Protecting Integrity and Confidentiality of Network Traffic with Media Access Control Security (MACsec)

by

Zain Ul Abdin
B.Sc., University of Sindh, Pakistan, 2015

A Report Submitted in Partial Fulfillment of the Requirements for the Degree of

MASTER OF ENGINEERING

in the Department of Electrical and Computer Engineering

Protecting Integrity and Confidentiality of Network Traffic with Media Access Control Security (MACsec)

by

Zain Ul Abdin
B.Sc., University of Sindh, Pakistan, 2015

Supervisory Committee

Dr. T. Aaron Gulliver, Supervisor
(Department of Electrical and Computer Engineering)

Dr. Mihai Sima, Departmental Member
(Department of Electrical and Computer Engineering)

ABSTRACT

Networks have increasingly become subject to sophisticated attacks to either interrupt network services in the form of Denial of Service (DoS) attacks or to steal information in the form of Man-in-the-Middle (MITM) attacks. According to the IBM X-Force Threat Intelligence 2018 index, 35% of exploitation activities involved MITM attacks [4]. To prevent networks from attacks such as MITM and to protect data integrity and confidentiality, a security solution is required to provide seamless layer 2 encryption in Local Area Networks (LANs) and Wide Area Networks (WANs).

Media Access Control Security (MACsec) secures an Ethernet link for traffic including Dynamic Host Configuration Protocol (DHCP), Address Resolution Protocol (ARP), and other protocols that are not typically secured by other security solutions such as Internet Protocol Security (IPsec) which operates at layer 3 or Secure Socket Layer (SSL) which protects layer 7 of the Open System Interconnection (OSI) model. In this work, MACsec is implemented to secure LANs and WANs. Network performance analysis is performed to evaluate the impact of MACsec on network performance. MACsec is also used to protect networks against MITM attacks. Results are presented which show that MACsec successfully protects networks from MITM attacks and provides end-to-end encryption to protect network traffic.

Contents

List of Tables

List of Figures

Glossary

AN ..... Association Number

ARP ..... Address Resolution Protocol

CA ..... Connectivity Association

CAK ..... Connectivity Association Key

CKN ..... Connectivity Association Key Name

DHCP ..... Dynamic Host Configuration Protocol

DOS ..... Denial of Service

GNS3 ..... Graphical Network Simulator 3

HTTPS ..... Hypertext Transfer Protocol Secure

ICMP ..... Internet Control Message Protocol

ICV ..... Integrity Check Value

IPSec ..... Internet Protocol Security

ISP ..... Internet Service Provider

LAN ..... Local Area Network

MAC ..... Media Access Control

MACsec ..... Media Access Control Security

MITM ..... Man-in-the-Middle

MKA ..... MACsec Key Agreement Protocol

MPLS ..... Multiprotocol Label Switching

MSDU ..... MAC Service Data Unit

OSI ..... Open System Interconnection

OVS ..... Open vSwitch

PN ..... Packet Number

PSK ..... Pre-shared Key

QoS ..... Quality of Service

RTT ..... Round Trip Time

SAK ..... Secure Association Key

SCI ..... Secure Channel Identifier

SDN ..... Software Defined Network

SECTAG ..... Security TAG

SL ..... Short Length

SSL ..... Secure Socket Layer

TCI ..... Tag Control Information

VLAN ..... Virtual Local Area Network

VMs ..... Virtual Machines

VPN ..... Virtual Private Network

VXLAN ..... Virtual Extensible LAN

WAN ..... Wide Area Network

ACKNOWLEDGEMENTS

I would like to thank:

My Parents, for supporting me in the low moments.

Dr. T. Aaron Gulliver, for mentoring, support, encouragement, and patience.

My Siblings, for their love and motivation.

"A Journey of a thousand miles begins with a single step."
Laozi

DEDICATION

This work is dedicated to my parents for their endless love, support, and encouragement. Thank you for teaching me to believe in myself, and in my dreams.

Chapter 1

Introduction

The internet has become central to the global information and communication infrastructure. It links 1.8 billion people around the world to exchange ideas and services. The internet provides a platform for growth and innovation in sectors and services such as manufacturing, energy, transportation, public safety, healthcare, and finance [1]. As a consequence, securing networks has become a top priority for corporations and governments around the world [2].

Networks have increasingly become the subject of sophisticated attacks to either interrupt network services in the form of Denial of Service (DoS) attacks or to steal electronic information via Man-in-the-Middle (MITM) attacks. Therefore, it is important for organizations to have an appropriate security architecture in place to protect networks from threats and to protect the integrity of the electronic data shared on a network. An MITM attack targets information shared in a network and poses a great threat to data privacy. An MITM attacker intercepts communication between two hosts in a network to secretly eavesdrop or modify their traffic. A successful MITM attack can also be used to initiate a Distributed Denial of Service (DDoS) attack using hosts as bots by installing malicious code on them [19]. An MITM attack is typically carried out by spoofing the hardware address which is commonly known as the Media Access Control (MAC) address.

According to Netcraft, 95% of the Hypertext Transfer Protocol Secure (HTTPS) servers in 2016 were vulnerable to MITM attacks [3]. IBM reported that 35% of the exploitation activities in 2018 involved attackers attempting these attacks [4]. Figure 1.1 gives the percentage of each exploitation type in 2018. This shows that MITM attacks were the second highest form of attack. Media Access Control Security (MACsec) is an IEEE 802.1AE security standard that provides secure communications for traffic on Ethernet links. MACsec provides point-to-point and point-to-multipoint security between hosts connected in a network to secure traffic and can identify and prevent most security threats

[5]. MACsec can also be used to encrypt traffic on Ethernet links so it is a solution for most of the security challenges organizations face [5]. MACsec will be discussed in detail in Chapter 2.

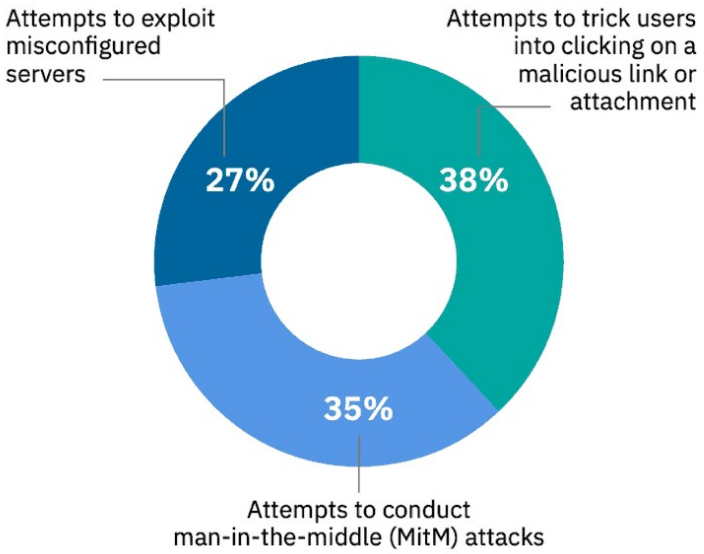

Figure 1.1: Percentage of different types of exploitations in 2018 [4].

1.1 Problem Statement

In the current networking world, organizations no longer operate on a single platform and are required to engage with multiple service providers, cloud infrastructure, and large enterprise networks. This makes network traffic vulnerable to data tampering in the form of attacks such as DOS, network intrusion, MITM, masquerading, passive wire-tapping, and replay/playback. To prevent such malicious and damaging attacks, a security solution is required to provide seamless layer 2 encryption in LANs and WANs. This will allow network traffic to safely move across service providers networks, cloud infrastructure, and enterprise networks.

MACsec is an efficient security solution that is intended to secure network traffic. It can be used to secure Ethernet links for traffic including Dynamic Host Configuration Protocol (DHCP), Address Resolution Protocol (ARP), and other protocols that are not typically secured by other security solutions such as IPsec which operates on layer 3 and SSL which protects layer 7.

The goal of this work is to implement MACsec to investigate the features and capa-

bilities of MACsec to secure LANs and WANs. MACsec is also used to protect networks against MITM attacks. Network performance is measured with and without MACsec to determine if MACsec reduces network performance.

1.2 Related Work

MACsec has been used to secure cloud networks such as communications between a Virtual Extensible LAN (VXLAN) and Virtual Machines (VMs) to safely exchange traffic across network cloud platforms [6]. MACsec has been implemented in a layer 2 Virtual Private Network (VPN) over a Multiprotocol Label Switching (MPLS) network between two sites [7]. MACsec was used between two premises connected via Open vSwitches (OVS) in a Software Defined Networking (SDN) environment. Network throughput was measured, and normal traffic, which is the traffic on a network without MACsec, was found to have a higher throughput than MACsec traffic [8].

MACsec over a WAN was implemented in [9] for traffic between two remote sites connected via a layer 2 tunneling protocol called Generic Routing Encapsulation (GRE). It was found that the network throughput was greater for normal traffic as compared to MACsec protected traffic. MACsec was proposed in [10] to protect network links between P4 switches in a Software Defined Network (SDN). Network performance in terms of throughput and Round Trip Time (RTT) was presented. The results obtained show higher throughput and lower RTT when MACsec is not used between switches. In addition, better network throughput and RTT were observed when MACsec was configured without encryption as compared to MACsec with encryption.

1.3 Report Organization

This report is organized as follows.

Chapter 1 introduced and provided an overview of the work. The problem statement and motivation were also presented. The related work was briefly discussed, and the organization of this report was given.

Chapter 2 provides an overview of MACsec. MACsec terminology, benefits, and configuration attributes are also discussed.

Chapter 3 presents the design and implementation of LANs and WANs. It also provides details of the tools and utilities used along with their use cases, technical specifications, and configuration parameters. The metrics used to evaluate network performance are also discussed.

Chapter 4 presents the results and discussion of securing LANs and WANs using MACsec. The performance of normal and MACsec protected networks is compared. The results of protecting networks from MITM attacks using MACsec are also discussed.

Chapter 5 concludes the report and provides suggestions for future work.

Chapter 2

Media Access Control Security (MACsec)

Media Access Control Security (MACsec) as defined in the IEEE 802.1AE standard is a layer 2 security protocol intended to secure communications on Ethernet links. MACsec provides point-to-point and point-to-multipoint security on links between connected hosts at layer 2. It provides secure access to the network by ensuring data integrity and authentication. It also provides an option to encrypt traffic between hosts. MACsec can identify and prevent most security threats including DOS, intrusion, MITM, masquerading, passive wiretapping, and playback attacks. MACsec establishes a secure link after security keys are exchanged and verified between hosts at the ends of the link. These keys can be configured manually or generated dynamically depending on the security mode used in MACsec [5].

2.1 Overview of MACsec

To ensure data integrity, MACsec appends a 16 byte Security TAG (SecTAG) and a 16 byte Integrity Check Value (ICV) to all frames on the MACsec secured link. The header and tail are checked by the receiving interface to ensure that the data was not compromised while traversing the link. The frames are dropped if a data integrity check detects anything irregular about the traffic. Furthermore, MACsec encryption ensures that the data in an Ethernet frame cannot be viewed by anybody monitoring traffic on the link. As mentioned earlier, MACsec encryption is optional and user configurable. It is possible to enable MACsec data integrity checks while still sending unencrypted data over the MACsec secured link. The MACsec frame format is similar to a standard Ethernet frame

format except that it includes an additional 32 bytes (SecTAG and ICV) [5]. Figure 2.1 shows the standard Ethernet frame format which comprises the source MAC address, destination MAC address, VLAN tag, EtherType, payload, and CRC fields.

Figure 2.1: Standard Ethernet frame format [11].

Figure 2.2 shows the MACsec frame format which includes fields such as source MAC address, destination MAC address, and a 16 byte 802.1AE header (SecTAG). A MACsec SecTAG contains an EtherType to allow MACsec frames to be distinguished from other frames. The SecTAG also contains an Association Number (AN) and Tag Control Information (TCI) to identify secure association and designate the MACsec version number. A Secure Channel Identifier (SCI) is used in a MACsec SecTAG to identify secure association by combining the MAC address and port number. The SecTAG also includes Short Length (SL) to set the length of the encrypted data and Packet Number (PN) for replay attack protection. A MACsec frame also include a 16 byte ICV to ensure the integrity of the data.

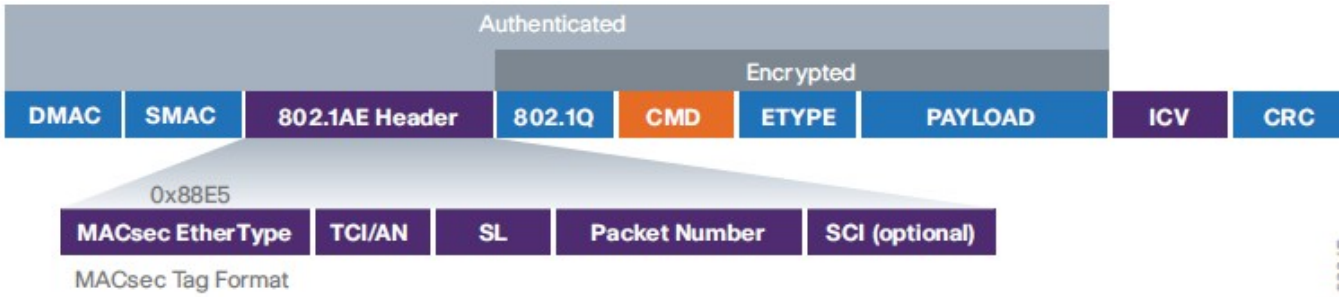

Figure 2.2: MACsec protected Ethernet frame format [12].

2.2 Terminology and Functions

The MACsec terminology with the descriptions for MACsec session establishment are given below [13].

MACsec Key Agreement Protocol (MKA) is the key agreement protocol for discovering MACsec peers and negotiating keys between MACsec peers.

Connectivity Associations (CA) refers to the security relationship between MACsec capable devices. Endpoints that share a Connectivity Association Key (CAK) are part of the same Connectivity Association (CA). There can be more than two endpoints in a CA based on the support enabled by the vendor.

Connectivity Association Key (CAK) refers to the key used to establish CA and can either be a static pre-shared key or dynamically derived.

Connectivity Association Key Name (CKN) identifies the connectivity association key.

Primary Key refers to the CAK used for the current MKA session.

Fallback Key is a key used in case the primary key does not establish a connection.

Secure Association Key (SAK) is the key used by the network ports to encrypt traffic in a session.

Key Server is a MACsec peer in the CA which creates and distributes secure association keys for encryption.

2.3 MACsec Attributes

MACsec has attributes which are used to establish secure communication channels for inbound traffic and outbound traffic. MACsec attributes include cipher suite selection, encryption, clear tag mode, encryption offset, replay protection window size, and Pre-shared Key (PSK). These attributes are discussed below.

2.3.1 Cipher Suite

A cipher suite is used to encrypt traffic on a link that is secured with MACsec. Four cipher suites are available, namely GCM-AES-128, GCM-AES-256, GCM-AES-XPN-128, and GCM-AES-XPN-256 [15]. GCM–AES–128 and GCM–AES–256 use a 32-bit PN that must be unique for every packet sent with a given SAK. When packet numbers are exhausted, the SAK must be refreshed. The frequency of SAK refresh can be reduced by using GCM-AES-XPN-128 and GCM-AES-XPN-256 cipher suites which increase the packet number to 64 bits. The same cipher suite should be used between MACsec peers. If a MACsec cipher suite is not configured, the default cipher suite GCM-AES-128 is used [15].

2.3.2 Encryption

MACsec allows encryption of traffic between hosts. When encryption is enabled, protocol-specific control information and user data will be encrypted, authenticated, and an integrity check performed using ICV. When encryption is not enabled, protocol-specific control information and user data will be sent in clear text. Figure 2.3 shows the MACsec frame format without encryption and Figure 2.4 shows the MACsec frame format with encryption. User data will be encrypted when MACsec is configured with encryption enabled [14].

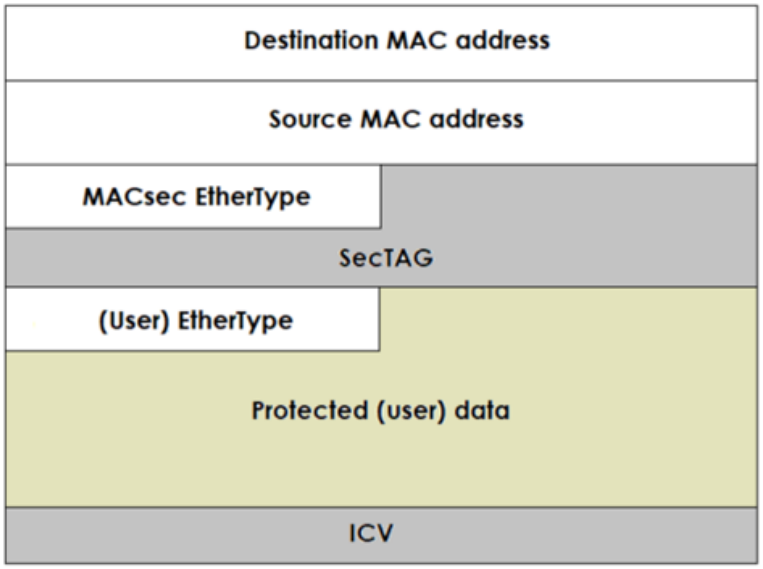

Figure 2.3: MACsec protected Ethernet frame format without encryption [14].

2.3.3 Clear Tag Mode

Clear tag mode is an attribute which allows the IEEE 802.1Q Virtual Local Area Network (VLAN) tag to be in clear text inside a MACsec encrypted frame. This permits service providers to provide service multiplexing so that multiple point-to-point or multipoint services can coexist on a physical interface, differentiated based on the unencrypted VLAN ID. The VLAN tag in clear text also enables service providers to provide Quality of Service (QOS) in a MACsec protected network. If clear tag mode is not configured, the VLAN tag is encrypted by default inside the MACsec encrypted frame [16]. Figure 2.5 shows the MACsec frame format where clear tag mode is used and the 802.1Q tag is not encrypted.

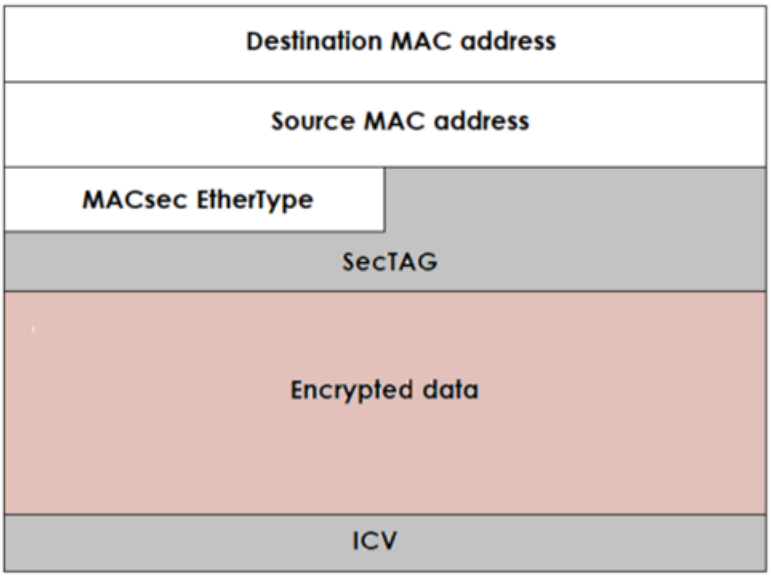

Figure 2.4: MACsec protected Ethernet frame format with encryption [14].

Figure 2.5: Unencrypted VLAN tag in a MACsec encrypted frame [4].

2.3.4 Encryption Offset

Encryption offset inside the MACsec CA is used to specify the number of octets in a MACsec encrypted frame that will be sent in clear text. This is used to expose IPv4 or IPv6 headers to devices such as firewalls or monitoring devices. It is also useful for load balancing which typically needs to see the IP and TCP/UDP headers in the first 30 or 50 octets to properly balance the traffic load [17].

2.3.5 Replay Protection Window Size

Replay protection is another feature of MACsec used to protect against replay attacks. Each encrypted packet is assigned a unique sequence number which is then verified at the remote end for replay protection. If a packet arrives out of sequence and the difference between the packet numbers is higher than the replay protection window size, the packet is dropped. The replay protection window size can be configured between 0 and $2^{32}-1$

[12].

2.3.6 MACsec PSK

A pre-shared key includes a CKN and a CAK. This key is exchanged between devices at each end of a point-to-point link to enable MACsec. The MACsec Key Agreement (MKA) protocol is enabled after the keys are successfully verified and exchanged. The pre-shared keys, CKN and CAK, must match on both ends of a link to enable the MKA protocol [12].

Chapter 3

MACsec Implementation

This chapter explains the MACsec implementation in LANs and WANs. The network design and configuration parameters are discussed and the utilities used and their use cases are explained. The metrics used for MACsec performance evaluation in LANs and WANs are also presented.

3.1 MACsec implementation in a LAN

MACsec is configured between hosts in a LAN which is set up in a virtualized environment using VMware Workstation and Graphical Network Simulator 3 (GNS3). Figure 3.1 shows the network topology for MACsec implementation in a LAN where a MACsec secure transmit channel was created between hosts connected via a switch. The hosts acquire IP addresses from a DHCP server. The management station is used to configure and perform operations on MACsec hosts.

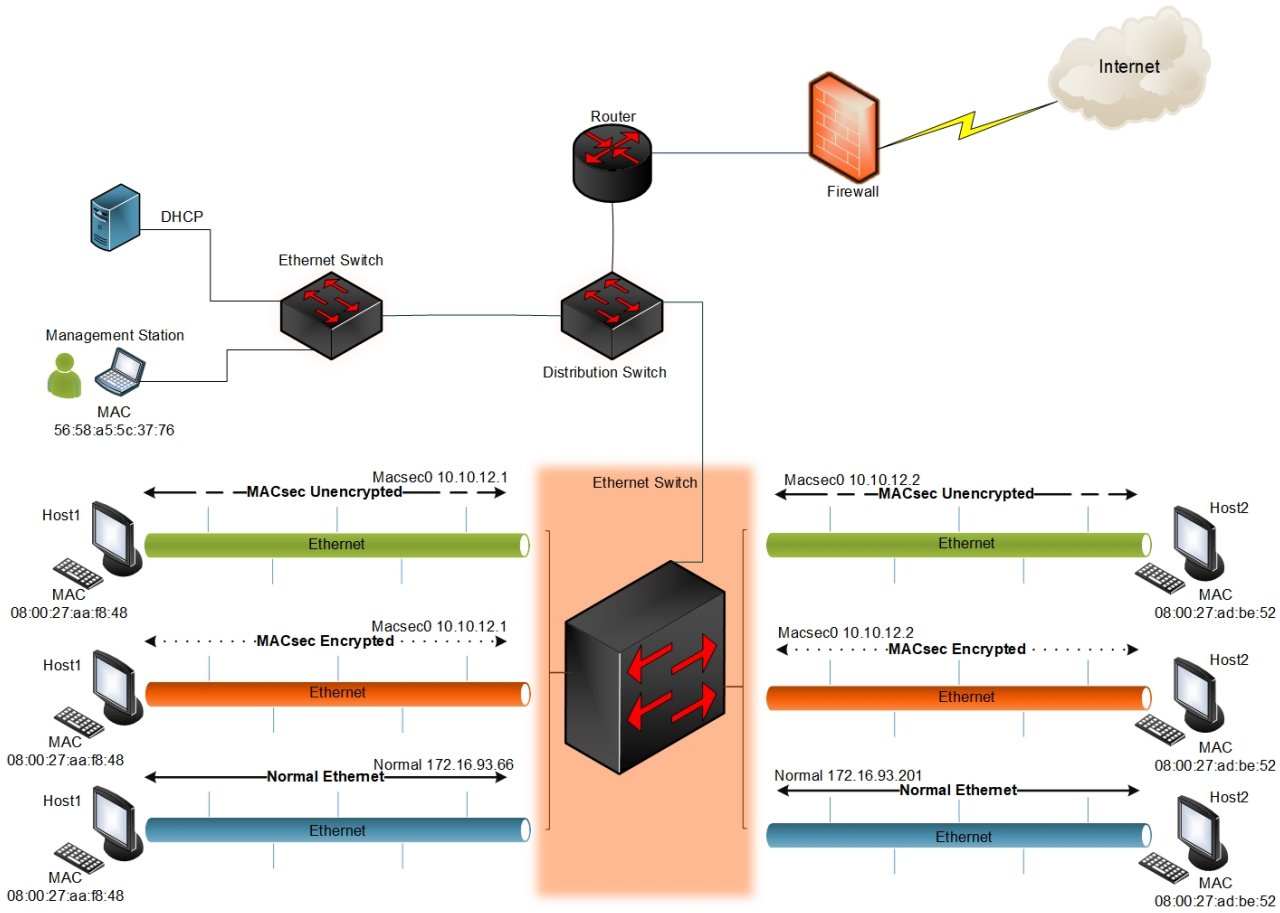

Figure 3.1: The MACsec LAN network topology.

3.2 MACsec implementation in a WAN

MACsec is configured between hosts in a WAN which is set up in a virtualized environment using VMware workstation and GNS3. Figure 3.2 shows the network topology for MACsec implementation in a WAN where a MACsec secure transmit channel was created between hosts. In addition, WAN and GRETAP devices are used to create a WAN and to link MACsec hosts via a layer 2 secure communication tunnel (shown as a red link in the figure). Furthermore, Linux bridges and virtual routers are used to establish connectivity between MACsec hosts in the WAN.

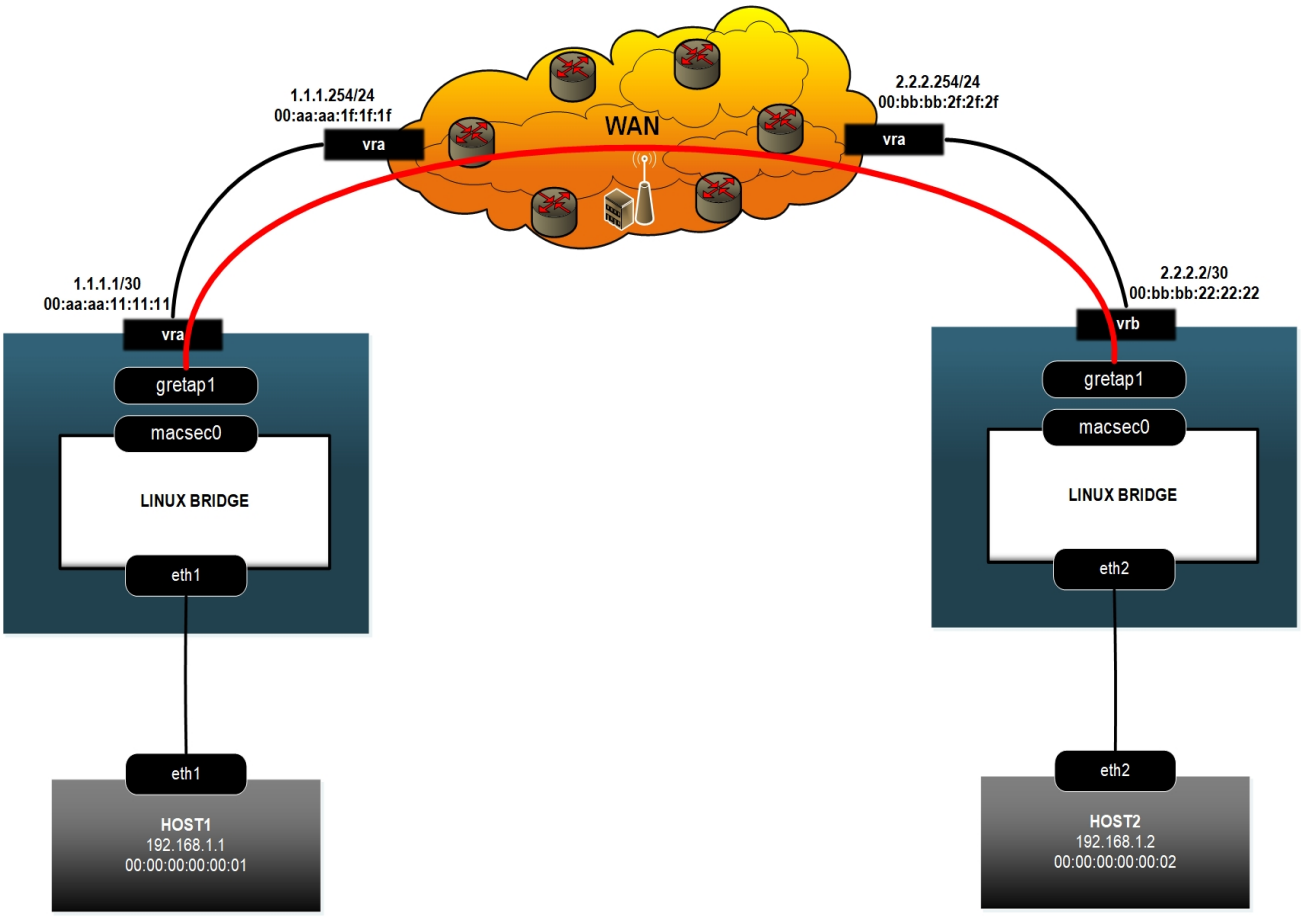

Figure 3.2: The MACsec WAN network topology.

3.3 Tools, Utilities and Use Cases

Table 3.1 gives the specifications of the tools used to design and implement the normal and MACsec protected LAN and WAN networks used in this work. The utilities along with their use cases are presented in Table 3.2.

Title	Technical Specification
Manufacturer	Dell Technologies Inc.
CPU	3.4 GHz Turbo Intel Core i7 (7th Generation)
Memory	32 GB DDR4
Hypervisor	VMware Workstation Pro v15.0
Operating Systems	Microsoft Windows 10 and Linux Kernel v4.19
Virtual Machines	Ubuntu 18.04 LTS and Kali Linux 2019.2
Network Simulator	Graphical Network Simulator 3 (GNS3) v2.2.9
Scripting Language	Bash (Unix shell and command language)
Switches	Cisco IOSv 156.2
Routers	Cisco 7200 Series (IOSXRv)

Table 3.1: Specifications of the tools used in this work.

3.4 MACsec Secure Channel Configuration Parameters

The MACsec configuration parameters are discussed below.

Secure Association (SA) is a transmit secure association number configured in MACsec to create a secure channel with a peer having the same SA.

Packet Number (PN) is configured in MACsec for the identification of packets ex-changed between MACsec peers. The PN is checked and tracked by MACsec peers for replay attack protection.

Cipher Suite Key is a 128-bit key used for encryption and decryption as MACsec uses the GCM-AES-128-bit cipher suite in Linux. Two different keys are configured in MACsec. The first key is used by the first MACsec peer as a transmit secure association key and is the receiving key of the receiving MACsec peer. Similarly, the second key is used by the second MACsec peer as a transmit secure association key and is used by the first MACsec peer as its receiving key.

Receiving (RX) Address is the address configured in MACsec as the receiving MACsec peer MAC address used to create a receive association with a MACsec peer.

Port is a port configured in MACsec for use as a Secure Channel Identifier (SCI). This helps in identification when more than one secure channel is used by a host (i.e., for a point-to-multipoint channel).

Utility	**Description**
GNS3	GNS3 is used to provide connectivity for network devices such as switches, routers, firewalls, DHCP servers, and docker containers. GNS3 allows the integration of virtual machines for use with network devices in real network environment simulation.
Virtual Machines (VM)	The Linux kernel version 4.19 is used which includes support to implement MACsec. MACsec is configured on VMs and MACsec protected peers communicate through MACsec protected secure transmit channels.
Kali Linux 2020	Kali Linux is a Debian based Linux distribution which is used to provide penetration testing tools for network security testing. It is used to test penetration in unprotected and MACsec protected networks.
EtterCap	EtterCap is a network security tool in Kali Linux VM which is used to launch MITM attacks against unprotected and MACsec protected networks.
Netcat	Netcat is used to create TCP client-server sessions between unprotected and MACsec protected hosts.
TCPDUMP and WireShark	TCPDUMP and WireShark is used to sniff network traffic and perform analysis on captured traffic traces.
QPerf	Qperf is used for network performance testing including throughput, latency, message rate, number of transmitted bytes, number of received bytes, and CPU utilization.
ICMP	The Internet Control Message Protocol (ICMP) is used to obtain the RTT.
Bash Scripting	Bash scripting is used to configure and implement MACsec. It is also used to configure MACsec attributes and to obtain MACsec related statistics.
Linux Bridge	Linux bridge is used to share the Network Interface Card (NIC) with virtual NICs as an alternative to using a Network Address Translation (NAT) based network in WANs.
DHCP	DHCP is used to assign IP addresses to hosts.

Table 3.2: Use cases of the utilities.

3.5 Performance Evaluation Metrics

The network performance is evaluated for normal and MACsec protected networks using the following metrics.

Throughput is the amount of data transferred from source to destination within a given time interval. Throughput is generally measured in bits per second and is controlled by the available bandwidth.

Latency is the delay in a network due to factors such as low throughput and packet loss. In high latency networks, the time for a data packet to travel from source to destination will be higher than in networks with low latency.

Message Rate is the number of messages that have been transferred successfully in a given time interval. The message rate depends on other network performance metrics such as latency and throughput. A high throughput, low latency connection can transfer more messages in a given time interval.

Total Bytes Transmitted (TX) is the number of bytes successfully transmitted from a source to destination in a given time interval.

Total Bytes Received (RX) is the number of bytes successfully received at a destination in a given time interval.

Round Trip Time (RTT) is the time for a data packet to travel from source to destination plus the time for the destination to send a response back to the source. RTT is an important metric in determining the performance of a network connection.

CPU Utilization is the percentage of the CPU used by the system. CPU utilization will vary according to the type and number of tasks performed by the system.

Chapter 4

Results and Discussion

This chapter presents the results and discusses the effectiveness of MACsec in protecting LANs and WANs. The performance of normal and MACsec protected networks is compared. Network protection against MITM attacks using MACsec is also examined. In this chapter, normal denotes a network without MACsec configuration, MACsec unencrypted denotes a network with MACsec configuration but without encryption, and MACsec encrypted denotes a network with MACsec and encryption.

4.1 Securing Local and Wide Area Networks

In this section, MACsec is used to secure LANs and WANs and the effectiveness of MACsec is examined. The implementation of MACsec with and without encryption is also compared.

4.1.1 Securing a LAN with MACsec

Figure 4.1 shows a traffic capture from a normal LAN obtained using WireShark. ICMP traffic is exchanged between two hosts and includes a series of ICMP requests and responses. The frame size in a normal LAN is 98 bytes. Figure 4.2 presents a traffic capture from a MACsec protected LAN obtained using WireShark. ICMP traffic is exchanged between two hosts and includes a series of ICMP requests and responses. In comparison to a normal LAN, the Ethernet frame format in a MACsec protected network contains MACsec EtherType 0x88e5 which denotes protected traffic. It can be observed that the MACsec protected frame size is 130 bytes. This is longer than a normal network frame since it includes an additional 32 bytes of SecTag and ICV.

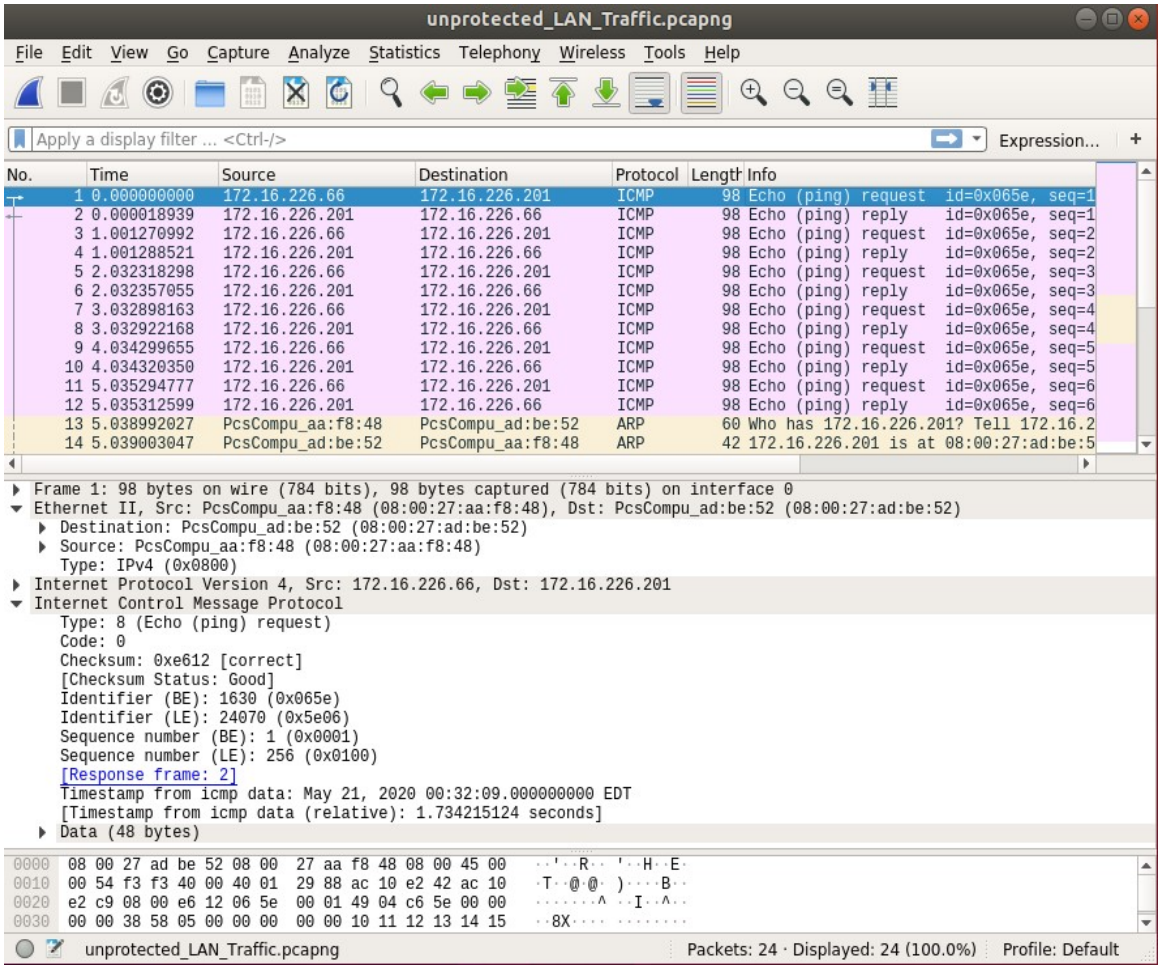

Figure 4.1: Traffic capture from a normal LAN.

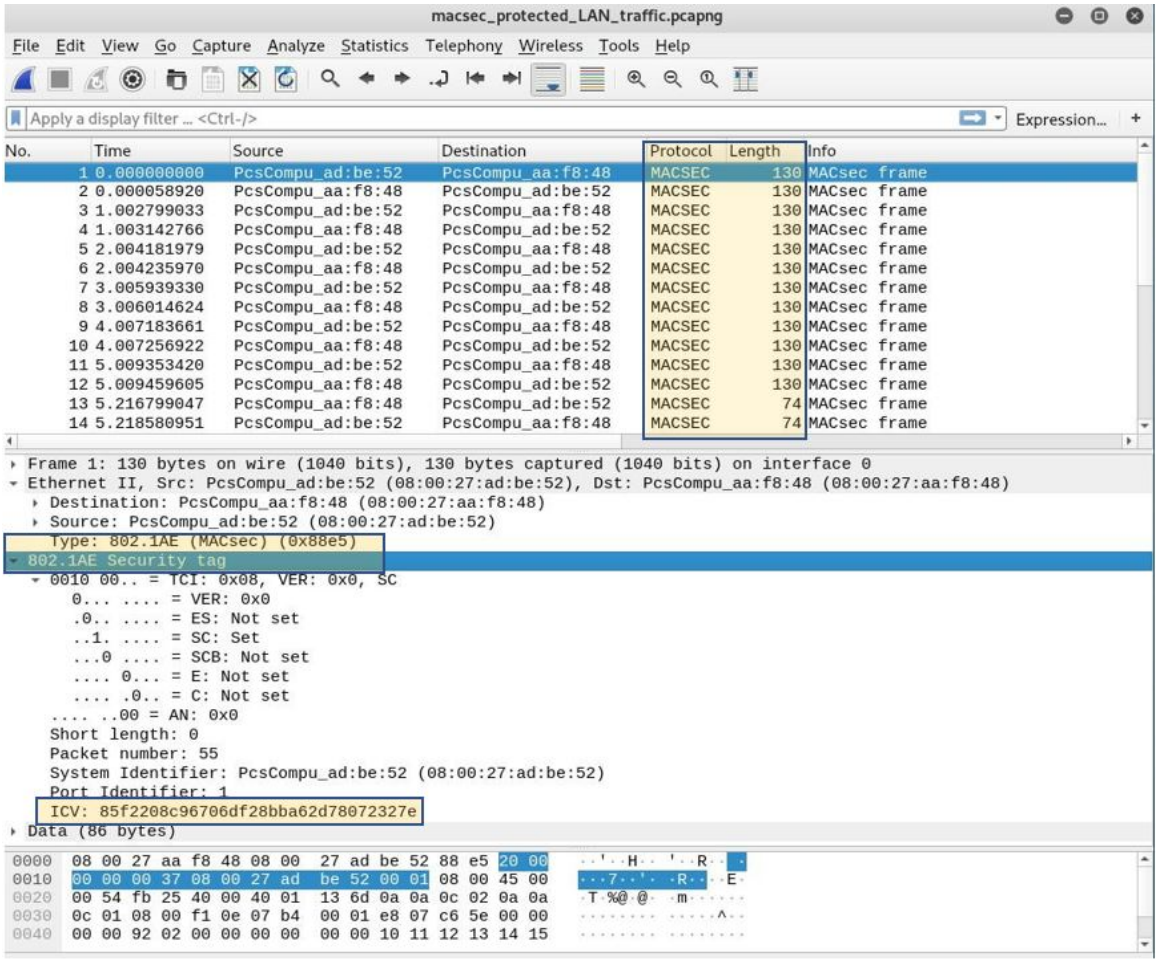

Figure 4.2: Traffic capture from a MACsec protected LAN.

4.1.2 Securing a WAN with MACsec

Figure 4.3 presents a traffic capture from a normal WAN obtained using WireShark. ICMP traffic is exchanged between two hosts and includes a series of ICMP requests and responses. The frame size in a normal WAN is 136 bytes. Figure 4.4 presents a traffic capture from a MACsec protected WAN obtained using WireShark. ICMP traffic is exchanged between two hosts and includes a series of ICMP requests and responses. In comparison with a normal WAN, the Ethernet frame format in a MACsec protected WAN contains MACsec EtherType 0x88e5 which denotes protected traffic. An additional 32 bytes is required for SecTAG and ICV, so a MACsec protected frame is 168 bytes versus a frame size of 136 bytes in a normal network.

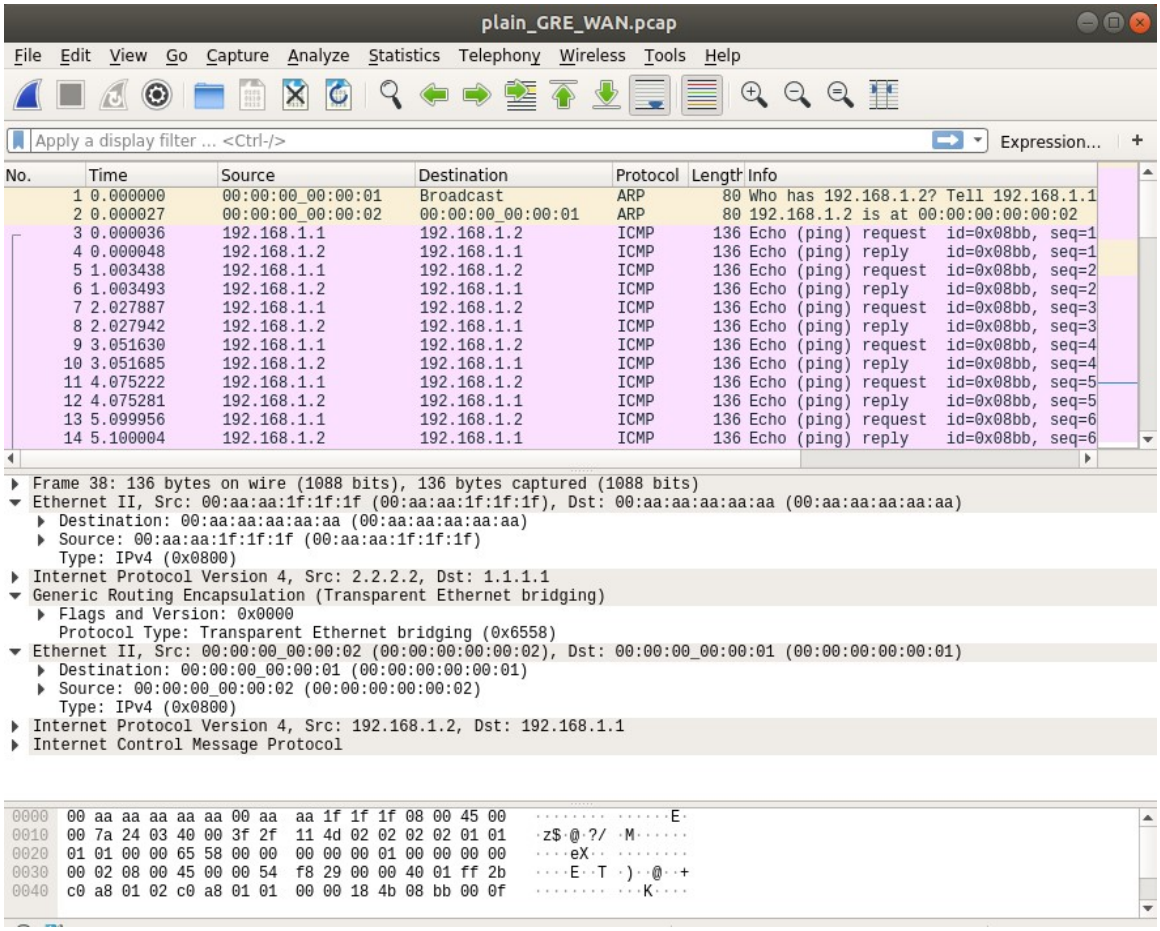

Figure 4.3: Traffic capture from a normal WAN.

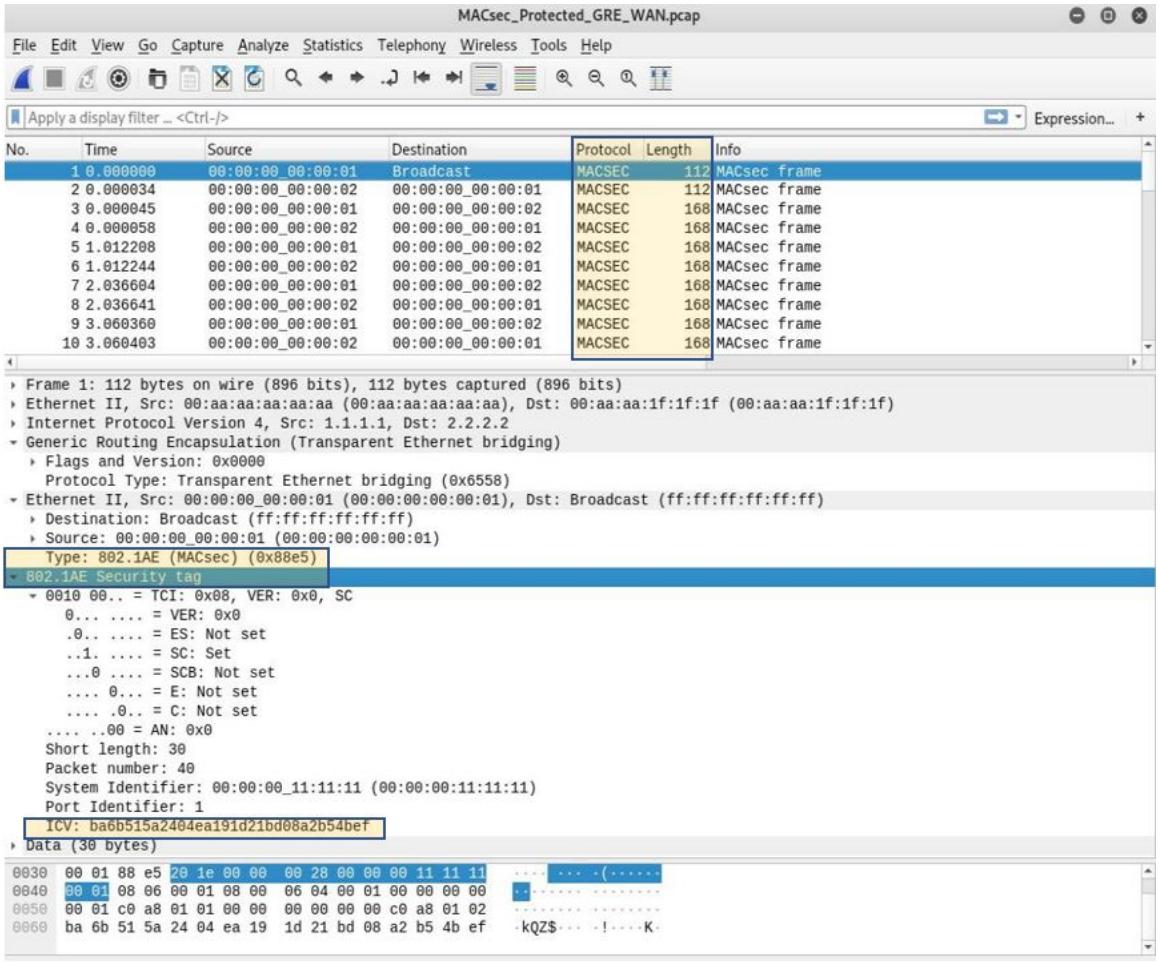

Figure 4.4: Traffic capture from a MACsec protected WAN.

4.1.3 MACsec Unencrypted

Figure 4.5 shows a traffic capture obtained using WireShark for a MACsec protected host without encryption enabled. The message content in the data field is plain text and the E bit is not set in the SecTAG. Table 4.1 presents the statistics of a MACsec protected host configured with the default configuration, i.e., without encryption. The number of transmitted (TX) packets are 108 and OutPktsEncrypted is zero. However, since MACsec is providing protection and validation to protect data integrity and authenticity, all 108 transmitted packets are protected which is indicated by OutPktsProtected.

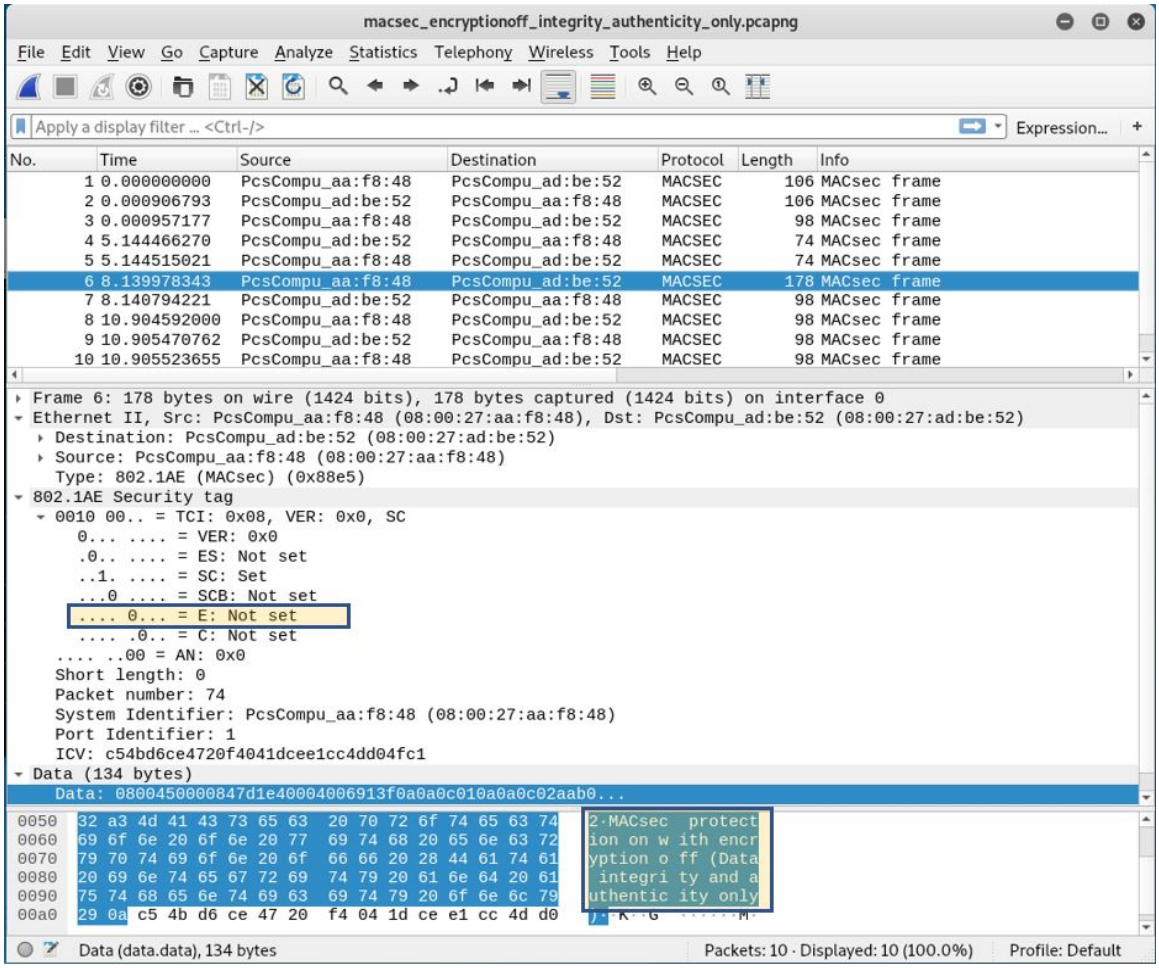

Figure 4.5: MACsec protected traffic without encryption.

Parameter	Number
TX Packets	108
OutPktsProtected	108
OutPktsEncrypted	0

Table 4.1: MACsec unencrypted statistics.

4.1.4 MACsec Encrypted

MACsec configuration with encryption enabled provides data integrity, data authenticity, and encryption of payload and protocol-specific information for greater security. Figure 4.6 shows a traffic capture for a MACsec protected host with encryption enabled. Message content in the packet is encrypted as shown in the data field and the E bit is set in the SecTAG which denotes that encryption is enabled. Table 4.2 present the statistics for a MACsec protected host configured with encryption enabled. The number of transmitted packets is 172 where 64 packets were transmitted after enabling encryption and these were encrypted. By default, MACsec with encryption enabled increments OutPktsEncrypted but not OutPktsProtected even though it is protecting packets.

Parameter	Number
TX Packets	172
OutPktsProtected	108
OutPktsEncrypted	64

Table 4.2: MACsec encrypted statistics.

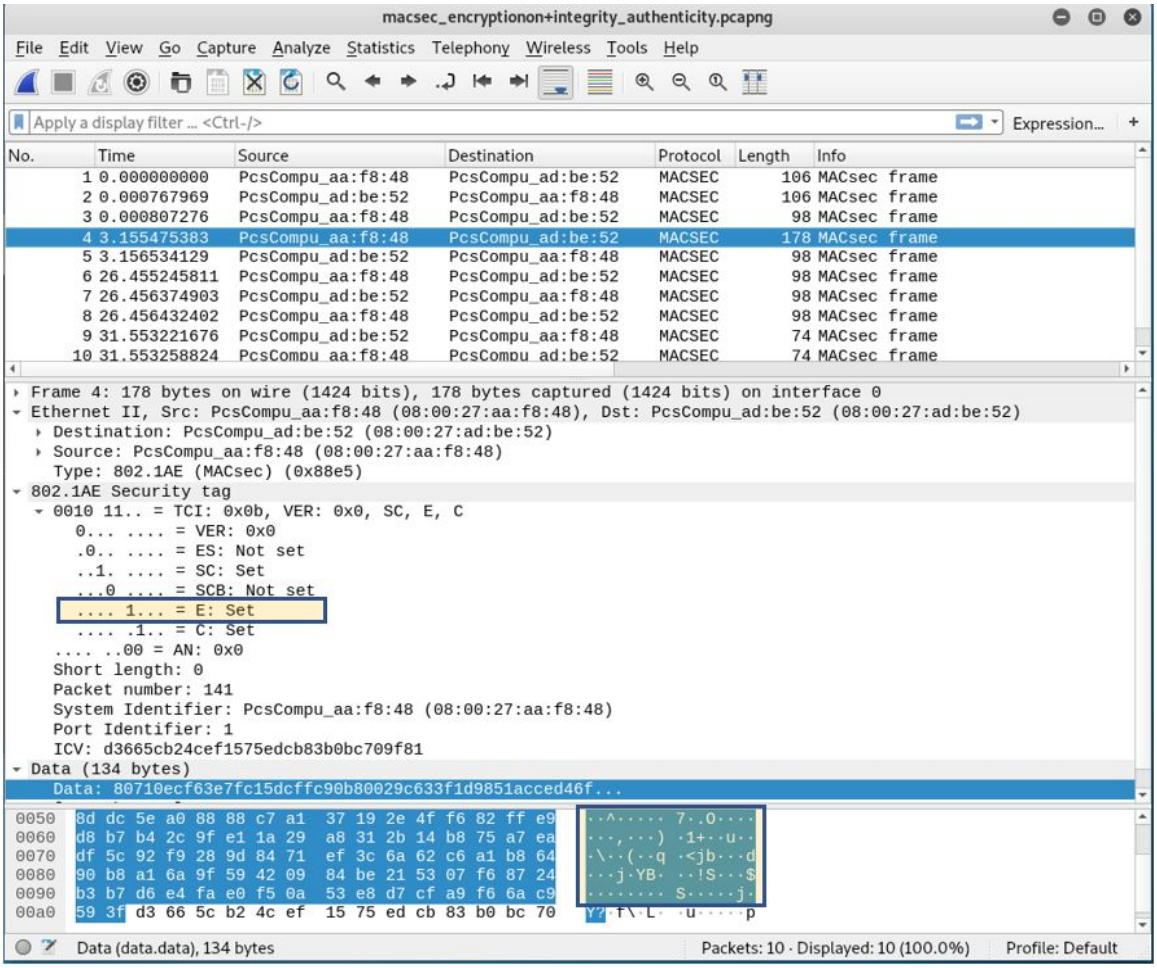

Figure 4.6: MACsec protected traffic with encryption.

4.1.5 MACsec and 802.1Q VLAN Tags

MACsec can be used with 802.1Q VLAN tags to take advantage of the security provided by VLANs which logically group hosts in a network. Figure 4.7 shows a traffic capture with an 802.1Q VLAN tag in a normal network. It can be observed that the 802.1Q VLAN tag and ID is visible in the 802.1Q Virtual LAN field. The packet size is 102 bytes which includes 4 bytes for a VLAN tag. Figure 4.8 shows a traffic capture from a MACsec protected network. In comparison to a normal network, the VLAN tag is not visible as it is encrypted by MACsec. The packet size is 134 bytes which contains 4 bytes for an encrypted VLAN tag and an additional 32 bytes for SecTAG and ICV.

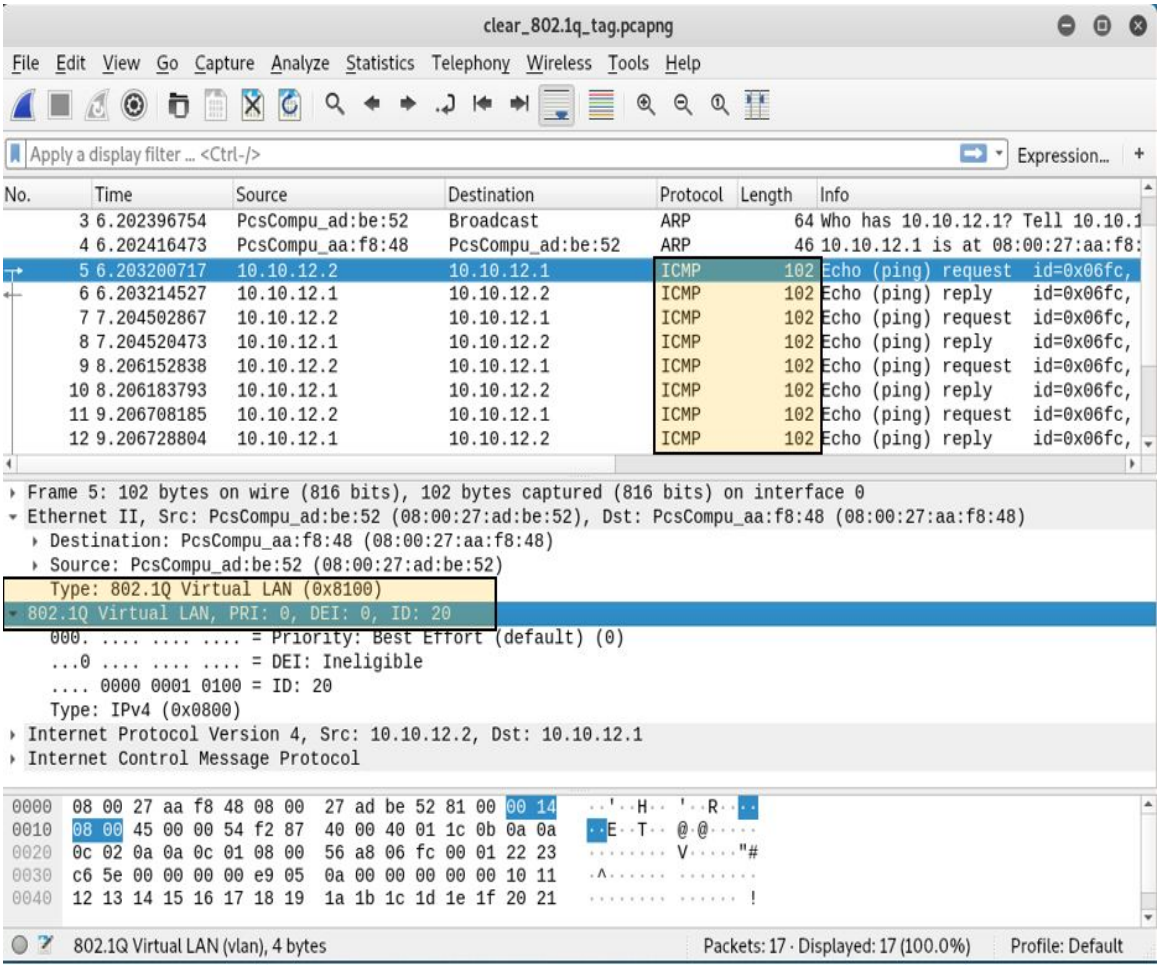

Figure 4.7: Traffic capture from a normal network with an 802.1Q VLAN tag.

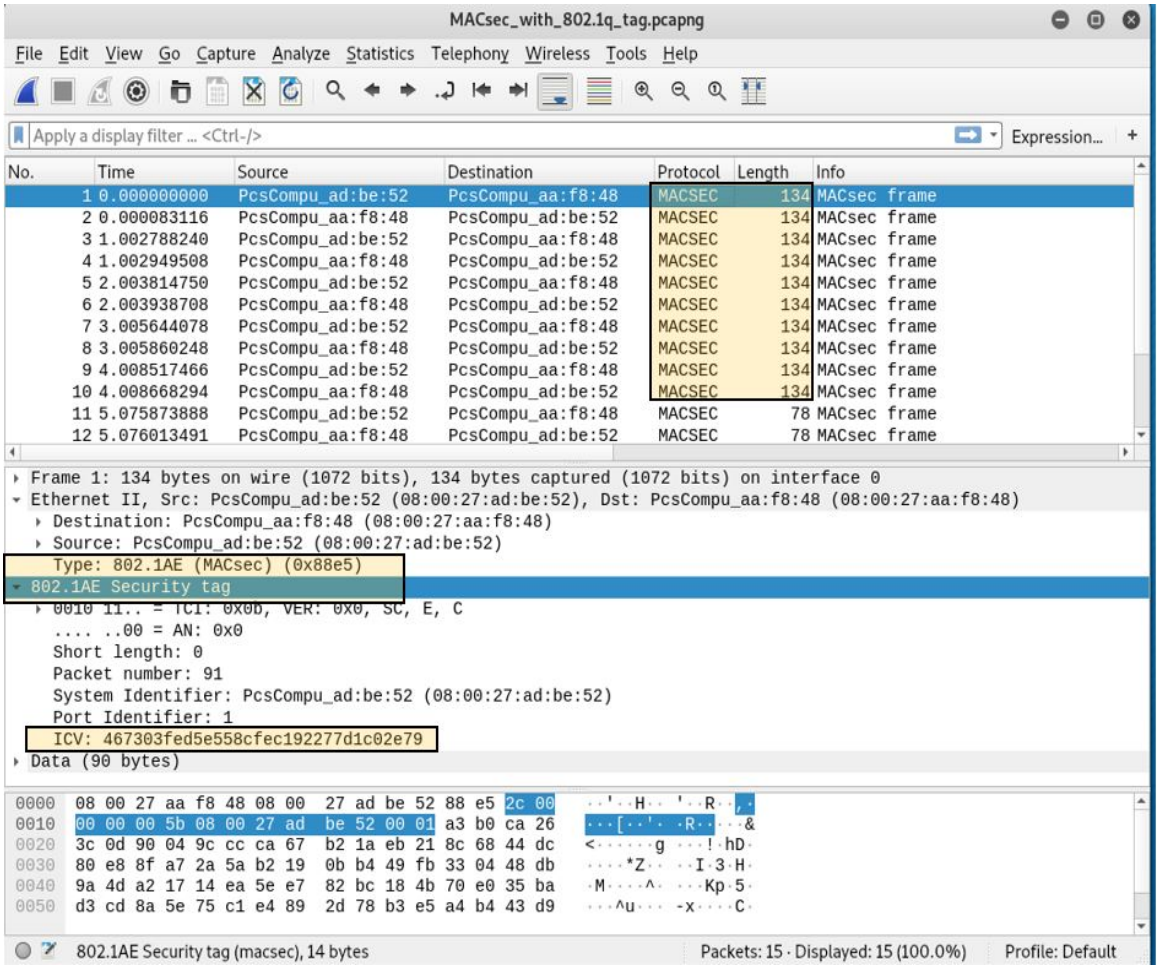

Figure 4.8: Traffic capture from a MACsec protected network with an 802.1AE security tag.

4.2 Network Performance Analysis

The use of MACsec to identify and prevent security threats such as DOS, intrusion, MITM, passive wiretapping, and playback attacks has an effect on network performance. This is because encryption creates additional overhead in a network. In this section, the performance of normal and MACsec protected LANs and WANs with and without encryption is evaluated. The LAN link bandwidth is 300 Mbps which is typical for an Internet Service Provider (ISP). For WANs, the typical link bandwidth of 1 Gbps is used. The results are obtained using Qperf.

4.2.1 Average Throughput

This subsection presents the average LAN and WAN throughput for normal and MACsec protected traffic with and without encryption. The average throughput was obtained at one minute intervals for a period of 10 minutes. Figure 4.9 presents the average throughput of normal, MACsec unencrypted, and MACsec encrypted traffic in the LAN. The average throughput of normal LAN is 140 Mbps while the average throughput for MACsec unencrypted and MACsec encrypted is 129 Mbps and 124 Mbps, respectively. Figure 4.10 presents the average throughput of normal, MACsec unencrypted, and MACsec encrypted traffic in the WAN. The average throughput of normal WAN is higher than MACsec protected links at 471 Mbps, while the average throughput for MACsec unencrypted and MACsec encrypted is 412 Mbps and 387 Mbps, respectively. Table 4.3 presents the average throughput of normal and MACsec protected LAN and WAN traffic.

There is a slight variation in the average throughput since throughput relies on factors such as response time from the router or switch and latency. An increase in latency and response time results in a decrease in throughput. It was further observed that MACsec protection reduces network throughput. This is expected since introducing additional fields in an Ethernet frame and the need to establish a secure channel with encrypted payloads creates additional overhead.

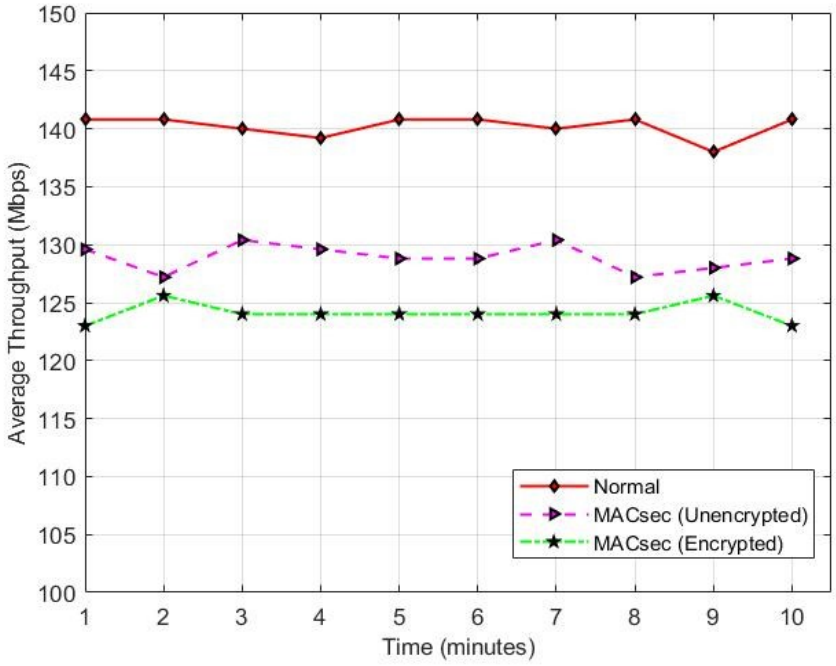

Figure 4.9: Average throughput of normal and MACsec protected LAN traffic.

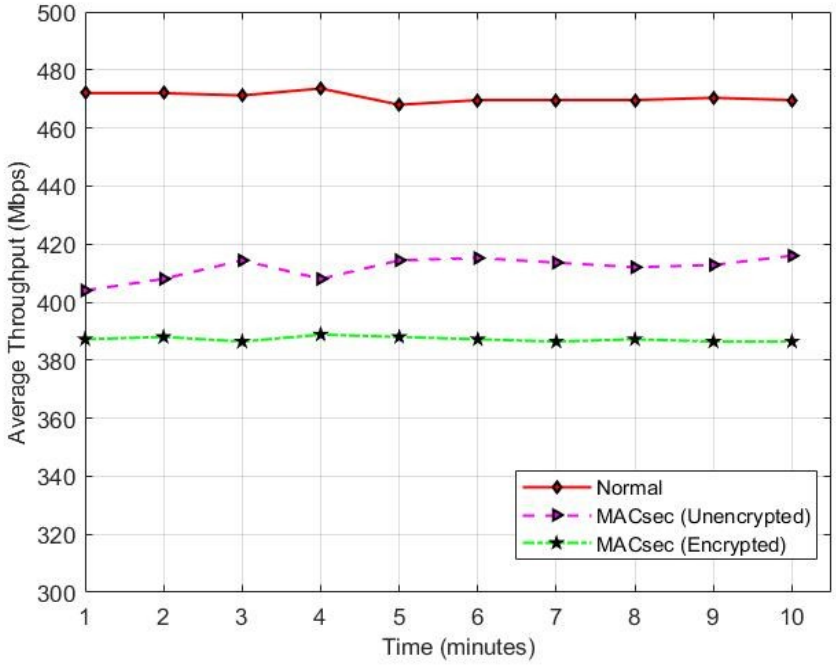

Figure 4.10: Average throughput of normal and MACsec protected WAN traffic.

Average Throughput (Mbps)						
	Local Area Network			Wide Area Network		
Time (min)	Normal	Unencrypted	Encrypted	Normal	Unencrypted	Encrypted
1	141	130	123	472	404	387
2	141	127	126	472	408	388
3	140	130	124	471	414	386
4	139	130	124	474	408	389
5	141	129	124	468	414	388
6	141	129	124	470	415	387
7	141	130	124	470	414	386
8	141	127	124	470	412	387
9	138	128	126	470	413	386
10	140	129	123	470	416	386
Average	140	129	124	471	412	387

Table 4.3: Average throughput of normal and MACsec protected LAN and WAN traffic.

4.2.2 Average Latency

This subsection presents the average LAN and WAN latency for normal and MACsec protected traffic with and without encryption. The average latency was obtained at one minute intervals for a period of 10 minutes. Figure 4.11 presents the average latency of normal, MACsec unencrypted, and MACsec encrypted traffic in the LAN. The average latency of normal traffic is 0.189 ms. The average latency of MACsec unencrypted traffic is 0.194 ms, while MACsec encrypted traffic has the highest latency at 0.200 ms. Figure 4.12 presents the average latency of normal, MACsec unencrypted, and MACsec encrypted traffic in the WAN. The average latency of normal traffic is 0.0110 ms, while the average latency for MACsec unencrypted and MACsec encrypted traffic is 0.0120 ms and 0.0122 ms, respectively. Table 4.4 presents the average latency of normal and MACsec protected LAN and WAN traffic.

It was observed that MACsec slightly increases the latency in a network. The highest latency was observed for MACsec protected traffic with encryption enabled. This is expected due to the time it takes for the sender to encrypt and the receiver to decrypt the payload in a MACsec frame.

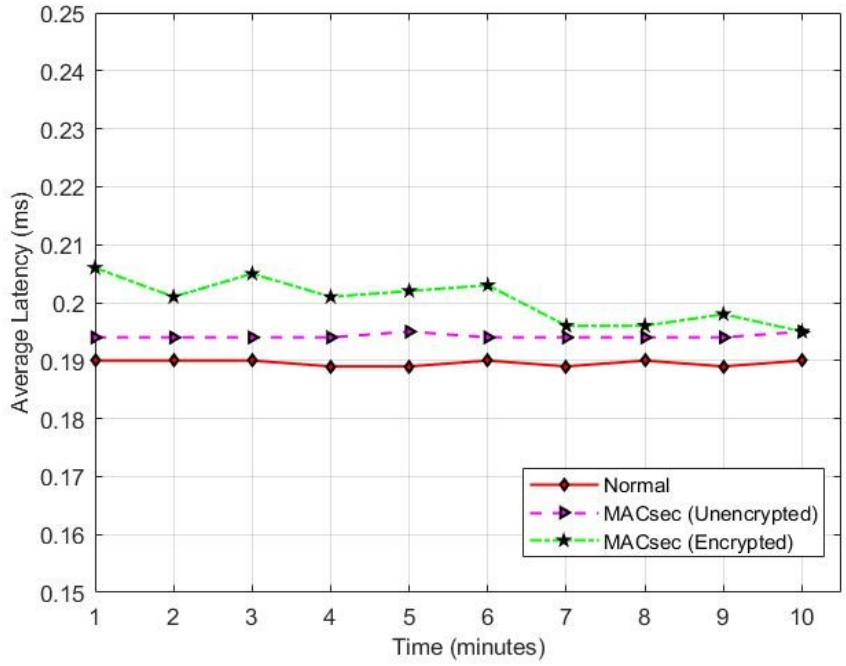

Figure 4.11: Average latency of normal and MACsec protected LAN traffic.

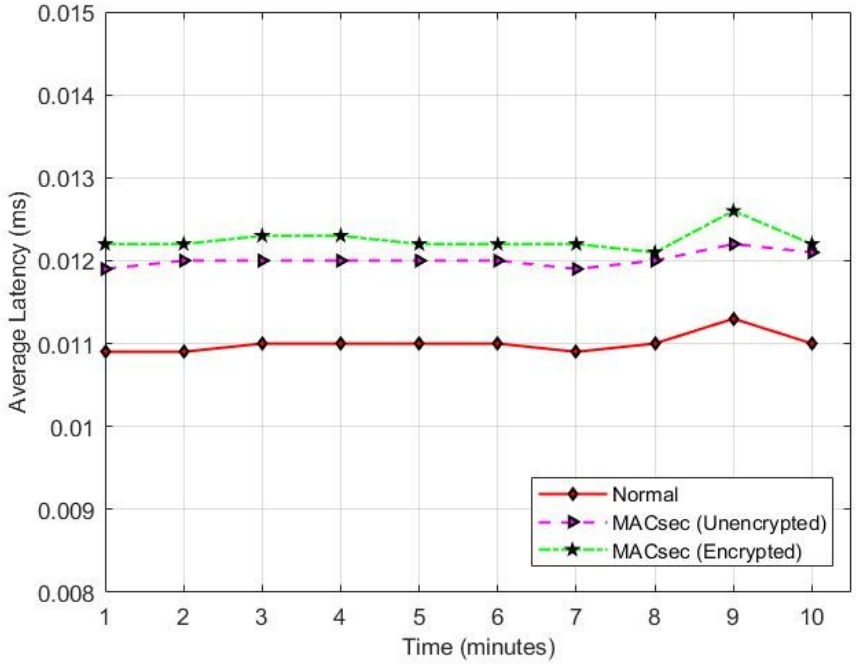

Figure 4.12: Average latency of normal and MACsec protected WAN traffic.

Average Latency (ms)						
	Local Area Network			Wide Area Network		
Time (min)	Normal	Unencrypted	Encrypted	Normal	Unencrypted	Encrypted
1	0.190	0.194	0.206	0.0109	0.0119	0.0122
2	0.190	0.194	0.201	0.0109	0.0120	0.0122
3	0.190	0.194	0.205	0.0110	0.0120	0.0123
4	0.189	0.194	0.201	0.0110	0.0120	0.0123
5	0.189	0.195	0.202	0.0110	0.0120	0.0122
6	0.190	0.194	0.203	0.0110	0.0120	0.0122
7	0.189	0.194	0.196	0.0109	0.0119	0.0122
8	0.190	0.194	0.196	0.0110	0.0120	0.0121
9	0.189	0.194	0.198	0.0113	0.0122	0.0126
10	0.190	0.195	0.195	0.0110	0.0121	0.0122
Average	0.189	0.194	0.200	0.0110	0.0120	0.0122

Table 4.4: Average latency of normal and MACsec protected LAN and WAN traffic.

4.2.3 Average Message Rate

This subsection presents the average LAN and WAN message rate for normal and MACsec protected traffic with and without encryption. The average message rate was obtained at one minute intervals for a period of 10 minutes. Figure 4.13 presents the average message rate of normal, MACsec unencrypted, and MACsec encrypted traffic in the LAN. Normal traffic has the highest message rate of 267 msg/s. The average message rate of MACsec unencrypted is 245 msg/s, while MACsec encrypted has the lowest average message rate of 235 msg/s. Figure 4.14 presents the average message rate of normal, MACsec unencrypted, and MACsec encrypted traffic in the WAN. The average message rate of normal traffic is the highest at 898 msg/s, while the average message rate for MACsec unencrypted and MACsec encrypted traffic is 786 msg/s and 739 msg/s, respectively. Table 4.5 presents the average message rate of normal and MACsec protected traffic in the LAN and WAN.

The message rate is dependent on the latency and throughput in a network. As shown earlier, MACsec reduces average throughput and increases average latency in a network, which further decreases the message rate. Therefore, normal traffic in a LAN and WAN achieved a higher message rate compared to MACsec unencrypted and encrypted traffic.

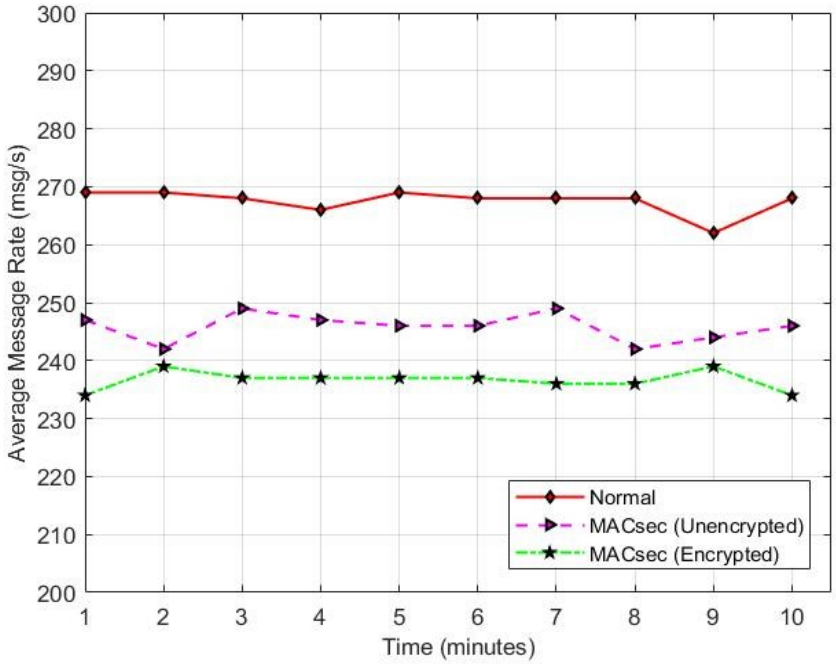

Figure 4.13: Average message rate of normal and MACsec protected LAN traffic.

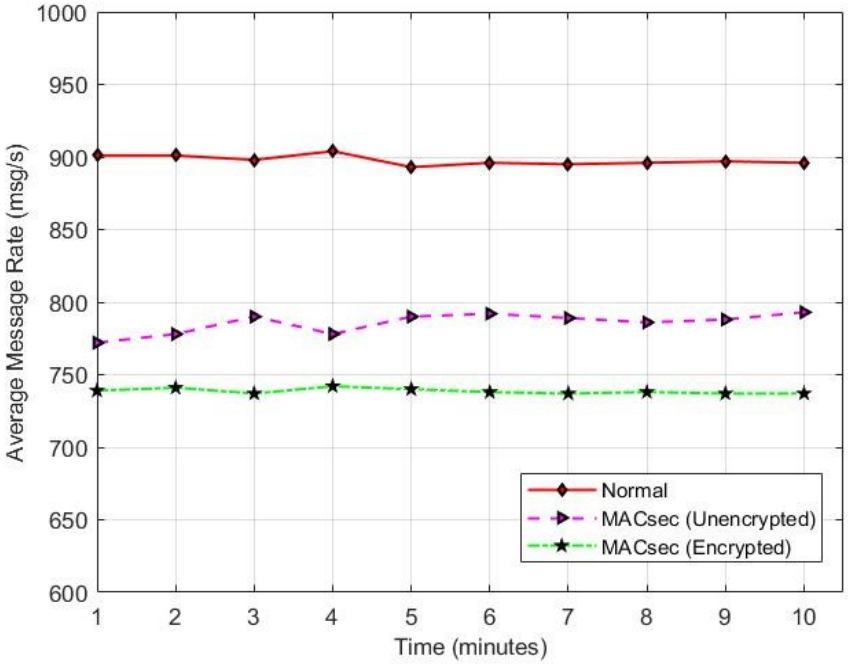

Figure 4.14: Average message rate of normal and MACsec protected WAN traffic.

Average Message Rate (msg/s)						
	Local Area Network			Wide Area Network		
Time (min)	Normal	Unencrypted	Encrypted	Normal	Unencrypted	Encrypted
1	269	247	234	901	772	739
2	269	242	239	901	778	741
3	268	249	237	898	790	737
4	266	247	237	904	778	742
5	269	246	237	893	790	740
6	268	246	237	896	792	738
7	268	249	236	895	789	737
8	268	242	236	896	786	738
9	262	244	239	897	788	737
10	268	246	234	896	793	737
Average	267	245	235	898	786	739

Table 4.5: Average message rate of normal and MACsec protected LAN and WAN traffic.

4.2.4 Total Number of Bytes Transmitted

This subsection presents the total number of bytes transmitted in the LAN and WAN for normal and MACsec protected traffic with and without encryption. The total number of bytes transmitted was obtained at one minute intervals for a period of 10 minutes. Figure 4.16 presents the total number of bytes transmitted by normal, MACsec unencrypted, and MACsec encrypted traffic in the LAN. Normal LAN transmitted the highest number of bytes at 10.6 GBytes, while the number of bytes transmitted by MACsec unencrypted and encrypted was 9.7 GBytes and 8.76 GBytes, respectively. Figure 4.15 presents the total number of bytes transmitted by normal, MACsec unencrypted, and MACsec encrypted traffic in the WAN. Normal WAN has the highest number of transmitted bytes at 35.2 GBytes, while the number of bytes transmitted by MACsec unencrypted and encrypted was 31.2 GBytes and 29 GBytes, respectively. Table 4.6 presents the total number of bytes transmitted as normal and MACsec protected traffic in the LAN and WAN.

The amount of data transmission depends on the throughput and latency in a network. Therefore, normal LAN and WAN transmitted a higher number of bytes than MACsec protected. Further, MACsec unencrypted transmitted a higher number of bytes than MACsec with encryption enabled.

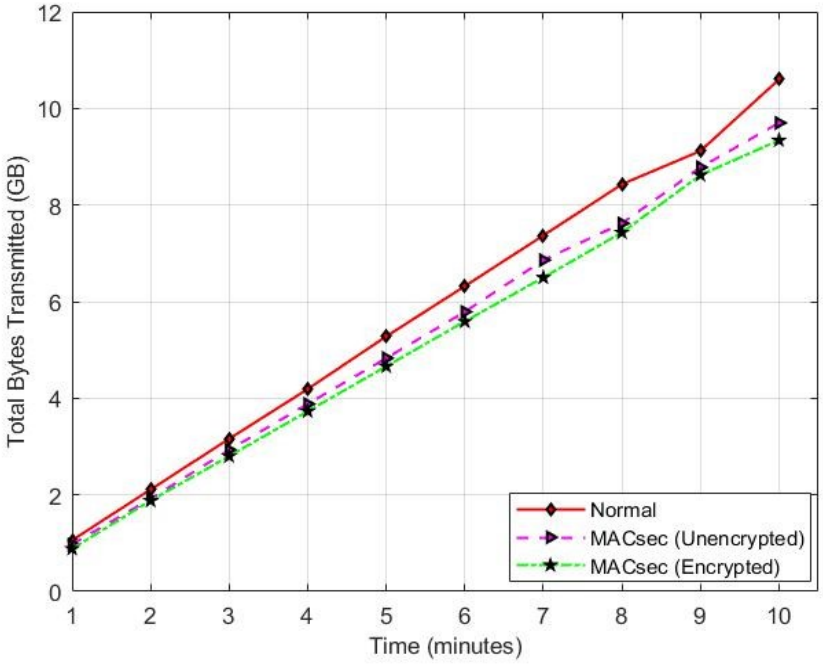

Figure 4.15: Total number of bytes transmitted as normal and MACsec protected traffic in the LAN.

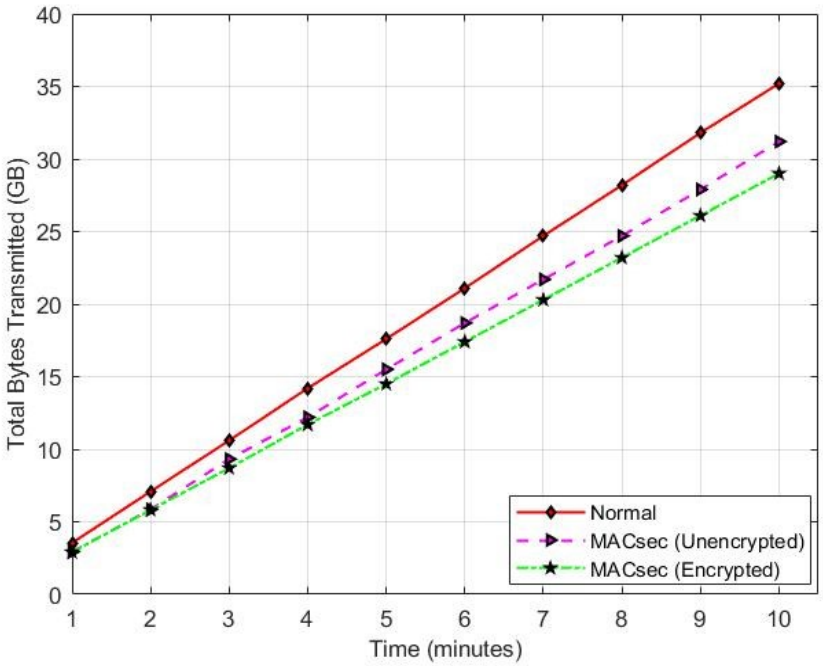

Figure 4.16: Total number of bytes transmitted as normal and MACsec protected traffic in the WAN.

Total Number of Bytes Transmitted (GB)						
	Local Area Network			Wide Area Network		
Time (min)	Normal	Unencrypted	Encrypted	Normal	Unencrypted	Encrypted
1	1.06	0.97	0.88	3.54	2.93	2.91
2	2.11	1.88	1.88	7.09	5.85	5.82
3	3.16	2.93	2.80	10.6	9.32	8.70
4	4.19	3.88	3.73	14.2	12.2	11.7
5	5.28	4.83	4.66	17.6	15.5	14.5
6	6.32	5.79	5.59	21.1	18.7	17.4
7	7.37	6.86	6.50	24.7	21.7	20.3
8	8.43	7.62	7.43	28.2	24.7	23.2
9	9.12	8.48	8.62	31.8	27.9	26.1
10	10.6	9.70	8.76	35.2	31.2	29.0

Table 4.6: Total number of bytes transmitted as normal and MACsec protected traffic in the LAN and WAN.

4.2.5 Total Number of Bytes Received

This subsection presents the total number of bytes received in the LAN and WAN for normal and MACsec protected traffic with and without encryption. The total number of bytes received was obtained at one minute intervals for period of 10 minutes. Figure 4.17 presents the total number of bytes received by normal, MACsec unencrypted, and MACsec encrypted traffic in the LAN. Normal LAN received the highest number of bytes at 10.6 GBytes, while the number of bytes received by MACsec unencrypted and encrypted was 9.7 GBytes and 8.8 GBytes, respectively. Figure 4.18 presents the total number of bytes received by normal, MACsec unencrypted, and MACsec encrypted traffic in the WAN. Normal WAN received the highest number of bytes at 35.2 GBytes. The number of bytes received by MACsec unencrypted WAN was 31.2 GBytes, while the number of bytes received by MACsec encrypted WAN was 29 GBytes. Table 4.7 presents the total number of bytes received as normal and MACsec protected traffic in the LAN and WAN.

The amount of data received depends on the throughput and latency in the network. Therefore, normal LAN and WAN received a higher number of bytes than MACsec protected. Further, MACsec unencrypted received a higher number of bytes than MACsec encrypted.

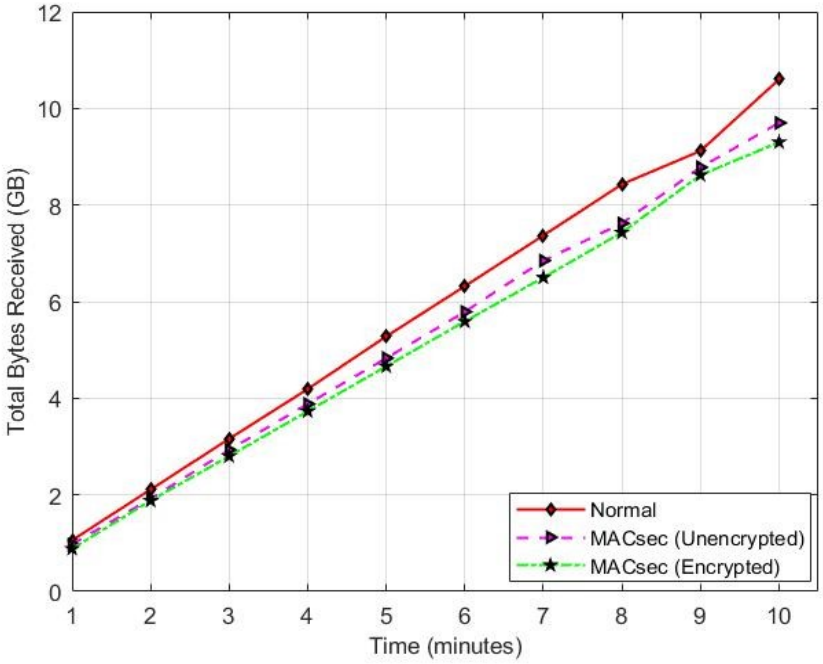

Figure 4.17: Total number of bytes received as normal and MACsec protected traffic in the LAN.

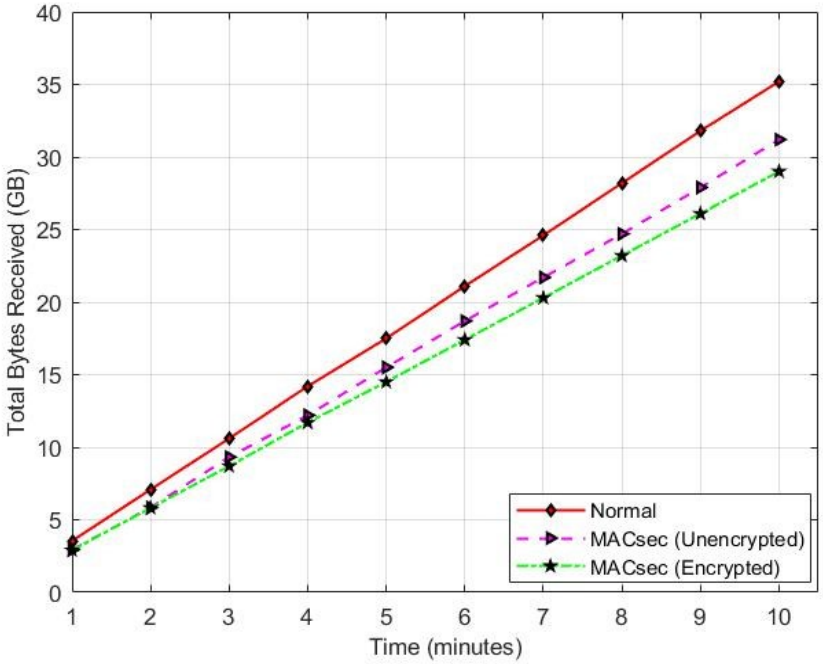

Figure 4.18: Total number of bytes received as normal and MACsec protected traffic in the WAN.

Total Number of Bytes Received (GB)						
	Local Area Network			Wide Area Network		
Time (min)	Normal	Unencrypted	Encrypted	Normal	Unencrypted	Encrypted
1	1.06	0.97	0.88	3.54	2.93	2.91
2	2.11	1.88	1.88	7.09	5.85	5.82
3	3.16	2.93	2.80	10.6	9.32	8.70
4	4.19	3.88	3.73	14.2	12.2	11.7
5	5.28	4.83	4.66	17.6	15.5	14.5
6	6.32	5.79	5.59	21.1	18.7	17.4
7	7.37	6.86	6.50	24.7	21.7	20.3
8	8.43	7.62	7.43	28.2	24.7	23.2
9	9.12	8.48	8.62	31.8	27.9	26.1
10	10.6	9.70	8.76	35.2	31.2	29.0

Table 4.7: Total number of bytes received as normal and MACsec protected traffic in the LAN and WAN.

4.2.6 Average CPU Utilization

This subsection presents the average CPU utilization in the LAN and WAN for normal and MACsec protected traffic with and without encryption. The average CPU utilization was obtained at one minute intervals for a period of 10 minutes. Figure 4.19 presents the average CPU utilization of normal, MACsec unencrypted, and MACsec encrypted traffic in the LAN. The normal LAN used 32.5% of the CPU. MACsec unencrypted and encrypted used a similar amount of CPU at 55%. Figure 4.20 presents the average CPU utilization of normal, MACsec unencrypted, and MACsec encrypted traffic in the WAN. The normal WAN used the lowest amount of CPU with an average of 16.7%. The average CPU utilization for MACsec with and without encryption was similar at 19.7%. Table 4.8 presents the average CPU utilization of normal and MACsec protected traffic in the LAN and WAN.

Overall, normal LAN and WAN traffic utilized less of the CPU than MACsec protected. This is because processing MACsec frames containing encrypted information and additional fields in MACsec protected frames including SecTAG and ICV creates additional demands on the CPU.

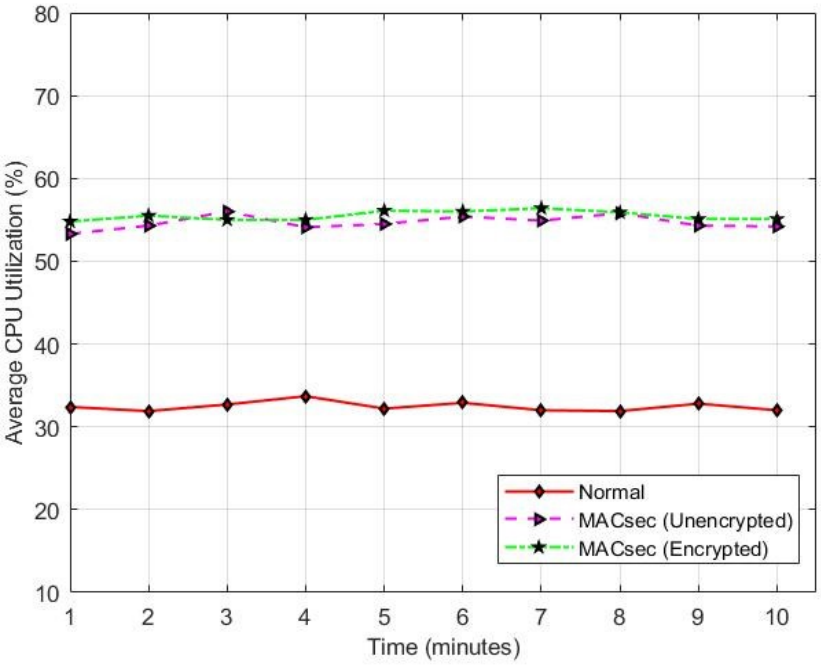

Figure 4.19: Average CPU utilization for normal and MACsec protected LAN traffic.

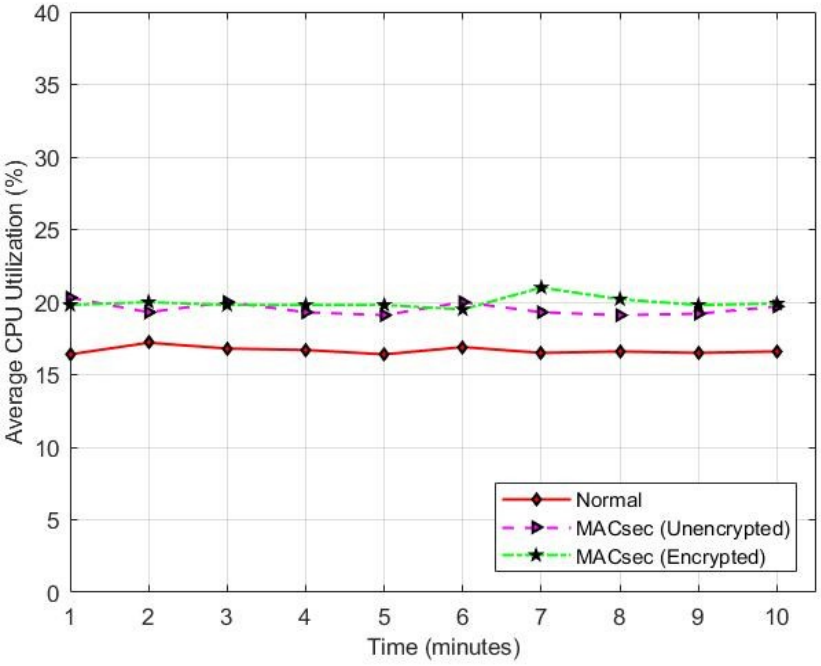

Figure 4.20: Average CPU utilization for normal and MACsec protected WAN traffic.

Average CPU Utilization (%)						
	Local Area Network			Wide Area Network		
Time (min)	Normal	Unencrypted	Encrypted	Normal	Unencrypted	Encrypted
1	32.4	53.3	54.8	16.4	20.3	19.8
2	31.9	54.3	55.5	17.2	19.3	20.0
3	32.7	56.0	55.0	16.8	20.0	19.8
4	33.7	54.1	55.0	16.7	19.3	19.8
5	32.2	54.5	56.1	16.4	19.1	19.8
6	32.9	55.4	56.0	16.9	20.0	19.5
7	32.0	54.9	56.4	16.5	19.3	21.0
8	31.9	55.8	55.9	16.6	19.1	20.2
9	32.8	54.3	55.1	16.5	19.2	19.8
10	32.0	54.2	55.1	16.6	19.7	19.9
Average	32.5	54.7	55.5	16.7	19.5	20.0

Table 4.8: Average CPU utilization for normal and MACsec protected LAN and WAN traffic.

4.2.7 Average Round Trip Time

This subsection presents the average LAN and WAN Round Trip Time (RTT) for normal and MACsec protected traffic with and without encryption. The average RTT in the network was obtained five times by transmitting 10 thousand (10k) packets each time. Figure 4.21 presents the average RTT of normal, MACsec unencrypted, and MACsec encrypted LAN traffic. The average RTT of normal LAN traffic is 1.898 ms. The average RTT for MACsec unencrypted is 2.016 ms, while MACsec encrypted has the highest RTT at 2.091 ms. Figure 4.22 presents the average RTT of normal, MACsec unencrypted, and MACsec encrypted WAN traffic. The average RTT of normal WAN traffic is 0.103 ms, whereas the average RTT of MACsec unencrypted and MACsec encrypted WAN traffic is 0.127 ms and 0.131 ms, respectively. Table 4.9 presents the average RTT of normal and MACsec protected LAN and WAN traffic.

It was observed that MACsec slightly increases the RTT in the network. The highest RTT is with MACsec protected traffic with encryption enabled. This is expected because of the time it takes for the sender to encrypt and the receiver to decrypt the payload in a MACsec frame.

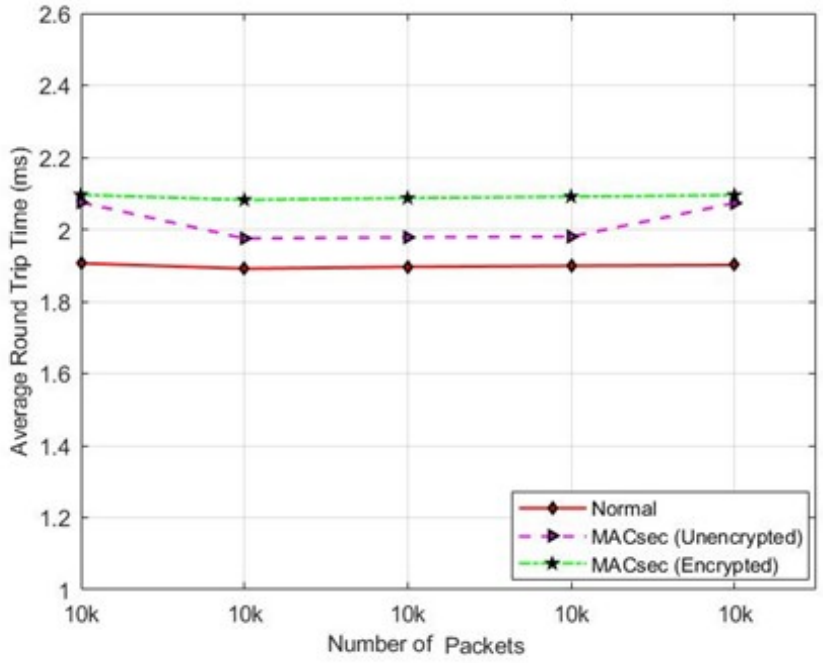

Figure 4.21: Average RTT of normal and MACsec protected LAN traffic.

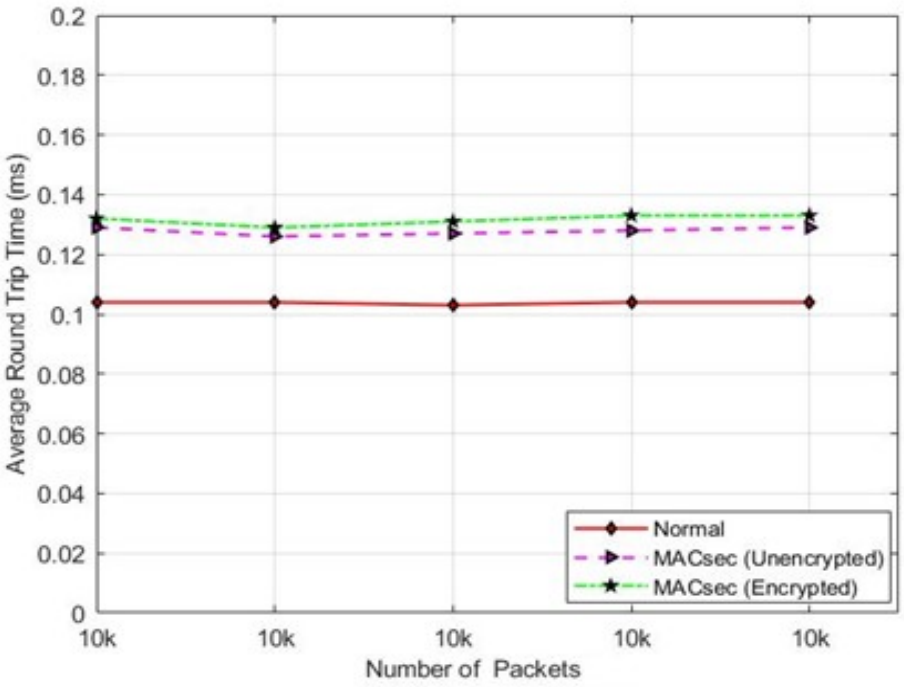

Figure 4.22: Average RTT of normal and MACsec protected WAN traffic.

Average Round Trip Time (ms)						
	Local Area Network			Wide Area Network		
No. of Packets	Normal	Unencrypted	Encrypted	Normal	Unencrypted	Encrypted
10k	1.906	2.075	2.096	0.104	0.129	0.132
10k	1.891	1.975	2.082	0.104	0.126	0.129
10k	1.896	1.978	2.087	0.103	0.127	0.131
10k	1.899	1.980	2.091	0.104	0.128	0.133
10k	1.901	2.073	2.095	0.104	0.129	0.133
Average	1.898	2.016	2.091	0.103	0.127	0.131

Table 4.9: Average round trip time of normal and MACsec protected LAN and WAN traffic.

4.3 Protecting Networks from Man-in-the-Middle (MITM) Attacks

This section presents the execution of a MITM attack. It also presents the results for MITM attacks in normal and MACsec protected networks.

4.3.1 Executing a Man-in-the-Middle Attack

The communications between hosts in a network is associated with the port they are connected to. Traffic exchanged between hosts passes through the network device responsible for providing communications (i.e., switches or routers). This device forwards traffic to a specific source or destination and ensures other hosts connected to the same network device cannot observe this traffic. However, an attacker can spoof its MAC address to either the source or destination host to divert network traffic and act as a legitimate peer of the target (a man in the middle). Figure 4.23 shows an attacker that has spoofed its MAC address on two hosts (Host1 and Host2), using ARP poisoning to divert network traffic from its original path. ARP poisoning is a method where an attacker uses malicious ARP packets to associate its IP address with any MAC address in a network. Then traffic exchanged between Host1 and Host2 will be diverted and passed through the attacker who will have access to the information being shared.

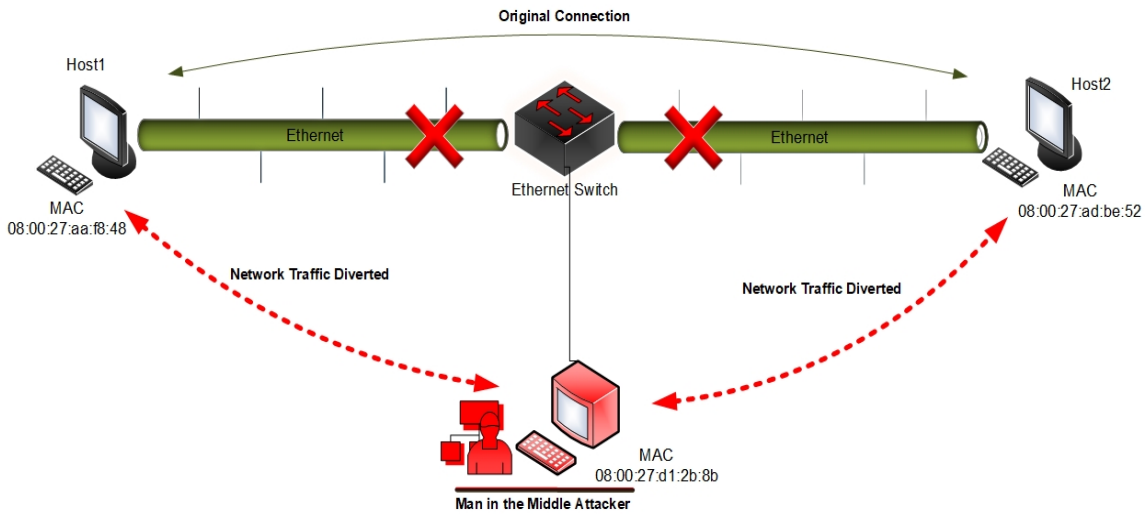

Figure 4.23: Traffic diverted as a result of an MITM attack.

The steps an attacker must perform to successfully penetrate and execute an MITM

Name	IP Address – Normal	IP Address - MACsec	MAC Address
Host1	172.16.93.66	10.10.12.1	08:00:27:aa:f8:48
Host2	172.16.93.201	10.10.12.2	08:00:27:ad:be:52
Attacker	172.16.93.90	10.10.12.10	08:00:27:d1:2b:8b

Table 4.10: Network configuration details for the hosts and MITM attacker.

attack are as follows.

1. Gain access to the ports to which hosts are connected to.
2. Sniff and listen on these ports to obtain information such as subnet information.
3. Scan the subnets to discover the available hosts in the subnets.
4. Scan the hosts and select one or multiple hosts from these to target.
5. Initiate an MITM attack using ARP poisoning on the selected target hosts.
6. Once the attack is successful, sniff the traffic sent or received by the hosts.

In this work, Ettercap is used to execute an MITM attack against hosts. Table 4.10 presents the IP address and MAC address information of the hosts and attackers. Figure 4.24 shows an attacker searching for available hosts in a subnet which can be targets. Figure 4.25 shows the IP and MAC addresses of the three hosts the MITM attacker was able to identify in the subnet. These can be targets for an attack.

Figure 4.26 shows that the attacker has selected two hosts as targets, Host1 with IP address 172.16.93.66 and Host2 with IP address 172.16.93.201. The attacker can now use ARP poisoning and spoof its MAC address into these hosts. Figure 4.27 shows ARP poisoning initiated by the attacker on the targets. After successful ARP poisoning, the attacker is able to spoof its MAC address on the targets. As a result, the MITM attacker can obtain any information shared between Host1 and Host2 in the network.

Figure 4.24: MITM attacker scanning the subnet for hosts to target.

Figure 4.25: List of hosts identified by the MITM attacker.

Figure 4.26: Hosts selected by the MITM attacker as targets.

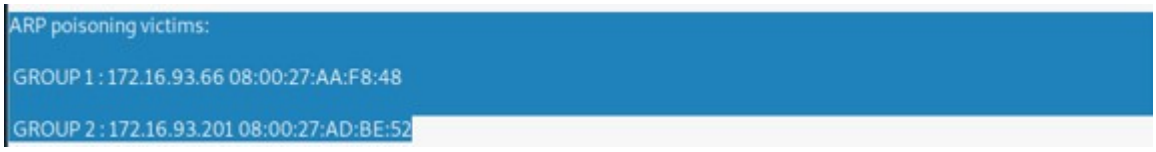

Figure 4.27: ARP poisoning of the victims by the MITM attacker.

4.3.2 Man-in-the-Middle Attack in a Normal Network

As noted above, the attacker selected Host1 and Host2 as targets and executed an MITM attack using ARP poisoning. Figure 4.28 shows the ARP table of Host1 before the MITM attack was executed. This table contains the peer (Host2) IP address 172.16.93.201 and MAC address 08:00:27:ad:be:52. Similarly, Figure 4.29 shows the ARP table of Host2 before the MITM attack was executed. This table contains the peer (Host1) IP address 172.16.93.66 and MAC address 08:00:27:aa:f8:48.

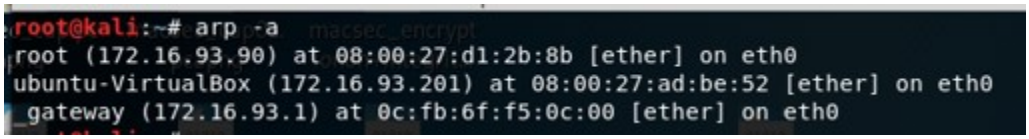

Figure 4.28: ARP table of Host1 before the MITM attack in a normal network.

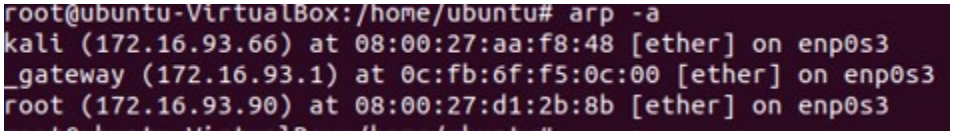

Figure 4.29: ARP table of Host2 before the MITM attack in a normal network.

After the MITM attack was executed, the attacker was able to spoof its MAC address to the MAC addresses of the hosts. Figure 4.30 shows the ARP table of Host1 after the MITM attack. This table contains the IP and MAC address information of Host2. However, the MAC address of Host2 (08:00:27:ad:be:52) is now replaced with the MAC address of the attacker (08:00:27:d1:2b:8b). This will result in any traffic forwarded from Host1 to Host2 to be diverted. Similarly, Figure 4.31 shows the ARP table of Host2 after the MITM attack. This table contains the IP and MAC address information of Host1. However, the MAC address of Host1 (08:00:27:aa:f8:48) is now replaced with the MAC address of the attacker (08:00:27:d1:2b:8b). This will result in any traffic forwarded from Host2 to Host1 to be diverted.

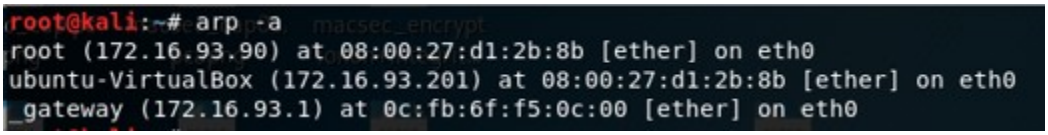

Figure 4.30: ARP table of Host1 after the MITM attack in a normal network.

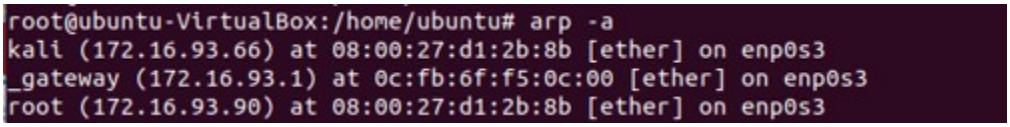

Figure 4.31: ARP table of Host2 after the MITM attack in a normal network.

Figure 4.32 shows the traffic capture for the MITM attacker. This indicates that the attacker is now in the middle of the targeted hosts and can sniff the traffic between Host1 and Host2. There were four ICMP packets, two ICMP requests and two ICMP responses generated with the same sequence number. Duplicate ICMP request and response packets are due to the MITM attack as every request packet sent by Host 1 to Host 2 is first received by the MITM attacker due to the successful spoofing of the IP and MAC address of Host2. Similarly, every response packet from Host2 to Host1 is first received by the MITM attacker since they have also spoofed the IP and MAC address of Host1. Therefore, any traffic exchanged between these hosts in a normal network will pass through the attacker affecting data confidentiality and integrity.

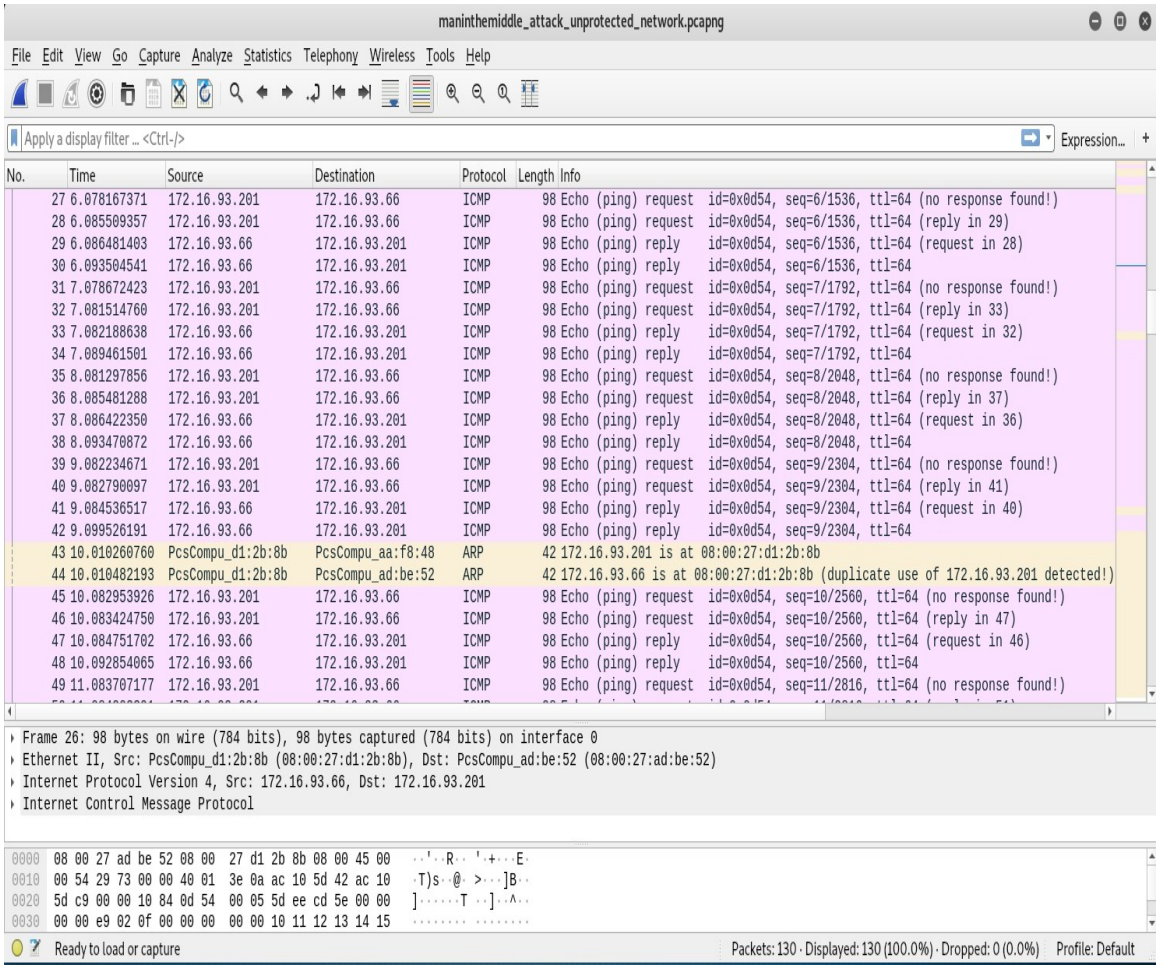

Figure 4.32: Traffic capture for the MITM attacker in a normal network.

4.3.3 Man-in-the-Middle Attack in a MACsec Protected Network

This subsection presents the results of a MITM attack against MACsec protected hosts. Figure 4.33 shows the ARP table of Host1 before the MITM attack was executed. This table contains the peer (Host2) IP address 10.10.12.2 and MAC address 08:00:27:ad:be:52. Similarly, Figure 4.34 shows the ARP table of Host2 before the MITM attack was executed. The ARP table contains the peer (Host1) IP address 10.10.12.1 and MAC address 08:00:27:aa:f8:48.

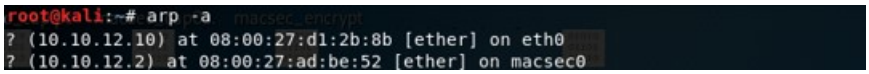

Figure 4.33: ARP table of MACsec protected Host1 before the MITM attack.

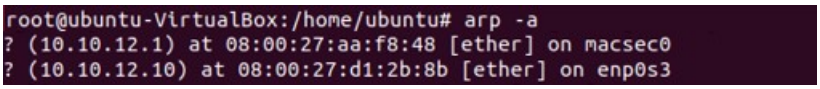

Figure 4.34: ARP table of MACsec protected Host2 before the MITM attack.

After the MITM attack against the MACsec protected hosts, the attacker was not able to spoof its MAC address to the MAC addresses of the hosts. Figure 4.35 shows the ARP table of Host1 after the MITM attack. This table contains the IP and MAC address information of the peer (Host2). The MAC address of Host2 (08:00:27:ad:be:52) has not changed as the attack was unsuccessful. Similarly, Figure 4.36 shows the ARP table of Host2 after the MITM attack. The ARP table contains the IP and MAC address information of the peer (Host1). The MAC address of Host1 (08:00:27:aa:f8:48) did not change as the attack was unsuccessful due to MACsec protection. These results show that the attacker cannot access information shared between MACsec protected hosts.

Figure 4.35: ARP table of MACsec protected Host1 after the MITM attack.

Figure 4.37 shows the packet capture for the MITM attacker in a MACsec protected network. There are no ICMP request or response packets shown since they were unable to sniff the traffic exchanged between MACsec protected hosts. As discussed in Chapter 2, in a MACsec protected network only authenticated peers which are part of the same secure

```
root@ubuntu-VirtualBox:/home/ubuntu# arp -a
? (10.10.12.1) at 08:00:27:aa:f8:48 [ether] on macsec0
? (10.10.12.10) at 08:00:27:d1:2b:8b [ether] on enp0s3
```

Figure 4.36: ARP table of MACsec protected Host2 after the MITM attack.

association can access the information. Therefore, the MITM attacker was not able to spoof its MAC address for an MITM attack. As a result, data integrity and confidentiality in MACsec protected networks cannot be compromised by an MITM attack.

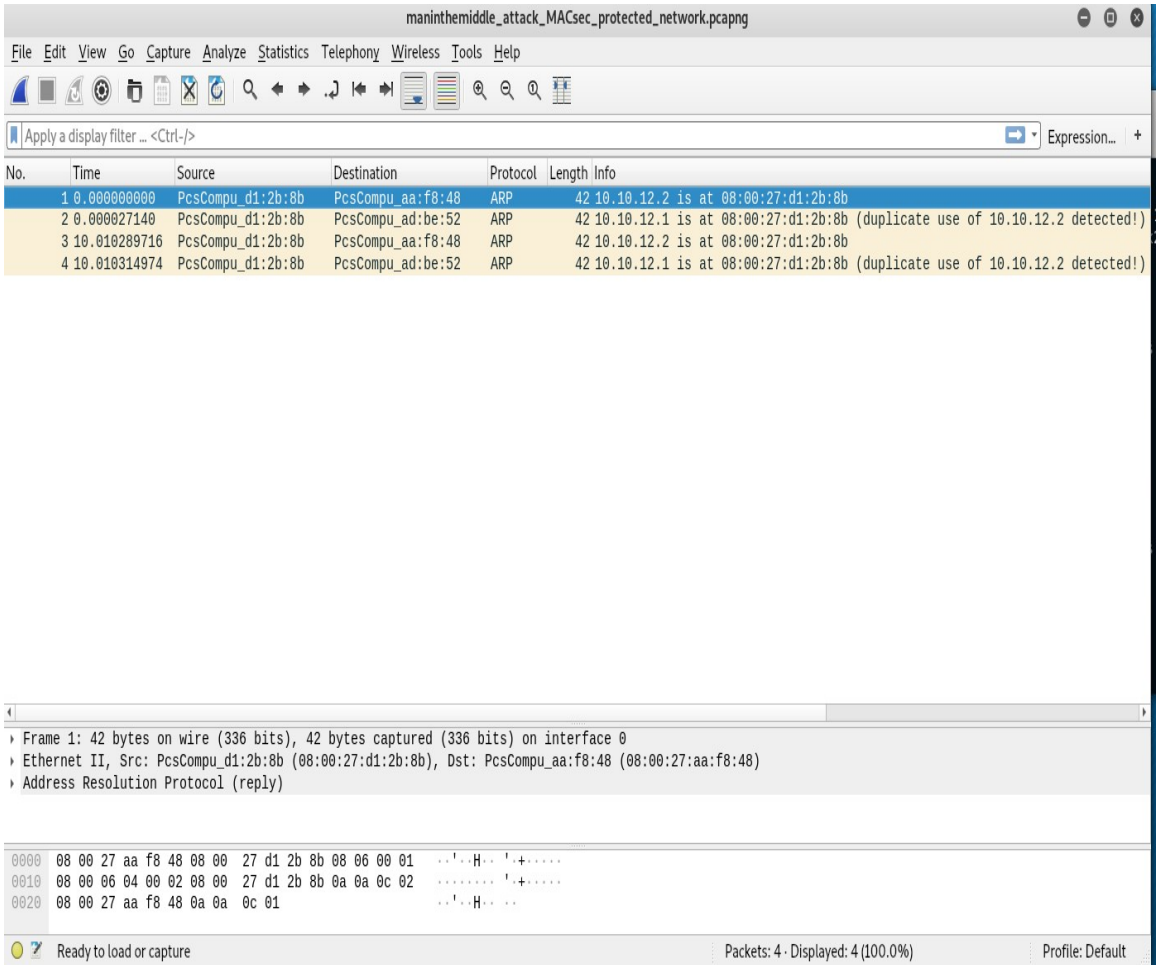

Figure 4.37: Traffic capture for the MITM attacker in a MACsec protected network.

Chapter 5

Conclusion and Future Work

Network traffic is vulnerable to data tempering in the form of attacks such as Denial of Service (DOS), replay, and Man-in-the-Middle (MITM) attacks. With the rapid increase in data being shared electronically, the problem of protecting data confidentiality and integrity has become very important. Thus, there is significant interest in security solutions which can protect all network traffic at layer 2. Furthermore, there is a need for a security solution that can provide end-to-end encryption of layer 2 data on Ethernet links.

In this work, a layer 2 security standard defined in IEEE 802.1AE, Media Access Control Security (MACsec), was implemented to secure traffic in Local Area Networks (LANs) and Wide Area Networks (WANs). The network performance was evaluated with and without MACsec to determine the additional overhead as a result of using MACsec. MACsec was also configured in a network to protect against MITM attacks.

The network performance metrics used were average throughput, average latency, average message rate, total number of bytes transmitted and received, average CPU utilization, and average Round Trip Time (RTT). MACsec was implemented with and without encryption and network performance was compared with that of a normal network. The MACsec protected LAN without encryption had increased network overhead. As a result, average throughput decreased by 7.85% and average latency increased by 2.64% in the LAN. In the WAN, average throughput decreased by 12.52% and average latency increased by 9.09%. MACsec with encryption further degraded the network performance due to the data encryption at the source and decryption at the destination. When a normal LAN was compared with a MACsec protected LAN with encryption, average throughput decreased by 11.42% and average latency increased by 5.82%. When a normal WAN was compared with a MACsec protected WAN with encryption, average throughput decreased by 17.83% and average latency increased by 10.90%.

Results were also obtained which show that MACsec can protect the network against MITM attacks. An MITM attacker was not able to spoof the MAC address and sniff the traffic exchanged between MACsec protected hosts. This is because MACsec provides end-to-end encryption of the data transmitted and received in the LAN and WAN.

5.1 Future Work

In the future, MACsec can be enhanced by using encryption offset inside the MACsec connectivity association to specify the number of octets in the MACsec encrypted frame to be sent unencrypted. It can be useful to have specific octets such as IPv4 and IPv6 headers in plain text for monitoring or security devices that are unable to handle encrypted traffic. MACsec can also be used in clear tag mode to leave IEEE 802.1Q tags (VLAN tags) in plain text for services such as Quality of Service (QoS) to apply network traffic prioritization policies based on VLAN association. Moreover, an analysis can be conducted to determine the effectiveness of MACsec in an enterprise network environment where other security technologies such as IPsec and 802.1x are also configured.

Bibliography

[1] Office of the Privacy Commissioner of Canada. *Privacy and cyber security emphasizing privacy protection in cyber security activities.* Research Group, Legal Services, Policy and Research, Office of the Privacy Commissioner of Canada, 2014.

https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2014/cs_201412/

[2] R. Deibert. *Distributed security as cyber strategy: Outlining a comprehensive approach for Canada in cyberspace.* Canadian Defence and Foreign Affairs Institute, 2012.

[3] P. Mutton. *95% of HTTPS servers vulnerable to trivial MITM attacks.* Netcraft, 2016.

https://news.netcraft.com/archives/2016/03/17/95-of-https-servers-vulnerable-to-trivial-mitm-attacks.html

[4] IBM. *X-Force threat intelligence index 2018.* IBM Security, 2018.

https://www.ibm.com/security/data-breach/threat-intelligence

[5] Juniper. *Understanding MACsec benefits.* Juniper Networks Inc., USA, 2014.

https://www.juniper.net/documentation/en_US/release-independent/nce/topics/concept/macsec-benefits-understanding.html

[6] S. Dubroca. *MACsec: A different solution to encrypt network traffic.* Red Hat Developers, Red Hat, 2016.

https://developers.redhat.com/blog/2016/10/14/macsec-a-different-solution-to-encrypt-network-traffic/

[7] P. Arau. *MACsec on Linux.* A networkers blog, Next Header, 2016.

https://nextheader.net/2016/10/14/macsec-on-linux/

[8] V. Tuure. *Configure MACsec in SDN.* Cyber Trust, Jyväskylä University of Applied Sciences, Finland, 2017.

https://gitlab.labranet.jamk.fi/cybertrust/public/blob/

[9] C. Serban. *MACsec over WAN.* Costiser Network Engineering, 2019.

https://costiser.ro/2019/10/08/macsec-over-wan/#.YDXeW-hKhPZ

[10] F. Hauser, M. Schmidt, M. Häberle and M. Menth. *P4-MACsec: Dynamic topology monitoring and data layer protection with MACsec in P4-based SDN.* IEEE Access, vol. 8, pp. 58845-58858, 2020.

[11] M. Wadekar. *Ethernet header.* Handbook of Fiber Optic Data Communication (Fourth Edition), Academic Press, 2013.

[12] Cisco. *WAN MACsec deployment,* White Paper. Cisco Systems, 2016.

[13] Arista. *MACsec configuration and operation,* White Paper. Arista Networks, 2019.

[14] S. Dubroca. *MACsec encryption for the wired LAN.* Proceedings of Netdev1.1, Seville, Spain, 2016.

[15] Juniper. *Cipher-suite (MACsec),* White Paper. Juniper Networks Inc., 2020.

[16] Cisco. *WAN MACsec and MKA support enhancements.* Cisco Systems, 2020.
`https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/macsec/configuration/xe-16/macsec-xe-16-book/wan-macsec-mka-support-enhance.html`

[17] Juniper. *MACsec confidentiality offset,* White Paper. Juniper Networks Inc., 2020.

[18] B. Bhushan, G. Sahoo, and A. K. Rai. *Man-in-the-middle attack in wireless and computer networking — A review.* Proceedings of the International Conference on Advances in Computing, Communication and Automation, pp. 319-322, Chennai, India, 2017.

[19] B. Dobran. *What are man in the middle attacks and how to prevent MITM attack with examples.* PhoenixNAP Global IT Services, 2019.
`https://phoenixnap.com/blog/man-in-the-middle-attacks-prevention`