network performance is measured in terms of throughput and latency, depends on a number of variables such as the number of users, the media used, the hardware, and the efficiency of the software. However, reliability is quantified by a frequency metric that calls for a security goal or primitive metric. Intrusion Detection Systems are necessary to prevent the frequent occurrence of security primitive or objective violations (IDS)[19].

An Intrusion-Detection Model inspired the creation of the Intrusion Detection Expert System (IDES) at Stanford Research Institute (SRI) [20]. That system identified malicious network activity by using statistical anomaly detection (SAD), user and host system signatures, and behavioral profiles. IDES used a two-pronged strategy [21]. To identify common intrusion methods, it combined user, host, and target system characteristics with a statistical anomaly detection system. A resource's availability, confidentiality, and/or integrity may all be jeopardized by intrusions, and an IDS can help find them [22]. As researchers look towards the future of intrusion detection systems, they are discovering that IDS may be applied everywhere throughout networks [23].

The period of widespread internet connectivity may now be considered mature. As the internet continues to evolve, so do the risks and

opportunities for malicious intrusions. It is crucial that the security mechanisms of a system be designed to prevent unauthorized access to system resources and data. However, at this time it appears unrealistic to expect zero security breaches at all times [24].

Intrusion Detection is the name given to this area of study. Wireless technology has given us access to a whole new and thrilling world. Its technology evolves and grows in sophistication every day, and so does its user base. However, security has been the major issue with wireless technology. Additionally, enhanced encryption systems, the Wireless Intrusion Detection System is a novel approach to combating this issue. This has rapidly become an essential part of network security in the wireless security community. Moreover, any hardware, software, or hybrid that keeps an eye on a system or network of systems for signs of intrusion is known as an intrusion detection system [25]. When people hear "intrusion detection system," they may think of a firewall's security features, but IDS is really much more than that. In contrast to IDS, which is designed to detect network attacks, a firewall is depicted as a massive barrier that would safeguard all information flow and will prevent invasions from occurring. Network security is improved when a firewall is used in conjunction with an intrusion detection system (IDS), since the IDS may be automatically set to prevent any suspicious threads or assaults[26].

The initials of intrusion and detection system form the acronym "IDS." When someone breaks into your computer or network without your permission, they are committing an intrusion. This compromises the security of your data and makes it less reliable for you to use. On the other hand, a detection system is a kind of security equipment designed to uncover such criminal activities [27]. So, an IDS is a security tool that keeps a close eye on host and network traffic in order to spot any unusual

activity that can endanger the system's privacy, safety, or availability. When malicious activity is identified, the IDS will send an alert to the host or network administrators. Connecting NIDS to a network switch using port mirroring technology is an example of a passive deployment, as shown in Figure (2.1). All incoming and outgoing network traffic must be mirrored to the NIDS so that traffic can be monitored and intrusions may be seen. To ensure that all network traffic is inspected, NIDS may be placed inline between the firewall and the network switch [28].

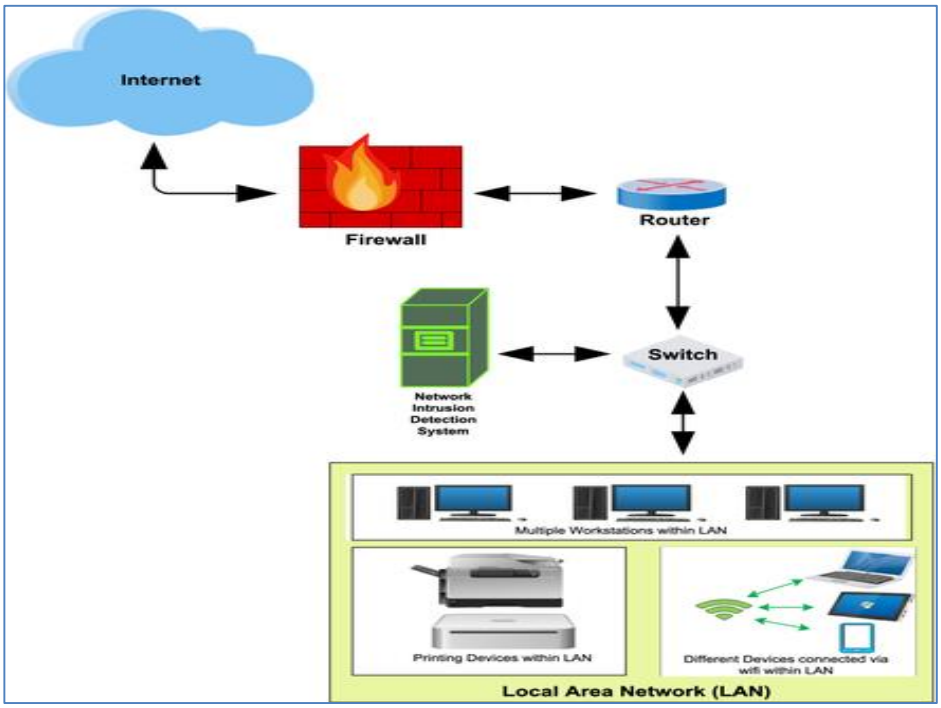


Figure (2.1): Systemic passive deployment of network-based intrusion detection [13]

One of the key mathematical underpinnings of current day wireless communications is the field of information theory [29]. For the context of wireless networks, information theory provides useful insights into the subject of how best to transmit data across several nodes[30].

2.2 Intrusion Detection System

2.2.1 Intrusion Detection System Architecture

The intrusion detection system architecture is shown in the following diagram. Data collection, analysis, and response are the three (3)

phases of the IDS architecture shown in Figure (2.2). Sensors collect information on the state of the system over time and provide a timetable of events that reflects this evolution. The analyzer then determines which of the sensor's inputs best represents the characteristics of an aggressive act. The manager then collects the sensor data and alerts the administrator[31].

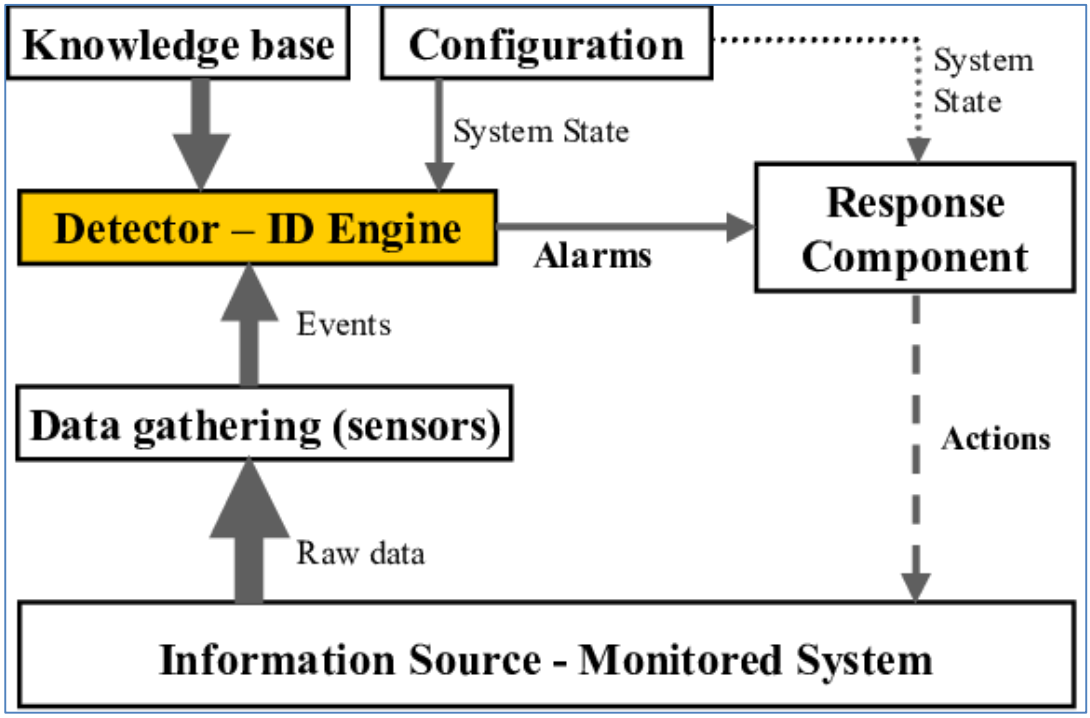


Figure (2.2) : IDS Architecture [31]

A plethora of intrusion detection systems (IDSs) have been suggested in both academia and industry since Dorothy Denning at SRI International established the first model for intrusion detection. Although these systems are quite different in the strategies they utilize to receive and analyses data, most of them depend on a relatively general architectural structure, which consists of the following components [32].

The monitored system's data is gathered by a data gathering device (sensor), which is then processed by a detector (Intrusion Detection (ID) analysis engine) to identify any malicious intrusions. Finally, the monitored system's knowledge base (database) stores the data collected by

the sensors in a preprocessed format (e.g. knowledge base of attacks and their signatures, filtered data, data profiles, etc.). Experts in networks and security often provide this data. The IDS's configuration device details the current status of the system. The IDS's reaction component takes action in response to an intrusion, which may be fully automated (active) or need human intervention (inactive)[33][34].

2.2.2 Intrusion Detection System Network Layers

Any effort to obtain unauthorized access to a computer system, steal sensitive information, or alter system settings by means other than a legitimate user is considered an intrusion [35] . Trojan horse software is a deceptively harmful application that seems to be genuine. Multiple entry points are used by hackers to compromise a system[36]. Software flaws are a common access point because they allow for unintended behavior . Many accounts are vulnerable because they use either an easily-guessed password or an old, unused default account and password[37]. All systems are vulnerable to a skilled hacker. Most studies group assaults into four broad categories:

- Probing
- DoS
- U2R
- R2L

Which may be broken down into four subcategories depending on TCP/IP layer dependent show in figure (2.3)[38].

- Application layer attacks: Attacks such as back, pod, surf, buffer overflow, and load are unique to the application layer of the network protocol stack.

- Land, Neptune, port sweep, and many more assaults are examples of transport layer attacks.
- There are assaults that target the network itself, known as network layer attacks, and these include smurfing, ping-of-death (POD) attacks, IP sweep attacks, and so on.
- Attacks targeted at the link layer of the network protocol stack (e.g., media access control (MAC) attacks, Dynamic Host Configuration Protocol (DHCP) attacks) include NAT (Network Address Translation) attacks, ARP (Address Resolution Protocol) attacks, STP, and VLAN (Virtual Local Area Network) assaults.

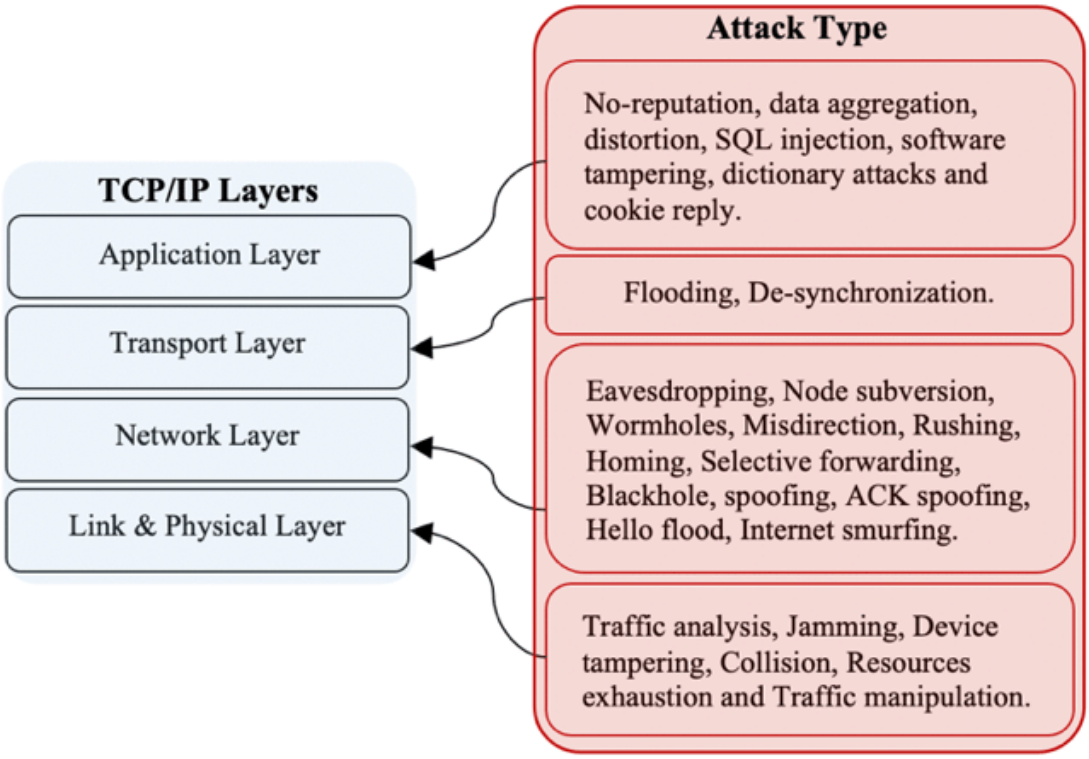


Figure (2.3): TCP /IP layer attacks [38]

To better identify attacks at each layer of the TCP/IP network and boost the overall performance of IDS, it consists of four distinct forms of IDS based on the TCP/IP network model: Anomaly intrusion detection system (AIDS), Trust intrusion detection system (TIDS), Network

intrusion detection system (NIDS), and Linux intrusion detection system(LIDS),Show in figure (2.4) .

According to this method, there are four distinct kinds of IDS, each of which is responsible for monitoring a certain set of network nodes at a specific level of the TCP/IP stack [38].

The NIDS is a software application that runs on network layer devices (i.e. a router) at the network's edge or on a standalone host that is linked to the network's edge in order to monitor and inspect data flowing between the two Independent systems. The TIDS may be installed on transport layer equipment (such as a switch) or on an isolated system that is linked to those devices in order to monitor incoming network traffic. Also, LIDS may be set up in either the link or physical layer. Devices or standalone machines attached to transport layer devices for the purpose of identifying a variety of transport layer threats[39].

Finally, the category of intrusion detection systems known as AIDS resides on and monitors a single host computer. Each computer on the network must have the AIDS installed on it. Instead of employing all connection characteristics, as has been the case in earlier works, we utilise just a particular amount of features for each IDS type, depending on its TCP/IP network layer. When developing various intrusion detection systems (IDSs) such as AIDS, TIDS, NIDS, and LIDS, we may use any features selection method to determine which feature set is most suitable for each layer of the TCP/IP architecture [40]. Intrusion detection system types showed in Figure 2.4.

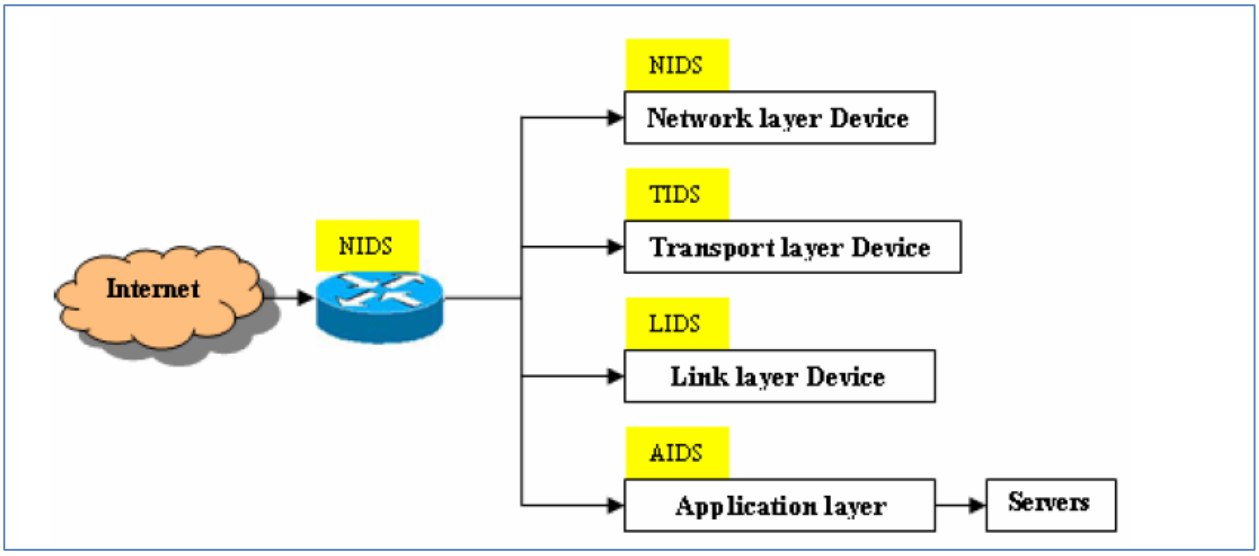


Figure (2.4): IDS Types [38]

2.2.3 Intrusion Detection System Technique

The most common techniques used to detect intrusions:

A. Artificial Neural Networks (ANNs)

Artificial neural networks provide flexible pattern recognition capabilities. In ANNs, special kind of training is given to the system so that it can recognize various arbitrary patterns that are provided to it as input data. When system fully recognizes these patterns it is then asked to match these patterns with the output produced. By matching various input and output arbitrary patterns, it is detected that intrusion has occurred or not [42].

B. State Transition Tables

In State Transition Table, sequence of actions performed by an intruder is described in the form of a state transition diagram and behavior of the system is observed. When it matches with identifiable compromised state and penetrated sate, an intrusion is detected [42]. The proposed system is based on this technique as it stores the normal behavior with max data rate during specific period and compared it with the abnormal DDoS attack state.

C. Genetic Algorithms (GAs)

The function of Genetic Algorithms (GAs) is to imitate or mimic the natural reproduction system in nature. After undergoing recombination and various random changes, only the fittest individual will be reproduced in subsequent generations. In 1995, the application of GAs appeared in IDS research. It involves evolving a signature that indicates intrusion . Learning Classifier System (LCS) is the related technique, in which binary rules that recognize intrusion patterns are evolved [42].

D. Bayesian Network

In Bayesian Network, graphical models are defined by a set of transition rules, represented as probabilistic interdependencies [41] . In this model, a conditional probability table and the state of random variables are described in each node. A conditional probability table determines the probabilities of the node in a state, given a state of its parent [42]. This approach can handle incomplete data [43].

E. Fuzzy Logic

Fuzzy Logic is designed to handle vague and imprecise data. To indicate an intrusion, a relationship between input and output variables is defined by creating different set of rules. It uses membership functions to examine the intensity of truthfulness [42][44].

2.2.4 Advantages of Intrusion detection system

The content of network packets can be targeted precisely: While firewalls may provide insight into the IP addresses and ports in use between hosts, an NIDS can be configured to display the precise data contained inside each packet. This may be used to detect intrusions like botnet endpoint compromises or exploitation threats[45].

- it can access to information within the framework of the Protocol: When analyzing protocols, an NIDS parses the data sent through TCP and UDP. Because they are familiar with how the protocols should operate, the sensors are able to identify any deviations[45].
- It can classify and measure attacks with: An intrusion detection system may examine the frequency and kind of intrusions. The data gathered here may be utilized to upgrade existing security measures or provide novel, more efficient controls. Furthermore, it may be studied to spot software flaws or incorrectly configured network hardware. Later on, these indicators will be useful in conducting risk evaluations[42].
- It facilitate compliance with rules and regulations: Intruder detection systems (IDSs) make it simpler to conform to security standards by providing enhanced visibility throughout the whole network. Your IDS logs might also serve as documentation to help you fulfill some of the criteria[42][45].
- As a result, they may improve productivity: When IDS sensors locate hosts and devices on a network, they may analyse the packets' contents to determine which services and operating systems are being used. The time savings over doing it by hand are substantial. Another way in which an IDS might save time and effort is by automating hardware inventory checks. These boosted efficiency may help cover the initial investment in the IDS by cutting down on the need for as many employees[45].
-

2.2.5 Disadvantages of Intrusion Detection System

It is important to note that an IDS does not stop or prevent attacks; rather, it helps to detect them. Therefore, an IDS must be integrated

into a larger security strategy that also includes other preventative measures and trained personnel[46].

- To manage them effectively, a seasoned engineer is required : Intruder Detection Systems (IDSs) are very beneficial for keeping tabs on the network, but how you utilize that data is key to its value. Due to their inability to prevent or fix problems, detection technologies only offer a false sense of security if neither the proper people nor the appropriate policies are in place to act on the information they provide[46].
- It cannot handle packets with encryption :encrypted packets provide a backdoor for hackers since IDSs can't read their contents. These intrusions will go undetected by an IDS until they have progressed farther into the network, leaving your systems exposed until the intrusion is uncovered. Given the increasing use of encryption to safeguard personal data, this is a major worry[47].
- Still Possible to Fake IP Packets: however, even if an IDS reads the data included in an IP packet, a faked network address may still be used. Because of this, it is more challenging to identify and evaluate an attack if the attacker is using a spoofed address[47].
- It's common to get a false positive: false positive alerts are a major problem with intrusion detection systems. True threats are rarer than false positives. While tuning an IDS may help cut down on false positives, it still requires work from your team's engineers. True attacks might be missed or disregarded if they don't keep an eye on the false positives[48].

- It can be attacked using protocol-based methods: since an NIDS examines recorded protocols in real time, it is vulnerable to the same kinds of protocol-based attacks that affect network hosts. It is

possible for an NIDS to fail because to flawed protocol analyzers or corrupted data[48].

- Keeping the signature library up-to-date is crucial for identifying modern security risks. If it isn't regularly updated, it won't pick up on new threats and warn you about them. Another problem is that the newest assaults will always be a major worry since your systems won't be protected until the signature library has been updated to include the new danger[49].

2.3 Implementation tools

There are many implementation tools used to implement DDOS attack in wireless network as follow :

2.3.1 OMNET ++

Modeling communication networks, multiprocessors, and other distributed or parallel systems is the focus of OMNeT++[1][2], a C++ based discrete event simulator. Because of its open development and distribution, OMNeT++ is free for educational and research purposes under the Academic Public License. In order to facilitate the modelling of computer networks and distributed or parallel systems, OMNeT++ is developed as a robust open-source discrete event simulation tool for usage by academic, educational, and research-oriented commercial organisations. Between free, research-oriented programmes like NS-2 and costly commercial options like OPNET, OMNeT++ aims to bridge the gap[50].

Uses either the GCC tool chain or the Microsoft Visual C++ compiler, making it compatible with Linux, Mac OS X, and Windows. One such framework strategy is OMNeT++[50] .

OMNET++ provides modular architecture which enables the simulation kernel to be easily embedded into any application . A

component-based framework and library is provided which makes building of a network simulators an easier task. It offers eclipse IDS and a graphical user defined environment . OMNET++ does not provide the components directly for simulation but instead it just provides the basic tools and machinery required to write such simulators. Many simulation models and frameworks, such as the Mobility Framework and the INET Framework, are available to serve a wide variety of applications. These models go through their own release schedules and are produced fully apart from OMNeT++ . Wireless and ad hoc networks, sensors, IP and IPv6 networks, MPLS, wireless channels, P2P networks, SANs, optical networks, queuing networks, file systems, high-speed interconnections, and many more have all seen simulation models built since its first release. While some of the simulation models are adapted from existing protocol implementations like the Quagga Linux routing daemon and the BSD TCP/IP stack, others are created from scratch just for OMNeT++ [51] .

From its inception, OMNeT++ was intended to provide massively parallel network simulation. The following essential design criteria emerged from this goal [52]:

- Simulation models, in order to support large-scale simulation, should be hierarchical and constructed from reusable components whenever feasible.
- Debugging time, which often accounts for a major part of simulation projects, may be reduced if the simulation software makes it easier to see and debug simulation models. (The software's identical set of features is also helpful for its instructional potential.)
- In addition to being flexible and adaptable, simulation software should also support embedding simulations into other applications, such as network design programmes. (The simulation's memory

management, restart ability, etc., must meet stricter criteria when embedded.)

- An open data interface means that input and output files may be created and processed using standard programmes.

Should provide an Integrated Development Environment that makes building models and evaluating their outputs more easier.

2.3.2 INet

Are supported IPv4, IPv6, TCP, SCTP, and UDP by the INET Framework, along with a number of other application types. In order to provide static routing, either network autoconfigurators or routing protocol implementations may be used[51]. Wireless and mobile simulations are also supported by the INET Framework. The INET Framework is based on OMNeT++ and employs the same core idea: modules that exchange data through message forwarding. Compound modules in OMNeT++ stand in for hosts, routers, switches, and other nodes in a network. Modules representing protocols, applications, and other functional elements are combined to form these more complex modules. Again, in OMNeT++, a network is a compound module that incorporates not just the host and router but also additional modules [52].

2.4 Wireless Network Evaluation Metrics

Wireless network evaluated with different parameters sorted as follow:

2.4.1 network Evaluation

A. Throughput

It is used to describe how much data the network can move in a given length of time, Mbps (mega bits per second) is used to measure the data transfer rate. To determine how much data is sent for this flow, the

server (and the intermediary process, if present) analyses the final statistics file. The first and final packet's arrival times are also used. Formula is used to determine throughput [53].

$$\text{Throughput} = \frac{Request}{time} \text{ ---------- [2.1]}$$

Simply explained, throughput is the rate at which data travels from one end of a network to the other. Throughput is the rate at which data is successfully sent via a communication channel in a network. Throughput of a network is often measured in bits per second (bit/s or bps).When advertising high-speed Internet service, providers often talk about "Internet Connection Speed" or "Internet Connection Bandwidth," however this phrase often refers to throughput, or the actual rate at which packets are sent across a given media. Because of this, Speed Tests are the finest resource for learning how to accurately gauge a network's transfer rates[53].

B. Packet loss rate or packet drop rate

It is the measure of the number packets dropped due to malicious node (DDoS attack). To use this metric, the client must relay information about the total number of packets transmitted to the server . Using the total number of packets sent and locally received, the server and the intermediary process may calculate the loss rate they see. Formula for determining the fraction of packets that never made it to their destination [54].

$$\textbf{Packet drop rate} = \frac{Send\ Packet - Received\ Packet}{Time} \text{ ---------- [2.2]}$$

It is the proportion of data packets that are sent out from a certain node in a network but are lost before reaching their final destination. To guarantee data can be delivered properly, it is crucial that your IT staff

monitor and track the amount of packet loss occurring throughout the network. Being able to quantify packet loss allows one to evaluate the efficiency of a network [54].

C. Network Delay in sec

It is the difference in time from the generation of a packet at the source to the moment when it is received at the destination. An additional measure of network performance, end-to-end latency is the average time it takes from when a data packet is issued by a wireless host until it reaches the destination node[54].

D. Packet delivery ratio

It represents as the Number of packets per second for Different Packets Size. This statistic measures the efficiency of a network by comparing the amount of data packets sent by the source to the amount of data packets received at the destination[54][55].

$$\text{Packet Rate} = \frac{Sum(sent\ packet + reseived\ packet)}{Time} \text{ ----------[2.3]}$$

E. Maximum data rate

It represents the maximum data rate transmit through specific request from the wireless node to the server or destination node. It is calculated in equation [2.4]

$$\text{Maximum data rate} = \frac{MAX\ data\ value}{Time} \text{ ----------[2.4]}$$

F- Mean

The mean is the average or a calculated central value of a set of numbers and is used to measure the central tendency of the data. Central tendency is the statistical measure that recognizes the entire set of data or

distribution through a single value. It provides an exact description of the whole data.

$$\text{Mean} = \frac{Sum\ of\ all\ data\ point}{Number\ of\ Data\ points} \quad \text{----------[2.5]}$$

G- Median

The median is known as a measure of location; that is, it is showed where the data are. Thus the median does not use all the information in the data and so it can be shown to be less efficient than the mean or average, which does use all values of the data. To calculate the mean we add up the observed values and divide by the number of them.

H- Standard Deviation

A calculation of the amount of variance or dispersion of a set of values is the standard deviation.

2.4.2 DDoS Attack Evaluation

DDoS attack can be evaluated with different evaluation metrics sorted as follow :

2.4.2.1 Firewall delay

Firewalls are hardware or software that regulates data transmissions between two networks or hosts with different security policies. It used to be that firewalls are mostly used at the edges of networks. Some internal hosts are protected in this way, but not entirely, and assaults delivered from one internal host to another typically bypass network firewalls since they come from inside the same organization [55].

To combat these and other threats, especially to safeguard mobile devices connected directly to external networks, network designers often include firewall capability at locations outside than the network

perimeter. It's becoming more difficult for firewalls to prevent threats spread through network communications since the majority of attacks have shifted from being concentrated in lower levels of network traffic to the application layer. There are still major risks operating at the lower levels of network traffic, however, therefore firewalls are still necessary. To enhance the capabilities of other network security solutions, firewalls may also offer some protection at the application layer[56].

Firewalls come in a variety of types , each with its own set of tools for parsing network traffic and deciding whether to let or block individual packets based on how closely they match predefined regulations. Protecting network traffic flows requires an understanding of firewall capabilities, the creation of firewall rules tailored to the organization's requirements, and the acquisition of firewall technologies that can successfully handle those needs[56].

2.5 Security Requirements

2.5.1 Data Security

Security refers to the safeguarding of valuables (including but not limited to buildings, machinery, supplies, and personnel) against unauthorized access or use. the protection of information from a wide range of threats to ensure business continuity, minimise business risk, and maximise return on investments and business opportunities is one definition of data security (or information security), While there is overlap between data security, information security, and cybersecurity, each word may have a somewhat different focus. Data, communications, and information that are generally recorded on, processed by, communicated through, stored in, shared from, transferred to, or received from such information systems are the primary focus of protection, regardless of the name given to them[57].

The measures used to ensure the safety of computer networks and their associated data often fall into one of three broad categories.

- Network elements such as servers, access devices, storage devices, and other physical components of the computer systems and networks that process, transmit, and store the data may be protected by implementing physical security measures. You may use things like locks, safes; armed guards; sensors and alarm bells; and fences, walls, and other obstacles[58].
- Safeguards built into computer hardware, software, and other devices are examples of technical security measures. The goals of these safeguards are to guarantee access to the system, verify the identities of users requesting access, prevent unauthorised changes to data, keep data in transit and at rest undamaged, and keep sensitive data private when necessary. Security measures such as these include firewalls, intrusion detection systems, access control systems, antivirus software, passwords, PIN numbers, smart cards, biometric tokens, and encryption procedures[59].
- Administrative security measures: These security measures include management procedures and constraints, operational procedures, accountability procedures, policies, and supplemental administrative controls to prevent unauthorised access and provide an acceptable level of protection for computing resources and data[59].

Security measures may be either preventive, detective, or reactionary, with each category subdivided further under those three broad headings. In order to avoid any security issues, you should take preventative precautions. A lock on the door (to keep people out of the room with the computers) or a firewall (to block anyone from accessing

the network) are both examples of preventive security measures. After-the-fact security breaches may be discovered with the use of detective security procedures [60]. Detection-based security measures include smoke alarms and intrusion detection software, both of which work to prevent and respond to potential threats. Reactive security measures are implemented after a security breach has already occurred, and its goals are to halt or limit the intrusion, determine who is responsible for the breach, and restore any data that is compromised [61].

Both good and negative outcomes may be used to describe the goals of implementing security measures. Typical descriptions of the desired outcomes include :

(1) assuring the availability of systems and information.

(2) regulating who has access to systems and information

(3) protecting the privacy, security, and veracity of data.

Unauthorized access, use, disclosure or transfer, modification, change, or processing of data, as well as unintentional loss or destruction of data, are typically cited as examples of the types of damage to be avoided. Implementing security measures to shield systems and data from potential dangers is essential to achieving these goals [62].

2.5.2 Communication Security

The goal of communications security (COMSEC) is to ensure that no unauthorised parties get access to confidential information during transmission via a network or in the form of a written message. Among the many subfields that make up COMSEC are[63]:

- Data is encrypted and unintelligible until it is decoded, a process known as cryptographic security.

- Maintaining the confidentiality and integrity of a network's cryptographic data, records, and infrastructure is the responsibility of the network's physical security team.
- When data is being physically transported, it must be protected from illegal access during this time to avoid problems like service interruptions.

Moreover, protections against eavesdropping on transmissions are an important part of communications security. In the federal government, the National Security Agency defines communications security (COMSEC) as follows: Security procedures and checks set up to prevent unauthorized access to and verify the integrity of telephonic transmissions. Crypto security (the act of encrypting or decrypting data), transmission security, emission security (the detection and analysis of signals emitted by devices), and physical security of COMSEC data are all components of communications protection . To prevent a breach in operations, consider using the following four measures of communication security [64]:

1- Safeguarding one's body: the operator of a communication network is responsible for ensuring the network's physical security. It is essential that all alarm systems be in full functioning condition to provide the quickest possible reaction time in the event of an emergency [64].
2- Building blocks and layout of the network: when the network's configuration and topology are chosen, and even earlier when its system software is built, a substantial portion of its security is specified. The following are necessary components of this plan:Servers and base stations, This manner, the failure of a single component would not compromise the functionality of the whole

system. To properly support its users, the network must also have enough capacity[64].

3- Communication services: The security of the whole system is enhanced by the communication network's services. The network must naturally include safeguards to prevent unauthorised parties from gaining access to communications via means such as eavesdropping or the use of a stolen or pirated equipment[64].

4- Information security: Passwords and encryption algorithms are two of the first things that spring to mind when the topic of data security is broached. Encryption is crucial, but so is making sure the encryption keys are handled securely. The data stored on or accessed by user devices is vulnerable to loss of confidentiality and data corruption. This is why it's important for consumer devices to have privacy and security measures of their own [64].

2.5.3 Device Security

Computer and network security prevents theft, damage, and misuse of sensitive data and hardware. Although "device security" isn't as common as "cybersecurity," it's still an important concept that encompasses all of the methods used to protect electronic gadgets including computers, laptops, smartphones, tablets, and IoT gadgets. For current security threats to be effectively countered, a device's security approach must be multilayered, with different security solutions working together and centred on the same set of procedures [65].

There are three main features that make a device secure:

1- The people behind a device's security, whether they work in-house or for a cloud provider, are its backbone. They make choices about what kinds of tools and controls to put in place and keep an eye out for any security issues. Leaders in security are crucial in informing employees

of the best practises for securing sensitive information and avoiding potentially harmful actions, particularly when employees are working from home[66].

2- Methods: Implementing best-in-class security policies and strategies is crucial for protecting sensitive information and preventing unauthorised access to devices. The National Institute of Standards and Technology, for instance, provides a paradigm consisting of an iterative cycle of "identify," "protect," "detect," "respond," and "recover" when malware or ransomware is encountered.

3- Many technological options exist to protect sensitive ecosystems from danger. Tools including antimalware software, email encryption, web application firewalls (WAFs), analytics, bot detection and management platforms, and more are widely used for this purpose [65].

2.5.4 Wireless Security Challenge and Solusion

A. Security Issues In Wi-Fi

1- Exfiltration of Information, Information sent by radio waves is vulnerable to interception. Integrity of the message is attacked, causing damage to both the sender and the recipient[67].

2- Unauthorized Access Point. Unauthorized access points have long been considered one of a network's biggest security concerns[67].

3- The Denial-of-Service Attack Because of security flaws in WLAN, this attack is possible. Unlicensed frequencies are used by everyone[67].

4- Cracking Attacks Passwords for wireless networks may be broken using a number of different programmers. Strong passwords are required for all Wi-Fi security methods. This includes WEP, WPA, and WPA2[67].

5- Wi-Fi Security, The creation of WEP is very effective at early years, but with the evolution of computer technology and the reduced cost of computational power, WEP is easily defeated[67].
6- To Change Your Default Password, The manufacturer-issued default password is vulnerable to attack. Hackers may use these easily guessed passwords to gain access to your network and steal critical data[67][68].

B. Security Solutions For Wi-Fi

1- Encryption: The company may choose from a number of different encryption strategies. This is among the most reliable approaches of preserving the confidentiality of data while in transit across a network. For organizations that must comply with rules and regulations, using both symmetric and asymmetric encryption is crucial[68].
2- Protecting the WAP: A wireless access point that has been configured without proper authorization poses a significant threat to the security of the network. The following countermeasures may help an organisation lessen the danger posed by wireless access points: Remove unwanted access points and undertake secure setup of allowed access by altering the default settings[68][69].
3- Denial-of-service attacks may be mitigated by conducting regular audits of wireless networking activity and removing the problematic devices if necessary [68].
4- Wi-Fi Protocols: WEP and WPA are the most widely used Wi-Fi protocols, and they are responsible for maintaining the high degree of security that Wi-Fi provides. WEP is used to encrypt data sent between access points and client devices. While the WPA protocol is an improvement over WEP[69][70].

Chapter Three

The Proposed system

3.1 Introduction

The rapid proliferation of wireless networks applications has changed the landscape of network security. The nature of mobility creates new vulnerabilities that do not exist in a fixed wired network, and yet many of the proven security measures turn out to be ineffective. Therefore, the traditional way of protecting networks with encryption software is no longer sufficient. It need to develop new architecture and mechanisms to protect the wireless networks applications. In the proposed system, the adaptive detection method has been applied to analysis traffic in the network on each wireless node based on maximum data rate.

3.2 Proposed System Model

The anomaly based detection is based on defining the network behavior. The network behavior is in accordance with the predefined behavior, then it is accepted or else it triggers the event in the anomaly detection. The accepted network behavior is prepared or learned by the specifications of the network administrators.

The main contribute of the proposed anomaly detection method based on maximum data rate is that it does not require prior knowledge of intrusion and can thus detect new intrusions. The proposed system based on the maximum data rate approach to determine maximum size of data rare of each wireless nodes. The proposed approach implemented in Firewall-Allow-Deny-rule to filter network traffic of incoming packets into accepted and rejected by measuring size of incoming wireless packets and it matched with the accepted packets size as normal or discarded and rejected if the size is larger from the accepted threshold.

It has simulated by using OMNET++ and c++ programming language to implement the IDS system with firewall to manage rate limits,

MDR and packets size to mitigate DDoS attack which occurs when adversaries flood a large amount of bogus data to interfere or disrupt the service on the server , show details the OMNET++ in table 3.1.

The used system describes a flexible approach for intrusion detection in wireless environment in OMNET++. All of the used IDS area components in the proposed regions contain (4, 8, 16) normal wireless hosts and (2, 4, 8) DDoS attack nodes .

The important phase in defining the network behavior is the IDS engine(Firewall-Engine) capability to manage traffic before arrived to the servers.

The Firewall-Engine must be able to process each request of wireless devices and understand its final destination. Though this protocol analysis is computationally expensive, the benefits it generates like increasing the rule set helps in less false positive alarms. It was challenge of anomaly detection through defining its rule setup to determine the maximum size of data rate. The efficiency of the system depends on how well it is implemented and tested on all cases. Rule defining process is also affected by various data traffic and number of wireless nodes.

When the request arrived to the Firewall it determine max data rate and record source IP address and timestamp for each interface port of Firewall and matched MDR metric as block data size and block source IP if arrived request size large than MDR and if arrived request size less or equal it will be allowed and verified as normal.

3.3 Proposed System Architecture

3.3.1 Wireless devices :

It is a group of computers or hosts used to transmit and received packets to the servers.

3.3.2 Network elements:

a- Access point

It is part of the network elements and extends the range of the wireless network and connects wireless devices together and send the request to router.

b- Router

It is part of the network elements and is received the request from access point and wireless devices and send the request to firewall ،in short, it redirects the packet to the server

c- Firewall

It is part of the network elements and it contains on the proposed algorithm, like the router device that has algorithmic characteristics and is located before the area which want to protect. Through it, it can filter the traffic when high traffic comes in, it did not go to the server directly, but we filter it through the firewall, and it is filtered through to two points max data rate, and time. The firewall is filtration the traffic as allow and deny .

3.3.3 Server

It is the device that accepts and responds to requests made over a network from network elements. The device that makes the request, and receives a response from the server, is called a client.

3.4 Proposed System Methodology

The proposed DDoS attack detection model has the advantage of dealing with attacks of unknown anatomy and different strengths through training phase with legitimate traffic, and then it decides the normal from abnormal traffic based on the log file traffic model of data traffic for each wireless device as the network analyzer model to verify each hosts.

The proposed method in firewall create two log configuration rule. The first one is normal rule with allow feature for normal request from source IP, source MAC address, and time stamp under or equal to the used threshold and then add the Host details to the white list. The second abnormal rule deny for abnormal request with source and MAC addresses and verify it after matched with the used value and add the Host details to the black list.

It assigned a trust host IP identifier for every wireless host relying on a threshold MDR value that changes dynamically and assists in detecting the DDoS attack by measuring maximum data rate for each interface port and identify normal wireless with allow rule data packets and abnormal wireless with deny rule data packets, the goal is to minimize the impact of the DDoS attack (huge data rate) on the network so that regular users can perform their tasks well without suffering from poor network performance and high latency. as it showed in Figure (3.2).

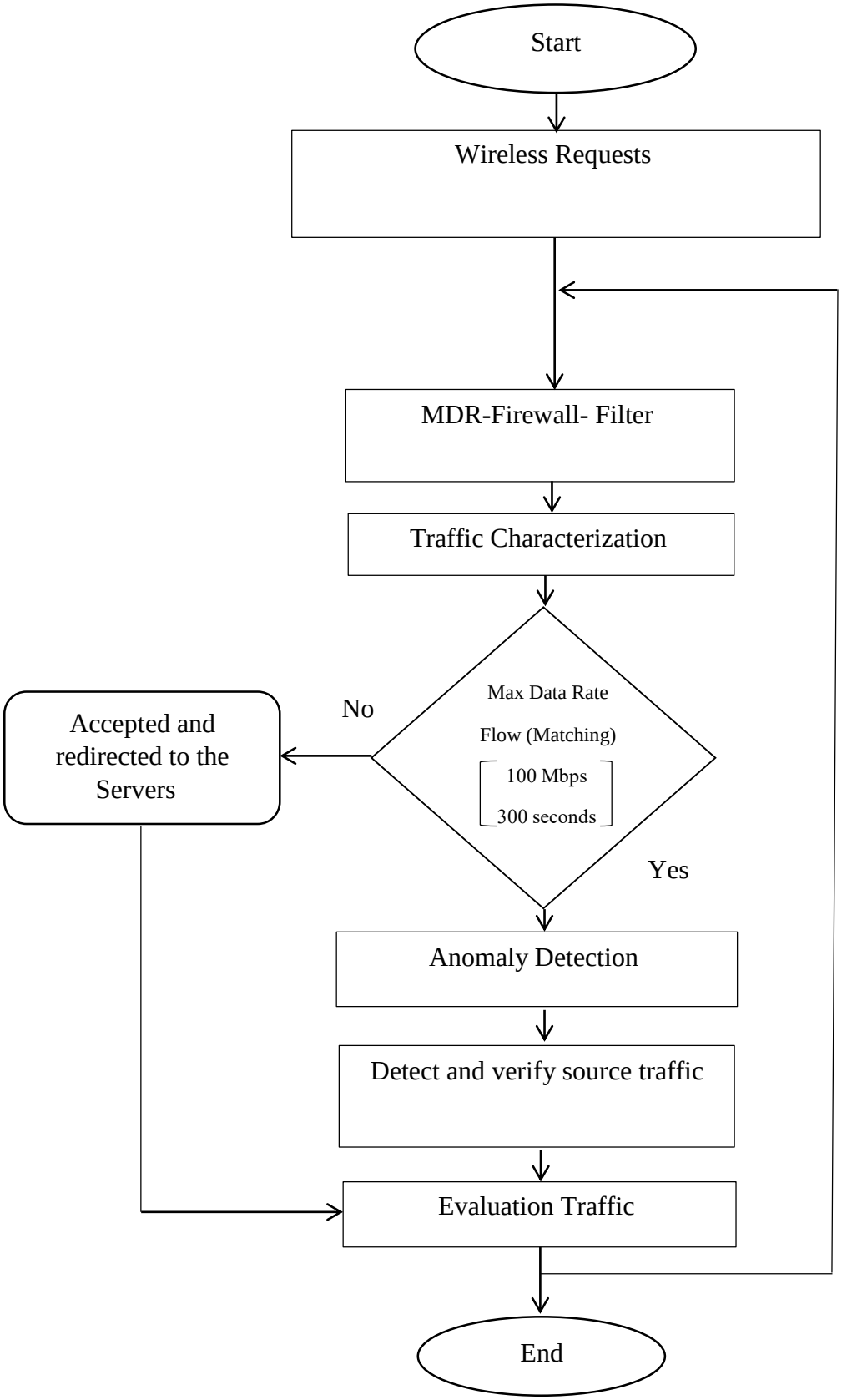


Figure (3.1): The Proposed Methodology of IDS in wireless network.

The main steps of the proposed methodology sorted as follows :

1. **Start**

   - Initialize data traffic from client (incoming request).

2. **Wireless request**

   - It created by wireless nodes to specific network application such as HTTP request.

3. **Network elements**

   - Access point : It is Net element used for coverage area purposes.

   - Router : It is Net element used for routing incoming requests to the particular server dara on route table.

4. **DDOS Firewall Filter**

   - Is filtration the request and is classify the incoming request as normal and Abnormal.

5. **Traffic characterization**

   - It work as matching (low or high)
   - If traffic data rate is low than threshold is accept and redirection to the servers.
   - If traffic data rate is high than threshold is considered as anomaly detection then make block and deny source traffic .

6. **Evaluation traffic** .

   - Evaluated the system with network evaluation metrics as packet loss rate and Packet Delivery Ratio.

7. **End**

* Request analysis

- After system running for 10 times and qualify the Maximum Data Rate value which identified as 7.5 value of 4 nodes , 9.5 value of 8 nodes, 12.5 value of 16 nodes as normal.

- Matching MDR and classify data traffic :-

a- Normal data traffic value calculated less than threshold.

b- Abnormal calculated greater than threshold.

* Connection management :-

- Allow ---------- Normal.
- Block ---------- Abnormal client (Black list of firewall table: Event log configuration which contains on :
  - Event ID
  - source IP address
  - source MAC address
  - inbound-outbound port-interface numbers
  - timestamp
  - MDR metric

In addition, the proposed methodology caculated typically in terms of bandwidth/capacity, which is measured in bits per second (bps), or forwarding rate, which is measured in packets per second (PPS) as the maximum data rate for data traffic in router interface port. The choice of terms used can significantly change the meaning of any blanket statements about what attacks would be in the running for the DDoS attack in log configuration file:

- The first, determining the amount of data that can travel through an network interfaces.

- The second, measuring total number of packets incoming from specific interface that can be processed by wireless network devices into the firewall interface.

The main processes of the Algorithm 3.1 which showed connect to wirless host to provide known host as normal devices to added to the route table of router in addition to classify them by firewall device as follow:

Each wireless Host send beacon messages to connect with access point and then to connect to the network through the router and using socket connect attribute, connected device create log configuration file with source IP, source MAC and max data rate with time stamp and identify Host if normal recognized the socket port number is opened and accessed the normal traffic will pass to the router then to firewall and server and firewall registered Host behavior in log configuration file with source IP, and source MAC, else if Host traffic request recognized as abnormal, when the request arrived to the firewall which verified DDoS Host due to the huge amount size of traffic generated in small period so it block the user by deny traffic and discarded source packet IP.

Algorithm 3.1: Connect to wireless hosts

Input:beacon messages

Output: result = sock.connect_ex((host, port))

Begin

1- Connectin hosts
   - Initial socket, time
2- Save hosts that already accessed
   - known_hosts = []
3- Check **if** port from given host is open
   - def is_open(host, port):
   - sock = socket.socket(socket.AF_INET, socket.SOCK_DGRAM)
4- Open nc connection to receive the file (Start connection)
   global known_hosts
5- Add own IPs to known hosts

```
for ip in ips:
    if ip not in known_hosts:
        known_hosts.append(ip)
            for network in networks:
                print("Searching hosts for network:", network)
                    hosts = search.search_hosts(network)
                      for host in hosts:
                          if not is_open(host, 23):
                          print("Port 23 is closed at host:", host)
                        End for
                End for
        End if
End for
      continue
        elif host in known_hosts:
      continue
```

End Algorithm

Algorithm 3.2 showed the flood traffic and classify the flood as attack and normal. Firewall will recognizing load traffic size of each incoming request as FTP request and verify flooding traffic requests and record source port of UDP Flooding to fixed IP and Port number, firewall running match functions to compare incoming data rate with max data rate and message size the max normal is 100 Mbps, if incoming request block size larger than determined threshold the firewall closed the port and block source IP, and source MAC.

Algorithm 3.2: Recognizing load traffic types

Input: FTP flood traffic requests

Output: Normal traffic, Abnormal traffic

```
Begin
    1- UDP Flooding to fixed IP and Port
     - Intialize socket, match functions
    2- Define max data rate and message size
       Max Message size is 100 Mbps
       def udp_flood(host, port, amount):
        sock = socket.socket(socket.AF_INET, DGRAM)
        while True:
            sock.sendto(MESSAGE, (host, port))
         else
             for i in range(0, amount):
                 sock.sendto(MESSAGE, (host, port))
                  index = randint(0, length - 1)
               try
                  udp_flood(host, int(open_ports[index]), amount)
               except
                  print("Cannot flood port", open_ports[index])
              End for
       End while
End Algorithm
```

Algorithm 3.3 showed the matched traffic among network elements (wireless Host, access point, router, and firewall). To identify Host type as normal Host or DDoS attack Host, it required main metrics as source IP, nmap requests and source MAC address, after each incoming request firewall recognized Host type inside the network and matched IP with the routing table within firewall, establishing socket connection and creating list of addresses, then open ports is updated after requests and filter blocked source IP of DDoS Host and deny port number with post scanner, firewall created Whitehost for normal Hosts and Blackhost for DDoS Hosts and it updated log file configuration for last updated requests.

Algorithm 3.3: Identify Host type

Input: IP, nmap requests

Output: normal ip host, attack ip host

Begin

1- Host search inside a network

def get_ip_address():

- Returns the ip of the current Host

2- Find all IP addresses of the computer

networks = list()

ips = list()

Match only valid source IP Address (IPs)

3- Get open UDP ports of given host

def scan_udp_ports(host):

udp_ports = nm[host]['udp'].keys()

4- Only add open ports

for port in udp_ports:

state = nm[host]['udp'][port]['state']

if state == 'open' or state == 'open|filtered':

ports.append(port)

End if

5- Search hosts on given network address (IPs)

```
def search_hosts(address):
    hosts = list()
    nm = nmap.PortScanner()
    for host in nm.all_hosts():
        if nm[host].state() == 'up':
            hosts.append(Whitehost) and allow
            return hosts ip
        else
            hosts.append(Blackhost) and deny
        return hosts ip and block (deny)
    End For
```

End Algorithm

Chapter Four

Simulation Results and Discussion

4.1 Introduction

This chapter introduced the simulation and discussion of results for the proposed DDoS attack detection presented in chapter three. It has simulated by using OMNET++ and c# programming language to implement the IDS system with firewall to manage rate limits, channel capacity and packets size to mitigate DoS attack which occurs when adversaries flood a large amount of bogus data to interfere or disrupt the service on the server. The proposed method in Firewall IDS provides the anomaly detection unit calculates detection thresholds as functions of this approach issuing an attack alarm when they are exceeded by the last max channel capacity data traffic estimates

The used system describes a flexible approach for intrusion detection in wireless environment in OMNET++. All of the used IDS area components in the proposed regions contain (4, 8, 16) normal wireless hosts and (2, 4, 8) DDoS attack nodes shown in Table 4.1.

Table 4.1: The used installation requirement.

Tools	**Installation Requirements**	**Goal of using the tool**
Omnet++ 4.6	1. Windows 10 (32-bit or 64-bit) 2. 1 GB (32-bit) or 2 GB (64-bit) RAM	Simulating the proposed IDS for DDoS attack mitigation in wireless environment.

Besides, the main simulation parameters are showed as Table 4.2:

Table 4.2: The main simulation parameters for the all case studies.

Parameters	**Value**
Simulation Time	5 m = 300 second
Total Frames	2028
Rule Priority	0 normal to 1 abnormal DDoS
Max data rate	100Mbps

Action	Authorize, and Refuse
Protocol	TCP/IP
Number of nodes	4,8,16 Normal- 2,4,8 DDoS
Source / destination ports	TCP only
Mitigation	Log
Sensitivity	High
TX Packet Size	1024 KB
Acknowledgement Packet size	64 Byte

The proposed system results based on the three main case studies as :

4.2 Normal Operation of wireless network

4.2.1 The case of 4 wireless Hosts

The first state of the 4 Hosts and the evaluation parameters based on the different variables . The data traffic details showed in Table 4.3. It showed the sum of total bit rate of all wireless hosts is large due to the incoming request is proceeds directly as normal data rate so firewall added all incoming source IP address to the route table and redirect requests to the server as accepted data rate. To explain the results as :

The summation of Packet Rate KBps is (2368.9934 KBps) which converted into Mbps by divide the digital storage value by 125 as:

Total bit Rate in Mbps = 2368.9934 KBps / 125 = 18.95194 Mbps

Table 4.3: bit Rate KBps Mean, Median, SD, and Total Bit Rate in Mbps of 4 Hosts normal traffic.

Wireless Host Type	**bit Rate KBps**	**Mean**	**Median**	**SD**	**Total bit Rate in Mbps**
Host 1	723.6695	592.2484	612.7296	129.0088	18.95194 Mbps
Host 2	419.8647				
Host 3	580.301				
Host 4	645.1582				

Simulated data packet size is processed as 1024 KB data class which is multiplied with number of sent packets to get the total size of each host traffic and it showed the normal data rate is better due to the allowed rule is configured as accepted due to the normal traffic exchanged among wireless hosts and servers.

Table 4.4: Total number of sent packets, Total number of Acknowledge packets, and Total Throughput in Mbps of 4 Hosts normal traffic.

Wireless Host Type	Total number of sent packets	Total number of Acknowledge packets	Total Throughput in Mbps
Host 1	212	201	Sum(send)*1024 KB/300 = 18.9508 Mbps
Host 2	123	116	
Host 3	170	161	
Host 4	189	179	

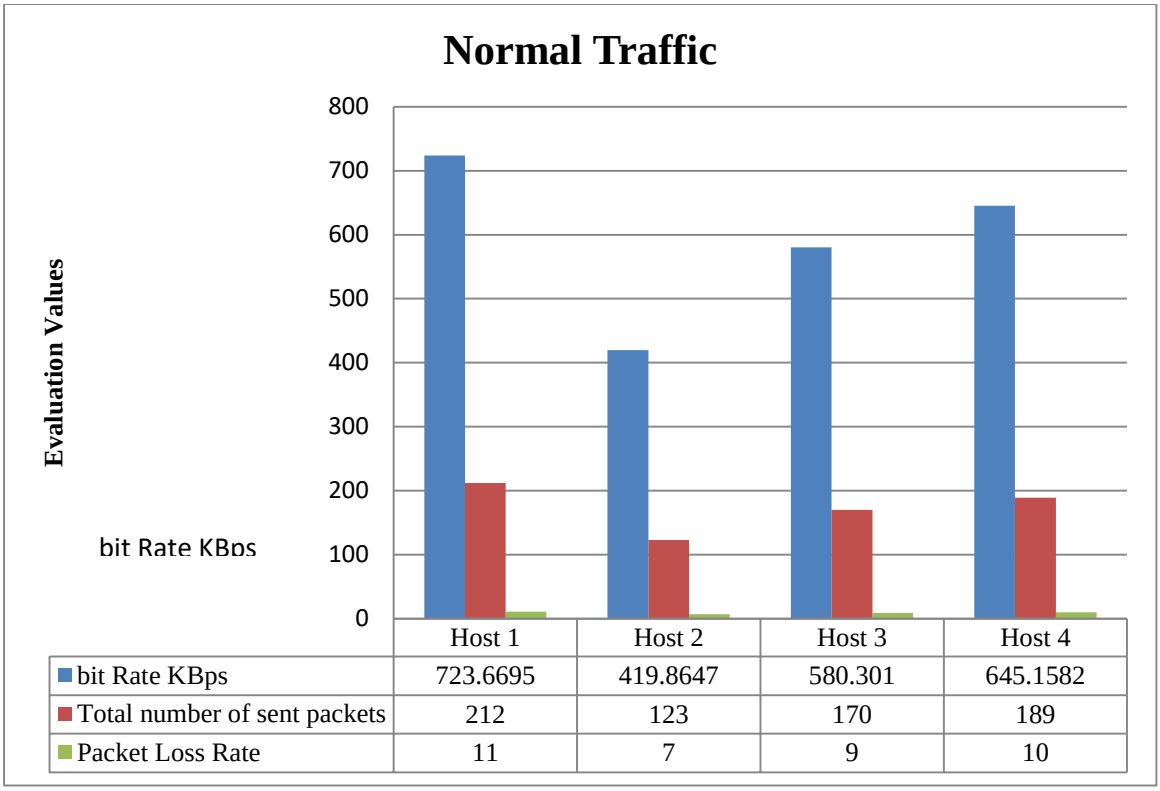
The packet deliver ratio is calculated by divided the Total number of Acknowledge packets into Total number of sent packets as the ratio of successful packets as follow : Total number of Acknowledge packets/ Total number of sent packets.

Table 4.5: Packet Loss Rate, and Packet Delivery Ratio of fourth Host normal traffic.

Wireless Host Type	Packet Loss Rate	Packet Delivery Ratio %
Host 1	11	94.8113 %
Host 2	7	94.3089 %
Host 3	9	94.7059 %
Host 4	10	94.709 %

Table 4.6: Router to Firewall Delay , and Firewall to Server Delay of 4 Hosts normal traffic.

Wireless Host Type	Router to Firewall Delay in ms	Firewall to Server Delay in ms
Host 1	64503.67	74102.44
Host 2	64442.45	60947.08
Host 3	64454.66	70550.52
Host 4	63072.32	61766.28



	Host 1	Host 2	Host 3	Host 4
bit Rate KBps	723.6695	419.8647	580.301	645.1582
Total number of sent packets	212	123	170	189
Packet Loss Rate	11	7	9	10

Figure 4.1: bit rate and total number of sent packets, and packet loss rate of 4 Hosts normal traffic.

4.2.2 The case of 8 wireless Hosts

The second state of the 8 Normal wireless nodes simulated and the evaluation parameters based on the different variables. The data traffic details showed in Table 4.7, and Table 4.8 as the total packet rate is effected with increasing number of Hosts and delay of each Host also is effected and increased which caused decreased total packet rate of 8 Hosts compared with 4 Hosts.

Table 4.7: bit Rate and mathematical Evaluations of 8 Hosts normal traffic.

Wireless Host Type	bit Rate KBps	Mean	Median	SD	Total bit Rate in Mbps
Host 1	283.3229	280.3363	283.3229	16.36449	17.94152 Mbps
Host 2	273.0825				
Host 3	262.8418				
Host 4	283.3233				
Host 5	283.3229				
Host 6	256.0149				
Host 7	307.2181				
Host 8	293.5642				

Table 4.8: Throughput for the data signals of 8 Hosts normal traffic.

Wireless Host Type	Total number of sent packets	Total number of Acknowledge packets	Total Throughput in Mbps
Host 1	83	76	17.94048 Mbps
Host 2	80	74	
Host 3	77	71	
Host 4	83	78	
Host 5	83	76	
Host 6	75	70	
Host 7	90	85	
Host 8	86	82	

Table 4.9 showed the packet delivery ratio of the 8 Hosts which decreased due to the increasing packet loss rate with increasing total number of Hosts compared with 4 Hosts of normal data rate.

Table 4.9: Packet Loss Rate, and Packet Delivery Ratio of 8 Hosts normal traffic.

Wireless Host Type	Packet Loss Rate	Packet Delivery Ratio
Host 1	7	91.5663 %
Host 2	6	92.5 %
Host 3	6	92.2078 %
Host 4	5	93.9759 %
Host 5	7	91.5663 %
Host 6	5	93.3333 %
Host 7	5	94.4444 %
Host 8	4	95.3488 %

Table 4.10: Router to Firewall Delay, and Firewall to Server Delay of 8 Hosts normal traffic.

Wireless Host Type	Router to Firewall Delay	Firewall to Server Delay
Host 1	16125.92	16287.18
Host 2	16110.61	16271.72
Host 3	16113.67	16274.81
Host 4	15768.08	15925.76
Host 5	16974.65	17144.4
Host 6	16958.54	17128.13
Host 7	16961.75	17131.37
Host 8	16597.98	16763.96

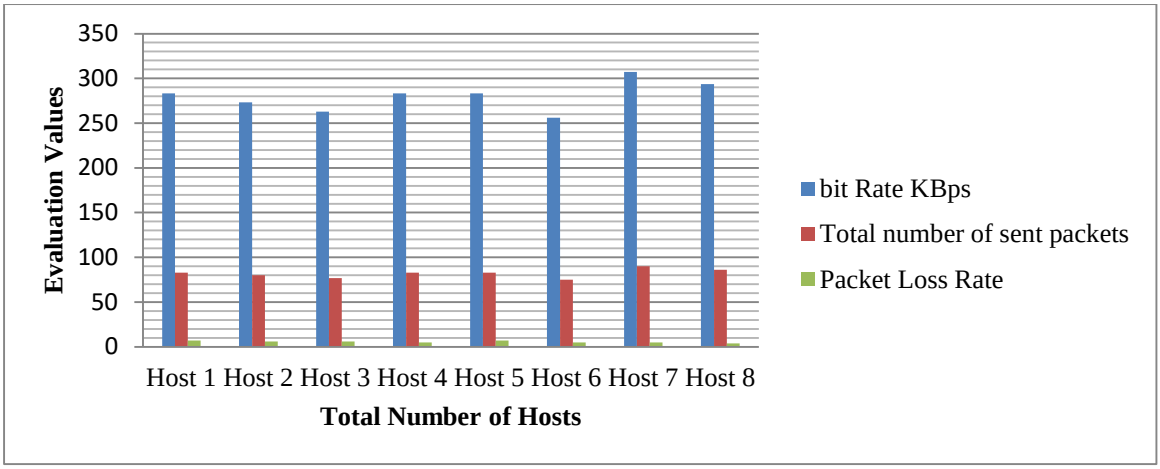


Figure 4.2: bit rate and total number of sent packets, and packet loss rate of 8 Hosts normal traffic.

4.2.3 The case of 16 wireless Hosts

The third state of the 16 normal wireless hosts simulated with 8 DDoS node and the evaluation parameters based on the different variables . The details showed in Table 4.11. It showed with increased number of Hosts effected on total bit rate ratio due to increased delay of Hosts

Table 4.11: bit Rate and mathematical Evaluations of 16 Hosts normal traffic.

Wireless Host Type	bit Rate KBps	Mean	Median	SD	Total bit Rate in Mbps
Host 1	129.7137	129.9274	133.1277	11.5232	16.63070 Mbps
Host 2	122.8868				
Host 3	136.5412				
Host 4	126.3008				
Host 5	143.3681				
Host 6	122.8864				
Host 7	133.1277				
Host 8	102.406				
Host 9	136.5406				
Host 10	139.9543				
Host 11	143.3685				
Host 12	133.1279				
Host 13	126.3008				
Host 14	109.2331				
Host 15	133.1277				
Host 16	139.9548				

Table 4.12: Throughput for the data signals of 16 Hosts normal traffic.

Wireless Host Type	Total number of sent packets	Total number of Acknowledge packets	Total Throughput in Mbps
Host 1	38	33	16.62976 Mbps
Host 2	36	32	
Host 3	40	37	
Host 4	37	35	
Host 5	42	38	
Host 6	36	30	
Host 7	39	36	
Host 8	30	28	
Host 9	40	34	
Host 10	41	36	
Host 11	42	40	
Host 12	39	37	
Host 13	37	35	
Host 14	32	30	
Host 15	39	36	
Host 16	41	38	

Table 4.13: Packet Loss Rate, and Packet Delivery Ratio of 16 Hosts normal traffic.

Wireless Host Type	Packet Loss Rate	Packet Delivery Ratio
Host 1	5	86.8421 %
Host 2	4	88.8889 %
Host 3	3	92.5 %
Host 4	2	94.5946 %
Host 5	4	90.4762 %
Host 6	6	83.3333 %
Host 7	3	92.3077 %
Host 8	2	93.3333 %
Host 9	6	85.0 %
Host 10	5	87.8049 %
Host 11	2	95.2381 %
Host 12	2	94.8718 %
Host 13	2	94.5946 %
Host 14	2	93.75 %
Host 15	3	92.3077 %
Host 16	3	92.6829 %

Table 4.14: Router to Firewall Delay, and Firewall to Server Delay of 16 Hosts normal traffic.

Wireless Host Type	Router to Firewall Delay	Firewall to Server Delay
Host 1	7256.664	5700.513
Host 2	7249.775	5695.102
Host 3	7251.152	5696.184
Host 4	7095.636	5574.016
Host 5	5941.128	6000.54
Host 6	5935.489	7492.103
Host 7	5936.613	7484.991
Host 8	7469.091	7486.413
Host 9	5644.072	7325.85
Host 10	5638.714	7886.424
Host 11	5639.785	7878.94
Host 12	5518.828	7880.43
Host 13	7638.593	7711.422
Host 14	7631.343	5994.846
Host 15	7632.788	5995.98
Host 16	5809.293	5867.386

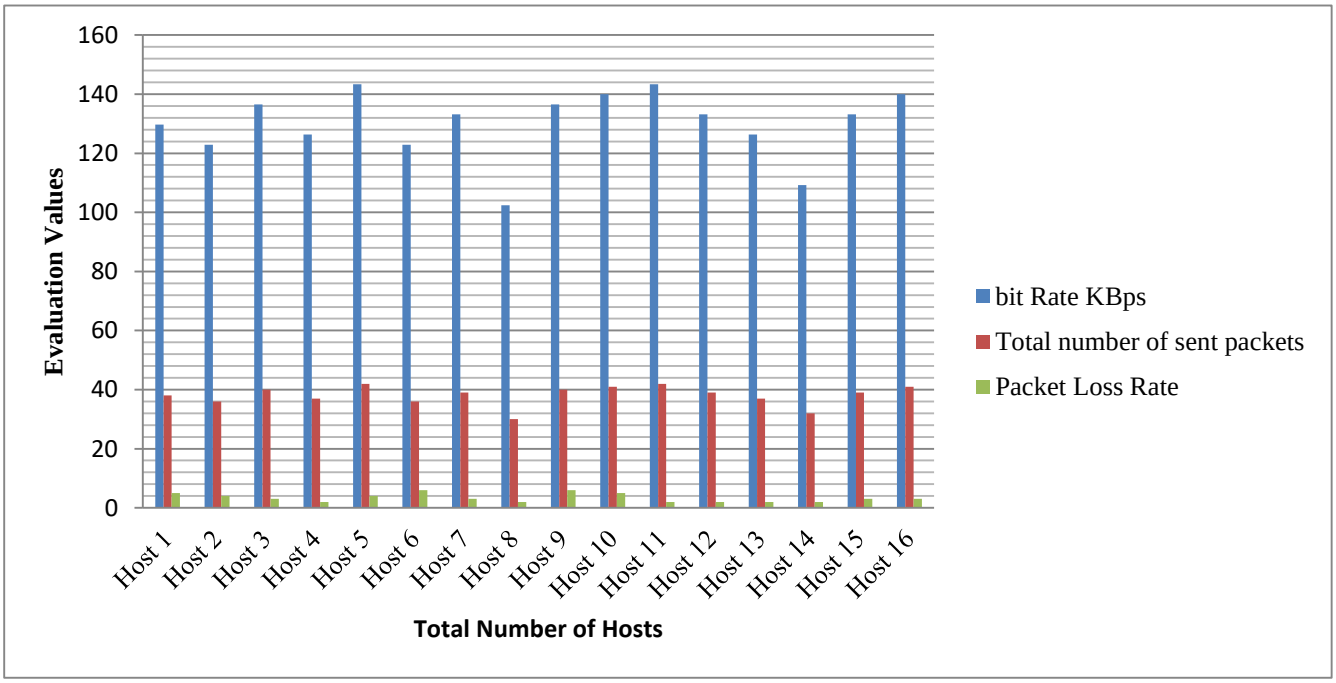


Figure 4.3: bit rate and total number of sent packets, and packet loss rate of 16 Hosts normal traffic.

4.3 Distributed Denial of Service (DDoS) attacks of wireless network

4.3.1 The case of 4 wireless Hosts

The first state of the 4 Hosts of normal traffic, and 2 Hosts of DDoS attack, the evaluation parameters based on the different variables . The data traffic details showed in Table 4.15. It showed total bit rate is decreased due to increased error rate bits of malicious Hosts, also delay packets are increased of normal packets due to the network is flooded with unwanted packets which effects on total network bandwidth.

Table 4.15: bit Rate Kbps Mean, Median, SD, and Total Bit Rate in Mbps of 4 Host DDoS traffic.

Wireless Host Type	bit Rate KBps	Mean	Median	SD	Total bit Rate in Mbps
Host 1	433.5159	354.1517	366.9523	78.20715	11.3328544
Host 2	249.1863				
Host 3	348.1779				
Host 4	385.7267				
DDoS Host 1	1300.48	1230.507	1230.507	98.95724	19.68810
DDoS Host 2	1160.533				

Table 4.16: Total number of sent packets, Total number of Acknowledge packets, and Total Throughput in Mbps of 4 Hosts DDoS traffic.

Wireless Host Type		Total number of sent packets	Total number of Acknowledge packets	Total Throughput in Mbps
Normal	Host 1	127	106	Sum(send)*1024KB/300 = 11.3322 Mbps
	Host 2	73	61	
	Host 3	102	84	
	Host 4	113	94	
DDoS	DDoS Host 1	381		10.4038 Mbps
	DDoS Host 2	340		

Table 4.17: Packet Loss Rate, and Packet Delivery Ratio of 4 Hosts DDoS traffic.

Wireless Host Type	Packet Loss Rate	Packet Delivery Ratio %
Host 1	21	83.4646 %
Host 2	12	83.5616 %
Host 3	18	82.3529 %
Host 4	19	83.1858 %

Table 4.18: Router to Firewall Delay, and Firewall to Server Delay of 4 Hosts DDoS traffic.

Wireless Host Type	Router to Firewall Delay in ms	Firewall to Server Delay in ms
Host 1	80629.59	91146
Host 2	80553.06	74964.91
Host 3	80568.33	86777.14
Host 4	78840.4	75972.52

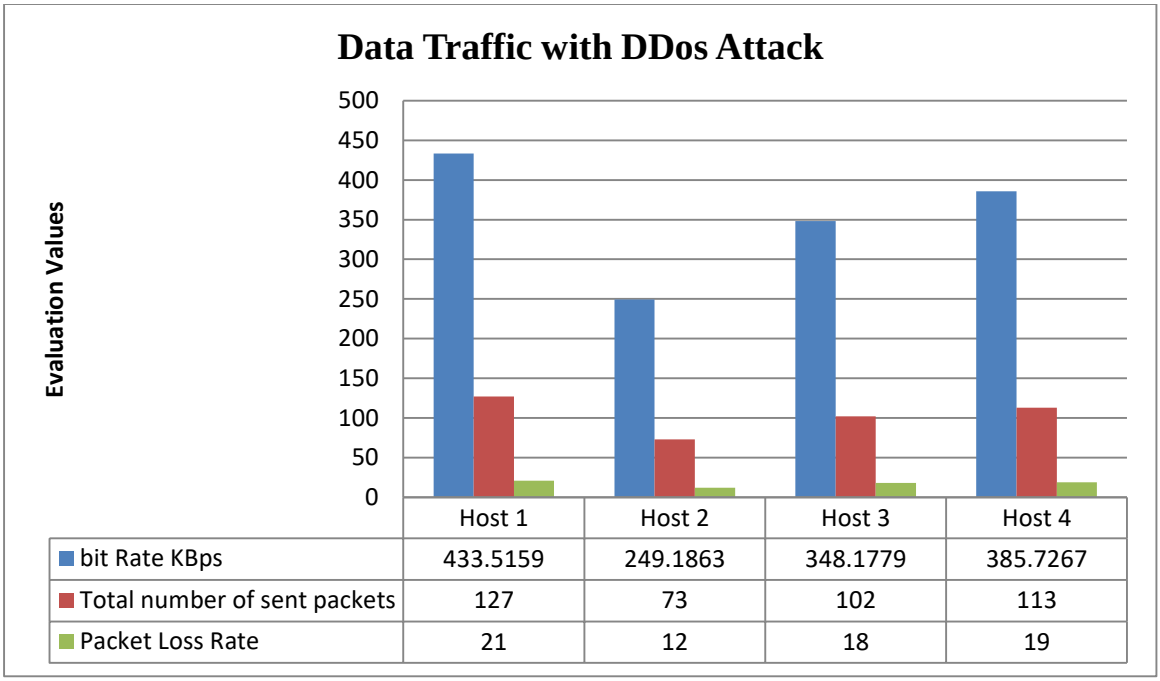


Figure 4.4: bit rate and total number of sent packets, and packet loss rate of 4 Hosts DDoS traffic.

4.3.2 The case of 8 wireless Hosts

It consists of 8 hosts of normal traffic and 4 hosts of DDoS attacks to effect on the network traffic and Table 4.19 showed the network evaluation of the case.

Table 4.19: bit Rate, with mathematical calculation of 8 Hosts DDoS traffic.

Wireless Host Type	bit Rate KBps	Mean	Median	SD	Total bit Rate in Mbps
Host 1	167.261	166.8345	167.261	9.557386	10.67741
Host 2	163.8477				
Host 3	157.0208				
Host 4	167.2612				
Host 5	167.261				
Host 6	153.6073				
Host 7	184.3287				
Host 8	174.0885				
DDoS Host 1	508.5867	519.68	517.12	26.19979	16.62976
DDoS Host 2	491.52				
DDoS Host 3	552.96				
DDoS Host 4	525.6533				

Table 4.20: Throughput for the data signals of 8 Hosts DDoS traffic..

Wireless Host Type	Total number of sent packets	Total number of Acknowledge packets	Total Throughput in Mbps
Host 1	49	36	10.67690 Mbps
Host 2	48	36	
Host 3	46	35	
Host 4	49	37	
Host 5	49	36	
Host 6	45	34	
Host 7	54	41	
Host 8	51	40	
DDoS Host 1	149		16.62976 Mbps
DDoS Host 2	144		
DDoS Host 3	162		
DDoS Host 4	154		

Table 4.21: Packet Loss Rate, and Packet Delivery Ratio of 8 Hosts DDoS traffic.

Wireless Host Type	Packet Loss Rate	Packet Delivery Ratio
Host 1	13	73.4694 %
Host 2	12	75 %
Host 3	11	76.087 %
Host 4	12	75.5102 %
Host 5	13	73.4694 %

Host 6	11	75.5556 %
Host 7	13	75.9259 %
Host 8	11	78.4314 %

Table 4.22: Router to Firewall Delay, and Firewall to Server Delay of 8 Hosts DDoS traffic.

Wireless Host Type	Router to Firewall Delay	Firewall to Server Delay
Host 1	20157.4	20033.23
Host 2	20138.26	20014.22
Host 3	20142.09	20018.02
Host 4	19710.1	19588.68
Host 5	21218.31	21087.61
Host 6	21198.18	21067.6
Host 7	21202.19	21071.59
Host 8	20747.48	20619.67

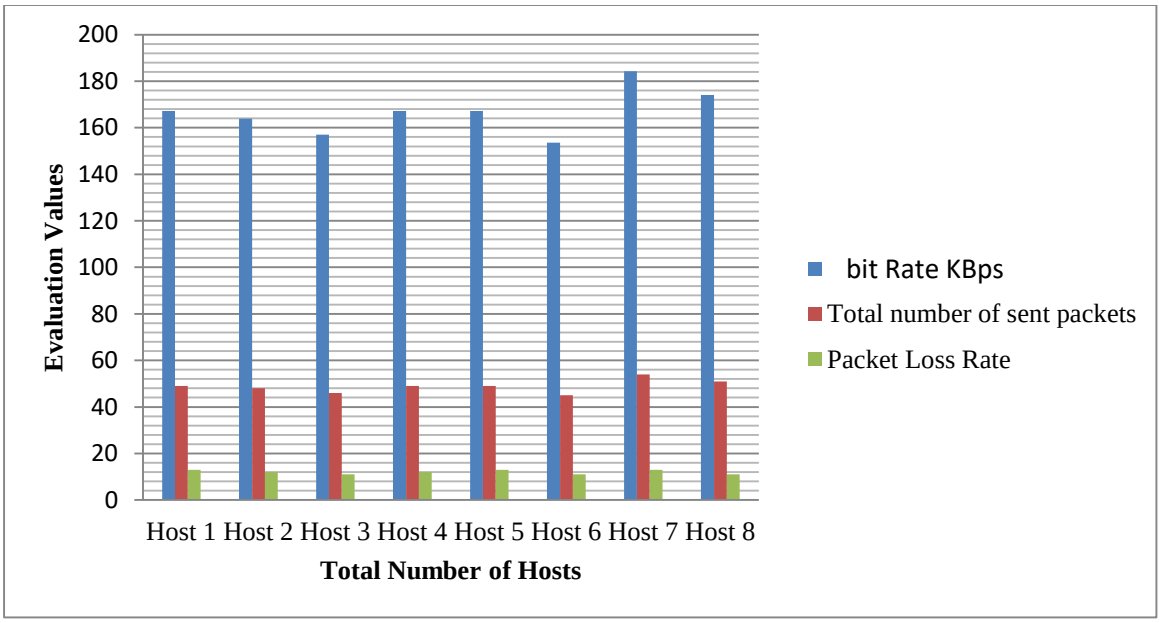


Figure 4.5: bit rate and total number of sent packets, and packet loss rate of 8 Hosts DDoS traffic.

4.3.3 The case of 16 wireless Hosts

The third state of the 16 normal wireless hosts simulated with 8 DDoS node and the evaluation parameters based on the different variables, as the topology . The data traffic details showed in Table 4.23. with increased number of Hosts the network latency is increased as total

delay of each Hosts and malicious DDoS Hosts generated error packets and flood network.

Table 4.23: Packet Rate with Total Bit Rate of 16 Hosts DDoS traffic.

Wireless Host Type	bit Rate KBps	Mean	Median	SD	Total bit Rate in Mbps
Host 1	75.09675	76.80367	78.51051	6.82699	9.83086
Host 2	71.68341				
Host 3	81.92384				
Host 4	75.09696				
Host 5	85.33739				
Host 6	71.6832				
Host 7	78.51051				
Host 8	61.44299				
Host 9	81.92363				
Host 10	81.92384				
Host 11	85.3376				
Host 12	78.51051				
Host 13	75.09696				
Host 14	64.85653				
Host 15	78.51051				
Host 16	81.92405				
DDoS Host 1	218.4533	227.84	228.6933	14.56749	14.58176
DDoS Host 2	232.1067				
DDoS Host 3	242.3467				
DDoS Host 4	235.52				
DDoS Host 5	225.28				
DDoS Host 6	211.6267				
DDoS Host 7	208.2133				
DDoS Host 8	249.1733				

Table 4.24: Throughput for the data signals of 16 Hosts DDoS traffic..

Wireless Host Type	Total number of sent packets	Total number of Acknowledge packets	Total Throughput in Mbps
Host 1	22	16	9.8304
Host 2	21	16	
Host 3	24	18	
Host 4	22	17	
Host 5	25	19	

Host 6	21	15	
Host 7	23	18	
Host 8	18	14	
Host 9	24	17	
Host 10	24	18	
Host 11	25	20	
Host 12	23	18	
Host 13	22	17	
Host 14	19	15	
Host 15	23	18	
Host 16	24	19	
DDoS Host 1	64		14.58176
DDoS Host 2	68		
DDoS Host 3	71		
DDoS Host 4	69		
DDoS Host 5	66		
DDoS Host 6	62		
DDoS Host 7	61		
DDoS Host 8	73		

Table 4.25: Packet Loss Rate, and Packet Delivery Ratio of 16 Hosts DDoS traffic.

Wireless Host Type	**Packet Loss Rate**	**Packet Delivery Ratio**
Host 1	6	72.7273 %
Host 2	5	76.1905 %
Host 3	6	75 %
Host 4	5	77.2727 %
Host 5	6	76 %
Host 6	6	71.4286 %
Host 7	5	78.2609 %
Host 8	4	77.7778 %
Host 9	7	70.8333 %
Host 10	6	75 %
Host 11	5	8 %
Host 12	5	78.2609 %
Host 13	5	77.2727 %
Host 14	4	78.9474 %
Host 15	5	78.2609 %
Host 16	5	79.1667 %

Table 4.26: Router to Firewall Delay, and Firewall to Server Delay of 16 Hosts DDoS traffic.

Wireless Host Type	Router to Firewall Delay in ms	Firewall to Server Delay in ms
Host 1	9070.83	7011.631
Host 2	9062.219	7004.975
Host 3	9063.94	7006.306
Host 4	8869.545	6856.04
Host 5	7426.41	7380.664
Host 6	7419.361	9215.287
Host 7	7420.766	9206.539
Host 8	9336.364	9208.288
Host 9	7055.09	9010.796
Host 10	7048.393	9700.302
Host 11	7049.731	9691.096
Host 12	6898.535	9692.929
Host 13	9548.241	9485.049
Host 14	9539.179	7373.661
Host 15	9540.985	7375.055
Host 16	7261.616	7216.885

Table 4.26 and Figure 4.6 showed the total average delay from router to firewall of each wireless host request which arrived to the Firewall through router is less than request delay from host to router to firewall to server due to the firewall delay after checkpoint of each request arrived to the server and match packet rate size if acceptable or not.

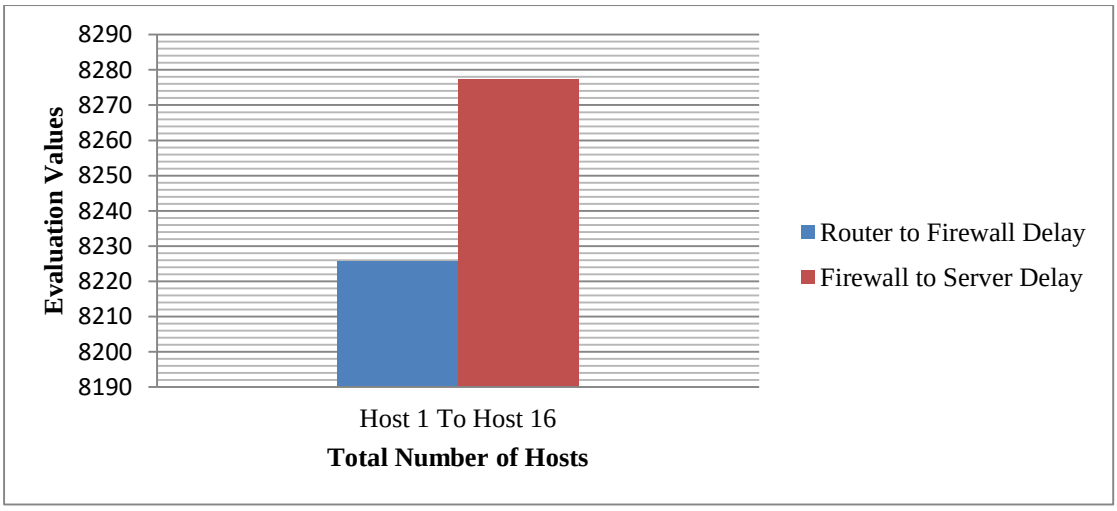


Figure 4.6 : Total average delay from router to firewall and from firewall to server of 16 Host DDOS traffic.

4.4 Distributed Denial of Service (DDoS) attacks mitigation of wireless network

4.4.1 The case of 4 hosts of the mitigation DDos attack system

The first state of the 4 Hosts with 2 DDoS attack hosts and the evaluation parameters based on the different variables, as the topology. The data traffic details showed in Table 4.27. It showed normal data rate is increased due to the filtration firewall of huge traffic from DDoS hosts which effected on network performance in overall and caused flooding unwanted packets in the used wireless network. In addition, DDoS attack traffic is decreased and limited by dropping large packet size and discarded with block source IP packet from the route table interface of firewall.

Table 4.27: bit Rate Kbps Mean, Median, SD, and Total Bit Rate in Mbps of 4 Hosts in system mitigation DDoS traffic.

Wireless Host Type	bit Rate KBps	Mean	Median	SD	Total bit Rate in Mbps
Host 1	614.4	506.0267	525.6534	108.7054	16.19285 Mbps
Host 2	358.4				
Host 3	501.76				
Host 4	549.5467				
DDoS Host 1	167.2533	158.72	158.72	12.06796	2.53952 Mbps
DDoS Host 2	150.1867				

Table 4.28 showed the increased total throughput of successful packets of normal hosts and decreased DDoS host traffic on the network compared with previous case study of DDoS attack case which is registered as 10.4038 Mbps of the DDoS Hosts traffic.

Table 4.28: Total number of sent packets, Total number of Acknowledge packets, and Total Throughput in Mbps of 4 Hosts in system mitigation DDoS traffic.

Wireless Host Type	Total number of sent packets	Total number of Acknowledge packets	Total Throughput in Mbps
Host 1	180	167	Sum(send)*1024KB/300 = 16.1928533 Mbps
Host 2	105	97	
Host 3	147	136	

Host 4	161	150	
DDoS Host 1	49		
DDoS Host 2	44		2.53952 Mbps

Table 4.29 showed the packet delivery ratio of normal packet is enhanced and decreased compared with the case of DDoS attack detection case due to the increased number of arrived packets without error and acknowledged from the final destination server and loss packet is decreased due to the network flooding is enhanced with the proposed firewall.

Table 4.29: Packet Loss Rate, and Packet Delivery Ratio of 4 Hosts in system mitigation DDoS traffic.

Wireless Host Type	Packet Loss Rate	Packet Delivery Ratio %
Host 1	13	92.7778 %
Host 2	8	92.381 %
Host 3	11	92.517 %
Host 4	11	93.1677 %

Table 4.30 showed the total average delay of the incoming request from Hosts to the router to the firewall in milliseconds is less than from the case of DDoS attack case due to the incoming request is processed more flexibility and fast in the network while in case of DDoS attack is not also server redirect reply in better speed compared with DDos attack due to the normal traffic packets is larger than abnormal packets.

Table 4.30: Router to Firewall Delay, and Firewall to Server Delay of 4 Hosts in system mitigation DDoS traffic.

Wireless Host Type	Router to Firewall Delay in ms	Firewall to Server Delay in ms
Host 1	72244.11	82253.71
Host 2	72175.54	67651.26
Host 3	72189.22	78311.08
Host 4	70641	68560.57

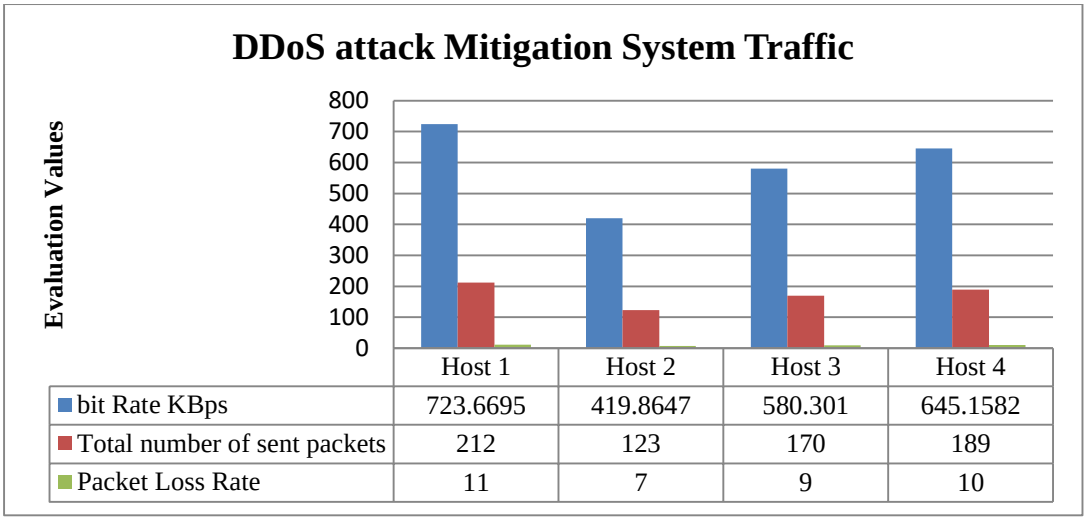


Figure 4.7: bit rate and total number of sent packets, and packet loss rate of 4 Hosts in system mitigation DDoS traffic.

4.4.2 The case of 8 Hosts of the mitigation DDos attack system

The second case of the proposed mitigation system is based on 8 normal traffic hosts, with 4 DDoS attack hosts which mitigated traffics through the determining data rate with required time of normal traffic and recognize the DDoS abnormal traffic during the traffic and adaptation approach. Table 4.31 showed the network evaluation of 8 hosts in the proposed DDoS mitigation system.

Table 4.31: Packet Rate and mathematical evaluation with Total Bit Rate of 8 Hosts in system mitigation DDoS traffic.

Wireless Host Type	bit Rate KBps	Mean	Median	SD	Total bit Rate in Mbps
Host 1	245.7737	242.3604	245.7737	14.48246	15.51106 Mbps
Host 2	235.5332				
Host 3	225.2928				
Host 4	245.7741				
Host 5	245.7737				
Host 6	221.8793				
Host 7	266.2554				
Host 8	252.6014				
DDoS Host 1	64.85333	66.56	66.56	4.406594	2.12992
DDoS Host 2	61.44				
DDoS Host 3	71.68				
DDoS Host 4	68.26667				

Table 4.32: Throughput for the data signals of 8 Hosts in system mitigation DDoS traffic.

Wireless Host Type	Total number of sent packets	Total number of Acknowledge packets	Total Throughput in Mbps
Host 1	72	64	15.51123 Mbps
Host 2	69	62	
Host 3	66	60	
Host 4	72	66	
Host 5	72	64	
Host 6	65	59	
Host 7	78	72	
Host 8	74	69	
DDoS Host 1	19		2.97642 Mbps
DDoS Host 2	18		
DDoS Host 3	21		
DDoS Host 4	20		

Table 4.33: Packet Loss Rate, and Packet Delivery Ratio of 8 Hosts in system mitigation DDoS traffic.

Wireless Host Type	Packet Loss Rate	Packet Delivery Ratio
Host 1	8	88.8889 %
Host 2	7	89.8551 %
Host 3	6	90.9091 %
Host 4	6	91.6667 %
Host 5	8	88.8889 %
Host 6	6	90.7692 %
Host 7	6	92.3077 %
Host 8	5	93.2432 %

Table 4.34: Router to Firewall Delay, and Firewall to Server Delay of 8 Hosts in system mitigation DDoS traffic.

Wireless Host Type	Router to Firewall Delay	Firewall to Server Delay
Host 1	18061.03	18078.77
Host 2	18043.88	18061.61
Host 3	18047.31	18065.04
Host 4	17660.25	17677.59
Host 5	19011.61	19030.28
Host 6	18993.56	19012.22
Host 7	18997.16	19015.82
Host 8	18589.74	18608

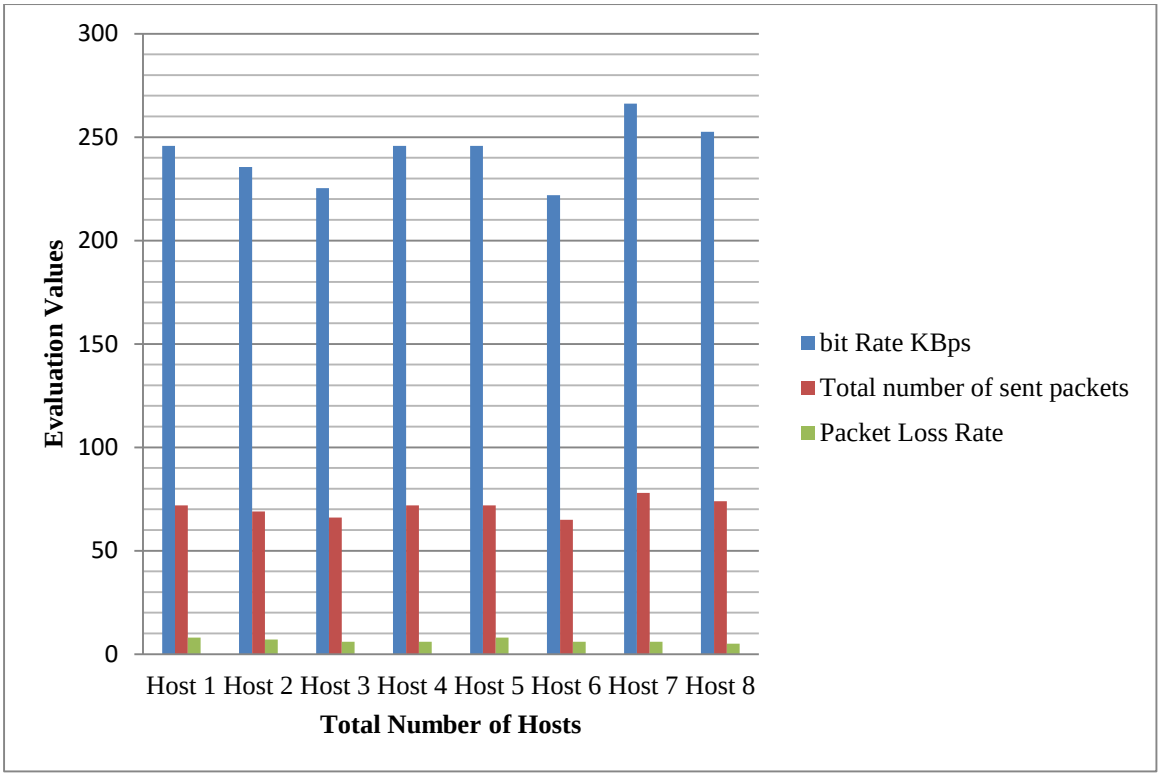


Figure 4.8: bit rate and total number of sent packets, and packet loss rate of 8 Hosts in system mitigation DDoS traffic.

4.4.3 The case of 16 wireless Hosts

The third state of the 16 normal wireless hosts simulated with 8 DDoS node and the evaluation parameters based on the different variables, as the topology . The data traffic showed in Table 4.35.

Table 4.35: bit Rate Mbps with mathematical evaluation of 16 Hosts in system mitigation DDoS traffic.

Wireless Host Type	bit Rate KBps	Mean	Median	SD	Total bit Rate in Mbps
Host 1	112.646	111.1529	112.6464	9.652408	14.22756 Mbps
Host 2	105.8191				
Host 3	116.0599				
Host 4	109.2329				
Host 5	122.8868				
Host 6	105.8187				
Host 7	112.6464				
Host 8	88.75157				
Host 9	116.0593				
Host 10	119.4731				

Host 11	122.8873				
Host 12	112.6466				
Host 13	109.2329				
Host 14	92.16533				
Host 15	112.6464				
Host 16	119.4735				
DDoS Host 1	27.30667				
DDoS Host 2	20.48				
DDoS Host 3	30.72				
DDoS Host 4	27.30667	26.45333	27.30667	3.533136	1.69301 Mbps
DDoS Host 5	23.89333				
DDoS Host 6	27.30667				
DDoS Host 7	23.89333				
DDoS Host 8	30.72				

Table 4.36: Throughput for the data signals of 16 Hosts in system mitigation DDoS traffic.

Wireless Host Type	**Total number of sent packets**	**Total number of Acknowledge packets**	**Total Throughput in Mbps**
Host 1	33	28	14.226773 Mbps
Host 2	31	27	
Host 3	34	31	
Host 4	32	29	
Host 5	36	32	
Host 6	31	25	
Host 7	33	30	
Host 8	26	23	
Host 9	34	28	
Host 10	35	30	
Host 11	36	34	
Host 12	33	31	
Host 13	32	29	
Host 14	27	25	
Host 15	33	30	
Host 16	35	32	
DDoS Host 1	8		1.69301 Mbps
DDoS Host 2	6		
DDoS Host 3	9		
DDoS Host 4	8		
DDoS Host 5	7		
DDoS Host 6	8		
DDoS Host 7	7		
DDoS Host 8	9		

Table 4.37: Packet Loss Rate, and Packet Delivery Ratio of 16 Hosts in system mitigation DDoS traffic.

Wireless Host Type	Packet Loss Rate	Packet Delivery Ratio
Host 1	5	84.8485 %
Host 2	4	87.0968 %
Host 3	3	91.1765 %
Host 4	3	90.625 %
Host 5	4	88.8889 %
Host 6	6	80.6452 %
Host 7	3	90.9091 %
Host 8	3	88.4615 %
Host 9	6	82.3529 %
Host 10	5	85.7143 %
Host 11	2	94.4444 %
Host 12	2	93.9394 %
Host 13	3	90.625 %
Host 14	2	92.5926 %
Host 15	3	90.9091 %
Host 16	3	91.4286 %

Table 4.38: Router to Firewall Delay, and Firewall to Server Delay of 16 Hosts in system mitigation DDoS traffic.

Wireless Host Type	Router to Firewall Delay	Firewall to Server Delay
Host 1	11703.55	9111.7
Host 2	11692.44	9103.051
Host 3	11694.66	9104.78
Host 4	11443.84	8909.508
Host 5	9581.851	9591.263
Host 6	9572.758	11975.38
Host 7	9574.57	11964.01
Host 8	12046.15	11966.28
Host 9	9102.76	11709.64
Host 10	9094.118	12605.66
Host 11	9095.845	12593.7
Host 12	8900.765	12596.08
Host 13	12319.52	12325.93
Host 14	12307.82	9582.162
Host 15	12310.16	9583.975
Host 16	9369.228	9378.43

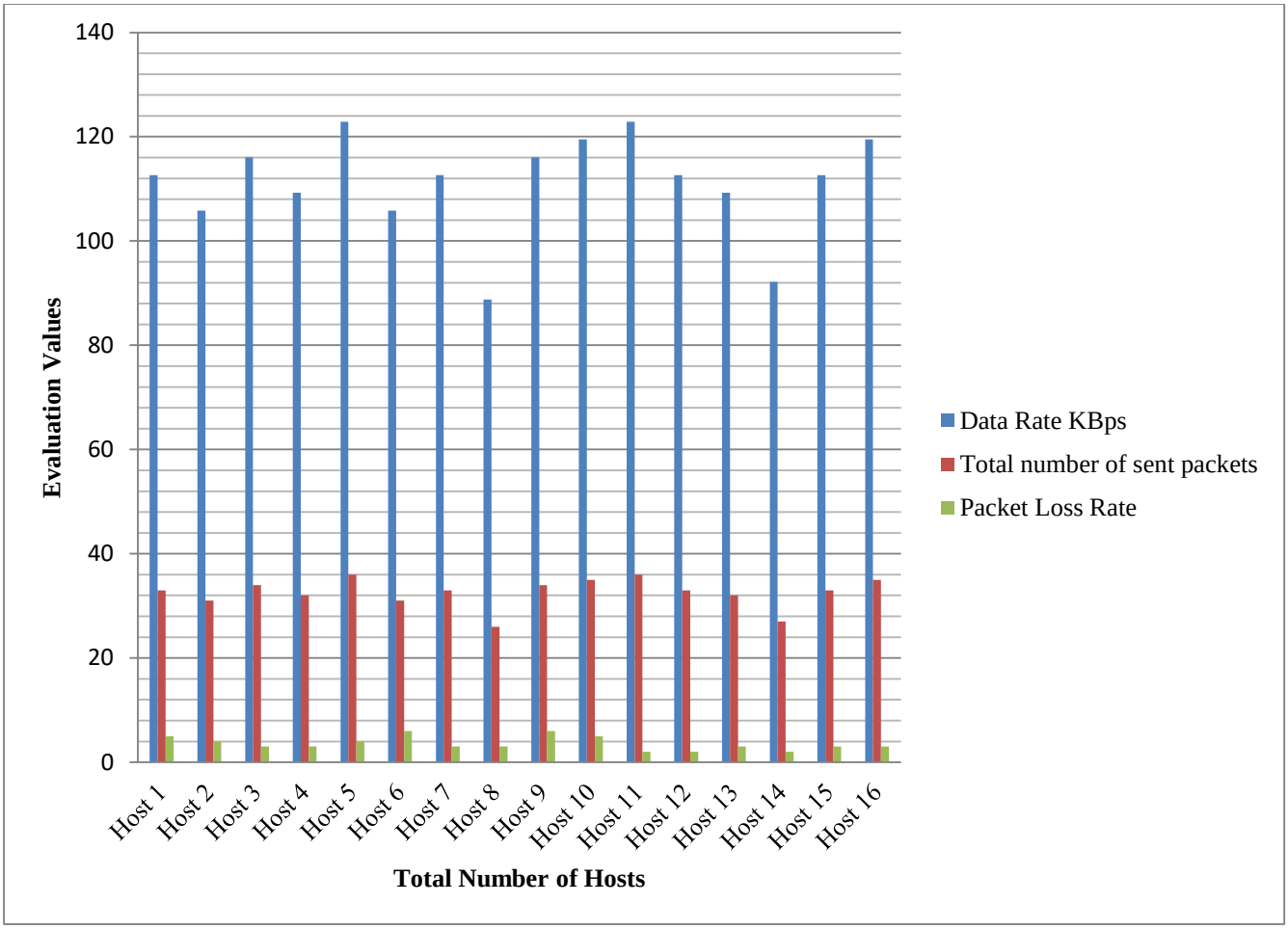


Figure 4.9: data rate and total number of sent packets, and packet loss rate of 16 Hosts in system mitigation DDoS traffic.

4.5 System Comparison

The proposed system compared among three main cases as showed in Figure(4.10), Figure(4.11) and Figure(4.12). It compared with the main network evaluation parameters with Total Bit Rate in Mbps, total throughput in Mbps, total packet loss rate in percentage, and average of total delay in seconds of three main cases as: 4, 8, and 16 Hosts data traffic.

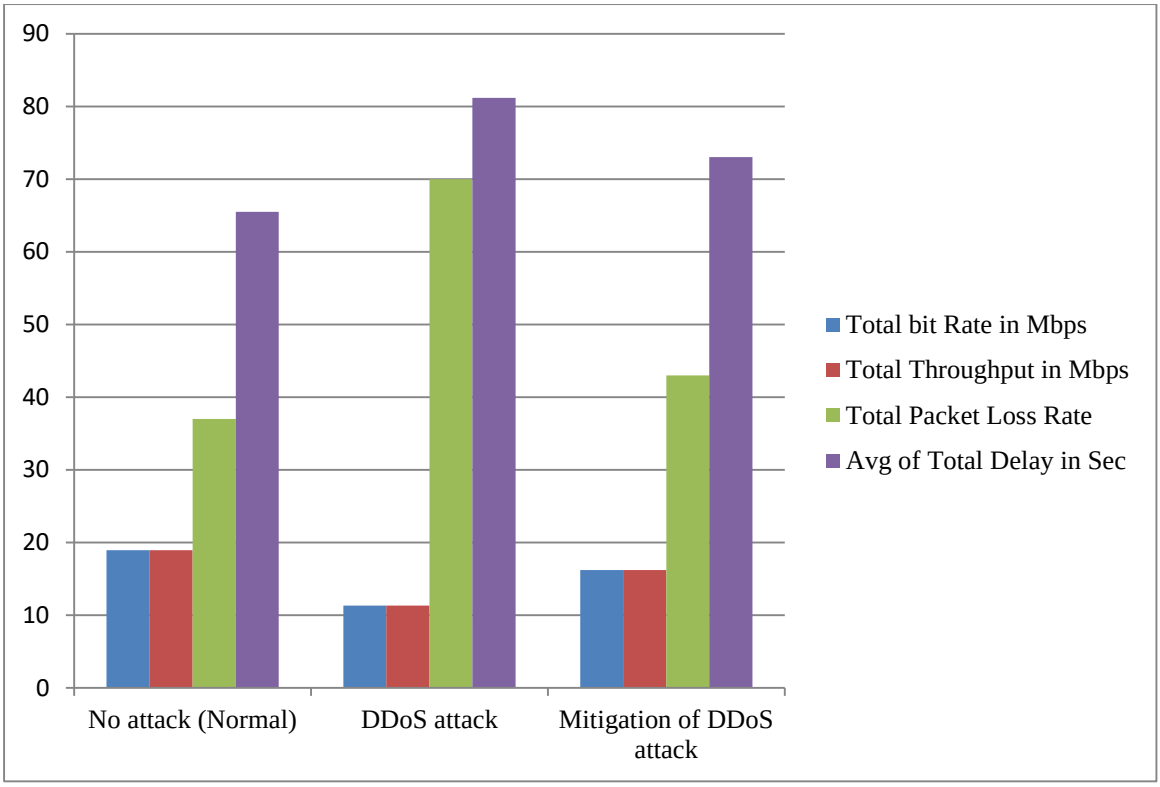


Figure 4.10: Total bit Rate in Mbps, Total Throughput in Mbps, Total Packet Loss Rate, Avg of Total Delay in Seconds of 4 Hosts data traffic.

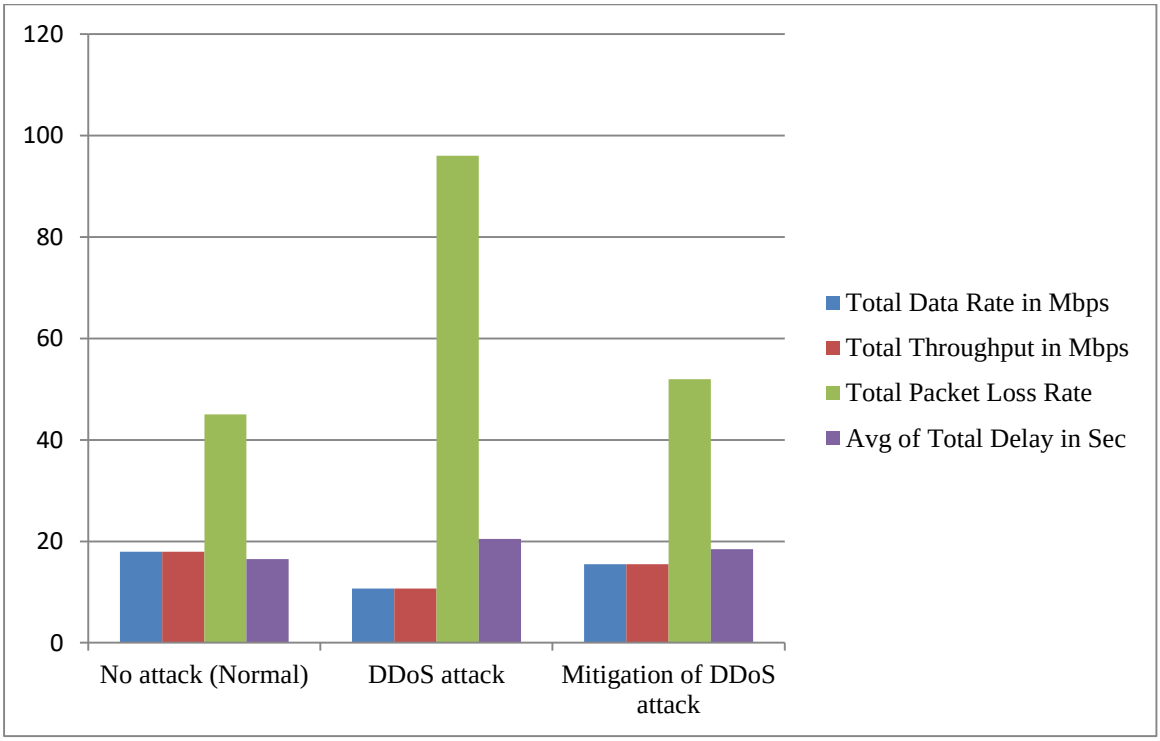


Figure 4.11: Total Bit Rate in Mbps, Total Throughput in Mbps, Total Packet Loss Rate, Avg of Total Delay in Seconds of 8 Hosts data traffic.

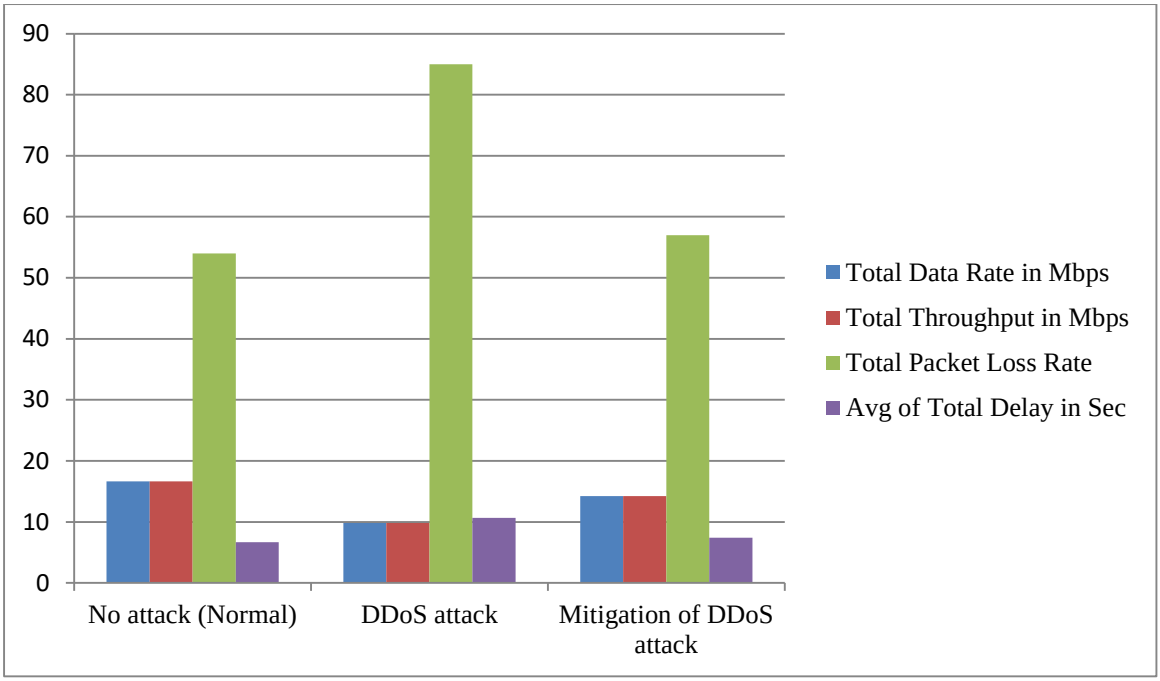


Figure 4.12: Total Bit Rate in Mbps, Total Throughput in Mbps, Total Packet Loss Rate, Avg of Total Delay in Seconds of 16 Hosts data traffic.

The proposed system compared with the two case studies and with other related works as showed in Table 4.39.

Table 4.39 : System Comparison among three case studies of Normal traffic, DDoS attack trffic, and DDoS attack mitigation systems.

Normal Traffic (No Attack)				
No. of Hosts	Total Bit Rate in Mbps	Total Throughput in Mbps	Total Packet Loss Rate	Avg of Total Delay in Sec
4 Hosts	18.9519472	18.9508	37	65.4799275
8 Hosts	17.94152	17.9405	45	16.53365813
16 Hosts	16.6307	16.6298	54	6.65500325
DDoS Traffic				
4 Hosts	11.3328544	11.3322	70	81.18149375
8 Hosts	10.67741	10.6769	96	20.50091438
16 Hosts	9.83086	9.8304	85	10.684737

Proposed System Mitigation against DDoS attack				
4 Hosts	16.1928536	16.19285	43	73.00331125
8 Hosts	15.51106	15.5112	52	18.43461688
16 Hosts	14.22756	14.22677	57	7.419956344

Table 4.40: The proposed system comparison with other related works.

Ref.No	Year	No. of nodes	Environment	Method	Packet Drop Rate %	PDR %	Throughput In KB
[11]	2020	4 nodes	MATLAB	Proactive DoS/DDoS mitigation technique	0.14 %	/	/
[12]	2020	20 nodes	NS-2 Simulator	(P-Secure) approach	0.15 %	85 %	1590 KB
				OBUmodelVaNET	0.52 %	38 %	500 KB
Proposed – Mitigation DDoS attack system		4 nodes	OMNET ++ Simulator	Maximum Data Rate as Traffic Analysis and Adaptation(TAA)	0.072513	92.71%	2024.106 KB
		8 nodes			0.091549	90.82%	1938.9 KB
		16 nodes			0.109405	89.04%	1778.346 KB

Chapter Five

Conclusion and Future Work

5.1 Conclusion

1- The proposed system based on the used MDR (Maximum data rate) algorithm to recognize normal and abnormal packet traffic as it match packet traffic compared with stored threshold in firewall scheme.

2- The proposed system is based on:-

A- Normal operation of Wireless network.

B- DDOS attack of wireless network.

3- The proposed Filtration rule in Firewall identify source IP and MDR metric with timestamp of each incoming request by verify source MAC and interface ID through Log configuration network performance file and recognize normal and abnormal behavior of connected wireless hosts.

4- The proposed system results showed that the used algorithm minimized lose rate packet and mitigation DDOS attack effectiveness on the wireless network in addition total delay is minimize.

4- Average of total Delay in sec of No attack (normal)is 6.65500325 seconds, DDos is 10.684737 seconds, and Mitigation of DDos attack is 7.419956344 seconds, Total Packet Loss Rate of No attack (normal)is 54, DDos is 85, and Mitigation of DDos attack is 57. Total Throughput in Mbps of No attack (normal)is 16.62976 Mbps , DDos is 9.8304 Mbps , and Mitigation of DDos attack is 14.226773 Mbps . Total Bit Rate in Mbps of No attack (normal)is 16.6307 Mbps , DDos is 9.83086 Mbps , and Mitigation of DDos attack is 14.22756 Mbps .

5.2 Future Work

There are numerous considerations can be realized for future expansion of present research through utilizing the following propositions:

1. Using Blockchain approach for DDOS attack mitigation in the proposed system.
2. Appling machine learning and deep learning in intelligent framework classify and mitigate in DDOS attack traffic and normal traffic in the proposed system.
3. Building a privacy-enhanced DDoS attack detection and defense for Cyber-Physical Systems.
4. Implement lightweight crypto system to authenticate wireless channel allocation to prevent malicious user to communication with authorize users.
5. Practical side implementation of DDOS attack prevention method with anomaly base real time.

REFERENCES

[1] Bhushan, B. (2022). Intrusion Detection System (IDS) for Security Enhancement in Wireless Sensing Applications. In *Innovations in Electronics and Communication Engineering: Proceedings of the 9th ICIECE 2021* (pp. 39-49). Singapore: Springer Singapore.

[2] Sharma, M., Jindal, K., & Sharma, B. K. (2014). Analysis of IDS Tools & Techniques. *International Journal of Emerging Technology and Advanced Engineering Website: www. ijetae. com (ISSN 2250-2459 (Online), Volume 4, Special Issue 1*.

[3] Agong, R. (2021). Wireless sensor and mobile ad-hoc networks for the internet of things: a survey. *J. Innov. Res. Solut.(JIRAS)*, *10*(1), 2.

[4] Mitchell, R., & Chen, R. (2014). A survey of intrusion detection in wireless network applications. *Computer Communications*, *42*, 1-23.

[5] Xia, T., Qu, G., Hariri, S., & Yousif, M. (2005, April). An efficient network intrusion detection method based on information theory and genetic algorithm. In *PCCC 2005. 24th IEEE International Performance, Computing, and Communications Conference, 2005.* (pp. 11-17). IEEE.

[6] Gu, G., Fogla, P., Dagon, D., Lee, W., & Skoric, B. (2005). *An information-theoretic measure of intrusion detection capability*. Georgia Institute of Technology.

[7] Behal, S., Kumar, K., & Sachdeva, M. (2018). A generalized detection system to detect distributed denial of service attacks and flash events for information theory metrics. *Turkish Journal of Electrical Engineering and Computer Sciences*, *26*(4), 1759-1770.

[8] Bala, K., Jothi, S., & Chandrasekar, A. (2019). An enhanced intrusion detection system for mobile ad-hoc network based on traffic analysis. *Cluster Computing*, *22*, 15205-15212.

[9] Tang, D., Dai, R., Tang, L., & Li, X. (2020). Low-rate DoS attack detection based on two-step cluster analysis and UTR analysis. *Human-centric Computing and Information Sciences*, *10*, 1-20.

[10] Islam, R., Refat, R. U. D., Yerram, S. M., & Malik, H. (2020). Graph-based intrusion detection system for controller area networks. *IEEE Transactions on Intelligent Transportation Systems*.

[11] 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*(4), 870-878.

[12] Fotohi, R., Ebazadeh, Y., & Geshlag, M. S. (2020). A new approach for improvement security against DoS attacks in vehicular ad-hoc network. *arXiv preprint arXiv:2002.10333*.

[13] Anand, C., & Vasuki, N. (2021). Trust based DoS attack detection in wireless sensor networks for reliable data transmission. *Wireless Personal Communications*, *121*(4), 2911-2926.

[14] Singh, V., Sharma, G., Poonia, R. C., Trivedi, N. K., & Raja, L. (2021). Source redundancy management and host intrusion detection in wireless sensor networks. *Recent Advances in Computer Science and Communications (Formerly: Recent Patents on Computer Science)*, *14*(1), 43-47.

[15] Pajila, P. B., Julie, E. G., & Robinson, Y. H. (2022). FBDR-Fuzzy based DDoS attack Detection and Recovery mechanism for wireless sensor networks. *Wireless Personal Communications*, 1-31.

[16] Sulaiman, N. S., Nasir, A., Othman, W. R. W., Wahab, S. F. A., Aziz, N. S., Yacob, A., & Samsudin, N. (2021, May). Intrusion Detection System Techniques: A Review. In *Journal of Physics: Conference Series* (Vol. 1874, No. 1, p. 012042). IOP Publishing.

[17] Oryspayuli, O. D. (2006). *What intrusion detection approaches work well if only TCP/IP packet header information is available* (Doctoral dissertation, Master Thesis, Faculty of Electrical Engineering, Mathematics and Computer Science, University of Twente, Enschede, The Netherlands).

[18] Bahrami, M., & Bahrami, M. (2012). An overview to software architecture in intrusion detection system. *arXiv preprint arXiv:1205.4385*.

[19] Mishra, A., & Srivastava, A. K. (2013). A Survey on Intrusion Detection System for Wireless Network. *International Journal of Computer Applications*, *73*(21), 37-40.

[20] Tewatia, R., & Mishra, A. (2015). Introduction To Intrusion Detection System. *International journal of scientific & technology research*, 219-223.

[21] Jatti, S. A. V., & Sontif, V. K. (2019). Intrusion detection systems. *International Journal of Recent Technology and Engineering*, *8*(2), 3976-3983.

[22] Asharf, J., Moustafa, N., Khurshid, H., Debie, E., Haider, W., & Wahab, A. (2020). A review of intrusion detection systems using machine and deep

learning in internet of things: Challenges, solutions and future directions. *Electronics*, *9*(7), 1177.

[23] Shanmugam, B., & Idris, N. B. (2011). Hybrid intrusion detection systems (HIDS) using Fuzzy logic. *Intrusion Detection Systems*, 1-21.

[24] Ayodeji, A., Liu, Y. K., Chao, N., & Yang, L. Q. (2020). A new perspective towards the development of robust data-driven intrusion detection for industrial control systems. *Nuclear engineering and technology*, *52*(12), 2687-2698.

[25] Khraisat, A. (2019). Gondal I Vamplew P Kamruzzaman J. *Survey of intrusion detection systems: techniques, datasets and challenges Cybersecurity*, *2*(1), 1.

[26] Hoque, M. S., Mukit, M. A., & Bikas, M. A. N. (2012). An implementation of intrusion detection system using genetic algorithm. *arXiv preprint arXiv:1204.1336*.

[27] Aminanto, E., & Kim, K. (2016). Deep learning in intrusion detection system: An overview. In *2016 International Research Conference on Engineering and Technology (2016 IRCET)*. Higher Education Forum.

[28] Agrawal, S., Sarkar, S., Aouedi, O., Yenduri, G., Piamrat, K., Alazab, M., ... & Gadekallu, T. R. (2022). Federated learning for intrusion detection system: Concepts, challenges and future directions. *Computer Communications*.

[29] Khan, M. A. (2021). HCRNNIDS: Hybrid convolutional recurrent neural network-based network intrusion detection system. *Processes*, *9*(5), 834.

[30] Niyaz, Q., Sun, W., Javaid, A. Y., & Alam, M. (2015, December). A deep learning approach for network intrusion detection system. In *Proceedings of the 9th EAI International Conference on Bio-inspired Information and Communications Technologies (Formerly BIONETICS), BICT-15* (Vol. 15, No. 2015, pp. 21-26).

[31] Zhang, D., & Yeo, C. K. (2010, January). A novel architecture of intrusion detection system. In *2010 7th IEEE Consumer Communications and Networking Conference* (pp. 1-5). IEEE.

[32] Ioulianou, P. P., & Vassilakis, V. G. (2019, September). Denial-of-service attacks and countermeasures in the RPL-based Internet of Things. In *International Workshop on the Security of Industrial Control Systems and Cyber-Physical Systems* (pp. 374-390). Cham: Springer International Publishing.

[33] Kizza, J., & Kizza, F. M. (2008). Intrusion detection and prevention systems. In *Securing the Information Infrastructure* (pp. 239-258). IGI Global.

[34] Garfinkel, T., & Rosenblum, M. (2003, February). A virtual machine introspection based architecture for intrusion detection. In *Ndss* (Vol. 3, No. 2003, pp. 191-206).

[35] Reis, M., Paula, F., Fernandes, D., & Geus, P. (2002, May). A hybrid ids architecture based on the immune system. In *Anais do II Workshop em Segurança de Sistemas Computacionais* (pp. 127-134). SBC.

[36] Semerci, M., Cemgil, A. T., & Sankur, B. (2018). An intelligent cyber security system against DDoS attacks in SIP networks. *Computer Networks*, *136*, 137-154.

[37] Toulouse, M., Minh, B. Q., & Curtis, P. (2015, August). A consensus based network intrusion detection system. In *2015 5th International Conference on IT Convergence and Security (ICITCS)* (pp. 1-6). IEEE.

[38] Singh, J., Kaur, L., & Gupta, S. (2012). A cross-layer based intrusion detection technique for wireless networks. *Int. Arab J. Inf. Technol.*, *9*(3), 201-207.

[39] Ponnusamy, V., Humayun, M., Jhanjhi, N. Z., Yichiet, A., & Almufareh, M. F. (2022). Intrusion Detection Systems in Internet of Things and Mobile Ad-Hoc Networks. *Comput. Syst. Sci. Eng.*, *40*(3), 1199-1215.

[40] Kabila, R. (2008). Network Based Intrusion Detection and Prevention Systems in IP-Level Security Protocols. *network security*, *7*, 11.

[41] Srivastav, N., & Challa, R. K. (2013, February). Novel intrusion detection system integrating layered framework with neural network. In *2013 3rd IEEE International Advance Computing Conference (IACC)* (pp. 682-689). IEEE.

[42] Uppal, H. A. M., Javed, M., & Arshad, M. (2014). An overview of intrusion detection system (IDS) along with its commonly used techniques and classifications. *International Journal of Computer Science and Telecommunications*, *5*(2), 20-24.

[43] Liu, H., & Lang, B. (2019). Machine learning and deep learning methods for intrusion detection systems: A survey. *applied sciences*, *9*(20), 4396.

[44] Jakić, P. (2019). The overview of intrusion detection system methods and techniques. In *Sinteza 2019-International Scientific Conference on Information Technology and Data Related Research* (pp. 155-161). Singidunum University.

[45] Amudha, P., Karthik, S., & Sivakumari, S. (2015). A hybrid swarm intelligence algorithm for intrusion detection using significant features. *The Scientific World Journal*, *2015*.

[46] Naveen, N. C. (2012). Application of relevance vector machines in real time intrusion detection. *International Journal of Advanced Computer Science and Applications*, *3*(9).

[47] Agranovskiy, A. V., Repalov, S. A., Khadi, R. A., & Yakubets, N. M. (2006). Disadvantages of Modern Intrusion Detection Systems. *Telecommunications and Radio Engineering*, *65*(6-10).

[48] Vyas, G., Meena, S., & Kumar, P. (2014). Intrusion detection systems: a modern investigation. *Int. J. Eng. Man. Sci.(IJEMS)*, *1*(11).

[49] MUTHUKUMAR, J. (2015). Intrusion Detection System (IDS): Anomaly Detection using Outlier Detection Approach. In *International Conference on Intelligent Computing, Communication & Convergence (ICCC-2015)* (Vol. 48).

[50] Peddisetty, N. R. (2005). State-of-the-art Intrusion Detection: Technology, Challenges, and Evaluation.

[51] Xu, H., Wen, S., Gimenez, A., Gamblin, T., & Liu, X. (2017, May). DR-BW: identifying bandwidth contention in NUMA architectures with supervised learning. In *2017 IEEE International Parallel and Distributed Processing Symposium (IPDPS)* (pp. 367-376). IEEE.

[52] Muslim, A. B., Christoph, C., & Toenjes, R. (2022, May). Modeling Time Synchronization in WLANs in OMNeT++. In *Mobile Communication-Technologies and Applications; 26th ITG-Symposium* (pp. 1-6). VDE.

[53] Hosseini, H., Rojas, E., & Carrascal, D. (2021). Implementation of RPL in OMNeT++. *arXiv preprint arXiv:2107.02551*.

[54] Velásquez, K., & Gamess, E. (2014). Network Performance Evaluation Based on Three Processes. *Journal of Computer Sciences and Applications*, *2*(2), 14-22.

[55] Khan, M. F., Felemban, E. A., Qaisar, S., & Ali, S. (2013, December). Performance analysis on packet delivery ratio and end-to-end delay of different network topologies in wireless sensor networks (WSNs). In *2013 IEEE 9th International Conference on Mobile Ad-hoc and Sensor Networks* (pp. 324-329). IEEE.

[56] Gali, T. A. B., AB, A., & Mustafa, N. (2015). The Impact of Firewall Security for Wireless Performance. *International Journal of Scientific & Technology Research*, *4*(6), 20-22.

[57] Dong, S., Abbas, K., & Jain, R. (2019). A survey on distributed denial of service (DDoS) attacks in SDN and cloud computing environments. *IEEE Access*, *7*, 80813-80828.

[58] Su, C. (2019, September). Big data security and privacy protection. In *2019 International Conference on Virtual Reality and Intelligent Systems (ICVRIS)* (pp. 87-89). IEEE.

[59] Saad, M., Thai, M. T., & Mohaisen, A. (2018, May). POSTER: deterring ddos attacks on blockchain-based cryptocurrencies through mempool optimization. In *Proceedings of the 2018 on Asia conference on computer and communications security* (pp. 809-811).

[60] Laskowski, P. P. (2017). Internet security–technology and social awareness of the dangers. *Studies in Logic, Grammar and Rhetoric*, *50*(1), 239-252.

[61] Gupta, V., Goswami, S., Kumar, A., & Singh, M. (2004). Networking and Security measures. *DESIDOC Bulletin of Information Technology*, *24*(2), 9-16.

[62] Hashiguchi, M., & Takamatsu, K. (2011). Security Measures for Production Control Systems. *Yokogawa Technical Report English Edition*, *54*(2).

[63] Ion, A. (2016). IMPLEMENTING ENISA'S CYBER SECURITY PLAN IN THE EUROPEAN UNION. In *International Scientific Conference" Strategies XXI"* (Vol. 3, p. 151). " Carol I" National Defence University.

[64] Landau, S. (2000). Standing the test of time: The data encryption standard. *Notices of the AMS*, *47*(3), 341-349.

[65] Tseng, Y., Nait-Abdesselam, F., & Khokhar, A. (2018, May). SENAD: Securing network application deployment in software defined networks. In *2018 IEEE International Conference on Communications (ICC)* (pp. 1-6). IEEE.

[66] Loukas, G., Gan, D., & Vuong, T. (2013). A review of cyber threats and defence approaches in emergency management. *Future Internet*, *5*(2), 205-236.

[67] Coruh, U., Khan, M., & Bayat, O. (2021, December). Lightweight Offline Authentication Scheme for Secure Remote Working Environment. In *2021 International Conference on Electrical, Computer and Energy Technologies (ICECET)* (pp. 1-9). IEEE.

[68] Tawalbeh, L. A., Muheidat, F., Tawalbeh, M., & Quwaider, M. (2020). IoT Privacy and security: Challenges and solutions. *Applied Sciences*, *10*(12), 4102.

[69] Abiodun, O. I., Abiodun, E. O., Alawida, M., Alkhawaldeh, R. S., & Arshad, H. (2021). A review on the security of the internet of things: challenges and solutions. *Wireless Personal Communications*, *119*, 2603-2637.

[70 Liao, H. J., Lin, C. H. R., Lin, Y. C., & Tung, K. Y. (2013). Intrusion detection system: A comprehensive review. *Journal of Network and Computer Applications*, *36*(1), 16-24.

.

الخلاصة

تعد أنظمة كشف المتسللين (IDS) أكثر الطرق فعالية للدفاع ضد الهجمات القائمة على الشبكة في انظمة الشبكات اللاسلكية. وتُستخدم هذه الأنظمة في جميع مكونات البنية التحتية واسعة النطاق تقريبًا ، وتتأثر بأنواع مختلفة من هجمات الشبكة مثل هجمات DDoS.

هجمات حجب الخدمات الموزعة (DDoS) التي تم إطلاقها ضد العديد من أجهزة الشبكة الرئيسية والتي تتطلب تدابير أمنية لحماية الشبكة ، تستخدم العديد من البروتوكولات والأنظمة المصممة لتقديم خدمات مثل الخوادم والتي تخضع بطبيعتها لهجمات DDoS. يمكن استخدام طريقة اكتشاف هجوم DDoS لحماية أنظمة الشبكة من هجمات DDoS في المرحلة المبكرة من التهديد ، ويمكن وضع الاستجابة لتقليل الأضرار ، وجمع الأدلة للتحقق ، وكذلك لأنشاء نظام حماية مضاد للهجمات.

يعتمد النظام المقترح على الانحراف (ABS) لبناء نموذج تكوين سجل يصف حركة مرور الشبكة العادية كقائمة بيضاء ، وأي سلوك غير طبيعي كقائمة سوداء توفر قاعدة اكتشاف ضد هجمات DDoS. يحدد عنوان IP المصدر وعنوان MAC والطابع الزمني. تعتمد المنهجية المقترحة على نهج مطابقة الحد الأقصى لمعدل البيانات (MDR) لمطابقة طلب الحد الأقصى لحركة المرور مع القيمة المخزنة لتحديد سلوك حركة المرور كحركة مرور عادية وغير طبيعية. بعد ذلك ، بعد ذلك يرفض حركة المرور غير الطبيعية عن طريق تصفية النموذج في جهاز جدار الحماية الفايرول او الجدار الناري. وأظهرت النتائج أن الأسلوب المقترح لهجمات حجب الخدمة (هجمات DDoS) كأفضل نتائج لاكتشاف DDoS لـ ١٦ عقدة هي ٠,١٠٩ معدل إسقاط و ٨٩,٠٤٪ معدل تسليم الحزم في الشبكة PDR ومعدل نقل ١٧٧٨,٣٤٦ كيلوبايت.

جمهورية العراق
وزارة التعليم العالي والبحث العلمي
جامعة بابل
كلية تكنولوجيا المعلومات
قسم شبكات المعلومات

إكتشاف وتخفيف هجمات DDOS
في الشبكات اللاسلكية أعتماداً على معدل البيانات الأقصى

رسالة مقدمة الى

مجلس كلية تكنلوجيا المعلومات – جامعة بابل كجزء من متطلبات نيل درجة الماجستير في تكنلوجيا المعلومات / شبكات المعلومات

من قبل

نور حسنين هاشم طارش

بأشراف

أ.د. ستار بدر سدخان

هـ 1444 م 2023