Republic of Iraq
Ministry of Higher Education and Scientific Research
University of Babylon
College of Science for Women
Department of Computer Science

PROTECTING AN IDENTITY OF IPv6 PACKET AGAINST DoS ATTACK BASED ON CRYPTOGRAPHY AND HIDING TECHNIQUE

A thesis

Submitted to the Council of the College of Science for Women at the University of Babylon in Partial Fulfillment of the Requirements for the Degree of Master in Science/ Computer Science

By

Maytham Hakim Ali

(The University of Babylon, College of Science for Women, Computer Department, *2022)*

Supervised *by*

Asst. Prof.Dr. Saif M.Kh Al-Alak

2022 A.D. **1443 A.H.**

بسم الله الرحمن الرحيم

قلْ هَلْ يَسْتَوِي الَّذِينَ يَعْلَمُونَ وَالَّذِينَ لَا يَعْلَمُونَ ۗ إِنَّمَا يَتَذَكَّرُ أُولُو الْأَلْبَابِ ﴿9﴾

صدق الله العظيم

سورة الزمر/اية 9

Certification of the Examination Committee

We, the chairman and members of the examining committee, certify that we have read this thesis entitled (**PROTECTING AN IDENTITY OF IPv6 PACKET AGAINST DoS ATTACK BASED ON CRYPTOGRAPHY AND HIDING TECHNIQUE**) and after examining the master student **(Maytham Hakim Ali)** in its contents in 31/3/2022 and that in our opinion it is adequate as a thesis Committee Chairman for degree on Master in Science \Computer Science with degree **(Excellent).**

Committee Chairman

Signature:

Name: **Mahdi Nsaif Jasim**

Scientific order: Asst. Prof. Dr.

Address: University of Information Technology and communication\

College of Business Informatics

Committee Member

Signature:

Name: **Muhammed A. Mahdi**

Scientific order: Asst. Prof. Dr.

Address: : University of Babylon\ College of Science for Women

Date: / 4/ 2022

Committee Member

Signature:

Name: **Aladdin Abbas Abdulhassan**

Scientific order: Lecturer. Dr

Address: University of Babylon /College Information Technology

Date: Date: / 4/ 2022

Committee Member (**Supervisor**)

Signature:

Name: **Saif M.Kh Al-Alak**

Scientific order: Asst. Prof. Dr.

Address: University of Babylon, College of Sciences for Women

Date: / 4/ 2022

Approved by the Dean of the College of Science for Women, University of Babylon

Signature:

Name: Faez Ali Al-Mamoori

Address: University of Babylon, College of Sciences for Women

Title: Prof . Dr.

Date: / 4/ 2022

Supervisor Certification

I certify that this thesis titled " Protecting an Identity of IPv6 Packet Against DoS Attack Based on Cryptography and Hiding Technique" was done by (Maytham Hakim Ali) under my supervision.

Signature:

Name: Asst. Prof. Dr. Saif M.Kh Al-Alak

Date:

Address: University of Babylon/College of Science for Women

The Head of the Department Certification

In view of the available recommendation, I forward the thesis entitled " Protecting an Identity of IPv6 Packet Against DoS Attack Based on Cryptography and Hiding Technique " for debate by the examination committee.

Signature:

Name: Lecturer. Dr. Farah Mohammed Hassan Al-Shareefi

Date:

Address: University of Babylon/College of Science for Women

Dedication

Thanks for ALLAH in the first and last place, my Creator, to teacher and messenger, Mohammed (May Allah bless and grant him), who taught us the purpose of life.

The great martyrs, the symbol of sacrifice, to the spirit of my dear father, God has mercy on him, and to my beloved family who encourages and supports me, and all the people in my life, I dedicate this thesis.

Maytham Hakim Ali 2022

Acknowledgments

Praise and thanks for God who enabled me to complete my study and facilitated the difficulties for me. Thanks for all my teachers in the college of science for women, particularly I am highly indebted expressing my thanks to the supervisor on this thesis Dr. Saif Al-Alak for his excellent guidance and encouragement to complete my thesis.

I would like to thank my family for their love, patience, and understanding to spend my time on this thesis. This accomplishment would not have been possible without them.

Finally, I would like to thank all my friends and all the people who helped me during my Master's study.

Maytham Hakim Ali 2022

Abstract

Nowadays, Information security has become an important issue in the digital life. The development of new technologies for data transmission may enforce particular strategies used for security mechanisms. Specific cases of data communication cases. Network security requires daily attention as a result of the volume of data that network transmission. Encryption and steganography each provided critical technologies for data security.

IPv6 provides an identification and location systems for computers on networks and routes traffic across the Internet. The proposed system is based on protecting an identity of IPV6 packet against the problem of Denial-of-Service (DoS) attack, depend on the proposed methods of cryptography and hiding. Reliable communication using the security aspect is the most visible issue, particularly in IPv6 network applications. Problems such as DoS attacks, IP spoofing and other kinds of passive attacks are common.

The used method suggests an approach based on generating a randomly unique identities for every node. The generated identity is encrypted and hided in the transmitted packets of the sender side, in the receiver side, the received packet verified to identify the source before processed. During this work involves implementing nine experiments that are used to test the proposed method based on creating the address of IPV6, then passing to the logistics map and then to the Rivest–Shamir–Adleman (RSA) and Secure Hash Algorithm (SHA2) algorithm. The results show that the suggested system generates a high random identity for each node and hides the node's identity within the package. In addition, network performance has be simulated using of OPNET modular.

The results showed that the case study of without DoS attack as traffic sent is 30,324 Packets/s, traffic received is 27,227 Packets/s, and lose packets is 3,097 Packets/s. In addition, the case study of with Dos attack as traffic sent is 33,412 Packets/s, traffic received is 24,139, and lose packets is 9,273 Packets/s.

Table of Contents

List of Tables

Table of Figures

Table of Abbreviations

ABS	Advanced Bits Security
AES	Advanced Encryption Standard
ASIC	Application-Specific Integrated Circuits
AH	Authentication Header
DAD	Duplicate Address Detection
DoS	Denial-of-Service
DCT	discrete cosine transform
DHCP	Dynamic Host Configuration Protocol
ESP	Encapsulating Security Payload
HLEN	Header length
ISO/OSI	International Standard Organization's Open System Interconnect
IP	Internet Protocol
IPv6	Internet Protocol version 6
IPsec	Internet Protocol Security
MTD	Moving Target Defense
MD 5	Message-Digest 5 algorithm
NIST	National Institute of Standards and Technology
NAT	Network Address Translators
NS	Neighbor Solicitation
NA	Neighbor Advertisement
OSI	Open System Interconnection
PDUs	Protocol Data Units
PMTUD	Path MTU Discovery
PLPMTUD	Packetization Layer Path MTU Discovery
QoS	Quality of service
RSA	Rivest, Shamir and Adleman algorithm
RC5	Rivest Cipher algorithm
SHA2	Secure Hash Algorithm algorithm
SFTP	Secure File Transfer Protocol

HTTPS	Secure Hypertext Transfer Protocol
SSL	Secure Socket Layer
SAD	Security Association Database
SPI	Security Parameter Index
SPD	Security Policy Database
TCP/IP	Transmission Control Protocol/Internet Protocol
TOS	Type of Service
Tor	The Onion Router

List of Thesis Related Publications

Name of Conference/ Journal: Journal of Physics: Conference Series (IF), Pub Date : 2021-09-21, DOI: 10.1088/1742-6596/1999/1/012120.

- **1st Paper Title: Using Unique Node ID TO Control IPv6 ID Spoofing.**
- **2nd Paper Title: Node Protection using Hiding Identity for IPv6 Based Network.**
  - Maytham Hakim Ali
  - Asst. Prof.Dr. Saif Al-Alak

Department of Computer Science, College of Science for Women, University of Babylon.

Email: **maytham.ali@student.uobabylon.edu.iq**

Email: **saif.mahmood@uobabylon.edu.iq**

https://iopscience.iop.org/article/10.1088/1742-6596/1999/1/012120/meta

IOP Publishing

2nd International Virtual Conference on Pure Science
College of Science, University of Al-Qadisiyah
21th-22th April 2021

No. Computer Science 14
Date: 15/04/2021

Acceptance Letter

We are pleased to inform you that your manuscript entitled

Using Unique Node ID TO Control IPv6 ID Spoofing

has been accepted for online publication in the 2nd International Virtual Conference on Pure Science that will held in College of Science, University of Al-Qadisiyah, Iraq, at the IOP publishing, Journal of Physics: Conference Series, April 2021.

Authors and Affiliation Details:

Maytham Hakim Ali Department of software, College of Science for Women, University of Babylon, Hillah, Iraq
Saif Al-Alak Department of software, College of Science for Women, University of Babylon, Hillah, Iraq

Thank you for your contribution to 2nd International Virtual Conference on Pure Science

Sincerely

Assist. Prof. Dr. Salwan Ali Abed
Conference Chairman
Copy to:
- Conference Secretary

For more details, please visit the conference website and do not hesitate to contact us if you want further info https://qu.edu.iq/2IVCPS (+9647800436997)

IOP Conference Series conferenceseries.iop.org
Journal of Physics: Conference Series

Indexed by:
Scopus THOMSON REUTERS

2nd Al-Muthanna International Conference on Engineering Science and Technology MICEST 2022

To:

13/03/2022

Maytham Hakim Ali, Saif Al-Alak

University of Babylon

Email: maytham.ali@student.uobabylon.edu.iq

We are pleased to inform you that the peer reviewed manuscript code **MIC-22222** entitled **(Node Protection using Hiding Identity for IPv6 Based Network) by** Maytham Hakim Ali and Saif Al-Alak has been accepted for oral presentation as well as inclusion in the conference proceedings of the 2nd Al-Muthanna International Conference on Engineering Science and Technology MICEST-2022 to be held at Al-Muthanna University, Samawah, Iraq during March, 16-17, 2022.

All the IEEE track accepted papers will also be considered for publication in the Scopus-indexed conference proceeding at IEEE Xplore

We are looking forward to welcoming you in the MICEST 2022: 2nd Al-Muthanna International Conference on Engineering Science and Technology.

Sincerely,
Conference co-chair, Prof. Dr. Ahmed Hasan Ali
MICEST 2022
https://micest.org/

Chapter One

General Introduction

1.1 Overview

In an increasingly connected world, more and more devices are being networked together than ever before. This trend will continue with not only more laptop and desktop computers needing to be able to talk to one another around the world, besides it based on personal digital assistant (PDA), cell phones, cars, and, eventually, even toasters, and other household items. Most networked devices today are connected through Internet Protocol version 4 (IPv4) and Internet Protocol version 6 (IPv6) as the most recent version of the Internet Protocol (IP), a layer three protocols of the International Standard Organization's Open System Interconnect (ISO/OSI) model[1].

The Open System Interconnection (OSI) model is a seven-layer structure that specifies the requirements for communications between two computers. This model allows all network elements to operate together, no matter who created the protocols and what computer vendor supports them. It offers a generic means to separate computer networking functions into multiple layers. Each of these layers relies on the layers below it to provide supporting capabilities and performs support to the layers above it. Such a model of layered functionality is also called a “protocol stack” or “protocol suite”[2].

Protocols, or rules, can do their work in either hardware or software or, as with most protocol stacks, in a combination of the two. The nature of these stacks is that the lower layers do their work in hardware or firmware (software that runs on specific hardware chips) while the higher layers work in software[3].

Internet Protocol version 6 is the most recent version of the Internet Protocol, the communications protocol that provides an identification and location system for computers on networks and routes traffic across the Internet. It is the next generation Internet Protocol (IP) standard intended to eventually replace IPv4[4].

Furthermore, the IPv6 offers many improvements over IPv4, and Table 1.1 compares IPv4 and IPv6 operation at a glance [5].

- More efficient routing. IPv6 routers no longer have to fragment packets, an overhead-intensive process that just slows a network down.
- Quality of service (QoS) built-in. IPv4 has no way to distinguish delay-sensi-tive packets from bulk data transfers, requiring extensive workarounds, but IPv6 does.
- Elimination of NAT to extend address spaces. IPv6 increases the IPv4 address size from 32 bits (about 4 billion) to 128 bits (enough for every molecule in the solar system).
- Network layer security built-in (IPsec). Security, always a challenge in IPv4, is an integral part of IPv6.
- Stateless address auto configuration for easier network administration. Many IPv4 installs were complicated by manual default router and address assignment. IPv6 handles this in an automated fashion.
- Improved header structure with less processing overhead. Many of the fields in the IPv4 header were optional and used infrequently. IPv6 eliminates these fields (options are handled differently)[6].

Besides, Table 1.1 showed the main IPv4 and IPv6 comparison.

Table 1.1 The Key IPv4 and IPv6 Comparisons[7].

IPv4	**IPv6**
32-bit (4 byte) address supporting 2^32 addresses (4.19 billion addresses)	128-bit (16 byte) address supporting 2^128 addresses (7.9 x 10^28 addresses)
NAT can be used to extend address limitations	No NAT support (by design)
IP addresses assigned to hosts by DHCP or static configuration	IP addresses self-assigned to hosts with stateless address auto-configuration or DHCPv6
IPSec support optional	IPSec support required
Options integrated in header fields	Options supported with extensions headers (simpler header format)

While, the Transport Layer is responsible for process-to-process delivery of the entire message.TL looks after the delivery of entire message considering all its packets & make sure that all packets are in order. On the other hand n/w layer treated each packet independently [8].

Besides, the Application Layer enables the user to access the network. It provides user interface & supports for services such as e-mail, file transfer, access to the world wide web. So it provides services to different user applications [9].

Alongside, the computer networks components comprise both physical parts as well as the software required for installing computer networks, both at organizations and at home. The hardware components are the server, client, peer, transmission medium, and connecting devices. The software components are operating system and protocols. The following Figure (1.1) shows a network along with its components[10].

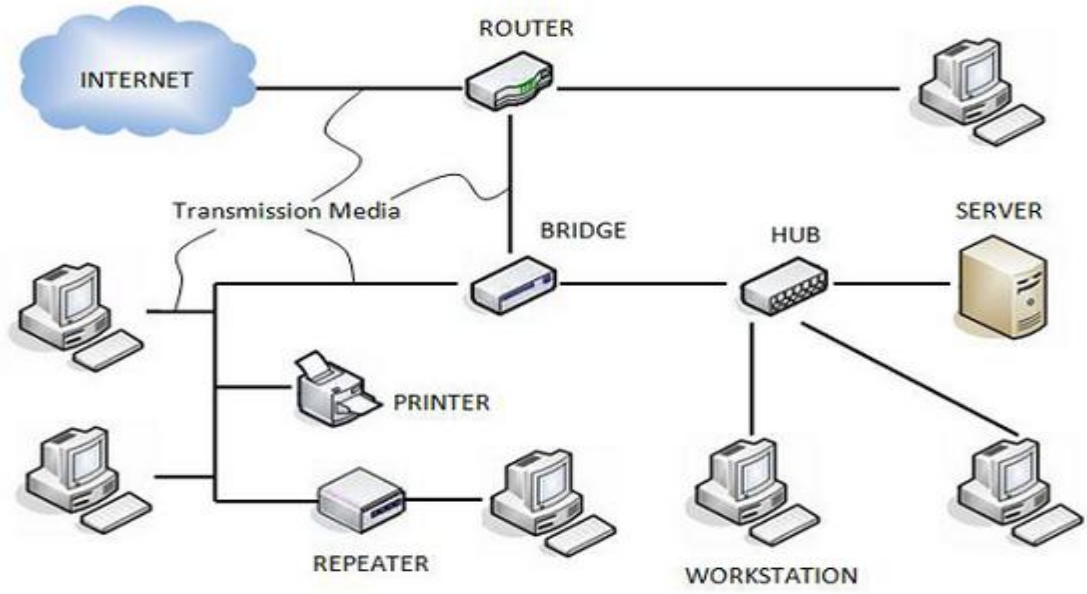


Figure 1.1: The computer Network Components[10].

Besides, there are different attacks effect on the network component for instance Denial-of-Service (DoS) attack, namely, the denial of service, which it is resulting in a network denial of service attack known as DoS attacks, and its purpose is to make the server or network fail to provide normal services[11].

The most common DoS attack against a computer network includes bandwidth and connectivity attacks. Bandwidth attack refers to attacks with great impact on network traffic, so that all available network resources are depleted, leading to legitimate users' requests cannot be passed[12].

Connectivity attack with plenty of connection requests that the impact of server operating systems so that all available resources are exhausted. As a result, the server cannot process legitimate user's request[13].

1.2 Related Works

In this section, the most related works have been discussed and overviewed as follow:

As well as, in (Hu et al., 2017), TrueID, an IPv6 header extension scheme which can embed hash-based, creditable and undeniable user identity code inside IPv6 packets. They present the system architecture ,header's format and viable implementation approaches with different credibility granularities. Meanwhile, to verify packet credibility and integrity, it designs an Autonomous System(AS) level public-key distribution system which can disseminate user's publickeys between allied ASes safely. Also, the proto type experiment has proved that the scheme possesses these features with desirable performance[14].

Besides in (Cabaj et al., 2018), they present a network steganography technique. The extension headers hide secret caring data it from point to point across a network. They focus on a malware exploiting information hiding in a broad sense, i.e., it does not focus on classical covert channels, but also discusses other camouflage techniques. Differently from other works, they solely focus on real-world threats. The observation indicates a growing number of malware equipped with some form of data hiding capabilities and a lack of effective and universal countermeasures[15].

In (Rahman et al., 2019) they aim to prevent those malicious nodes from sending spoof reply by securing both Neighbor Solicitation (NS) and Neighbor Advertisement (NA). The proposed Advanced Bits Security (ABS) technique is based on Blake2 algorithm and introducing a

creative option called ABS field that holds the hash value of tentative IP address and attached to both NA and NS message. They expect the ABS technique can prevent spoof reply during Duplicate Address Detection (DAD) procedure in link local network and can prevent DoS attack [16] .

Besides in (Fahrnberger et al., 2019) a description of network steganography methods has been proposed. The proposed framework acts as an effectively applicable method against all modeled threats and utilizes available cryptographic means. That utilize mechanisms for handling oversized IP packets: IP fragmentation, PMTUD (Path MTU Discovery) and PLPMTUD (Packetization Layer Path MTU Discovery). The used system of security and performance analyses rigorously evaluate the utility, quality, and efficacy of the framework[17].

Also, in (Pachghare et al., 2019) Secure data communication using protocol steganography in IPv6 as 20-bit flow label field of ipv6 protocol used as covert channel. It's worth mentioning that Rivest, Shamir and Adleman(RSA) algorithm was employed for data encryption. While, the chaotic method was used for data encoding [18] .

In (Hossen et al., 2019) they proposes a new approach to hiding the data using steganography techniques based on Advanced Encryption Standard (AES) and Rivest Cipher (RC5) algorithm cryptosystem. Steganography is the beauty of hiding secret data behind the digital images, videos, audios and text to cover the secret communication. Cryptosystem is the process which given the method more perfection. This propose method and algorithm capacity is highly flexible than other published algorithm. The

AES and RC5 algorithm has no complexity and it looks like very well to hiding the confidential data[19].

In (Mavani et al., 2020) reducing IPv6 spoofing attack disruption time in 6LoWPANs. Hence, it provides the resiliency against IPv6 spoofing threat. The time complexity analysis of the attack tree for the spoofing attack is performed to analyze the attack disruption time. The analytical results show that attack disruption window is directly proportional to the lifetime of the node addresses. Corrupted routing table as a result of spoofing attack and its countermeasure is simulated in Cooja running Contiki operating system. The higher frequency of address change decreases the attack disruption time with an increase in the communication cost. Simulations have been performed to compare the optimum value of address change periodicity concerning the communication cost for two private addressing schemes proposed in the literature[20].

While in (Čerňanský et al., 2020) they focuse on design, background and experimental results of real environment of DDoS attacks. In proposed testbed, Ansible orchestration tool is employed to perform and coordinate DDoS attacks. Moreover, no special hardware is required for the attacks execution, the testbed uses existing infrastructure in an organization. The case study of implementation of this environment shows straightforwardness to create a testbed comparable with a botnet with ten thousand bots. Furthermore, the experimental results demonstrate the potential of the proposed environment and present the impact of the attacks on particular target servers in IPv4 and IPv6 networks[21].

In (Zhou et al., 2021) a two-layer IP hopping-based MTD approach is proposed, in which device IP addresses or virtual IP addresses change or hop according to the network security status and requirements. The proposed Moving Target Defense (MTD) scheme is implemented in the developed MANET terminals, providing three level of network security: anti-intrusion in normal environment, intrusion detection in offensive environment and anti-eavesdropping in a hostile environment by combining the data encryption technology[22].

In (Zebari et al., 2021), a survey of recent swarm intelligence algorithms based on steganography is covered. The objective function for swarm intelligence algorithms is realized in a way that the quality and robustness of the object that has been used for hiding messages are acceptable. With a particular emphasis on the main purpose and the objective of the proposed method based on the particular swarm intelligence algorithm has been reviewed. To present a more secure, efficient steganography algorithm based on swarm intelligence algorithms for future work, this will be helpful[23].

In (Caviglione et al., 2022) presents the techniques used to inject data within IPv6 packets, the reference use case and the software architecture of the suite. It also showcases a performance evaluation of the different covert channels offered by IPv6CC, as well as an analysis of their ability to bypass some de-facto standard security tools[24].

The proposed system is differ from other related works by it is based on the different security approaches such as chaotic and RSA, SHA2, and hiding to create secure identity of IPv6 packets.

1.3 Problem Definition

- A denial of service (DoS) attack is a well-known on network, it leads to reduce the services provided by the adversary to do Dos attack, as IP spoofing attack which aims to control on the packet transferred through the network. To address the problem of the IP spoofing, many issues should be taken by the system.
- Increasing network traffic due to malicious nodes which leads to increase packet loose rate.

1.4 Research Objectives

The main objectives of the study are :

1) Increasing the network security through protecting the network from the malicious threats, which lead to the denial of service for instance IP spoofing.
2) Generating an individual random identity through high randomness for generated ID, and it hides identity of node inside packet.
3) Reducing the possibility of detecting the meaning of hidden data by encrypting it with one of the proposed encryption methods.
4) Decreasing the impact of hidden identity on send traffic.
5) Decreasing the impact of hidden identity on received traffic.
6) The ability of system to generate a random unique identity for each device on the network.
7) Keeping the identity of a device secure.
8) Making the identity of a device invisible during packet sending and receiving on a network.

1.5 Thesis Outline

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

Chapter Two: presents Network layer and IPv6 explanation, Network Layer, How packets pass from node to another node. Besides, the IPv6 Benefits , IPv6 Architecture, IPv6 Packet Header Format and so on.

Chapter Three: presents the proposed system and illustrates the practical stages of the system.

Chapter Four: describes the results and evaluates the used system based on case studies.

Chapter Five: presents the results conclusion. Also, it described the future works suggestions.

Chapter Two

Theoretical Background

2.1 Introduction

Network layer manages options pertaining to host and network addressing, managing sub-networks, and internetworking. Network layer takes the responsibility for routing packets from source to destination within or outside a subnet. Two different subnet may have different addressing schemes or non-compatible addressing types. Same with protocols, two different subnet may be operating on different protocols which are not compatible with each other. Network layer has the responsibility to route the packets from source to destination, mapping different addressing schemes and protocols[25].

The primary function of the network layer is to move data into and through other networks. Network layer protocols accomplish this goal by packaging data with correct network address information, selecting the appropriate network routes and forwarding the packaged data up the stack to the transport layer (Layer 4) [26].

The routing information contained within a packet includes the source address of the sending host and the eventual destination host address of the remote host. This information is contained within the network layer header that encapsulates network frames at the data link layer (Layer 2)[28].

The main part in network layer is the internet protocol (IP), and IPv6 is the next generation Internet Protocol (IP) address standard intended to supplement and eventually replace IPv4, the protocol many Internet services still use today. Every computer, mobile phone, home automation component, IoT sensor and any other device connected to the Internet needs a numerical IP address to communicate between other devices. The original

IP address scheme, called IPv4, is running out of addresses due to its widespread usage from the proliferation of so many connected devices[29].

The networking system was divided into layers. Within each layer, one or more entities implement its functionality, it is the OSI model in Figure (2.1), and the main benefits of the OSI model include the following [30]:

- Helps users understand the big picture of networking.
- Helps users understand how hardware and software elements function together.
- Makes troubleshooting easier by separating networks into manageable pieces.
- Defines terms that networking professionals can use to compare basic functional relationships on different networks.
- Helps users understand new technologies as they are developed
- Aids in interpreting vendor explanations of product functionality.

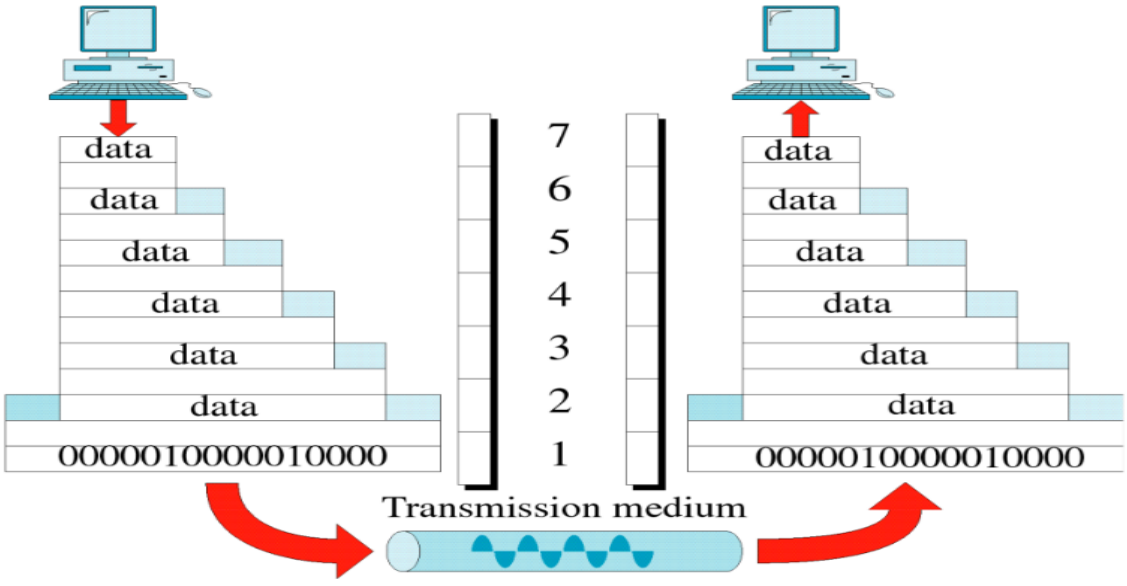


Figure 2.1 : Data Exchange Using the OSI Model[30].

The Transmission Control Protocol/Internet Protocol (TCP/IP) model is based on a five-layer model for networking. From bottom (the link) to top (the user application), these are the physical, data link, net-work, transport, and application layers.

The physical layer is the bottom layer of TCP/IP Model, and it is responsible for the actual physical connection between the devices. Such physical connection may be made by using twisted pair cable.Besides, it is concerned with transmitting bits over a communication channel [31].

Data Link Layer is responsible for node-to-node delivery of data. It receives the data from network layer and creates FRAMES , add physical address to these frames & pas them to physical layer [28].

Internet protocol version 4 (IPV4) was first published in 1981, by IETF publication (RFC 791) is the fourth version of internet protocol, and it is the first version of the protocol to be widely deployed in TCP/IP. The main function of protocol is to identify host on the network by their logical address in other to established communication between them on the network [29].

2.2 Network Layer

When using the internet, the devices send requests to servers stored in various data centers in packets. Likewise, the servers return responses to the requests using data packets. These packets' journey to the data center from the devices and vice versa form the internet's backbone[29].

Nevertheless, controlling these packets from the data source to the destination through the wide complicated global network is not a walk in the

park. This is where routing comes in. It is done by specialized networking hardware called routers. Routers select an appropriate path that will ensure the packets arrive quickly and safely[30].

Similarly, routers use algorithms to make logical data decisions when selecting the appropriate paths to forward the packets. It makes the decisions using the current network states of where the packets would pass through[30]. In the general sense, an internet is a computer network that connects several networks. The Internet is a publicly available internationally interconnected system of computers plus the information and services provided to their users using a TCP/IP suite of packet switching communications protocols1"[31].

To interconnect two or more computer networks it is necessary to have a routing device to exchange traffic, and steer traffic via several different nodes on the path across a network to its destination. The devices used to interconnect different networks are routers. Others devices with specific functions like gateways or bridge are also used. All network elements such as routers, switches, gateways, bridges, LAN cards, need to have at least one IP address, as it showed in Figure(2.2)[32].

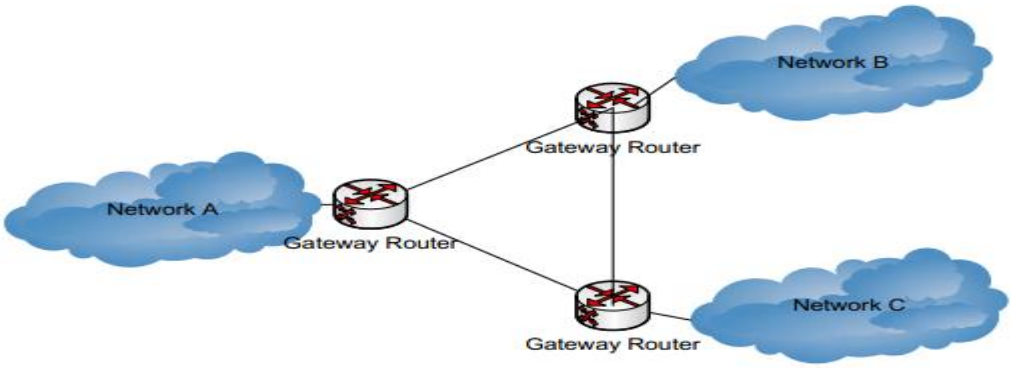


Figure 2.2: Use of routers[32]

Different IP packet networks are normally interconnected by Routers that have added functionality to permit accounting between the interconnected networks. In other configurations they act also as interworking devices between different protocols[33].

Network Layer is responsible for the source to destination delivery of a packet across multiple networks. If two systems are attached to different networks with devices like routers, then N/W layer is used. Thus Data Link Layer overseas the delivery of the packet between the two systems on same network and the network layer ensures that the packet gets its point of origin to its final destination, as it showed in Figure (2.3) [33].

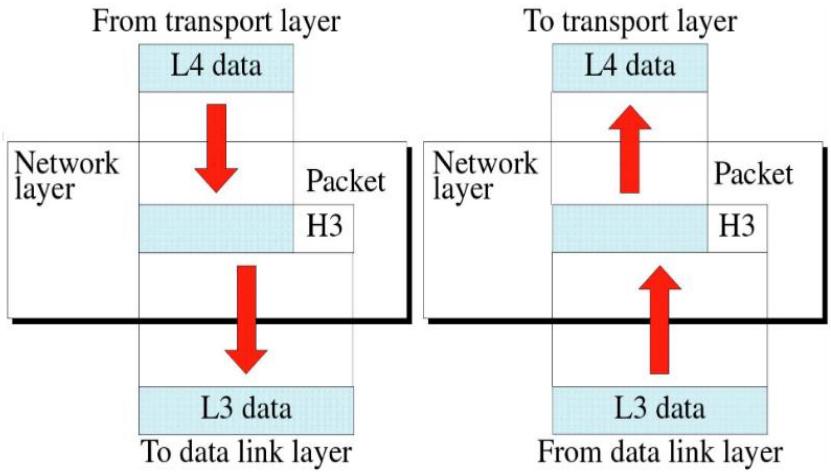


Figure 2.3 : The Network Layer explanation[33].

Moreover, the main functions of Network Layer are:

- Internetworking: It provides Internetworking.
- Logical Addressing: When packet is sent outside the network, N/W layer adds Logical (network) address of the sender & receiver to each packet.

- Network addresses are assigned to local devices by n/w administrator and assigned dynamically by special server called DHCP (Dynamic Host Configuration Protocol)
- Routing: When independent n/w are connected to create internetwork several routes are available to send the data from S to D. These n/w are interconnected by routers & gateways that route the packet to final destination [34].

Besides, Network layer protocols accomplish 3 main tasks , which they showed in Figure (2.4) [34]:

1. Data transfer over heterogeneous internetworked LANs, MANs, WANs
2. Routing decision management at the intermediate nodes
3. Control of the network (e.g. address mapping or transmission status)[34]

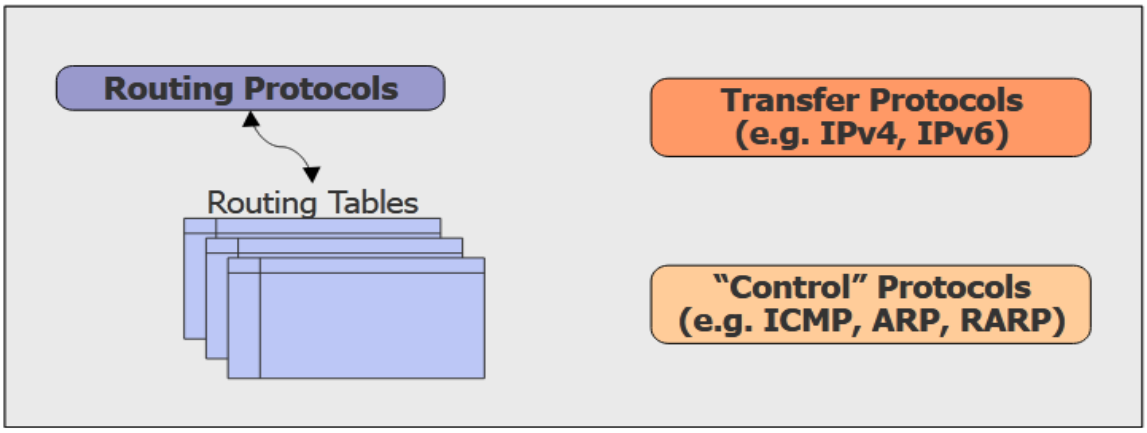


Figure 2.4: The Network layer protocols tasks[34].

The protocol at this layer is IP, either IPv4 or IPv6 (some think that IPv6 is distinct enough to be known as TCPv6/IPv6) [34].

2.3 Internet Protocol (IPv4)

An IP address is a binary number, which identifies any user's computer directly connected to the Internet. An IPv4 address consists of 32 bits, but it is usually represented by a group of four numbers (8 bits), from 0 to 255 ranges and separated by full stops, such as the representation is showed below[34]:

124.32.43.4

Several domain names can also be linked to the same IP address, in effect similar to having more than one name for the same person. The format of the IPv4 header is showed in Figure (2.5):

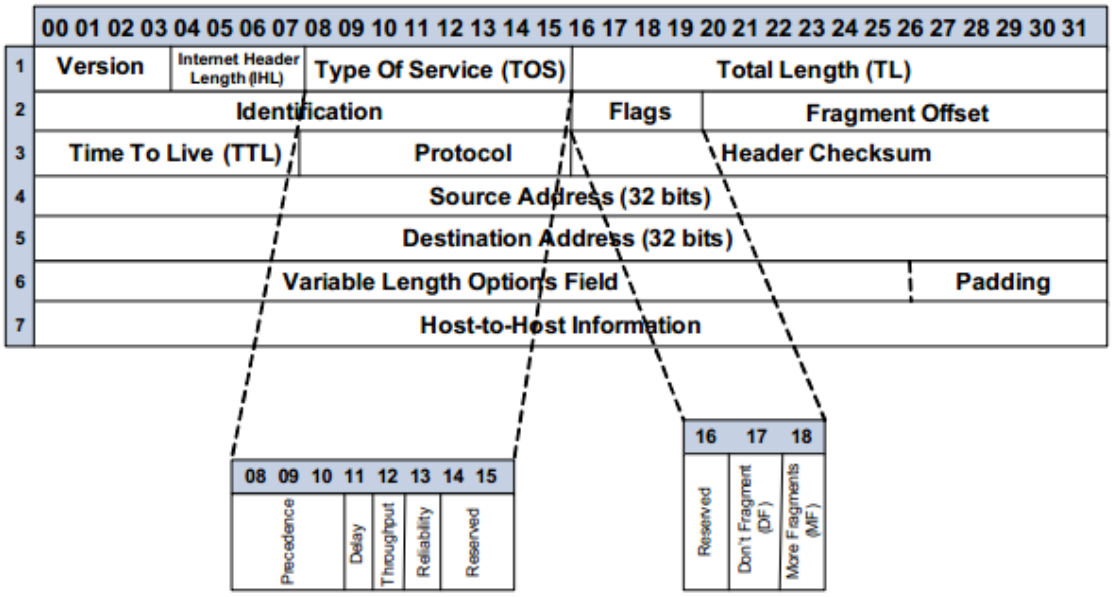


Figure 2.5: IPv4 Structure[34].

Packets in the network (internet) layer are called datagrams. A datagram is a variable-length packet consisting of two parts: header and data. The header is 20 to 60 bytes in length and contains information

essential to routing and delivery. It is customary in TCP/IP to show the header in 4-byte sections. The following Figure shows the IP datagram format[34].

A brief description of each field is in order[35].

- Version (VER): This 4-bit field defines the version of the IP protocol. If the machine is using some other version of IP, the datagram is discarded rather than interpreted incorrectly.
- Header length (HLEN): This 4-bit field defines the total length of the datagram header in 4-byte words. This field is needed because the length of the header is variable (between 20 and 60 bytes).
- Service type: In the original design of IP header, this field was referred to as type of service (TOS), which defined how the datagram should be handled. Part of the field was used to define the precedence of the datagram; the rest defined the type of service (low delay, high throughput, and so on). IETF has changed the interpretation of this 8-bit field. This field now defines a set of differentiated services.
- Total length: This is a 16-bit field that defines the total length (header plus data) of the IP datagram in bytes.
- Identification. This field is used in fragmentation.
- Flags. This field is used in fragmentation.
- Fragmentation offset. This field is used in fragmentation.
- Time to live. A datagram has a limited lifetime in its travel through an internet. this field is mostly used to control the

maximum number of hops (routers) visited by the datagram. When a source host

sends the datagram, it stores a number in this field. This value is approximately two times the maximum number of routes between any two hosts. Each router that processes the datagram decrements this number by one. If this value, after being decremented, is zero, the router discards the datagram.

- Protocol. This 8-bit field defines the higher-level protocol that uses the services of the IP layer. An IP datagram can encapsulate data from several higher level protocols such as TCP, UDP, ICMP, and IGMP. This field specifies the final destination protocol to which the IP datagram should be delivered.
- Checksum. Checksum only covers the header and not data
- Source address: This 32-bit field defines the IP address of the source Destination address: This 32-bit field defines the IP address of the destination[36].

2.4 Internet Protocol (IPv6)

The new version of IPv6 was conceived to replace the previous IPv4 standard that was adopted two decades ago as a robust, easily implemented standard. However IPv4 is being used successfully to support the communications systems in the emerging information society and has been updated to extend its useful life (e.g. NAT mechanism, IPsec protocol), MPLS, Tunnelling). However its capabilities are somewhat limited in the following areas[37]:

- Exhaustion of the IPv4 address space;

- Growth of the Internet and the maintenance of routing tables

- Auto-configuration

- Mobility Configuration

- Addition the Security

- Quality of service and the purpose of developing IPv6 is to overcome these limitations.

The areas where IPv6 offers improvement are [38]:

- Expansion capacity for addressing and routing – the IP address space is expanded from 32 bits to 128 bits, enabling a greatly increased number of address combinations, levels of hierarchical address organization and auto-configuration of addresses;

- Simplified header format – the IPv6 basic header is only 40 bytes long in spite of the greatly increased address allocation;

- Enhanced options support – several different, separate "extension headers" are defined, which enable flexible support for options without all of the header structure having to be interpreted and manipulated at every router point along the way;

- Quality of service – the Flow Label and the Priority fields in the IPv6 header are used by a host to identify packets that need special handling by IPv6 routers, such as non-default quality of service or "real-time" service[38].

This capability is important in that it needs to support applications that require some degree of consistent throughput, delay, and jitter[36];

- Auto-configuration – adds the concept of dynamic assignment of part of the address space, based on geographic and topographic features of a given physical connection

- Elimination of the need for NATs (network address translators) – since the IP address space supports approximately 3.4 x 1038 possible combinations, the need for private addressing schemes behind NATs is unnecessary on grounds of address conservation;

- Improved security with mandatory IPsec implementation – IPv6 provides for integral support for authentication, privacy and data integrity measures, by requiring all implementations to support these features;

- Mobility - mobile computers are assigned with at least two IPv6 addresses whenever they are roaming away from their home network. One (the home address) is permanent; the other (the IPv6 link-local address) is used temporarily. In addition, the mobile node will typically auto-configure a globally-routable address at each new point of attachment. Every IPv6 router supports encapsulation, so every router is capable of serving as a home agent on the network(s) to which it is attached[39].

The example of IPv6 is showed as follow:

[b191:1556:e4a5:bc63:c06c:3532:8f0b:4f922ca:bcd2:c900:7b2c:c37d:
a64b:376e:1390465b:6a6a:9ec7:f619:3fce:2c8f:8115:bcb05954:18d9:
5bbf:4395:61eb:ce71:acde:ac65a89e:c124:b087:be67:3aa6:a1de:d415:
d73a]

The leftmost three fields (48 bits) contain the site prefix. The prefix describes the public topology that is usually allocated to your site by an ISP or Regional Internet Registry (RIR)[40].

The next field is the 16-bit subnet ID, which you (or another administrator) allocate for your site. The subnet ID describes the private topology, also known as the site topology, because it is internal to your site[40].

The rightmost four fields (64 bits) contain the interface ID, also referred to as a token. The interface ID is either automatically configured from the interface's MAC address or manually configured in EUI-64 format[40].

2.4.1 Internet Protocol (IPv6) Architecture

The most recognized change from IPv4 to IPv6 is the length of network addresses. The IPv6 addresses have 128 bits length. The 128 bits provide approximately 3.4 X 10^{38} separate values. An IPv6 address consists of eight numbers in the hexadecimal format, from 0 to 65535 (decimal) ranges and separated by a colon ":". An example of this new representation is showed following [40]:

FECA:0000:234A:0043:AB45:FFFF:9A3E:000B

2.4.2 Internet Protocol (IPv6) Packet Header Format

The IPv6 protocol defines a set of headers, including the basic IPv6 header and the IPv6 extension headers. The following figure shows the fields that appear in the IPv6 header and the order in which the fields appear.

In other to compare with the IPv4 header next Figure (2.6) shows the IPv6 format header[40]:

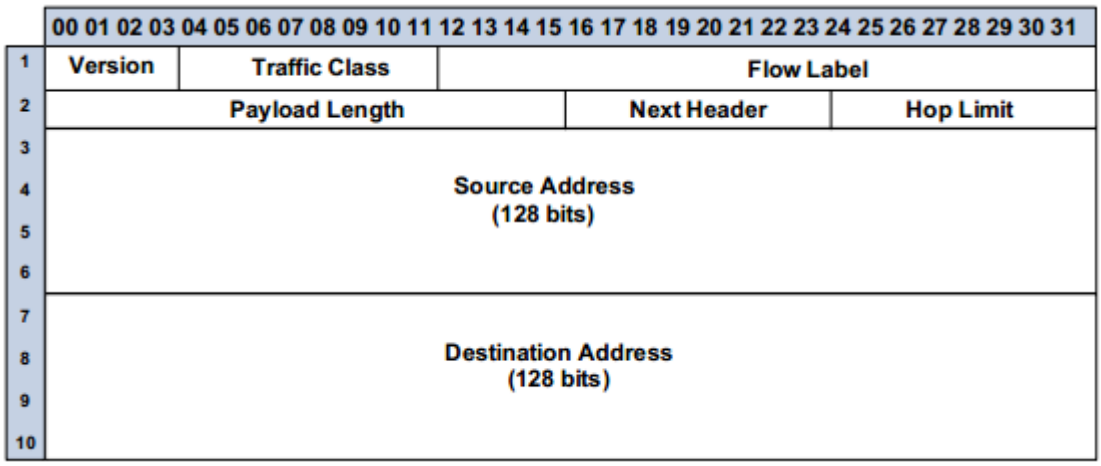


Figure 2.6: IPv6 Structure[40].

The following list describes the function of each header field[40].

- Version – 4-bit version number of Internet Protocol = 6.
- Traffic class – 8-bit traffic class field.
- Flow label – 20-bit field.
- Payload length – 16-bit unsigned integer, which is the rest of the packet that follows the IPv6 header, in octets.
- Next header – 8-bit selector. Identifies the type of header that immediately follows the IPv6 header. Uses the same values as the IPv4 protocol field.
- Hop limit – 8-bit unsigned integer. Decremented by one by each node that forwards the packet. The packet is discarded if the hop limit is decremented to zero.
- Source address – 128 bits. The address of the initial sender of the packet.

- Destination address – 128 bits. The address of the intended recipient of the packet. The intended recipient is not necessarily the recipient if an optional routing header is present.
- IPv6 Extension Headers
- IPv6 options are placed in separate extension headers that are located between the IPv6 header and the transport-layer header in a packet. Most IPv6 extension headers are not examined or processed by any router along a packet's delivery path until the packet arrives at its final destination[40].

This feature provides a major improvement in router performance for packets that contain options. In IPv4, the presence of any options requires the router to examine all options[40].

Unlike IPv4 options, IPv6 extension headers can be of arbitrary length. Also, the number of options that a packet carries is not limited to 40 bytes. This feature, in addition to the manner in which IPv6 options are processed, permits IPv6 options to be used for functions that are not practical in IPv4[41].

To improve performance when handling subsequent option headers, and the transport protocol that follows, IPv6 options are always an integer multiple of 8 octets long. The integer multiple of 8 octets retains the alignment of subsequent headers[42].

The following IPv6 extension headers are currently defined[43]:

1. Routing – Extended routing, such as IPv4 loose source route
2. Fragmentation – Fragmentation and reassembly
3. Authentication – Integrity and authentication, and security

4. Encapsulating Security Payload – Confidentiality
5. Hop-by-Hop options – Special options that require hop-by-hop processing
6. Destination options – Optional information to be examined by the destination node

2.4.3 Internet Protocol (IPv6) Security

This section identifies security mechanisms that can be employed in Internet Protocol version 6 (IPv6) environments. Many of these mechanisms are imported from the IPv4 world to identify some of the commonly available techniques, methods, and protocols that can be used to secure IPv6 networks. We view security in four realms[44]:

1. confidentiality and integrity of information while in transit (in a network);
2. perimeter/access security in reference to a defined set of private information technology (IT) assets;
3. system security/integrity (including both client and server systems);
4. security of data at rest (namely, security of database/storage systems). However, this section only deals with the first item. This kind of security can be seen as achievable using tunnels that carry encrypted information[44].

Confidentiality means that data, objects and resources are protected from unauthorized viewing and other access. Integrity means that data is protected from unauthorized changes to ensure that it is reliable and correct[45].

2.4.4 Protecting Identity of Ipv6 Packet: Benefits, weaknesses and challenges

Almost all electronic devices can be connected to the Internet these days. So, the IP addressing system needs to be able to accommodate that many devices. IPv6 has scalability in the network space to handle the outpouring devices being registered on the internet by providing lightweight data transport[46].

A- IPv6 weaknesses and challenges

1- System Issues

The IPv6 routing is to be enabled according to the system it has been run on. When the data is entered manually, the long IP addresses have to be typed. The addresses then would have to be remembered, because most IP addresses are very long, which involve letters and numbers.

2- Complexity in the Network Topology Drawings

IPv4 addresses had a short length, which was easy to lay on the topology drawing. With the IPv6 protocol, it becomes complicated to fit the prefixes. The text is barely legible in the case of IPv6[47].

3- Upgrading the devices

Business organizations are supposed to enhance their networking devices as they aren't designed for IPv6 adoption. This is not limited to the entities that regularly update their devices. Many businesses must bring an expert opinion. i.e., a consultant to make the transformation as easy as possible as reliable software may need a costly upgrade[48].

4- Local Networking Changes

Assigning new IP addresses manually is a complicated task, as Local Network Management involves assigning IP addresses to specific devices[48].

5. Communication

Communication between IPv4 and IPv6 is complex such that in very rare instances they will be able to. The communication cannot be made directly[49].

2.5 Network Security and Security Protocols

Network security protocols are a type network protocol that ensures the security and integrity of data in transit over a network connection. Network security protocols define the processes and methodology to secure network data from any illegitimate attempt to review or extract the contents of data[50].

There are various categories of protocols like routing protocols, mail transferring protocols, remote communication protocols, and many more. Network security protocols are one such category that makes sure that the security and integrity of the data are preserved over a network. Various methodologies, techniques, and processes are involved in these protocols to secure the network data from any illegitimate attempt to review or extract the actual content of data[51].

Network security protocols generally implement cryptography techniques to secure the data so that it can only be decrypted with a special algorithm, logical key, mathematical formula and/or a combination of all of

them. Some of the popular network security protocols include Secure File Transfer Protocol (SFTP), Secure Hypertext Transfer Protocol (HTTPS) and Secure Socket Layer (SSL)[52].

2.5.1 Internet Protocol Security (IPsec)

The IP Security architecture (IPsec) defines basic security mechanisms at the network level, so that they can beavailable to all the layered applications. The security techniques adopted in IPsec have been designed to be easily inserted in both IPv4 and IPv6[53].

IPsec security services are offered by means of two dedicated extension headers, the Authentication Header (AH) and the Encapsulating Security Payload (ESP), and through the use of cryptographic key management procedures and protocols[53].

The AH header was designed to ensure authenticity and integrity of the IP packet. It also provides an optional antireplay service. Its presence guards against illegal modification of the IP fixed fields, packet spoofing and, optionally, against replayed packets. On the other hand, the ESP header provides data encapsulation with encryption to ensure that only the destination node can read the payload conveyed by the IP packet. ESP may also provide packet integrity and authenticity, and an anti-reply service. The two headers can be used separately or they can be combined to provide the desired security features for IP traffic[54].

Each header can be used in one of the two defined modalities: transport mode and tunnel mode. While in transport mode the security headers provide protection primarily for upper layer protocols, in tunnel

mode the headers are applied to tunneled IP packets, thus providing protection to all fields of the original IP header[55].

Both AH and ESP exploit the concept of ”security association” (SA) to agree upon the security algorithms, transforms and parameters shared by the sender and the receiver of a protected traffic flow. Each IP node manages a set of SAs, at least one SA for each secure communication, as it showed in Figure (2.7)[56].

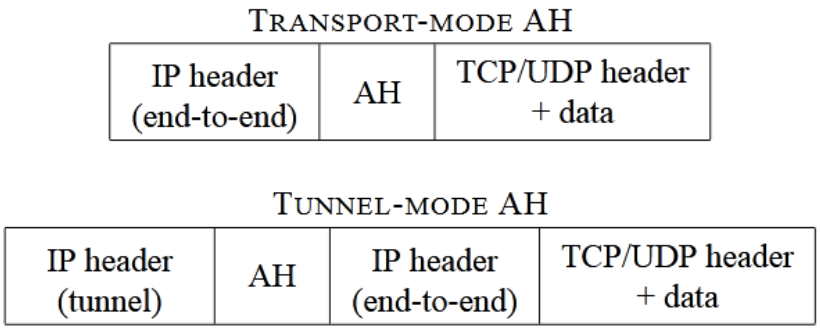


Figure 2.7: Examples the use of AH header[56].

The SAs currently active are stored inside a database, known as the Security Association Database (SAD). An entry in the SAD (i.e., a security association) is uniquely identified by a triple consisting of a Security Parameter Index (SPI), an IP Destination Address, and a security protocol (AH or ESP) identifier. The Security Parameter Index (SPI) is transmitted inside both the AH and ESP headers, since it used to choose the right SA to be applied for decrypting and/or authenticating the packet. In unicast transmissions, the SPI is normally chosen by the destination node and sent back to the sender when the communication is set up[57].

In multicast transmissions, the SPI must be common to all the members of the multicast group. Each node must be able to correctly

identify the right SA by combining the SPI with the multicast address. The negotiation of a SA (and the related SPI) is an integral part of the protocol for the exchange of security keys[58].

Specific security requirements are defined at each node usually by means of an ordered list of admission rules (or policies), which form the node's Security Policy Database (SPD). The protection provided to each incoming/outgoing traffic flow is verified/decided by consulting the SPD. In general, packets are selected for one of three processing modes based on IP and transport layer header information matched against entries in SPD. Each packet is either afforded IPsec security services, discarded, or allowed to bypass IPsec, based on the applicable policies found in the database[59].

A. **Authentication**

The Authentication Header (AH) protocol provides data origin authentication, data integrity, and replay protection. However, AH does not provide data confidentiality, which means that all of your data is sent in the clear 60]. The format of the AH header (depicted in Figure 2.8) is very simple as it is composed of a 96-bit fixed part followed by a variable number of 32-bit blocks. The fixed part contains:

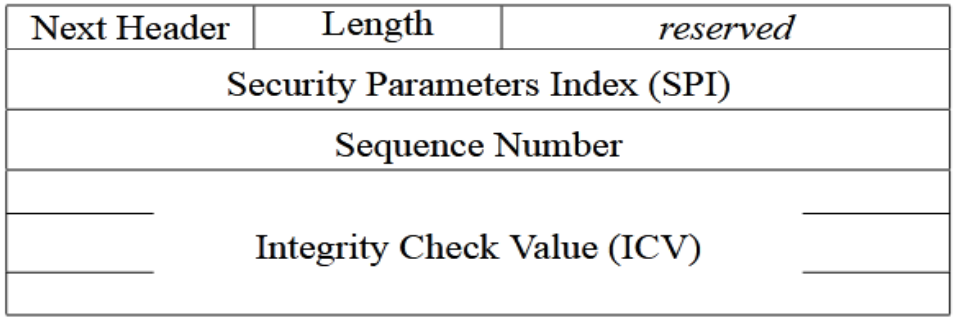


Figure 2.8: Structure of the AH header[60].

- The value of the next type of payload (8 bits);
- The Payload Length, which is the total length of the authentication data expressed as a multiple of 32-bit words .
- A reserved field (16 bits);
- The SPI used by this header (32 bits);
- - The sequence number for this header, contains a monotonically increasing counter value (32 bits)

B. Authentication techniques

Data integrity in telecommunication systems is normally ensured by computing and checking the value of a suitable cryptographic function of the data, often called Message Digest (MD). Among the most frequently used algorithms are CRC-16 and CRC-32).

These functions effectively perform their task when data modifications are due to random errors, but they are completely inadequate to protect the packets against deliberate modifications. In this case, a reasonable degree of protection can be ensured only by better digest algorithms, such as MD5 or SHA [60].

C. Encapsulating Security Payload

The Encapsulating Security Payload is identified by the value 52 in the Protocol field of the IP header. When used, this block must always be the last header because it completely hides both the upper level payload and all the next headers. The ESP header itself is only partly in clear (see Figure 2.9)[61]:

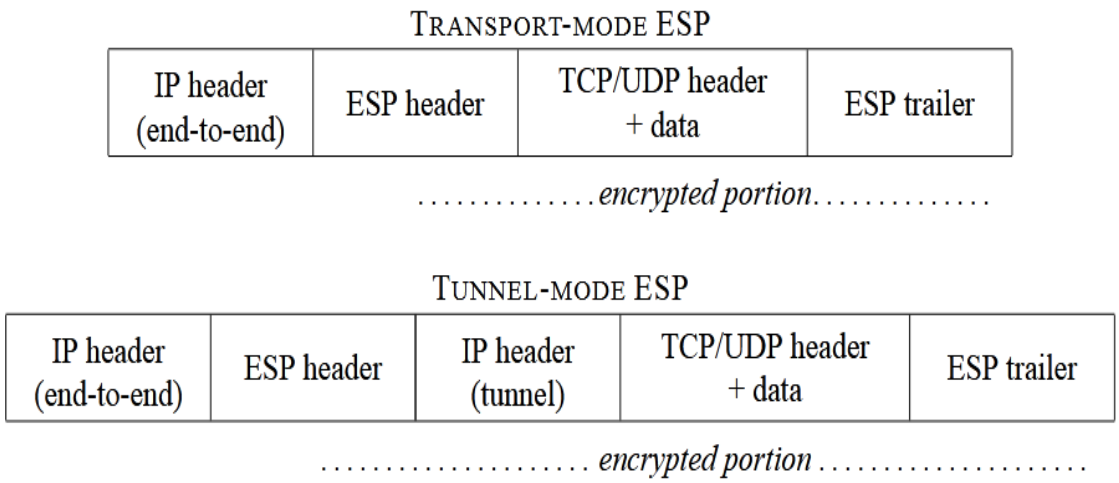


Figure 2.9: Examples of the use of ESP[61].

2.5.2 The Advantages and Disadvantages of IP security

There are several advantages and disadvantages of using IP Security as a protocol of security protection on computer networks[62].

A- The Advantages of IP Security

IP Security can protect any protocol that runs over IP and on any medium that IPs can use, so IPsec is a common method that can provide secure communications over a computer network.

- IP Security provides security in a transparent manner, so from the application side, the user does not need to be aware of its existence.
- IP Security is designed to meet the new IPv6 standard without forgetting which IPv4 is now in use.
- The design of IP Security does not require the use of certain encryption or hash algorithms so that if the frequently used algorithm has now been solved, its function can be replaced by other algorithms that are harder to solve.

B- The disadvantages of IP Security[63]:

- IP Security too complex, provision of some additional features by adding unnecessary complexity.
- Some of the documentation still contains some errors, not explaining some essential and ambiguous explanations.
- Some of the default algorithms used in IP Security is now unsafe.

2.6 Cryptographic and Steganography Techniques

Cryptographic techniques are used to ensure secrecy and integrity of data in the presence of an adversary. Based on the security needs and the threats involved, various cryptographic methods such as symmetric key cryptography or public key cryptography can be used during transportation and storage of the data.

In addition, a homomorphic encryption allows various computations to take place on encrypted data without requiring the data to be decrypted for processing. From the privacy perspective, these techniques are useful to protect personal information from being leaked during transportation and from storage servers[64].

Cryptography provides an inner line of defense. Like a wall safe that is there in case the burglars do make it inside your house—and to protect valuables from people who are authorized to come into your house—cryptography protects data from intruders who are able to penetrate the outer network defenses and from those who are authorized to access the network but not this particular data. Cryptographic techniques concern themselves with three basic purposes[65]:

- Authentication :Verifying the identity of a user or computer.

- Confidentiality : Keeping the contents of the data secret.
- Integrity : Ensuring that data doesn't change between the time it leaves the source and the time it reaches its destination.
- Non-repudiation security service that ensures that an entity cannot refuse ownership for a previous commitment or an action. For example- The order is placed electronically , user can't be denied the purchase order if Non-repudiation was enabled [66].

2.6.1 Symmetrical Encryption

It is a type of encryption that is used for the encryption and decryption of electronic data by just one key (a secret key). Substitution ciphers are symmetrical encryption techniques, but modern symmetric encryption can be much more complicated. Data are converted to a method that anyone cannot understand without a secret key to decrypt it using symmetrical encryption algorithms[67].

It is an old algorithm, but it is faster and efficient than asymmetric encryption. Because of great performance and fast speed of symmetric as compare to asymmetric encryption. Whereas Symmetric key cryptography involves the usage of the same key for encryption and decryption.

At the same time, Asymmetric key cryptography involves using one key for encryption and another different key for decryption. It is typical for big quantities of information, e.g. for database encryption, in bulk encryption. In the case of a database, the secret key can only be encrypted or decrypted by the database itself[68]. Symmetric encryption is showed in Figure 2.10:

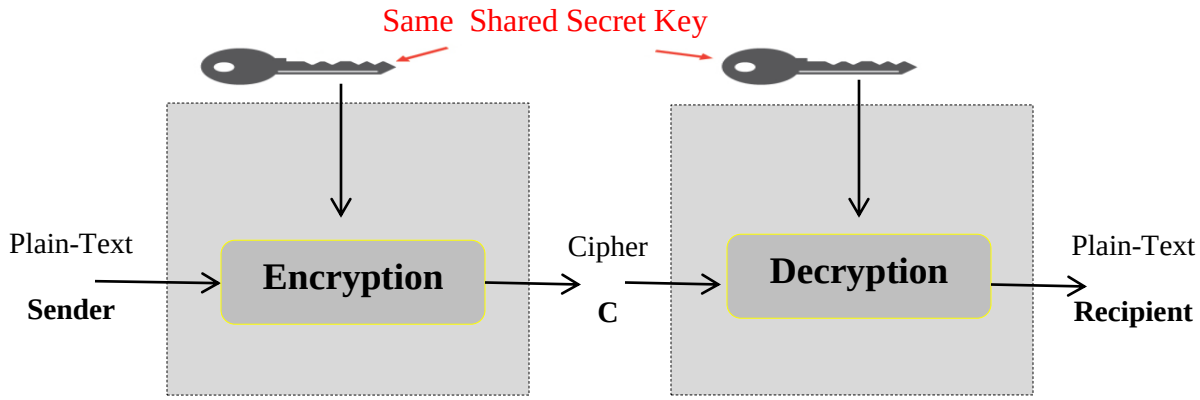


Figure 2.10: the main steps of Symmetrical encryption.

Two kinds of symmetrical encryption algorithms are available[69]:

A) Block Algorithm

The set of bits is encoded with a specific secret key in electronic data blocks. The system keeps the data in its memory while it is waiting to get complete blocks when the data are encrypted. Some important Block cipher algorithms are DES, Triple DES, AES, etc[70].

B) Stream Cipher Algorithm

Plain text numbers or characters are combined with pseudorandom cipher digit stream. Some important Stream cipher algorithms are RC4, A5, BLOWFISH, etc. In symmetric key encryption, The encryption code can be cracked if someone finds out the symmetric key. But this problem can be overcome with the Diffie-Hellman algorithm.

In the Diffie-Hellman key exchange or agreement algorithm, the sender and receiver must agree on a symmetric key using this technique. This key can then be used for encryption or decryption purpose[71].

2.6.2 Asymmetric Encryption

Asymmetric encryption is also called public-key cryptography. Asymmetric key encryption helps to resolve a key exchange problem of symmetric key Cryptography. In Asymmetric encryption, Two keys are used to encrypt plain text in asymmetrical encryption. Through the internet or big network, the secret keys are exchanged. It is necessary to notice that anyone with a secret key can decrypt the message, so asymmetric encryption uses two corresponding keys to increase safety[72].

Anyone who wishes to send you a message will have a public key freely accessible, but the second private key is held the secret for you to understand you only. A message encrypted with a public key can be decoded with a private key. A message encrypted with a private key can also be decrypted with a public key, as showed in Figure(2.11)[73].

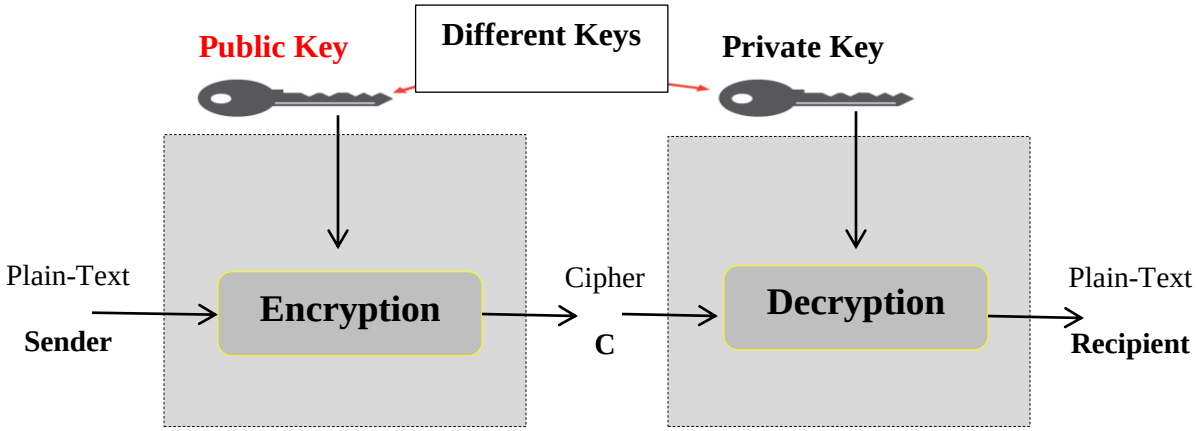


Figure 2.11 : Asymmetric Encryption[74].

2.6.3 Steganography

It is actually the science of hiding information from people who would snoop on you. The difference between Steganography and encryption is that the would-be snoopers may not be able to tell there's any

hidden information in the first place. Steganography hides the data by using some other media such as image, text, video etc, as it showed in Figure (2.12)[75].

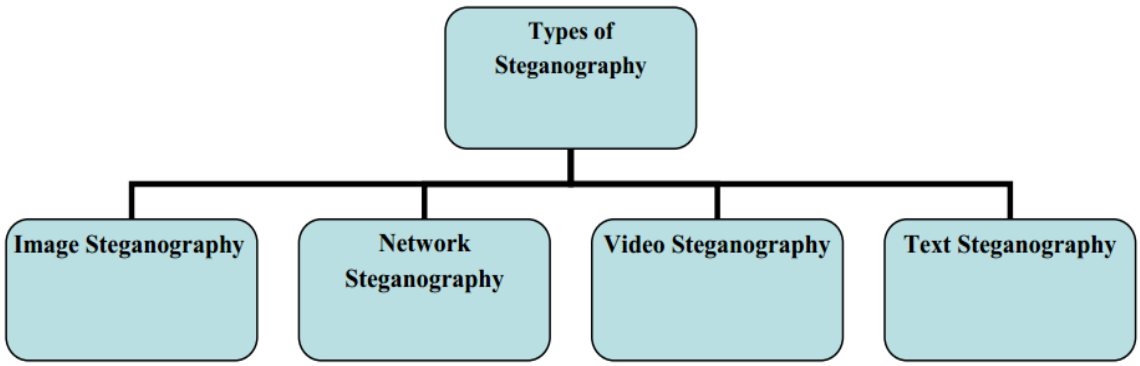


Figure 2.12: Digital Mediums to Achieve Steganography[76].

2.6.4 SHA-2 hashing

Hashing is the cryptographic technique that converts data that can be any form into a unique string. Regardless of size or type, any data can be hashed using a hashing algorithm. It takes data of random length and converts it into a fixed hashed value[77]. One of the key properties of hashing algorithms is determinism. Any computer in the world that understands the hashing algorithm you have chosen can locally compute the hash of the example sentence and get the same answer, as it showed in Figure (2.13)[77].

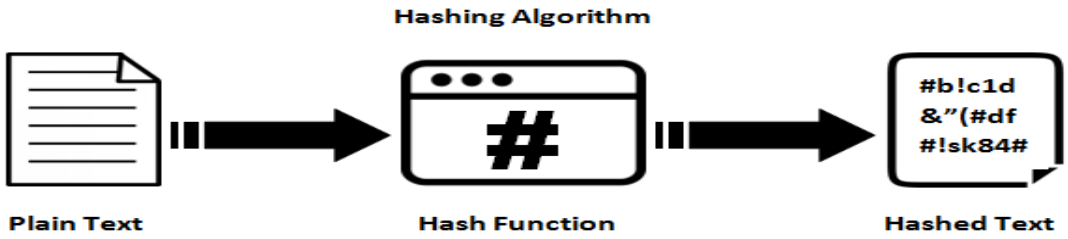


Figure 2.13 : Hashing function work[77].

The number in each variant represents the bit values. SHA-2 provides better prevention against collision, meaning the same input data always has a different hash value. SHA-2 uses from 64 to 80 rounds of cryptography operations, and it is commonly used to validate and sign digital security certificates and documents[78].

Hashing is different from other encryption methods because, in hashing, encryption cannot be reversed; that is cannot be decrypted using keys. MD5, SHA1, SHA 256 are the widely used hashing algorithms[79].

Cryptographic hash functions are a fundamental tool in modern cryptography, used mainly to ensure the data integrity when transmitting information over insecure channels. Hash functions are also used for the implementation of digital signature algorithms, keyed-hash message authentication codes and in random number generators. Many hash functions exist, but their actual security level is very difficult to estimate. Whenever weak-nesses are found, security is compromised and any stand-alone implementations must be phased out leading to costly upgrades toward a new hash function that is deemed secure at that time. For example, an algorithm has recently been discovered that decreases the resistance to collision of SHA-1 (Secure Hash Algorithm), the most popular hash function so far, reducing the number of necessary computations from 280 to 269 and putting it below the accepted security threshold for high-security operations. Since then[80].

The SHA-2 family of hash functions, developed by the National Insti-tute of Standards and Technology (NIST), has become the new standard. Due to their complexity and limited lifespan, the cryptographic

primitives are generally implemented in software on general purpose processors rather than on specialized hardware architectures. Hard-ware implementations are also far more expensive and often difficult to realize efficiently. On the other side, software based cryptographic algorithms are much slower than their hardware counterparts by typical factors from 1 to 3 orders of magnitude[81].

Many secure cryptographic algorithms such as AES (Advanced Encryption Standard) and SHA-1 were designed to be implemented in hardware, and are drastically less efficient when coded in software . In terms of hardware implementations, the two principal approaches are Application-Specific Integrated Circuits (ASIC) technology and Field Programmable Gate Arrays (FPGAs)[82].

2.6.5 Chaos Cryptography

Chaotic cryptology is the application of the mathematical chaos theory to the practice of the cryptography, the study or techniques used to privately and securely transmit information with the presence of a third-party or adversary[82].

Chaotic cryptology consists of two opposite processes: Chaotic cryptography and Chaotic cryptanalysis. Cryptography refers to encrypting information for secure transmission, whereas cryptanalysis refers to decrypting and deciphering encoded encrypted messages[82].

2.6.6 Logistic Map

The logistic map is a polynomial mapping (equivalently, recurrence relation) of degree 2, often cited as an archetypal example of how

complex, chaotic behaviour can arise from very simple non-linear dynamical equation(2.1).

$$x(n+1)=A[x(n)]\,[1-x(n)]\ldots\ldots\ldots(2.1)$$

where, the value of x equal (0 to 1)and the value of A equal 1 to 4 and the best randomness when the value of A (3.6 to 4)]83].

2.6.7 Lightweight Cryptographic

Many lightweight cryptographic algorithms have been developed and also existed algorithms are modified in terms of resource constraint environments. One of such new procedures is utilizing three prime numbers for RSA cryptosystem, which is not easily breakable[84].

It is hard to discover the factors of large integers, the supposition that the asymmetric key encryption system (RSA) depends on. In RSA, the private key is kept mysterious; however, the public key is sent to everybody in the framework. Key generation, message encryption, and message decryption, are the three steps used in the RSA algorithm[84].

Advanced Encryption Standard (AES) is the standardized block cipher, which is used in various applications. AES is well suited for software and hardware implementation with versions of 128,192,256 key sizes. In hardware implementation lightweight AES is advantageous as it is more secure, low cost, and has minimized hardware utilization. Lightweight block ciphers are developed for the efficient implementation in hardware[85].

2.6.8 Steganography Techniques

A Steganography is the science or art of hide the messages into other sources of information like text/documents, audios, videos and images etc. so that it is not visible to unauthorized users. It is known as invisible communication. A Steganography system made up of three components: cover-object means which hides the secret message, the secret message and the steganography object means which is the cover object with message embedded inside it[86].

2.6.8.1 Types of Steganography

A. Text Steganography

It consists of hiding information inside the text files. In this method, the secret data is hidden behind every nth letter of every words of text message. Numbers of methods are available for hiding data in text file. These methods are i) Format Based Method; ii) Random and Statistical Method; iii) Linguistics Method[87].

B. Network or Protocol Steganography

Network Steganography is a technique that uses common network protocols (the header field, the payload field or both) to hide a secret message. TCP/IP protocol suite has been a potential target for network steganography from the very beginning. It has a lot of possibilities for creation of hidden channels that can be used to communicate covertly[88].

Steganography using images, audio and video has been a favorite area of researchers since past two decades. However, Network Steganography is a recent emerging field in the area of research. Other Steganography techniques require extra bandwidth for sending the cover

media with hidden data. Whereas with Network Steganography, it is possible to use already existing Protocol Data Units (PDUs) as cover with modifications in redundant fields of the respective PDU. Many commonly used protocols are being proposed for implementing Network Steganography. This hiding of secret information in network protocols' payload or header or both, can be achieved through Network Steganography. Network Steganography offers a good bandwidth for secret data communication. This is because one can create new data packets to carry secret information or modify the already existing data packets to carry covert data. In some cases, hidden channel using the timestamp option of Internet Protocol version 6 (IPv6) which is an optional field of an IPv6 packet[89].

It involves hiding the information by taking the network protocol such as TCP, UDP, ICMP, IP etc, as cover object. In the OSI layer network mode l there exist covert channels where steganography can be used[89].

2.6.8.2 Application of Steganography

a) Confidential Communication and Secret Data Storing
b) Protection of Data Alteration
c) Access Control System for Digital Content Distribution
d) E-Commerce
e) Media
f) Database Systems.
g) digital watermarking[90].

2.7 Network Attacks

Network attacks are unauthorized actions on the digital assets within an organizational network. Malicious parties usually execute network attacks to alter, destroy, or steal private data. Perpetrators in network attacks tend to target network perimeters to gain access to internal systems[90].

There are two main types of network attacks: passive and active. In passive network attacks, malicious parties gain unauthorized access to networks, monitor, and steal private data without making any alterations for instance (Traffic analysis attack). Active network attacks involve modifying, encrypting, or damaging data for instance (DoS attack)[90].

2.7.1 Denial-of-Service (DoS) Attack

A Denial of Service (DoS) attack is an attempt to make a system unavailable to the intended user(s), such as preventing access to a website. A successful DoS attack consumes all available network or system resources, usually resulting in a slowdown or server crash[91].

A DoS attack can be perpetrated in a number of ways. There are different sides of Dos attacks effect on network performance and network elements to identify attacks appearance as follow [91]:

1- Consumption of computational resources, such as bandwidth, disk space, or CPU time.

2- Disruption of configuration information, such as Routing information. disruption of physical network components.

3- Unusually slow network performance (opening files or accessing web sites)

4- Unavailability of a particular web site inability to access any web site

5- dramatic increase in the number of spam emails received

6- IPv6 DoS and Protection Measures.

2.7.2 Traffic Attack

Similar to eavesdropping attacks, traffic analysis attacks are based on what the attacker hears in the network. However, in this type of attack, the attacker does not have to compromise the actual data. The attacker simply listens to the network communication to perform traffic analysis to determine the location of key nodes, the routing structure, and even application behaviour patterns[91].

The main focus of traffic attack is to develop algorithms and procedures to enable observing, analyzing, evaluating, and controlling communication. In the context of anonymity networks, such as The Onion Router (Tor) that helps maintain anonymity on the Internet, traffic analysis is used to reveal the identity of Tor's users, or understand their network behavior[91].

Traffic attacks success depends on how accurate the adversary information. The higher network coverage of the adversary model the more probable the traffic monitored will be accurate. However, the design of a threat model should be aware of impractical assumptions made about the duration of observation as well as the percentage of network coverage[92].

Traffic attacks challenge the design of traditional systems where encryption is typically used as the main method for protecting security and privacy. However, it is obvious that encryption cannot protect many other

important characteristics of traffic which may be mission critical and require protection[92].

2.8 Security Evaluation Metrics

The proposed system is based on different evaluation parameters which explained as follow[93]:

2.8.1 Randomness

Nine experiments were performed using the Java language. Moreover, the random test of identity generated using the Die Hard statistical tool[93].

It would be implemented by Diehard: is includes 15 Statistical tests[93]

1. **The Birthday Spacings Test**

Choose random points on a large interval. The spacings between the points should be asymptotically exponentially distributed. The name is based on the birthday paradox[93].

2. **The Overlapping5_permutation Test**

Analyze sequences of five consecutive random numbers. The 120 possible orderings should occur with statistically equal probability.

3. **The Binary Rank Test**

Select some number of bits from some number of random numbers to form a matrix over {0,1}, then determine the rank of the matrix. Count the ranks[93].

4. The Bitstream Test

The file under test is viewed as a stream of bits. Call them b_1, b_2, .. Consider an alphabet with two "letters", 0 and 1, and think of the stream of bits as a succession of 20-letter "words", overlapping. Thus the first word is $b_1b_2...b_{20}$, the second is $b_2b_3...b_{21}$, and so on[93].

5. The Overlapping Pairs Sparse Occupancy

The OPSO test considers 2-letter words from an alphabet of 1024 letters. Each letter is determined by a specified ten bits from a 32-bit integer in the sequence to be tested[93].

6. The Overlapping Quadruples Sparse Occupancy

OQSO is defined as Overlapping Quadruples Sparse Occupancy somewhat frequently[93].

7. The DNA Test

The DNA test considers an alphabet of 4 letters C,G,A,T, determined by two designated bits in the sequence of random integers being tested[93].

8. The count the 1 s Test

Consider the file under test as a stream of bytes (four per 32-bit integer). Each byte can contain from none to eight 1s, with probabilities 1, 8, 28, 56, 70, 56, 28, 8, 1 over 256. Now let the stream of bytes provide a string of overlapping 5-letter words, each "letter" taking values A, B, C, D, E[93].

9. The Parking Lot Test

In a square of side 100, randomly "park" a car – a circle of radius 1. Then try to park a 2nd, a 3rd, and so on, each time parking "by ear". That is, if an attempt to park a car causes a crash with one already parked, try

again at a new random location. (To avoid path problems, consider parking helicopters rather than cars.)

10.The Minimum Distance Test

It does this 100 times choose n = 8000 random points in a square of side 10000. Find d, the minimum distance between the (n2 − n) / 2 pairs of points[92].

11.The 3D Spheres Test

Choose 4000 random points in a cube of edge 1000. At each point, center a sphere large enough to reach the next closest point. Then the volume of the smallest such sphere is (very close to) exponentially distributed with mean 120π / 3. Thus the radius cubed is exponential with mean 30.

12.The Squeeze Test

Random integers are floated to get uniforms on [0,1). Starting with $k = 2^{31} = 2147483648$, the test finds j, the number of iterations necessary to reduce k to 1, using the reduction k = ceiling($k \times U$), with U provided by floating integers from the file being tested.

13.The Overlapping Sums Test

Integers are floated to get a sequence U(1), U(2), ... of uniform [0,1) variables. Then overlapping sums, S(1) = U(1) + ... + U(100), S(2) = U(2) + ... + U(101), ... are formed. The Ss are virtually normal with a certain covariance matrix[93].

14.The Runs Test

It counts runs up, and runs down, in a sequence of uniform [0,1) variables, obtained by floating the 32-bit integers in the specified file. This example shows how runs are counted: 0.123, 0.357, 0.789, 0.425, 0.224,

0.416, 0.95 contains an up-run of length 3, a down-run of length 2 and an up-run of (at least) 2, depending on the next values[93].

15.The Craps Test

It plays 200000 games of craps, finds the number of wins and the number of throws necessary to end each game. The number of wins should be (very close to) a normal with mean 200000p and variance 200000p(1 − p), with p = 244 / 495. Throws necessary to complete the game can vary from 1 to infinity, but counts for all > 21 are lumped with 21.

dThe ID would be produced by executing a chaotic and PUBLIC KEY encryption in Java programming language The total size of generated IDs should be 10-12 MB to be tested by DieHard . DieHard is producing 215 p _ values between (0,1] Data Analyzing would be done according to: Increasing number of p_values in safe area and decreasing them in failure and doubt area means randomness (Security) is improved[93].

2.8.2 Entropy

Entropy Test: Entropy is one of the most important measures to measure the degree of (randomness) or disorder in a system. The definition and interpretation have been provided by C.E. Shannon in 1948 and N. Wiener in 1961. The entropy of the uncertainty of the random variable (X) with probabilities (pi, …, pn), log means natural logarithm, as defined in equation (2.2) [93].

$$E(x) = -\sum_{i=1}^{n} P(i) \quad log_2(P\ (i)) \quad \ldots\ldots. (2.2)\ [93].$$

2.8.3 Histogram

A histogram is a bar graph-like representation of data that groups a range of results into columns along the x-axis. The y-axis represents the

number or percentage of frequency in the data for each column and can be used to visualize the distributions of the data[93].

2.9 Simulation Tools

The proposed system is simulated with OPNET Network simulator, MATLAB, Java, and DieHard.

2.9.1 OPNET

It is a tool to simulate the behavior and performance of any type of network. The main difference Opnet Network Simulator comparing to other simulators lies in its power and versatility. IT Guru provides pre-built models of protocols and devices. It allows you to create and simulation different network topologies. The set of protocols/devices is fixed you cannot create new protocols nor modify the behavior of existing ones[94].

Advantages of OPNET Network Simulator:

a) OPNET Network Simulator is an open free software
b) Large number of project scenarios that are offered information on OPNET Network Simulator
c) Can be overlooked using Opnet Network Simulator.

The main Uses of OPNET simulator:

a) Operational validation.
b) Application troubleshooting.
c) Network planning and design (IPv4, IPv6).
d) Validating hardware architecture.
e) Protocol modeling.
f) Traffic modeling of telecommunication networks.

g) Evaluating performance aspects of complex software systems.

OPNET recently released a new IPv6 Planning and Operations module with several facilities for facilitating IPv6 implementations. The IPv6 module adds IPv6 network modeling capabilities. But it also provides some interesting tools (OPNET calls them "Wizards") that address specific IPv6 implementation challenges: The IPv6 Readiness Assessment Wizard and the IPv6 Migration Wizard. The IPv6 capabilities can implemented with OPNET are :

A- Dual-Stack Addressing

- Stateless address autoconfiguration
- DHCPv6
- DHCPv6 prefix delegation
- Anycast addresses

B- IPv6 Tunneling

- Manually configured tunnels
- Native tunneling over MPLS LSPs (6PE)
- GRE tunnels
- ISATAP

C- Routing

- OSPFv3
- IS-IS IPv6 extensions
- Multiprotocol BGP IPv6 address family
- RIPng
- QoS
- Classification

- Policing
- Queuing
- WRED

D- Multicast

- MLDv2
- PIM-SM
- PIM-SSM
- Multiprotocol BGP IPv6 multicast address family
- IPv6 BSR
- IPv6 bidirectional BSR
- Mobile IPv6
- IPv6 Mobile Ad-Hoc Networks (MANET)[94]

OPNET is a cost effective way to conduct testing due the capability to simulate various network topologies, sizes, and conditions. The problem is that there are different network modeling tools that are IPv6 capable. One of the most popular simulator that claim to be IPv6 capable is OPNET. Of these, OPNET possesses the best capability to tie in live systems to a simulation environment[94].

OPNET's System in the Loop module is a way to test actual products on an IPv6 network without having to convert the code into simulation. This module was the focus of the study to test the extent of the IPv6 support. There are specific configuration details that are required for OPNET's System in the Loop module to operate properly. For example, it is important to signify the right interface by including the source Ethernet media access control (MAC) address in the packet filter. Other filters for

protocol can be used to further limit the traffic that the module translates into simulation[94].

The simplest interface configuration is to have one physical network interface per real device. This is not always feasible and so it is possible to have one interface handling the traffic of all real devices; however, the packet filter has to be very specific otherwise traffic can be sent through the wrong section of the simulated network[94].

Within the simulation environment, a System in the Loop node can only be connected to another node through Ethernet. This connection is defined as a duplex 10Gbps link. Half-duplex links are not allowed. Also within the simulation environment, the System in the Loop node has to define the translation function it's using as well. For this study, the default translation function was being assessed[94].

2.9.2 MATLAB

MATLAB is a high-performance language for technical computing. It integrates computation, visualization, and programming environment. Furthermore, MATLAB is a modern programming language environment: it has sophisticated data structures, contains built-in editing and debugging tools, and supports object-oriented programming. These factors make MATLAB an excellent tool for teaching and research[95].

MATLAB has many advantages compared to conventional computer languages (e.g., C, FORTRAN) for solving technical problems. MATLAB is an interactive system whose basic data element is an array that does not require dimensioning. The software package has been commercially available since 1984 and is now considered as a standard tool

at most universities and industries worldwide[95]. In the proposed system is used for Entropy and Histogram calculation.

2.9.3 JAVA

Java is a general-purpose, class-based, object-oriented programming language designed for having lesser implementation dependencies. It is a computing platform for application development. Java is fast, secure, and reliable, therefore. It is widely used for developing Java applications in laptops, data centers, game consoles, scientific supercomputers, cell phones, etc. In the proposed system is used for security experiments implementation[96].

2.9.4 DieHard

The diehard tests are a battery of statistical tests for measuring the quality of a random number generator. They were developed by George Marsaglia over several years and first published in 1995 on a CD-ROM of random numbers

DieHard provides two modes of operation: a stand-alone mode that replaces the default memory manager, and a replicated mode that runs several replicas simultaneously. Both rely on a novel randomized memory manager that allows the computation of the exact probabilities of detecting or avoiding memory errors[97]. It used in the proposed system for randomness calculations.

Chapter Three

The Proposed Approach

3.1 Introduction

One of the problems in the network security is ID spoofing. To address the problem of IP spoofing a secure network is proposed. The proposed work is based on generating a unique ID of each device in the network. The generated ID should be secure and it should be invisible to other device. The proposed work is going to deal with sender and receiver at the network level. Alongside, This chapter explains the main steps of the proposed system implementation, configuration and installation OPNET and DieHard system. The simulation has been carried out using Optimized Network Engineering Tool (OPNET) modeler to implementing IPv6 network architecture, while evaluation system parameters such as randomness as the state of Fail, Doubt and Safe based on DieHard.

3.2 System Design

The proposed system is based on the two main stages:

- ID generating and ID hiding.

As, before going to explain the details of the proposed system it should illustrate where the protocol is working.

The proposed protocol receives the data from higher layer in the TCP/IP layers, as the transport layer. The protocol passes the packets to the data link layer after finishing a processing, as illustrated in the Figure (3.1)

In the receiver side the packets are received from data link layer then after processing by the proposed protocol the data is passed to transport layer.

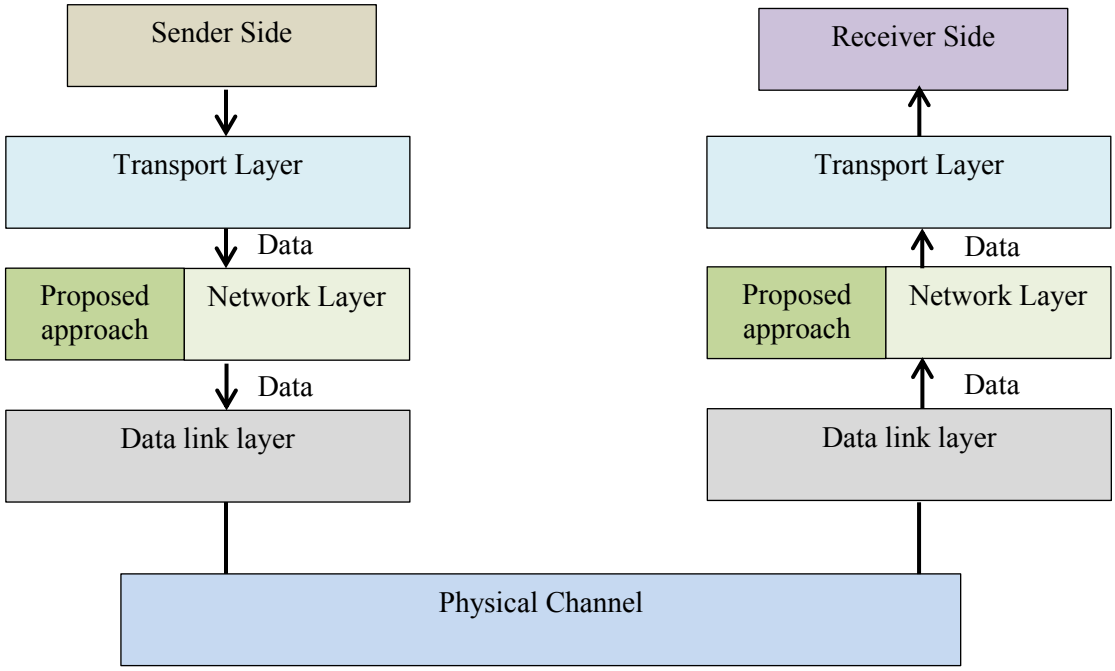


Figure 3.1 : The proposed work with TCP/IP Layers.

3.2.1 ID Generating

The generating of ID for each device is consisting of sequence of transformations. The ID generating transformations are Diffusion, Secreting and Hashing.

1) **Diffusion** : It is the first transformation that based on chaotic map to compute a diffused value according to equation (3.1).

   D= C (IPv6)…… (3.1) [90]

   Where :

   D: is a diffused value

   C: Chaotic function

   IPv6: Internet protocol address of advice.

2) **Secreting** : It is a transformation that used RSA function to reduce a secret value as shown in equation (3.2).

   S= RSA(D) ……(3.2) [90]

   Where:

S: is the secret value

RSA: is RSA encryption with receiver public key

D: is a diffuse value from equation (3.1)

3) **Hashing** : this transformation is using SHA2 or MD5 hash function to produce a new device ID as pointed in equation (3.3)

ID= Hash(S) …… (3.3)[90]

Where:

ID: is a new ID for the device.

Hash: is a SHA2 or MD5 function

S:secret value from equation (3.2).

3.2.2 ID Hiding

The suggested method is based on hiding the IPv6 identity in the Encapsulation field in the extension header to transmit data. Extension Headers are introduced in IPv6. The extension header mechanism is very important part of the IPv6 architecture. Next Header field of IPv6 fixed header points to the first Extension Header and this first extension header points to the second extension header and so on.

Figure (3.2) shows that the IPv6 header and the next header field is moved from the next header to another, so that the extension header is 1, then the extension header is 2, then the extension header 3 , then extension header... n, so on.

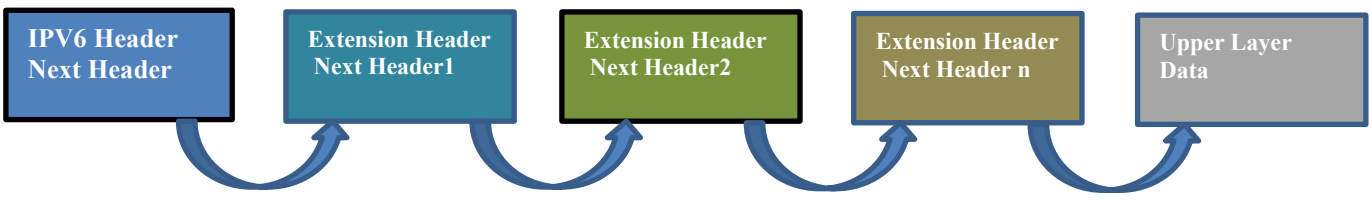


Figure 3.2 : Extension Header transferring from one header to another next header.

Besides, the proposed method based on the unique IPv6 identity, as the process of generate identity unique and it suggests to hide identity in extension header. The random unique identity is generating by using set of transformation on the IP address node, of which are encryption, chaotic transformation, and Hashing methods. While Figure (3.3) shows the extension header for hide IPv6.

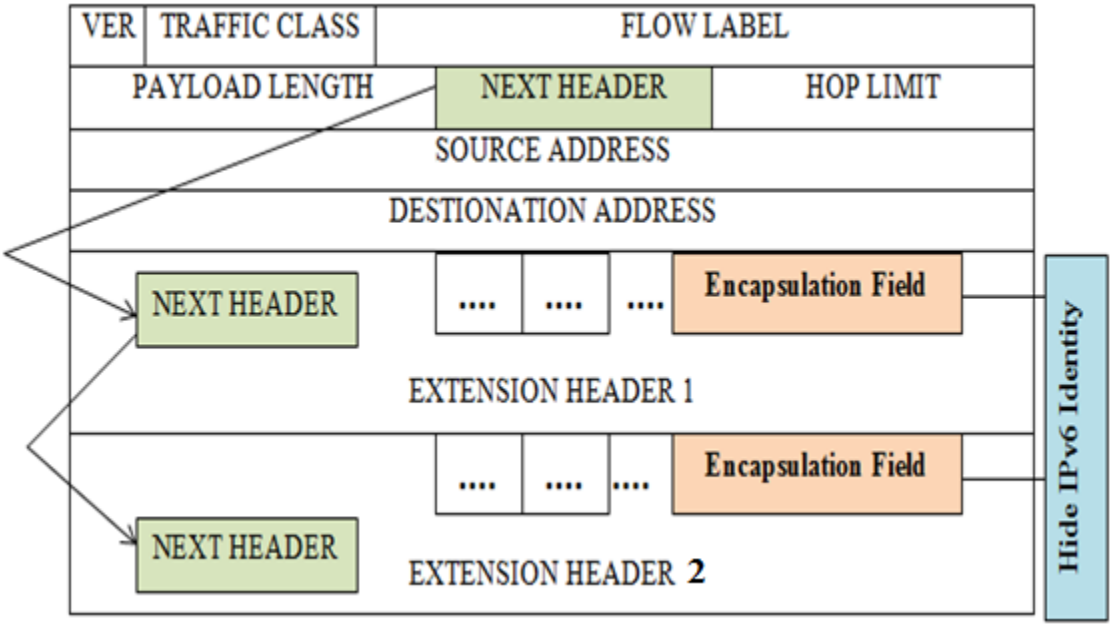


Figure 3.3: The proposed Extension Header for Hide Ipv6 Identity.

Extension headers ought to not either seen as a special IPv6 feature that as it were shows up in afterward stages of network and service deployment.Extension headers are an important and an integral part of the IPv6 protocol and support infrastructures.

The following IPv6 extension headers are commonly utilized:

A. **Hop-by-Hop**: It's an essential part of the Multicast Listener Discovery (MLD) process. The necessity of the Router notification is part of the multicast operations for MLD and Resource Reservation Protocol (RSV).

B. **Destination EH**: In IPv6 Mobility is applied to expand and support confirmed applications

C. **Routing EH**: Is utilized in IPv6 mobility and source routing.

D. **Fragmentation EH**: Is fundamental to preserve communication utilizing divided packets (in IPv6, the source of traffic must be divided; routers don't split the packets they send).

E. **Mobility EH**: This header is utilized to support Mobile IPv6 service (29).

F. **Authentication EH:** Similar in format and employ of the IPv4 authentication headers as mentioned RFC2402 RFC 4305: Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH), it is used to provide integrity, authentication, and security.

G. **The IPv4 ESP header** is similar to embedding a security payload in form and usage as described in EH RFC2406. All information following the Encapsulation security header (ESH) is encrypted and consequently now no longer available to intermediate network devices. ESH may be followed via way of means of an extra destination parameter EH and a high-level datagram. The expansion header was displayed in IPVn6. The expansion header in IPVn6 the expansion header instrument may be a basic a zone of the IPv6 design. The next field in IPv6 points to the main extension header, and that extension header points to another extension header.

3.3 Proposed System Block Diagram

At the initial stage, the system generates a new ID in the 16-bytes IPv6 represent as the identity between the sender and the recipient. Logistic

Map is used very chaotically for sparse addresses and provides random addresses.

RSA Algorithm is applied to encrypt values resulted by Chaotic. Whereas Hash (SHA2 or MD5) is applied to offer a completely unique address, that's hard to modification, as it regarded in Figure (3.4).

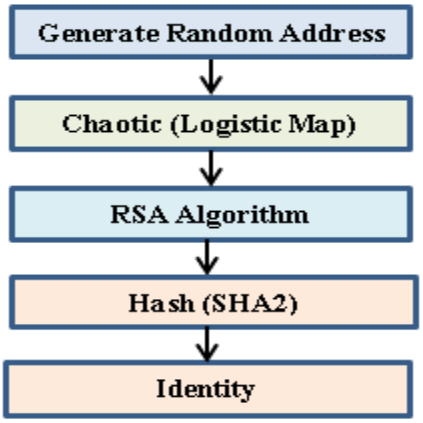


Figure 3.4: Block Diagram of the proposed identity generating steps.

The proposed system deals with the sender and receiver side, there is a different process in each side. In the sender side a new ID is generated and hided inside each packet. However, in the receiver side the hidden identity is extended then it is compared to a computed identity from current received packet.

Moreover, the proposed system steps between sender and receiver units are showed in Figure (3.5). As in the first step the IPv6 identity is processed with chaotic and then it is encrepted with public key RSA. The result is managed by Hash function to encode again then the result is proceed by steganography techniqe. The result is send as the stego-packet to the receiver. The receiver side is received the stego-packet then it retrives the stego-packect to pass to the Hash function (SHA2). The result value is passed to decrypt and retrive the original value through chaotic.

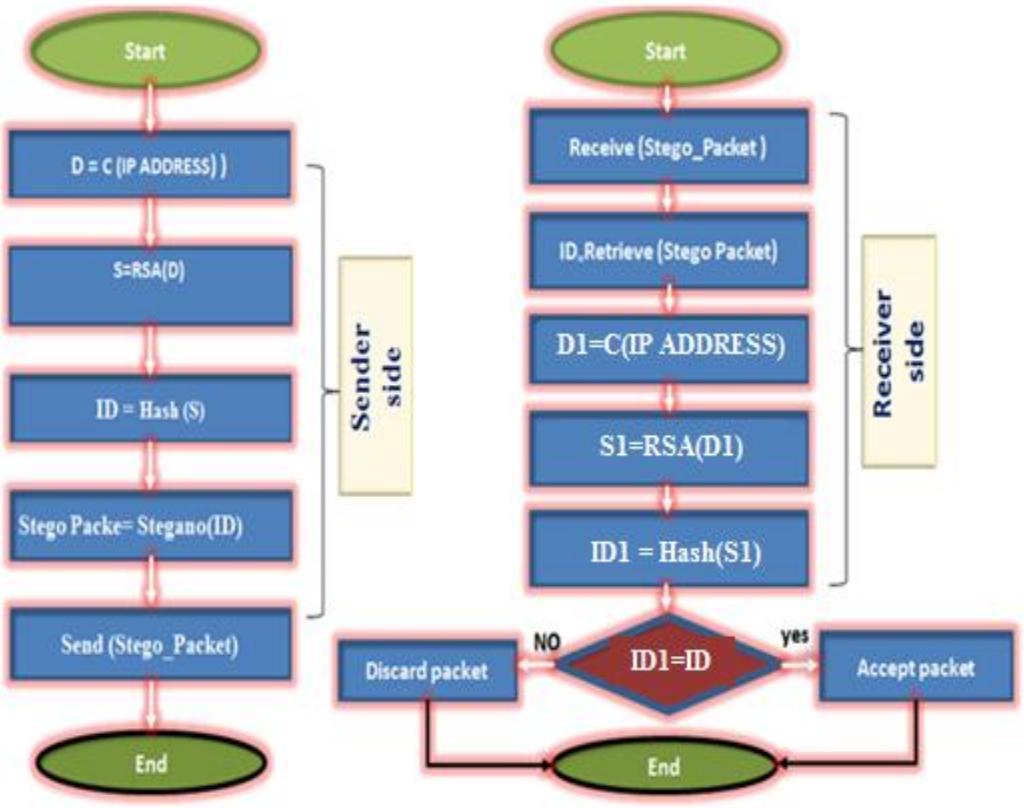


Figure 3.5:The proposed system steps.

The main steps of algorithms are explained as follows :

1- The input state contain on (IPv6 Address)

2- Implementing the diffusion with chaotic (Logistic Map) of IPv6 Address.

- Chaotic method used for data encoding. In the encoding system is based on using chaotic sequence. Chaotic sequence has the following characteristics.

a) A chaotic map can output fixed sequence with a random input. The generation of chaotic sequence can be controlled by user, that is, we can have a fixed length sequence.

b) Given a chaotic map and an input, the chaotic sequence can be calculated. But given an output sequence, it cannot find the

equivalent input. The chaotic sequence is pseudorandom, so it is impossible that two data in a certain length is same.

3- Passing the diffused value to the RSA function to creating secret value. The main steps of IPv6 RSA public key are :-

- **At Sender site**

Step 1: Enter Message and apply chaotic encoding algorithm. Encoded Message Generated.

Step 2: Apply RSA Encryption Algorithm on Encoded Message. Cipher text Generated.

Step 3: Convert Cipher text in Ascii Value and convert into Hex Value.

Step 4: Convert Hex into Binary

Step 5: Embed binary value.

Step 6: Binary data divided into specific size and it stored in binary data in each IPv6 Packet. As per data size packets are created.

- **At Receiver Site**

Step 1: Receiver capture Ipv6 number of Ipv6 packet

Step 2: Apply Decoding algorithm and Receive original packet

4- Hash (secret value) with :

SHA2-256 or MD5 — produces a 256-bit (32 byte) message digest.

5- Hiding ID of packets depending on steganography method used in sender side.

6- Then send packets to receive by the receiver with the opposite steps to return IPv6 address.

Figure (3.6) shows the algorithms with equations settings for sender/receiver sides.

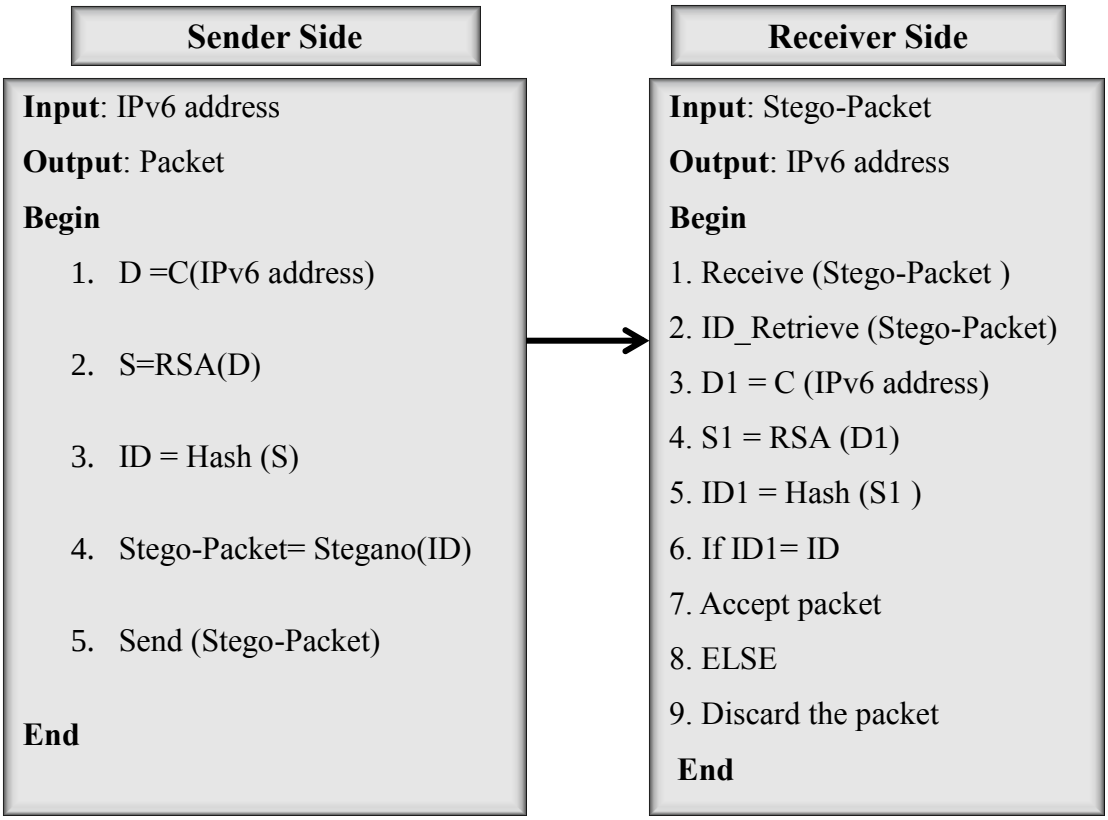


Figure 3.6 : The steps in the proposed system.

3.4 System Installation Requirements

The proposed system installation is based on deploying OPNET Modeler to simulate IPv6 network and multimode sites are installed on Windows 8 32-bits.

The proposed system is based on the two main tools to simulate and to implement the IPv6 environment and the main configuration for both showed as follow :

3.4.1 OPNET Modeler Configuration

OPNET Modeler provides the capability to simulate an IPv6 network and the OPNET System in the Loop, an add-on module, allows for

real devices to be tested over the simulated network. This study evaluates the support of IPv6 in OPNET Modeler 14.5 with the System in the Loop module. Besides, simulating a basic network is vital to examine for IPv6 readiness, many software and hardware vendors are adapting their technologies to support IPv6. There is a need to be able to test these products on an IPv6 network.

3.4.2 DieHard Configuration

Diehard test suite is a statistical analysis suite for testing randomness of the numbers produced. It designed to permit one to push a weak generator to unambiguous failure (at the e.g. 0.0001% level), not leave one in the "limbo" of 1% or 5% maybe-failure. It also contains many tests and is extensible so that eventually it will contain many more tests than it already does.

3.4.3 Java configuration

The proposed system based on implementing java security package of RSA in java library. Besides, the proposed method provides an encrypt and decrypt a generated Diffusion by leveraging RSA asymmetric encryption algorithm by generating a private key and public key using java KeyPairGenerator and a Cipher class that provided encryption and decryption functionalities.

3.4.4 MATLAB configuration

MATLAB environment enables advanced data processing and analysis, especially using its toolboxes like signal processing, and statistic. It used in the proposed system to measure Entropy value of 9 experiments of randomness strength and histogram calculations.

Chapter Four

The Implementation، Results and Discussion

4.1 Overview

This chapter explains the results described in chapter three. Four tests are implemented to evaluated a proposed system. The results showed as Robustness test, Randomness Test to measure randomness with higher randomness increases security level, Entropy to measure the randomness of IDs , Histogram to measure distributions of the data in the proposed method, and Network Test to measure network performance.

4.2 The Proposed System Implementation

The proposed approach based on two main case study. The system has been implemented in an environment with the specifications shown in Table (4.1). Moreover, The practical side has been implemented based on java programming language, DieHard, and OPNET.

Table 4.1: Environment specifications for the proposed system.

Operating Systems	windows 8.1 pro 32 bits
CPU	intel(R) cor(TM)i5-2450M CPU2.50GHz
RAM	4.00 GB
Implementation Tools	Java, OPNET modular Version 14.5, and DieHard

4.3 The Proposed System Evaluation

The evaluation of the proposed system is done through 4-tests, which are sorted as (Randomness Test, Entropy Test, Histogram Test, and Network Test):

4.3.1 Randomness Test

The subtest of this evaluation parameter are following :

The aim of this test is to compute a randomness of generated devices ID. The proposed work should generate a random ID. The test is accomplished using the diehard statistical software. This software is working with file size between (10 to 12)MB. DieHard software produces 215 p-values. The collected Data would organized as showed in Table 4.2.

Table 4.2: Data collected with DieHard tool.

Doubt Area	"0.1 < p-value ≤ 0.25 or 0.75 ≤ p-value < 0.9"
Failure Area	"0 < p-value ≤ 0.1 or 0.9 ≤ p-value ≤ 1"
Safe Area	"0.25 < p-value < 0.75"

Besides, the data analysing would be done according to the explanation:

- Increasing number of p_values in safe area and decreasing them in failure and doubt area means randomness (Security) is improved.
- Decreasing P-value in safe area. In random test 9 experiments are implemented in each experiment, a different scenario is used to generate set of IDs, The generated IDs of each experiment is tested by diehard. In the first experiment RSA (512) and MD5 (512) are used to generated (11 MB /16 B) = 687,500 IDs.
- From the second experiment to the ninth are implemented with the same proposed file size (11 MB)and with the different content depending on the RSA key size from (512 bits to 2048) while the hash function cipher text size from 256 bits to 512 bits.

Table 4.3:The nine experiments settings.

Experiment Number	RSA Key Size in Bits	Hash function cipher Text Size in bits
1	512	MD5 512
2	1024	MD5 512
3	2048	MD5 512

4	512	SHA2 256
5	1024	SHA2 256
6	2048	SHA2 256
7	512	SHA2 512
8	1024	SHA2 512
9	2048	SHA2 512

Besides, the Figure (4.1), showed the proposed 9 experiments and based on the three cases as Fail, Doubt and Safe.

The results show the state of Fail, Doubt and Safe based on DieHard . The proposed number of input values as 215 for each experiment, and the best result showed in Experiment 8 with Fail (34) and Safe (114). The RSA key size used between 512 bits to 2048 bits, Hash Function method as MD5 as 512 bits and Hash Function as SHA2 256 bits to 512 bits.

To measure the effectiveness and strength of the secret keys generated by the proposed method, the work calculates randomness. The first test of randomness is performed by using a Diehard statistical test, which consists of 15 sub-tests.

The result of statistical tests, called p-values are computed between (0,1] depending on distributing for the random variable. The area divided into three parts (safe, doubt, fail). The p-values in the fail area should reduce, and the p-values should increase in the safe area, to get better randomness and to increase the security.

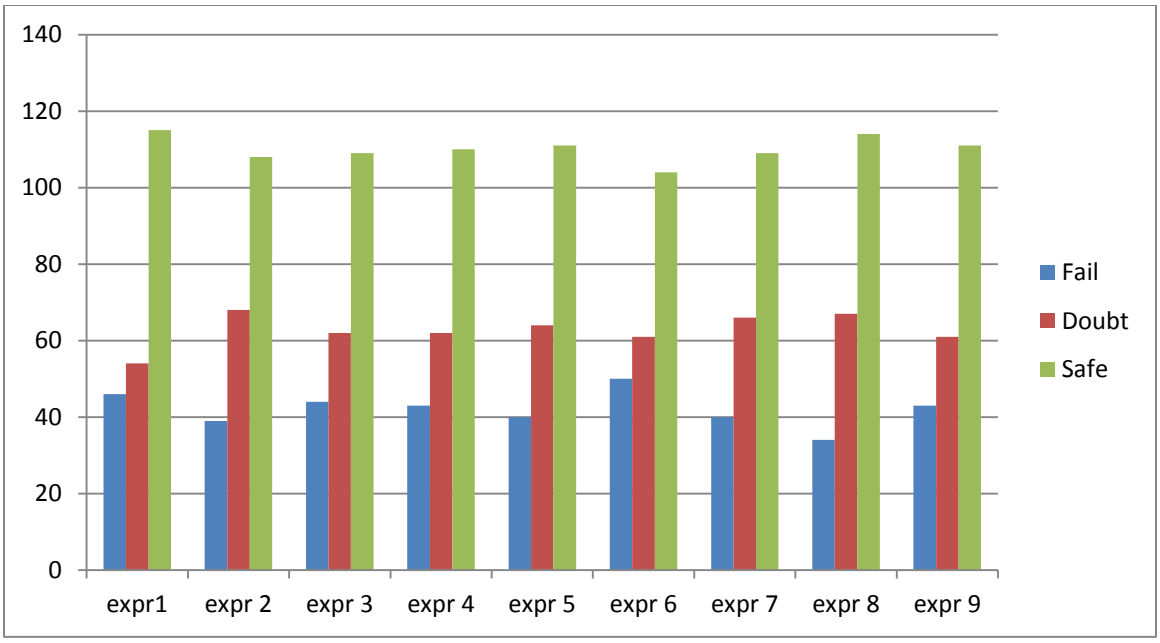


Figure 4.1 : The Fail, Doubt and Safe of the 9 Experiments.

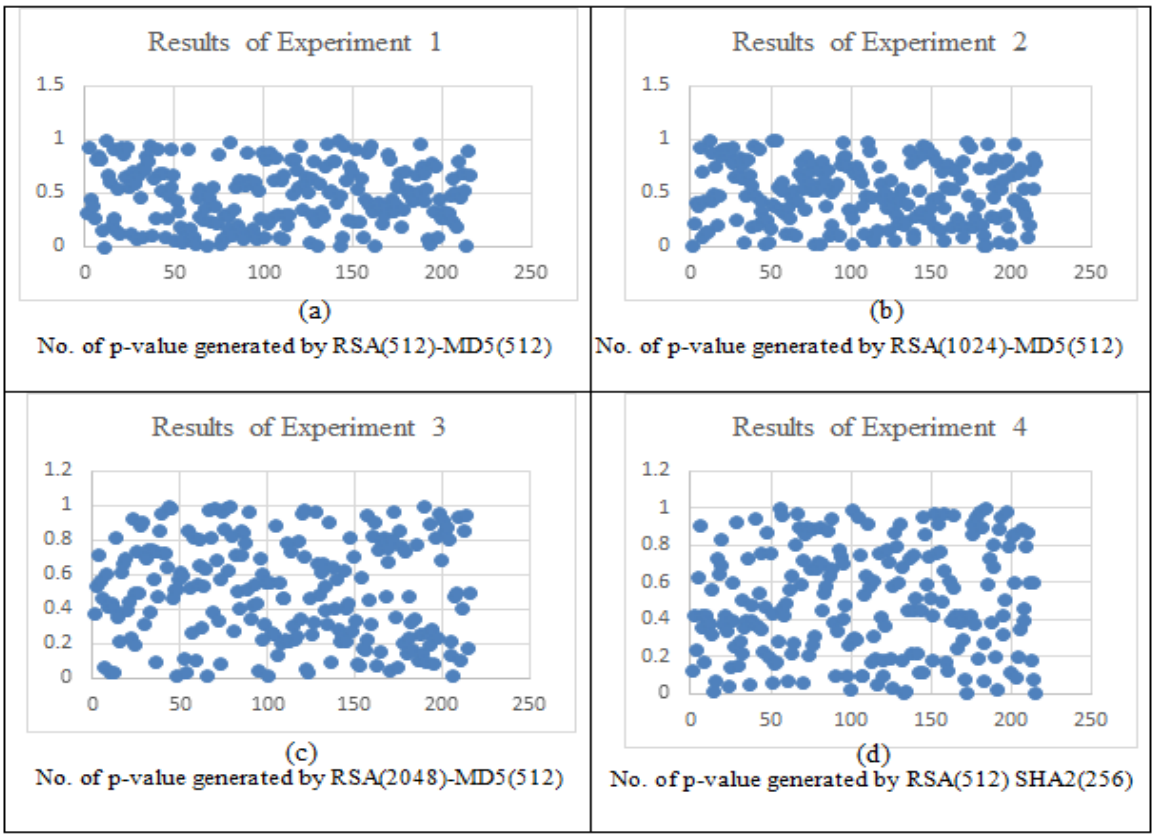
In addition, the results of Randomness Test explained as the ID would be produced by executing a chaotic, PUBLIC KEY encryption and Hash function in Java programming language The total size of generated IDs should be 10-12 MB to be tested by DieHard . DieHard is producing 215 p _ values between (0,1]. The randomness of an algorithm's performance is one of the most crucial factors in determining its security. The diehard tests are carried out by the 9 tests. These include 15 Statistical tests. These tests use p-values to divide the set into three categories: safe, doubt, and failure. The following regions can be used to describe these areas: In the region of Doubt, there are 0.1 p-values 0.25 or 0.75 $p > 0.9$. $0 <$ p-value ≤ 0.1 or $0.9 \leq$ p-value $\leq$ 1in the failure area. In a safe area, a p-value of 0.25 to 0.75. Alongside, as mentioned that the best result shows in experiment 8 as showed in Figure 4.1.

In the first case of the Figure (4.2) of (a) the cases of P-value is showed as the p-value of Fail is 46 (decreased), and Safe is 115 (increased),so the randomness is increased.

Besides, the Figure (4.2) of (b) the cases of P-value is showed as the p-value of Fail is 39 (decreased), and Safe is 108 (increased),so the randomness is increased.

The Figure (4.2) of (c) the cases of P-value is showed as the p-value of Fail is 44 (decreased), and Safe is 109 (increased),so the randomness is increased.

The Figure (4.2) of (d) the cases of P-value is showed as the p-value of Fail is 43 (decreased), and Safe is 110 (increased),so the randomness is increased.



(a to d)

Figure 4.2: Randomness of generated IDs.

The Figure (4.2) of (e) the cases of P-value is showed as the p-value of Fail is 40 (decreased), and Safe is 111 (increased),so the randomness is increased. The Figure 4.2 of (f) the cases of P-value is

showed as the p-value of Fail is 50 (decreased), and Safe is 104 (increased),so the randomness is increased. The Figure 4.2 of (g) the cases of P-value is showed as the p-value of Fail is 40 (decreased), and Safe is 109 (increased),so the randomness is increased. The Figure 4.2 of (h) the cases of P-value is showed as the p-value of Fail is 34 (decreased), and Safe is 114 (increased),so the randomness is increased. The Figure 4.2 of (i) the cases of P-value is showed as the p-value of Fail is 43 (decreased), and Safe is 111 (increased),so the randomness is increased.

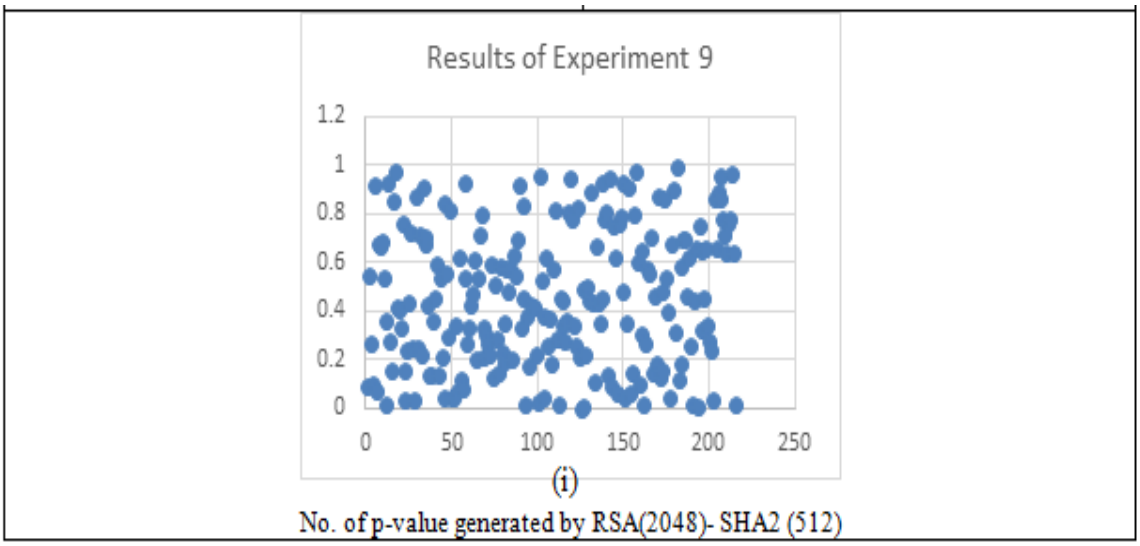
The results showed that the better randomnes from the experiment 8 with the p-vlaues as Fail is 34, and Safe is 114.

(e) No. of p-value generated by RSA(1024)-SHA2(256)

(f) No. of p-value generated by RSA(2048)SHA2 (256)

(g) No. of p-value generated by RSA(512)- SHA2 (512)

(h) No. of p-value generated by RSA(1024)SHA2 (512)



(e to i)

Figure 4.2: Randomness of generated IDs.

4.3.2 Entropy Test

Entropy Test which is executed by MATLAB. Entropy test is the second measure that is used to evaluate the quantity of randomness. The entropy of the uncertainty of the random variable (X) with probabilities (pi, …, pn), log means natural logarithm, as defined in equation within chapter 2, equation (2.2) .While the Entropy of each experiment value showed in Figure (4.3) with the highest entropy value from the experiment 3 as 7.999985109, which is the nearest value from the best result of Entropy as 8 value.

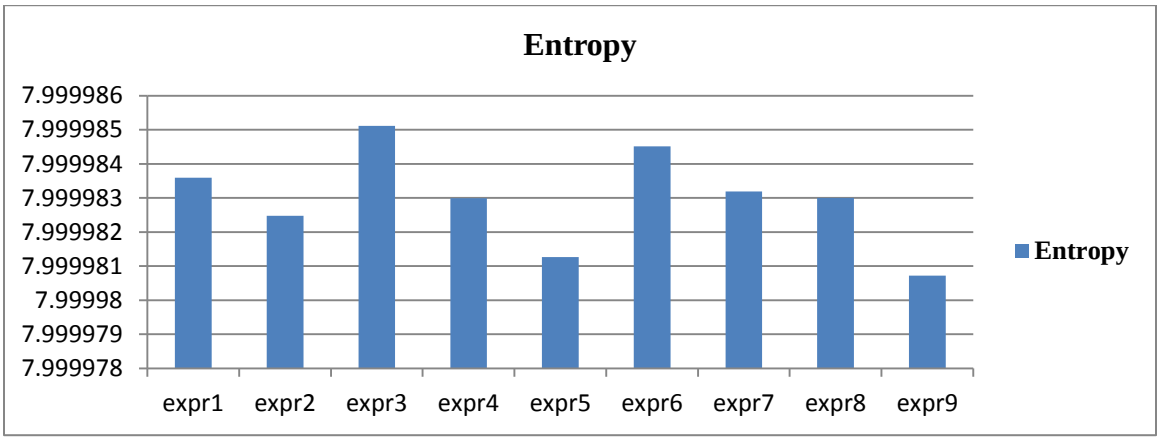
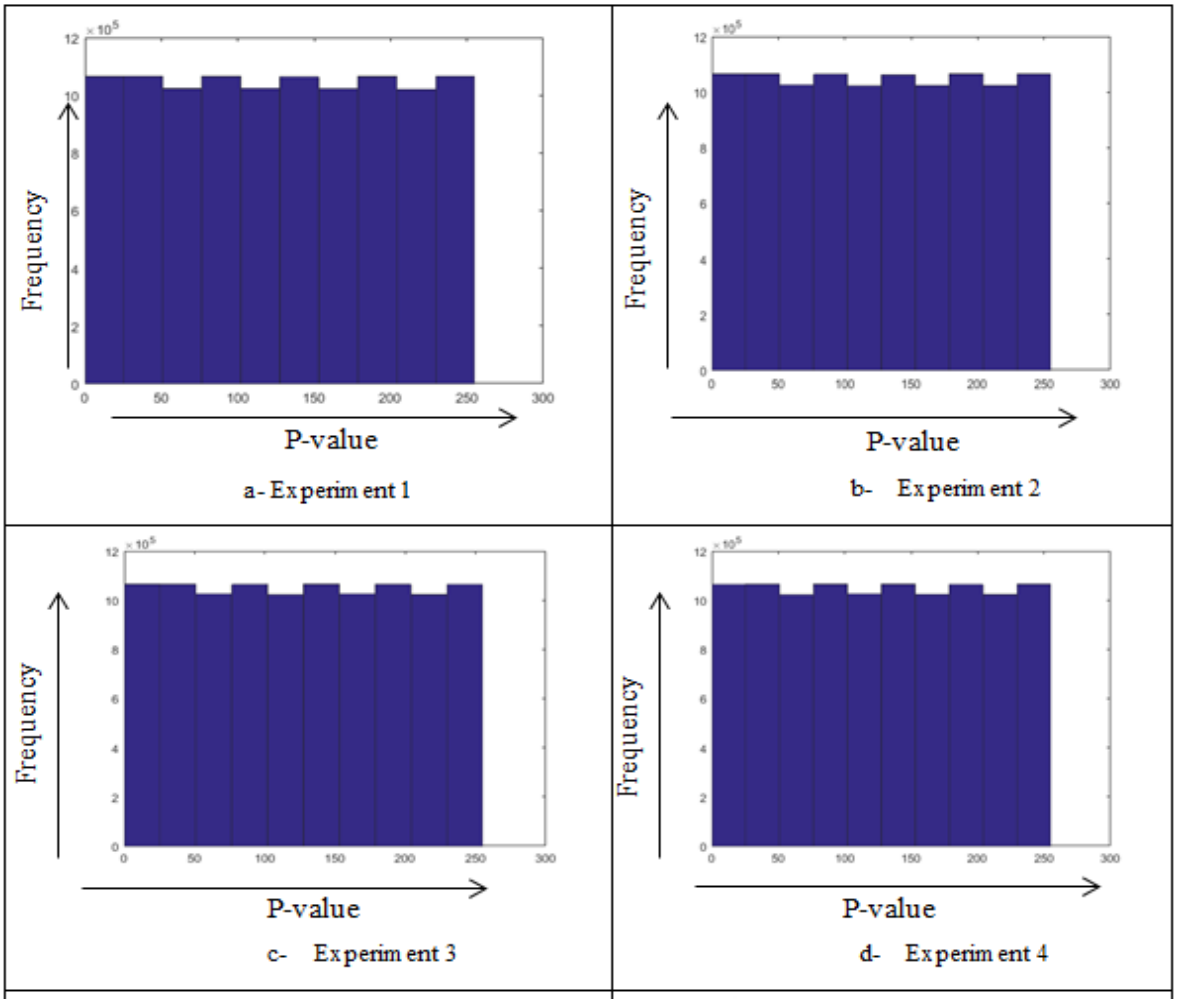


Figure 4.3: Entropy results of 9 experiments.

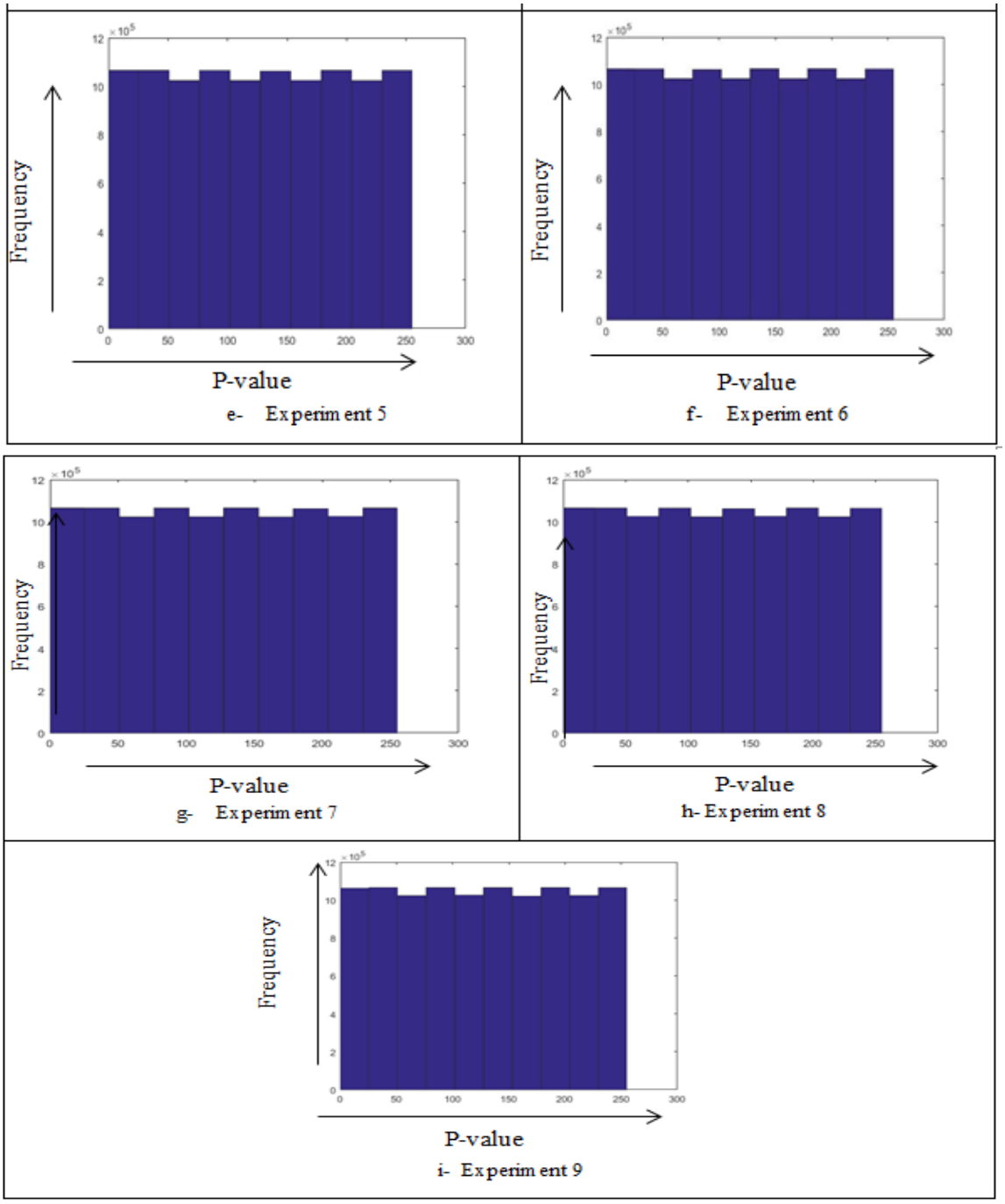
4.3.3 Histogram Test

A histogram is a bar graph-like representation of data that groups a range of results into columns along the x-axis. The y-axis represents the number or percentage of frequency in the data for each column and can be used to visualize the distributions of the data. Alongside, the histogram test is implemented on each experiment (9 experiments) are executed Figure 4.3. The results of Histogram test for generated IDs in (9 experiments) show that they have a good distribution as illustrated in Figure (4.4).The best result of Histogram values of Experiment explained as :



(a to d)

Figure 4.4: Histogram of the generated IDs.



(e to i)

Figure 4.4: Histogram of the generated IDs.

4.3.4 Network Test

The proposed system is based on the IPv6 implemented in Iraq sites, with 9 locations in different cities (has web and file clients), while the central network in the capital (Baghdad) has three servers (files, web and

database additionally work for database clients). This was implemented using OPNET Modeler 14.5. The network shown in Figure (4.5).

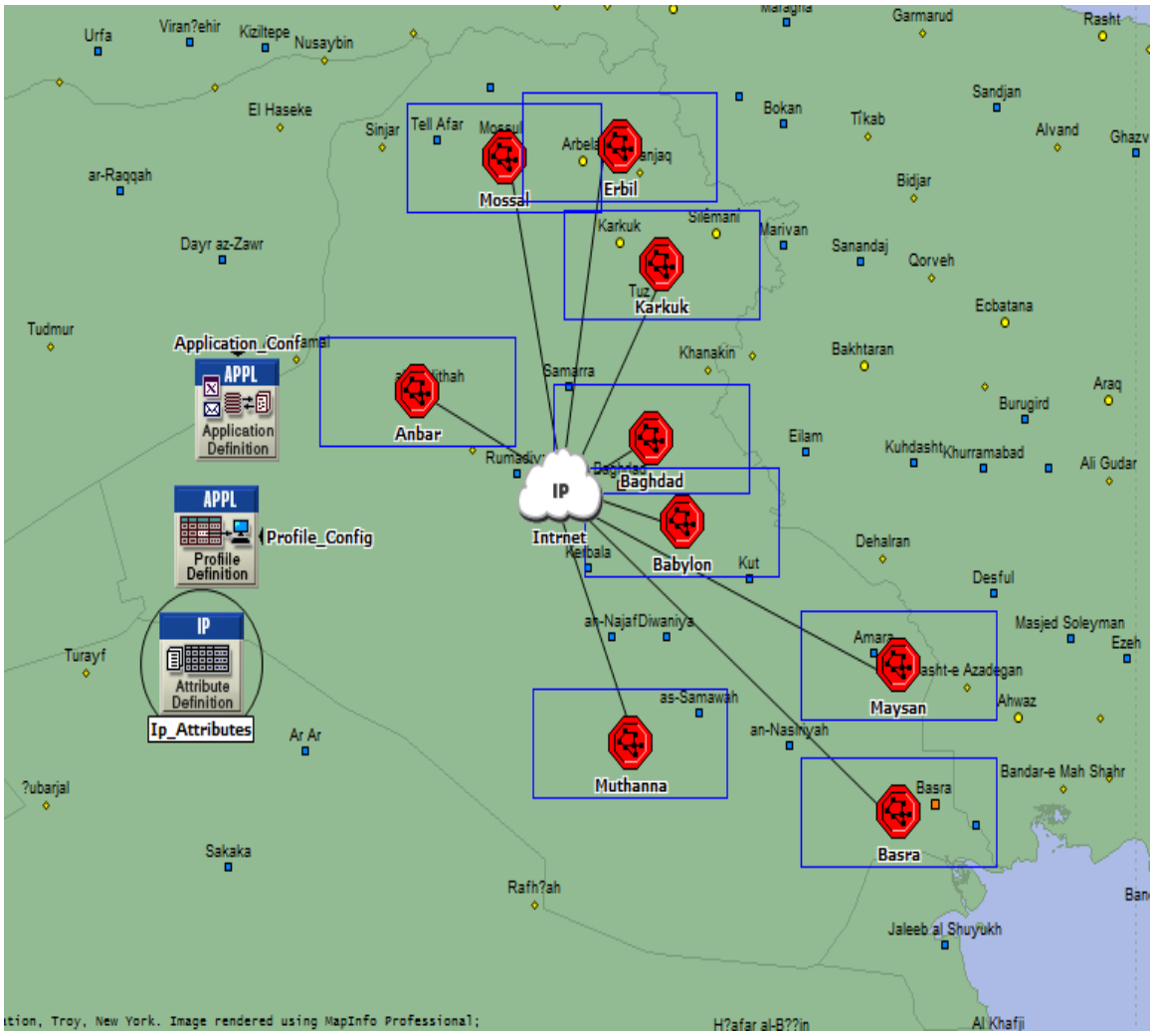


Figure 4.5: proposed network in Iraq

Two scenarios are implemented in network test in scenario 1 and scenario 2 a set of criteria in below has been calculated as follow:

- Average(in Email. Traffic sent (bytes/sec).
- Average(in Email. Traffic received (bytes/sec).
- Average(in FTP . Traffic sent (bytes/sec).
- Average(in FTP.Traffic received(bytes/sec).

In the scenario 1 it implemented the network without any hidden data(Node ID) as 485 bytes to check the network efficiency, while in scenario 2 added 16 bytes to be (501 bytes) invisible identity and it isn't discovered or altered by data transmission. The results show that the traffic attack can't discover any changes through network transmission through hide identity and filter packets through authentication process.

4.4 The Proposed System Simulation with OPNET

In addition, the methodology within the system used is based on two scenarios: without DoS attack scenario and with DoS attack. It is based on the unique IPv6 identity for both scenarios as it suggests the process of creating a unique identity and hiding the identity in the extension header. Create random unique identities using a set of transformations to the IP address node through encryption and chaos change methods. The proposed system topology based on OPNET is shown in Figure (4.6).

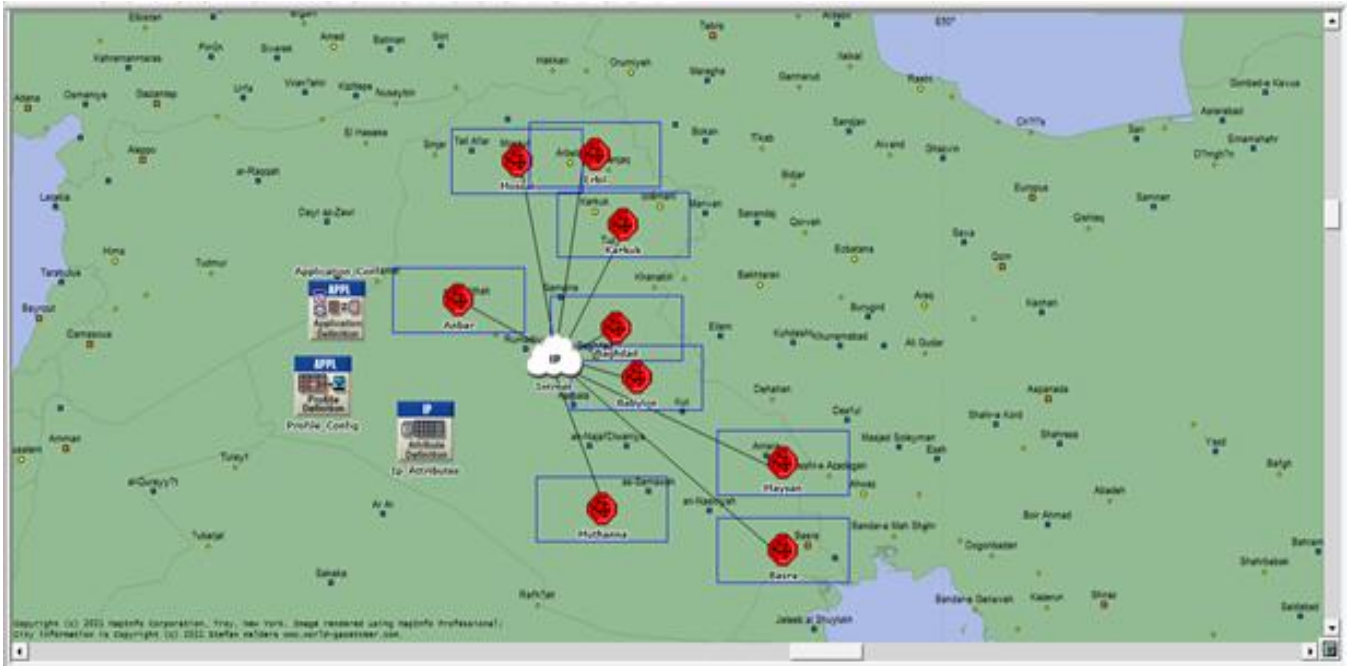


Figure 4.6: The Proposed System Topology based on OPNET.

In Table (4.4), the element name showed the network elements nodes, with the number of nodes, the standard scale showed the characteristics of the used technology based on the wired scenario, the name link represents the connection of the duplex link, the rate of transmitted data depending on the link type in Mbps.

Besides, Profile Config element used to create user profile, these users profiles can specify different node in the network to generate application layer traffic the application defined in the "Application config" objects are used by the object to configure profiles. Also, PPP DS3 link to connect two nodes running IP as duplex link of point to point nodes, while 10Base T as the duplex link Ethernet with 10 Mbps to connect different network elements except hub device.

While system elements and scale side of scenario explained in Table (4.4).

Table 4.4: The used network element names and feature characteristics.

Element Name	**The Number**	**Standard Scale**	**Scenario**
Application Config	1	/	Wired network
Profile Config	1	/	
Ip64_cloud	1	IEEE 802.3	
Ethernet server	3	IEEE 802.3	
10BaseT_LAN	17	IEEE 802.3	
ethernet4_slip8_gtwy	10	IEEE 802.3	
Ethernet 16_Switch	1	IEEE 802.3	
The Name Link	**The Number**	**Data Rate(Mbps)**	**Network Used**
PPP DS3	9	44.7	Wired network
10Base T	18	10	

The proposed system based on the static IPv6 route table which is recognize incoming request if it is authorized or not by matching the

incoming IPv6 route with the static route in the central router. If the route within the route table, the request will be accept and if the route is not within the route table, it will reject and delete route. This method simulated with the OPNET modular tool. Table (4.5) shows the static route of the IPv6 addresses of the 5 block of IPv6, while the proposed system based on the 9 sites, with the main services as File transmission, web, Email, database services.

Table 4.5: IPv6 addresses

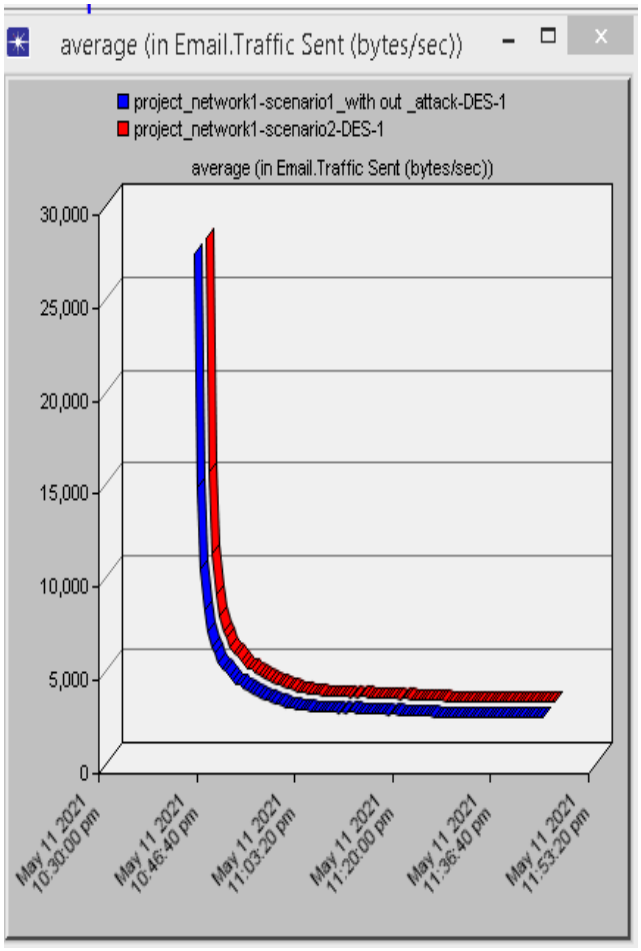
Site	IPv6	Next hop	Services	Prefix
Baghdad	**b191:1556:e4a5:bc63:c06c:3532:8f0b:4f92 2ca:bcd2:c900:7b2c:c37d:a64b:376e:1390 465b:6a6a:9ec7:f619:3fce:2c8f:8115:bcb0 5954:18d9:5bbf:4395:61eb:ce71:acde:ac65 a89e:c124:b087:be67:3aa6:a1de:d415:d73a**		**File, Web, Email, Database**	
Arbil	**d15:9049:2ff9:7819:f032:1aae:e7a1:f995 f0d7:ae6:3f64:916c:ae:350c:1c08:fe00 9b3d:97c7:4808:ebdf:207f:4988:4658:32f0 9cb1:f267:f4d8:3c84:3c67:8a03:44ac:b1ae f60b:c3c9:7a35:14f:a81c:73ef:4aa5:d956**		**File, Email**	
Anbar	**d97a:8588:d661:96ba:c050:3e4b:8037:2bab 96f4:1fe5:496a:821f:f45f:e3e8:b2c4:5d41 f7ff:a0f:e8ab:a122:6c36:6b15:1e4f:1661 a5cf:f056:9358:1174:9094:569d:2ef2:3a17 592a:220b:8d40:84f7:1038:4151:3ac9:7855**		**File, Email**	
Babylon	**6da:52c5:499a:3587:6c58:3b6a:818e:c653 22a0:d245:2968:d92:3e1b:c454:b840:2b71 a476:e52c:1a24:885e:9278:86e6:94c8:dbb3 4880:: ef:3624:34bd:ccb:129d:dc3b 609a:c400:d1b:45a9:670a:bcaf:8d5a:7c7**		**File, Email**	

Karkuk	**f1cb:eb4d:4525:c91c:1b0b:7ec:e21e:c279 9746: 68af:cf87:b8cb:1075:fefa:302:baec 1c84:6dad:7405:1841:5b19:a333:6166:4669 7898:deee:ee0f:8dac:9112:d283:7ca6:a2d ebec:f7cc:7ffa:b6ff:5d74:aa4d:f426:664b**	**8 routes**	**File, Email**	**/ 64**
Basrah	**415c:97aa:d57b:7dcc:9f68:f8a7:2e2c:1525 471: 1e9e:330b:952f:2465:98b:b89b:5fb6 a161:3a58:aed4:75b0:2fa0:fcfb:ffb5:8279 3a33:f862:29d7:57f3:cc19:2398:ce1c:7cf4 7570: 3ab6:6634:9a2f:d6b9:52e:4be:49d9**		**File, Email**	
Mesan	**2cca:da8c:65b8:f6e:9731:9993:8fcb:ea5a 45bb:d52e:dedf:419a:b4e:5e67:a2f6:8d 8fab:f403:7c07:4dee:bab0:edd6:1ddd:9e5a dca6:eb66:3f12:6237:ffde:1aee:41f8:c462 e963:c16b:7621:8e2b:ac70:f3ee:da21:feff**		**File, Email**	
Mothana	**8367:227e:97af:fc42:77fe:86bd:b18b:253e :79f11b:40b7:adbc:a8f8:faba:be75:ba12 :5053c652:6127:43f5:fae7:baf0:f3d:93db b679:47bf:f737:2f28:cc0b:5976:5668:2d6c 2e38:8417:b6a6:202c:2e43:696f:7acd:39ea**		**File, Email**	
Mosul	**1958:5aef:54a0:636d:77b6:699e:5a13:9a33 :5004b812:9384:3339:fd8d:cb5a:2774:c254 6487:2d30:e7a7:6e51:fa6f:1b09:bc3b:8e48 d10:a733:59d4:4f1a:bca6:98a0:ec6d:23cf 4507:204f:3733:4a3c:e6c:9f59:5a03:567b**		**File, Email**	

Utilize OPNET modellers ,it's used to simulate the network environment to evaluate its performance and to simulate against Dos attacks launched from boundary nodes, check the positive impacts, such as network stability, inside the source address authentication scheme within the setting of DoS attacks In addition, within a single degree of autonomy,

realize subnet real IPv6 source address verification. Figure (4.7), the network is simulated by adding a specific 16-byte packet inside the ipv6 header and the smaller one as a default size of 1500 bytes, as 1516 bytes and 485 bytes as 501 for both sent and received packets. The proposed system showed that there is not any change during send and received which it effect on the network performance traffic especially during attack cases.

Scenario 1= 485 byte and scenario 2 = 501 byte Sent packet for Email application



Scenario 1= 485 byte and scenario 2 = 501 byte received packet for Email application

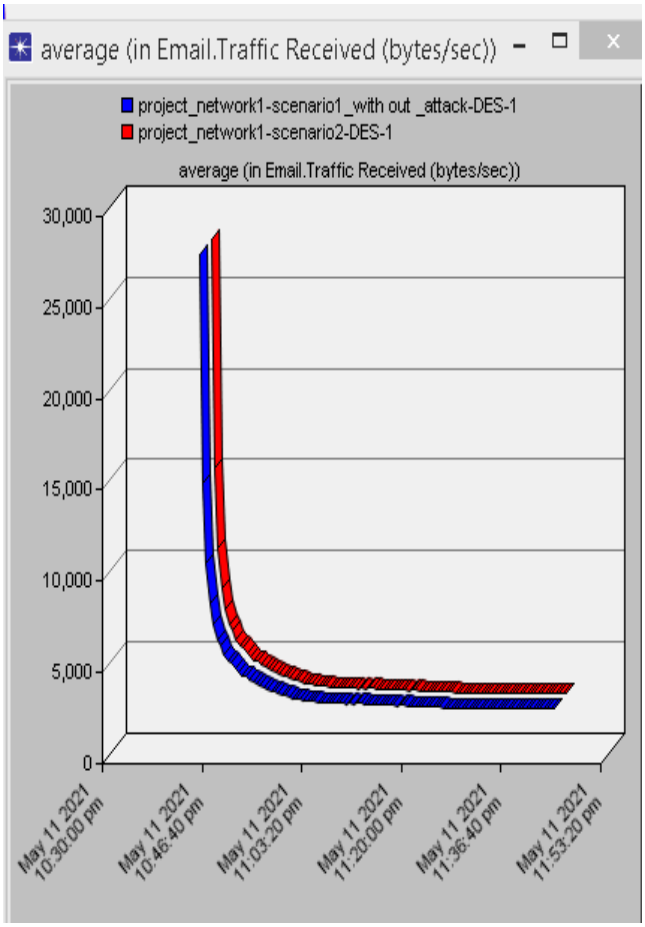


Figure 4.7: Traffic Send For Two Scenarios For Email Applications.

In addition, Figure (4.8) showed the FTP application of scenario 3 with 1500 bytes and scenario 4 with 1516 bytes.

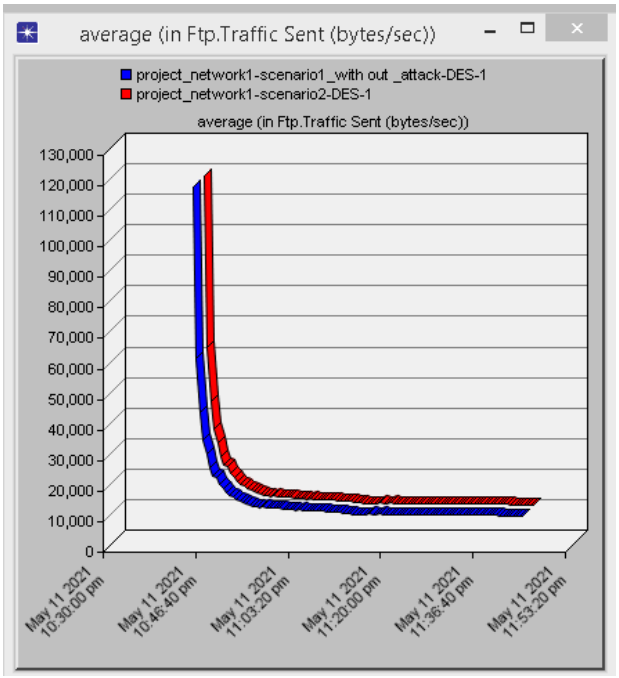
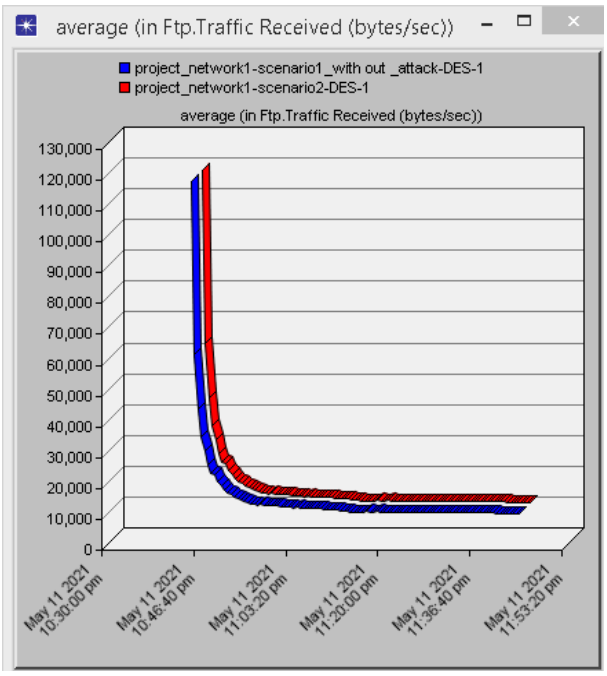
Scenario 1= 1500 byte and scenario 2 = 1516 byte sent packet for FTP application	Scenario 1= 1500 byte and scenario 2 = 1516 byte received packet for FTP application
	

Figure 4.8: Traffic Send For Four Scenarios For FTP Applications.

4.4.1 The proposed system simulation with DoS attack

The proposed system of DoS attack showed in the proposed system topology showed in Figure 4.9 . The results showed the loose packets as 9,273 per seconds and increased memory usage and number of Avg events increased due to DoS attack .

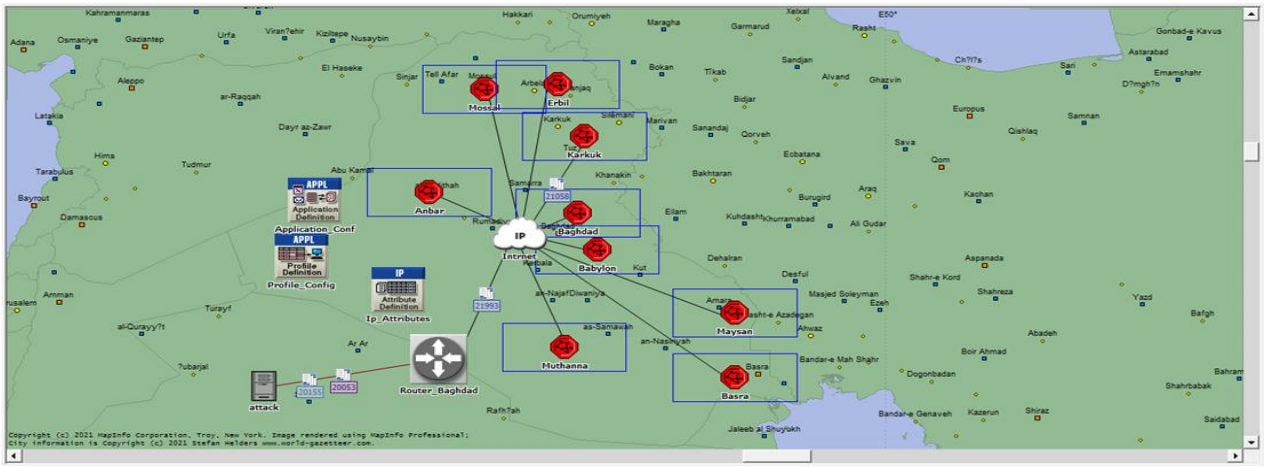


Figure 4.9: The proposed network with DoS attack.

Table 4.6: The proposed case study with DoS attack.

Host Name	Duration	Time Elapsed	No. of Events	Total Memory	Avg Events/sec	Traffic Sent	Traffic Received	Lose Packets
Local Host	5 m	57 s	8,235	36,731 KB	263,52	33,412	24,139	9,273

4.4.2 The proposed system simulation without DoS attack

The proposed system simulated in OPNET without DoS attack and the enhancement system state showed that the used methods decrease number of events effect on the computation power of system nodes and decreased number of lost packets beside memory usage also decreased, as showed in Table 4.7 .

Table 4.7: the results of without DoS attack

Host Name	Duration	Time Elapsed	No. of Events	Total Memory	Avg Events/sec	Traffic Sent	Traffic Received	Lose Packets
Local Host	5 m	45 s	8,235	35,523 KB	250,52	30,324	27,227	3,097

The comparison of the system case studies of with and without DoS attacks showed in Figure 4.10. It showed that the proposed system decrease loose rate from 9,273 to 3,097 Packets/s in the case of the proposed static IPv6 route matching method.

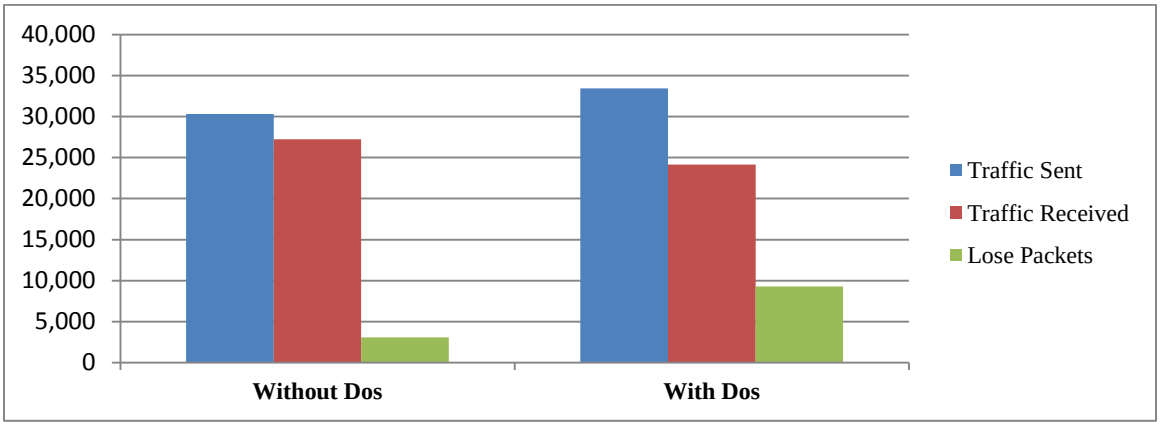


Figure 4.10: System comparisons for both with/without Dos attack case studies.

The proposed system compared with the related works have the same system specifications. It is based on the text packets, it showed the high packets sent per second as well as the traffic received also was highly. In addition, the evaluation metrics are summarized in Table 4.8.

Table 4.8: The proposed system comparison with related works.

Ref., Year	**Application Type**	**Network Size**	**Nature of Network**	**Duration**	**Traffic Sent/packet**	**Traffic Received/packet**	**Lose Packets**
[98], 2020	Email Traffic	4 sites	OPNET modeler	280 s	810	805	5
[99], 2020	Video Conferencing	3 sites	OPNET modeler	5 m	8.3	7.0	1.3
	Voice				24.6	13.9	11.6
[100],2021	VoIP (3DES, MD5)	3 sites	OPNET modeler	0.38930 s	1000	140	860.6
The proposed system	Local Host(With)-Text	9 sites	OPNET modeler	5 m	33,412	24,139	9,273
	Local Host(Without)-Text (RSA, chaotic, SHA2, Hiding)			5 m	30,324	27,227	3,097

Chapter Five

Conclusions and Suggestions for Future Works

5.1 Conclusions

This chapter explains the proposed system conclusions and the main suggestions for future works, they can be summarized as :

1- The data hides in Extension headers without discovering the data traffic. The complicity of the used algorithms increase randomness of identity, which leads to decrease the network performance.
2- The problems faced are increasing network traffic due to DoS attack and the system tested with two case studies as with DoS and without DoS.
3- Generating IPv6 address is authenticated and it is passed to the chaotic as logistic map function, and then passed to RSA function and SHA 2.
4- The proposed system provides the best randomness of experiment 8 is 34 Fail, and Safe is 114 value and it hides identity of source IPv6 address and encrypt packets, which it adds a challenge to attacker to deals with as well as, it provides secure data communications.
5- The proposed system showed better computation memory in case of without Dos attack and it evaluated with lost packet, average events, memory and time, as follow: the total memory is 35,523 KB, average events/sec is 250,52 events/sec, traffic sent is 30,324 Packets/s, traffic received is 27,227 Packets/s, and lose packets is 3,097 Packets/s.

5.2 Suggestions for Future Works

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

1- Simulating different networks attacks and how malicious user effect on network performance, and configure network to work in real IPv6 addressing with computer based system not in simulation state.

2- Emerging DDoS attack detection and mitigation strategies in IPv6 network environment.
3- Building a mechanism for multi-path concurrent transmission at the network layer based on the Identity Protocol (IDP) stack.
4- Implementing the proposed system with dynamic address assignment.

REFERENCES

[1] Li, S., Yi, Y., & Zhu, K. (2021, December). Implementation and scheme of IPv4 to IPv6 Transition in enterprise network architecture. In *2021 IEEE 2nd International Conference on Information Technology, Big Data and Artificial Intelligence (ICIBA)* (Vol. 2, pp. 457-461). IEEE.

[2] Cai, Y. W., & Shen, X. Y. (2021). International communication system of acupuncture-moxibustion based on OSI model. *Zhongguo Zhen jiu= Chinese Acupuncture & Moxibustion*, *41*(6), 677-681.

[3] Taylor, J. T., & Taylor, W. T. (2021). Software architecture. In *Patterns in the Machine* (pp. 63-82). Apress, Berkeley, CA.

[4] Romaniuk, A. V., Romaniuk, V. A., Sparavalo, M. K., Lysenko, O. I., & Zhuk, O. V. (2020). Synthesis of data collection methods by telecommunication airplatforms in wireless sensors networks.

[5] Tan, S., Wu, Y., Xie, P., Guerrero, J. M., Vasquez, J. C., & Abusorrah, A. (2020). New challenges in the design of microgrid systems: Communication networks, cyberattacks, and resilience. *IEEE Electrification Magazine*, *8*(4), 98-106.

[6] Mahmood, S., Mohsin, S. M., & Akber, S. M. A. (2020, January). Network Security Issues of Data Link Layer: An Overview. In *2020 3rd International Conference on Computing, Mathematics and Engineering Technologies (iCoMET)* (pp. 1-6). IEEE.

[7] Xia, Y., Su, J., Chen, R., & Huang, X. (2020). APGS: An Efficient Source-Accountable and Metadata-Private Protocol in the Network Layer. *IEEE Transactions on Information Forensics and Security*, *16*, 1245-1260.

[8] Badshah, F., Shah, S. T. U., Jan, S. R., & Rahman, I. U. (2017, March). Communication between multiple processes on same device using TCP/IP suite. In *2017 International Conference on Communication, Computing and Digital Systems (C-CODE)* (pp. 148-151). IEEE.

[9] Ali, A. N. A. (2012). Comparison study between IPV4 & IPV6. *International Journal of Computer Science Issues (IJCSI)*, *9*(3), 314.

[10] Badshah, F., Shah, S. T. U., Jan, S. R., & Rahman, I. U. (2017, March). Communication between multiple processes on same device using TCP/IP suite.

In *2017 International Conference on Communication, Computing and Digital Systems (C-CODE)* (pp. 148-151). IEEE.

[11] Khan, I. U., & Hassan, M. (2016). Transport layer protocols and services. *International Journal of Research in Computer and Communication Technology*, *5*, 2320-5156.

[12] Chao-Yang, Z. (2011, August). DOS attack analysis and study of new measures to prevent. In *2011 International Conference on Intelligence Science and Information Engineering* (pp. 426-429). IEEE.

[13] Ali, A. N. A. (2012). Comparison study between IPV4 & IPV6. *International Journal of Computer Science Issues (IJCSI)*, *9*(3), 314.

[14] Hu, G., Chen, W., Li, Q., Jiang, Y., & Xu, K. (2017). TrueID: A practical solution to enhance Internet accountability by assigning packets with creditable user identity code. Future Generation Computer Systems, 72, 219-226.

[15] Cabaj, K., Caviglione, L., Mazurczyk, W., Wendzel, S., Woodward, A., & Zander, S. (2018). The new threats of information hiding: The road ahead. IT professional, 20(3), 31-39.

[16] Rahman, M. M., Rahman, M. M., Reza, S. I., Sarker, S., & Islam, M. M. (2019). Proposed an Algorithm for Preventing IP Spoofing DoS Attack on Neighbor Discovery Protocol of IPv6 in Link Local Network. *European Journal of Engineering and Technology Research*, *4*(12), 65-70.

[17] Fahrnberger, G. (2019). Editing encrypted messages without decrypting nor understanding them (Doctoral dissertation, University of Hagen, Germany).

[18] Pachghare, V. K. (2019). Cryptography and information security. PHI Learning Pvt. Ltd.

[19] Hossen, M. S., Islam, M. A., Khatun, T., Hossain, S., & Rahman, M. M. (2020, September). A New Approach to Hiding Data in the Images Using Steganography Techniques Based on AES and RC5 Algorithm Cryptosystem. In *2020 International Conference on Smart Electronics and Communication (ICOSEC)* (pp. 676-681). IEEE.

[20] Mavani, M., & Asawa, K. (2020). Resilient against spoofing in 6LoWPAN networks by temporary-private IPv6 addresses. *Peer-to-Peer Networking and Applications*, *13*(1), 333-347.

[21] Čerňanský, M., Huraj, L., & Šimon, M. (2020). Controlled DDoS Attack on IPv4/IPv6 Network Using Distributed Computing Infrastructure. *Journal of Information and Organizational Sciences*, *44*(2), 297-316.

[22] Zhou, M., Wang, P., & Ding, Z. (2021). A Two-Layer IP Hopping-Based Moving Target Defense Approach to Enhancing the Security of Mobile Ad-Hoc Networks. *Sensors*, *21*(7), 2355.

[23] Zebari, D. A., Zeebaree, D. Q., Saeed, J. N., Zebari, N. A., & Adel, A. Z. (2020). Image steganography based on swarm intelligence algorithms: A survey. *people*, *7*(8), 9.

[24] Caviglione, L., Schaffhauser, A., Zuppelli, M., & Mazurczyk, W. (2022). IPv6CC: IPv6 covert channels for testing networks against stegomalware and data exfiltration. *SoftwareX*, *17*, 100975.

[25] Chebrolu, K., Raman, B., & Rao, R. R. (2005). A network layer approach to enable TCP over multiple interfaces. *Wireless Networks*, *11*(5), 637-650.

[26] Hill, G. R., Chidgey, P. J., Kaufhold, F., Lynch, T., Sahlen, O., Gustavsson, M., ... & Herrmann, H. (1993). A transport network layer based on optical network elements. *Journal of lightwave technology*, *11*(5/6), 667-679.

[27] Bhagwat, P., Perkins, C., & Tripathi, S. (1996). Network layer mobility: an architecture and survey. *IEEE Personal Communications*, *3*(3), 54-64.

[28] Neudecker, T., & Hartenstein, H. (2018). Network layer aspects of permissionless blockchains. *IEEE Communications Surveys & Tutorials*, *21*(1), 838-857.

[29] Bhagwat, P., Perkins, C., & Tripathi, S. (1996). Network layer mobility: an architecture and survey. *IEEE Personal Communications*, *3*(3), 54-64.

[30] Hill, G. R., Chidgey, P. J., Kaufhold, F., Lynch, T., Sahlen, O., Gustavsson, M., ... & Herrmann, H. (1993). A transport network layer based on optical network elements. *Journal of lightwave technology*, *11*(5/6), 667-679.

[31] Chebrolu, K., Raman, B., & Rao, R. R. (2005). A network layer approach to enable TCP over multiple interfaces. *Wireless Networks*, *11*(5), 637-650.

[32] Ford, M., Boucadair, M., Durand, A., Levis, P., & Roberts, P. (2011). Issues with IP address sharing. *IETF Request for Comment*, *6269*.

[33] Mohsin, M., & Prakash, R. (2002, October). IP address assignment in a mobile ad hoc network. In *MILCOM 2002. Proceedings* (Vol. 2, pp. 856-861). IEEE.

[34] Ashraf, S., Muhammad, D., & Aslam, Z. (2020). Analyzing challenging aspects of IPv6 over IPv4. *J. Ilm. Tek. Elektro Komput. Dan Inform*, *6*(1), 54-67.

[35] Beeharry, J., & Nowbutsing, B. (2016, August). Forecasting IPv4 exhaustion and IPv6 migration. In *2016 ieee international conference on emerging technologies and innovative business practices for the transformation of societies (emergitech)* (pp. 336-340). IEEE.

[36] Kumar, O. K., Chowdary, Y. J., Teja, P. V., Blessington, T. P., & Ravi, T. IPv6–the next generation Internet Protocol, International Journal of Engineering Research and Applications (IJERA), ISSN: 2248-9622 , Vol. 2, Issue 6, November- December 2012, pp.033-038.

[37] Colitti, L., Gunderson, S. H., Kline, E., & Refice, T. (2010, April). Evaluating IPv6 adoption in the Internet. In *International Conference on Passive and Active Network Measurement* (pp. 141-150). Springer, Berlin, Heidelberg.

[38] Moravejosharieh, A., Modares, H., & Salleh, R. (2012, February). Overview of mobile IPv6 security. In *2012 Third International Conference on Intelligent Systems Modelling and Simulation* (pp. 584-587). IEEE.

[39] Perkins, C. E. (1997). Mobile ip. *IEEE communications Magazine*, *35*(5), 84-99.

[40] Min, C. (2011, July). Research on network security based on IPv6 architecture. In *Proceedings of 2011 International Conference on Electronics and Optoelectronics* (Vol. 1, pp. V1-415). IEEE.

[41] Granjal, J., Monteiro, E., & Silva, J. S. S. (2010, December). Enabling network-layer security on IPv6 wireless sensor networks. In *2010 IEEE Global Telecommunications Conference GLOBECOM 2010* (pp. 1-6). IEEE.

[42] Carpenter, B., & Jiang, S. (2013). Transmission and Processing of IPv6 Extension Headers. *IETF Request for Comments*, *7045*.

[43] Montenegro, G., Kushalnagar, N., Hui, J., & Culler, D. (2007). Transmission of IPv6 packets over IEEE 802.15. 4 networks. *Internet proposed standard RFC*, *4944*, 130.

[44] Zagar, D., & Grgic, K. (2006, July). IPv6 security threats and possible solutions. In *2006 World Automation Congress* (pp. 1-7). IEEE.

[45] Askarov, A., & Myers, A. (2011). Attacker control and impact for confidentiality and integrity. *arXiv preprint arXiv:1107.5594*.

[46] Dunlop, M., Groat, S., Urbanski, W., Marchany, R., & Tront, J. (2011, November). Mt6d: A moving target ipv6 defense. In *2011-MILCOM 2011 Military Communications Conference* (pp. 1321-1326). IEEE.

[47] Kim, H. S., Ko, J., Culler, D. E., & Paek, J. (2017). Challenging the IPv6 routing protocol for low-power and lossy networks (RPL): A survey. *IEEE Communications Surveys & Tutorials*, *19*(4), 2502-2525.

[48] Perez-Costa, X., Torrent-Moreno, M., & Hartenstein, H. (2003). A performance comparison of mobile IPv6, hierarchical mobile IPv6, fast handovers for mobile IPv6 and their combination. *ACM SIGMOBILE Mobile Computing and Communications Review*, *7*(4), 5-19.

[49] Bulbul, H. I., Batmaz, I., & Ozel, M. (2008, January). Wireless network security: Comparison of wep (wired equivalent privacy) mechanism, wpa (wi-fi protected access) and rsn (robust security network) security protocols. In *Proceedings of the 1st international conference on Forensic applications and techniques in telecommunications, information, and multimedia and workshop* (pp. 1-6).

[50] Sakib, M., & Singh, J. (2020). Simulation based performance analysis of IPSec VPN over IPv6 networks. *International Journal of Electronics Engineering*, *12*(2), 92-104.

[51] Fielding, R., & Reschke, J. (2013). Hypertext transfer protocol (http/1.1): Authentication. *draft-ietf-httpbis-p7-auth-24 (work in progress)*.

[52] Malik, R., & Syal, R. (2010). Performance analysis of ip security vpn. *International Journal of Computer Applications*, *8*(4), 0975.

[53] Lopez-Millan, G., Marin-Lopez, R., & Pereniguez-Garcia, F. (2019). Towards a standard SDN-based IPsec management framework. *Computer Standards & Interfaces*, *66*, 103357.

[54] Spyropoulou, E., Agar, C., Levin, T., & Irvine, C. (2003). *IPsec modulation for quality of security service*. NAVAL POSTGRADUATE SCHOOL MONTEREY CA DEPT OF COMPUTER SCIENCE.

[55] Younglove, R. W. (2001). IP security: what makes it work?. *Computing & Control Engineering Journal*, *12*(1), 44-46.

[56] Singh, S. P., Bharti, V., Singh, B. K., Johri, P., & Sharma, M. (2016, April). Formation of security association database (SAD) in internet protocol version 6 (IPv6). In *2016 International Conference on Computing, Communication and Automation (ICCCA)* (pp. 491-497). IEEE.

[57] Bonelli, N., Giordano, S., Lucetti, S., Risi, G., & Tomasi, A. (2005, January). Automatic IPSec Security Association Negotiation in Mobile-Oriented IPv6 Networks. In *2005 Symposium on Applications and the Internet Workshops (SAINT 2005 Workshops)* (pp. 14-17). IEEE.

[58] Baltatu, M., Lioy, A., & Mazzicchi, D. (2000, September). Security policy system: status and perspective. In *Proceedings IEEE International Conference on Networks 2000 (ICON 2000). Networking Trends and Challenges in the New Millennium* (pp. 278-284). IEEE.

[59] Wang, Y., Vangury, K., & Nikolai, J. (2014, May). MobileGuardian: A security policy enforcement framework for mobile devices. In *2014 International Conference on Collaboration Technologies and Systems (CTS)* (pp. 197-202). IEEE.

[60] Manral, V. (2007). *Cryptographic algorithm implementation requirements for encapsulating security payload (esp) and authentication header (ah)*. RFC 4835, April.

[61] Sengar, H., Wijesekera, D., & Jajodia, S. (2005, April). Authentication and integrity in telecommunication signaling network. In *12th IEEE International Conference and Workshops on the Engineering of Computer-Based Systems (ECBS'05)* (pp. 163-170). IEEE.

[62] Oppliger, R. (1998). Security at the Internet layer. *Computer*, *31*(9), 43-47.

[63] Singh, K. K. V., & Gupta, H. (2016, March). A New Approach for the Security of VPN. In *Proceedings of the Second International conference on Information and Communication Technology for Competitive Strategies* (pp. 1-5).

[64] Khari, M., Garg, A. K., Gandomi, A. H., Gupta, R., Patan, R., & Balusamy, B. (2019). Securing data in Internet of Things (IoT) using cryptography and steganography techniques. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, *50*(1), 73-80.

[65] Schneier, B. (2015). *Secrets and lies: digital security in a networked world*. John Wiley & Sons.

[66] Farooq, H. (2017). A Review on cloud computing security using authentication techniques. *International Journal of Advanced Research in Computer Science*, *8*(2).

[67] Li, C. T., & Hwang, M. S. (2010). An efficient biometrics-based remote user authentication scheme using smart cards. *Journal of Network and computer applications*, *33*(1), 1-5.

[68] Kansal, S., & Mittal, M. (2014, December). Performance evaluation of various symmetric encryption algorithms. In *2014 international conference on parallel, distributed and grid computing* (pp. 105-109). IEEE.

[69] Abd Elminaam, D. S., Abdual-Kader, H. M., & Hadhoud, M. M. (2010). Evaluating The Performance of Symmetric Encryption Algorithms. *Int. J. Netw. Secur.*, *10*(3), 216-222.

[70] Sachin, M., & Kumar, D. (2010). Implementation and Analysis of AES, DES and Triple DES on GSM Network. *IJCSNS International Journal of Computer Science and Network Security*, *10*, 298-303.

[71] Robshaw, M., & Billet, O. (Eds.). (2008). *New stream cipher designs: the eSTREAM finalists* (Vol. 4986). Springer.

[72] Farah, S., Javed, Y., Shamim, A., & Nawaz, T. (2012, December). An experimental study on performance evaluation of asymmetric encryption algorithms. In *Recent Advances in Information Science, Proceeding of the 3rd European Conf. of Computer Science,(EECS-12)* (pp. 121-124).

[73] Agoyi, M., & Seral, D. (2010, September). SMS security: An asymmetric encryption approach. In *2010 6th International Conference on Wireless and Mobile Communications* (pp. 448-452). IEEE.

[74] Sallee, P. (2003, October). Model-based steganography. In *International workshop on digital watermarking* (pp. 154-167). Springer, Berlin, Heidelberg.

[75] Chaves, R., Kuzmanov, G., Sousa, L., & Vassiliadis, S. (2006, October). Improving SHA-2 hardware implementations. In *International Workshop on Cryptographic Hardware and Embedded Systems* (pp. 298-310). Springer, Berlin, Heidelberg.

[76] McEvoy, R. P., Crowe, F. M., Murphy, C. C., & Marnane, W. P. (2006, March). Optimisation of the SHA-2 family of hash functions on FPGAs. In *IEEE Computer Society Annual Symposium on Emerging VLSI Technologies and Architectures (ISVLSI'06)* (pp. 6-pp). IEEE.

[77] Roshdy, R., Fouad, M., & Aboul-Dahab, M. (2013). Design and implementation a new security hash algorithm based on MD5 and SHA-256. *International Journal of Engineering Sciences & Emerging Technologies*, *6*(1), 29-36.

[78] McEvoy, R. P., Crowe, F. M., Murphy, C. C., & Marnane, W. P. (2006, March). Optimisation of the SHA-2 family of hash functions on FPGAs. In *IEEE Computer Society Annual Symposium on Emerging VLSI Technologies and Architectures (ISVLSI'06)* (pp. 6-pp). IEEE.

[79] Glabb, R., Imbert, L., Jullien, G., Tisserand, A., & Veyrat-Charvillon, N. (2007). Multi-mode operator for SHA-2 hash functions. *journal of systems architecture*, *53*(2-3), 127-138.

[80] Chaves, R., Kuzmanov, G., Sousa, L., & Vassiliadis, S. (2006, October). Improving SHA-2 hardware implementations. In *International Workshop on Cryptographic Hardware and Embedded Systems* (pp. 298-310). Springer, Berlin, Heidelberg.

[81] Juliato, M., Gebotys, C., & Elbaz, R. (2009, March). Efficient fault tolerant SHA-2 hash functions for space applications. In *2009 IEEE Aerospace conference* (pp. 1-16). IEEE.

[82] Makris, G., & Antoniou, I. (2012, June). Cryptography with chaos. In *Proceedings of the 5th Chaotic Modeling and Simulation International Conference, Athens, Greece* (pp. 12-15).

[81] Ye, G., & Wong, K. W. (2012). An efficient chaotic image encryption algorithm based on a generalized Arnold map. *Nonlinear dynamics*, *69*(4), 2079-2087.

[82] Chen, C. K., & Lin, C. L. (2010, June). Text encryption using ECG signals with chaotic Logistic map. In *2010 5th IEEE Conference on Industrial Electronics and Applications* (pp. 1741-1746). IEEE.

[83] Dinu, D., Biryukov, A., Großschädl, J., Khovratovich, D., Le Corre, Y., & Perrin, L. (2015, July). Felics–fair evaluation of lightweight cryptographic systems. In *NIST Workshop on Lightweight Cryptography* (Vol. 128).

[84] Shah, A., & Engineer, M. (2019). A survey of lightweight cryptographic algorithms for iot-based applications. In *Smart innovations in communication and computational sciences* (pp. 283-293). Springer, Singapore.

[85] Sallam, S., & Beheshti, B. D. (2018, October). A survey on lightweight cryptographic algorithms. In *TENCON 2018-2018 IEEE Region 10 Conference* (pp. 1784-1789). IEEE.

[86] Bogdanov, A., Knezevic, M., Leander, G., Toz, D., Varici, K., & Verbauwhede, I. (2012). Spongent: The design space of lightweight cryptographic hashing. *IEEE Transactions on Computers*, *62*(10), 2041-2053.

[87] Hussain, M., & Hussain, M. (2013). A survey of image steganography techniques.

[88] Kour, J., & Verma, D. (2014). Steganography techniques–A review paper. *International Journal of Emerging Research in Management & Technology*, *3*(5), 132-135.

[89] Kaur, S., Bansal, S., & Bansal, R. K. (2014, March). Steganography and classification of image steganography techniques. In *2014 International Conference on Computing for Sustainable Global Development (INDIACom)* (pp. 870-875). IEEE.

[90] Fridrich, J. (2009). *Steganography in digital media: principles, algorithms, and applications*. Cambridge University Press.

[91] Ibrahim, H. H., Hamzah, A. E., Saeed, H. A., Qasim, H. H., Hamed, O. S., Alkhalaf, H. Y., & Hamza, M. I. (2020). A comprehensive study of distributed Denial-of-Service attack with the detection techniques. *International Journal of Electrical and Computer Engineering (IJECE)*, *10*(4), 3685-3694.

[92] Basyoni, L., Fetais, N., Erbad, A., Mohamed, A., & Guizani, M. (2020, February). Traffic analysis attacks on Tor: a survey. In *2020 IEEE International*

Conference on Informatics, IoT, and Enabling Technologies (ICIoT) (pp. 183-188). IEEE.

[93] LeMay, E., Ford, M. D., Keefe, K., Sanders, W. H., & Muehrcke, C. (2011, September). Model-based security metrics using adversary view security evaluation (advise). In *2011 Eighth International Conference on Quantitative Evaluation of SysTems* (pp. 191-200). IEEE.

[94] Chang, X. (1999, December). Network simulations with OPNET. In *WSC'99. 1999 Winter Simulation Conference Proceedings.'Simulation-A Bridge to the Future'(Cat. No. 99CH37038)* (Vol. 1, pp. 307-314). IEEE.

[95] Menon, V., & Trefethen, A. E. (1997, November). MultiMATLAB: Integrating MATLAB with high-performance parallel computing. In *Proceedings of the 1997 ACM/IEEE Conference on Supercomputing* (pp. 1-18).

[96] Bracha, G., & Ungar, D. (2004). Mirrors: design principles for meta-level facilities of object-oriented programming languages. *ACM SIGPLAN Notices*, *39*(10), 331-344.

[97] Berger, E. D., & Zorn, B. G. (2006). DieHard: Probabilistic memory safety for unsafe languages. *Acm sigplan notices*, *41*(6), 158-168.

[98] Hadi, T. H. (2020). How to Export/Import Dynamic Routing Protocols with Failure Recovery?. *memory*, *6*(12), 16.

[99] Jain, N., & Payal, A. (2020). Performance Evaluation of IPv6 Network for Real-Time Applications using IS-ISv6 Routing Protocol on Riverbed Modeler. *Procedia Computer Science*, *173*, 46-55.

[100] Alausa, O. A., Arekete, S. A., Odim, M. O., Oguntunde, A. O., & Ogunde, A. O. (2021).VoIP Codec Performance Evaluation on GRE with IPsec over IPv4 and IPv6.

الخلاصة

مؤخرا، أصبح أمن المعلومات مسألة مهمة في الحياة الرقمية. وقد يؤدي استحداث تكنولوجيا جديدة لنقل البيانات إلى إنفاذ استراتيجيات معينة تستخدم في آليات توفير الأمن. لحالات معينة من حالات اتصال البيانات. يتطلب أمن الشبكة اهتماما يوميا نتيجة لحجم البيانات التي يتم نقلها عبر الشبكة. ويوفر كل من التشفير وتقنيات الاخفاء تكنولوجيات حاسمة لضمان امن البيانات.

IPv6 يوفر خدمات التحديد و اثبات الموقع للعديد من اجهزة الحاسوب عبر الشبكة وكذلك عمليات توجيه الحزم عبر الانترنت. ويستند النظام المقترح على حماية هوية حزمة IPV6 من هجوم حجب او منع الخدمة DoS ، وتعتمد الطرق المقترحة على استخدام التشفير والاخفاء. يستخدم الاتصال الموثوق الجانب الأمني في العديد من الحالات ، لا سيما في تطبيقات الشبكات التي تستند على بروتوكول الانترنت IPv6. وهناك مشاكل شائعة مثل هجمات حجب الخدمة ، والخداع لبروتوكول الانترنت IP وأنواع أخرى من الهجمات السلبية الشائعة.

وتقترح الطريقة المستخدمة نهجاً يقوم على توليد هويات فريدة عشوائياً لكل جهاز في الشبكة .ان الهوية التي يتم توليدها تشفر ثم يتم اخفاءها داخل الحزمة المرسلة حيث يتم التحقق منها من قبل المستلم والتأكد من مصدرها قبل ان يتم معالجتها ضمن هذه العقدة المستلمة. وخلال هذا العمل يستند على تنفيذ تسع تجارب تستخدم لاختبار الطريقة المقترحة على أساس إنشاء عنوان IPv6 ، ثم الانتقال إلى Logistic Map ثم خوارزمية RSA ومن ثم خوارزمية SHA2. وتظهر النتائج أن النظام المقترح يولد هوية عشوائية عالية لكل عقدة ويخفي هوية العقدة داخل الحزمة. وبالإضافة إلى ذلك ، تمت محاكاة أداء الشبكة للنظام المقترح باستخدام المحاكي OPNET.

كما وأظهرت النتائج أن دراسة الحالة بدون هجوم حجب الخدمة تولد عدد حزم 30324 حزمة بالثانية لحركة المرور المرسلة ، 27227 حزمة بالثانية لحركة المرور المستلمة ، وفقدان الحزم 3097 حزمة بالثانية. وبالإضافة إلى ذلك ، فإن دراسة الحالة مع هجوم DoS عند إرسال حركة المرور تولد حزم 33412 حزمة بالثانية ، وحركة المرور المستلمة 24139 حزمة بالثانية ، وفقدان الحزم 9273 حزمة بالثانية.

جمهورية العراق
وزارة التعليم العالي والبحث العلمي
جامعة بابل
علوم البنات
قسم علوم الحاسبات

حماية الهوية لحزمة بروتوكولIPv6

ضد هجماتDoS بإستخدام تقنيات التشفير والاخفاء

رسالة مقدمة

إلى مجلس كلية علوم البنات في جامعة بابل والتي هي جزء من متطلبات

الحصول على درجة الماجستير في العلوم / علوم الحاسبات

من قبل الطالب

ميثم حاكم علي

(جامعة بابل ، كلية علوم البنات قسم الحاسبات ، 2022)

باشراف

أ.م.د سيف محمود خلف العلاق

هـ 1443 م 2022