SECURITY ANALYSIS FOR ARP CACHE POISONING ATTACKS USING DS-ARP AND S-ARP

KHING SHWE YE PHU

M.C.Sc. **SEPTEMBER 2022**

SECURITY ANALYSIS FOR ARP CACHE POISONING ATTACKS USING DS-ARP AND S-ARP

By

KHING SHWE YE PHU

B.C.Sc.

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

Master of Computer Science

(M.C.Sc.)

University of Computer Studies, Yangon

September 2022

ACKNOWLEDGEMENTS

I would like to take this opportunity to express my sincere thanks to those who helped me with various aspects of conducting research and writing this thesis. To complete this thesis, many things are needed like my hard work as well as the supporting of many people.

First and foremost, I would like to express my deepest gratitude and my thanks to **Dr. Mie Mie Khin,** Rector, the University of Computer Studies, Yangon, for her kind permission to submit this thesis.

I would like to express my appreciation to **Dr. Si Si Mar Win and Dr. Tin Zar Thaw,** Professor, Faculty of Computer Science of the University of Computer Studies, Yangon, for their superior suggestions, administrative supports and encouragement during my academic study.

My thanks and regards go to my supervisor, **Dr. Tin Tin Htar,** Associate Professor, Department of Information Technology Support and Maintenance, the University of Computer Studies, Yangon, for her support, guidance, supervision, patience and encouragement during the period of study towards completion of this thesis.

I also wish to express my deepest gratitude to **Daw Win Lai Lai Bo**, Assistant Lecturer, Department of English, the University of Computer Studies, Yangon, for her editing this thesis from the language point of view.

Moreover, I would like to extend my thanks to all my teachers who taught me throughout the master's degree course and my friends for their cooperation.

I especially thank to my parents, all of my colleagues, and friends for their encouragement and help during my thesis.

STATEMENT OF ORIGINALITY

I hereby certify that the work embodied in this thesis is the result of original research and has not been submitted for a higher degree to any other University or Institution.

…… ……

Date Khing Shwe Ye Phu

ABSTRACT

Address Resolution Protocol (ARP) is a very popular communication protocol in the local area network (LAN), working under the network layer, as per the open systems interconnection (OSI) model. ARP is used by computers to map logical addresses (IP) to physical addresses (MAC). However ARP is an all trusting protocol and is stateless which makes it vulnerable to many ARP cache poisoning attacks such as Man-in-the-Middle (MITM) and Denial of Service (DoS) attacks. These flaws result in security breaches thus the weakness of the computer can be found for exchanging of sensitive data. This system describes ARP, outline several possible ARP cache poisoning attacks and gives the detailed of some attack scenarios in network having wireless hosts. Hence, this system presents a DS-ARP that is able to cope up with all these types of attacks and is also a feasible solution. For the proposed system evaluation, this system will be compared with S-ARP protocol.

Keywords: **ARP, DoS, Man-in-the-Middle, DS-ARP, S-ARP**

CONTENTS

			Page
ACKNOWLEDGEMENTS			**i**
ABSTRACT			**iii**
CONTENTS			**iv**
LIST OF FIGURES			**vi**
LIST OF TABLES			**viii**
CHAPTER 1	**INTRODUCTION**		**1**
	1.1	Objectives of the Thesis	1
	1.2	Organization of the Thesis	2
CHAPTER 2	**BACKGROUND THEORY**		**3**
	2.1	Related Work	3
	2.2	Address Resolution Protocol (ARP)	3
		2.2.1 ARP Messages	5
		2.2.2 ARP Request and ARP Reply in ARP	7
		2.2.3 ARP Cache	8
	2.3	ARP Cache Poisoning	8
		2.3.1 ARP Cache Poisoning Methods	10
	2.4	Wireless Networks	11
		2.4.1 Modes of Wireless LANs	11
		2.4.2 Wireless Access Point	12
	2.5	ARP Cache Poisoning in Wireless Networks	13
		2.5.1 Attacks Scenarios	14
CHAPTER 3	**SECURE ADDRESS RESOLUTION PROTOCOL (S-ARP) AND DETECTION SCHEME ADDRES RESOLUTION PROTOCOL (DS-ARP)**		**19**
	3.1	S-ARP	20
		3.1.1 Message Format	20
	3.2	DS-ARP	21
		3.2.1 Operation Processes of DS-ARP	22
CHAPTER 4	**SYSTEM DESIGN AND IMPLEMENTATION**		**24**
	4.1	System Implementation	24

4.1.1 Sending ARP Request Frame from Sender to Receiver 27
4.1.2 Replying ARP Request by Receiver to Sender 31
4.1.3 Replying ARP Request by Attacker to Sender 36
4.2 Experimental Results 37
CHAPTER 5 CONCLUSION, LIMITATIONS AND FURTHER EXTENSIONS **40**
5.1 Conclusion 40
5.2 Limitations and Further Extensions 41
AUTHOR'S PUBLICATIONS **42**
REFERENCES **43**

LIST OF FIGURES

Figure		Page
Figure 2.1	The Architecture of the TCP/IP Reference Model	5
Figure 2.2	Format of an ARP Message	6
Figure 2.3	Host A Broadcasts Request for Host D	7
Figure 2.4	Host D Replies to Host A	8
Figure 2.5	Host C Performing the ARP Poisoning Attack on Host A and Host B	9
Figure 2.6	Denial-of-Service Attack	9
Figure 2.7	Man-in-the-Middle Attack	10
Figure 2.8	Infrastructure Mode	11
Figure 2.9	Ad-hoc Mode	12
Figure 2.10	General Set-Up of Wireless Network with the Wired Network	13
Figure 2.11	Wireless Client Attacking Wired Clients	15
Figure 2.12	Wireless Client Attacking a Wired Client and a Wireless Client	15
Figure 2.13	Attacking Wireless Clients	16
Figure 2.14	Attacking Roaming Wireless Hosts	16
Figure 2.15	Combined Home Gateway Device	17
Figure 2.16	Attacking Two Wired Clients via a Wireless Client in a Home Deployment	17
Figure 2.17	Attacking a Wired Client and a Wireless Client in a Home Network	18
Figure 3.1	S-ARP Packet Extension	21
Figure 3.2	The Architecture if DS-ARP	22
Figure 3.3	The Sequence Diagram of DS-ARP	23
Figure 4.1	Overall System Design	24
Figure 4.2	The System Flow of DS-ARP	25
Figure 4.3	The System Flow of S-ARP	27
Figure 4.4	Sender’s Login Page	28
Figure 4.5	Sender’s Main Page and Member List Page	29
Figure 4.6	Checking Receiver’s IP Address and MAC Address in Sender’s ARP Cache	30

Figure 4.7	Sending ARP Request to All Members	30
Figure 4.8	Check Sender's IP Address and MAC Address in Receiver's ARP Cache	31
Figure 4.9	Receiver Replies to Sender by S-ARP	32
Figure 4.10	Protection Stage	33
Figure 4.11	Detection Stage	33
Figure 4.12	Management Stage	34
Figure 4.13	Receiver Replies to Sender by DS-ARP	34
Figure 4.14	Sender Checks Ticket and Send Message to Receiver	35
Figure 4.15	Receiver Receives Sender's Message	35
Figure 4.16	Attacker Replies to Sender by MITM	36
Figure 4.17	Attacker Replies to Sender by DoS	36
Figure 4.18	Noticeable Stage by Sender	37
Figure 4.19	MITM Attack Detection Time Comparison	38
Figure 4.120	DoS Attack Detection Time Comparison	38

LIST OF TABLES

Table		Page
Table 2.1	OSI Model Layers	4
Table 4.1	Procedure of DS-ARP	26
Table 4.2	Procedure of S-ARP	26
Table 4.3	Comparison of Defense Methods of ARP Cache Poisoning Attack	39

CHAPTER 1

INTRODUCTION

The Network layer is where the Address Resolution Protocol (ARP) resides. Each PC in a LAN has a physical (MAC) address as well as an effective (IP) address. The MAC address of the destination machine is normal by the source machine in order to transmit something explicitly from one system to another in the same or different network(s). It is therefore assumed that an arrangement has been made between the IP address and the MAC address in order to obtain the actual MAC address of the source if it is missing from the ARP hold of source. ARP is thus employed. From this, it will be clear that ARP is a stateless protocol and a crucial component of the association layer. Computers employ the Address Resolution Protocol (ARP) to map logical addresses (IP) to physical addresses (MAC). However, because ARP is a stateless, all-trusted protocol, it is vulnerable to a variety of ARP cache poisoning attacks, including Man-in-the-Middle (MITM) and Denial of Service (DoS) attacks. The appeal of using computers to share sensitive data is diminished as a result of these weaknesses, which lead to security breaches. This system provides an explanation of ARP, lists numerous potential ARP cache poisoning attacks, and provides thorough information on several attack scenarios in networks with wireless hosts. Since all of these forms of attacks can be handled by DS-ARP, it also offers a feasible solution. The proposed system is compared with S-ARP protocol according to the detection time.

1.1 Objectives of the Thesis

The main objectives of this thesis are:

- To retain all of the good points of the ARP but blocks off its security weaknesses by stateful protocol
- To defense the cache poisoning attacks on ARP
- To present a good solution that does not require any additional host, new device or switches to be added to the network
- To compare DS-ARP and S-ARP in execution time

1.2 Organization of the Thesis

The thesis is organized into five chapters. In Chapter (1), introduction of the system, objectives of the thesis and thesis are described. In Chapter (2), related work and the background theory of address resolution protocol is presented. The Chapter (3) discusses about the control of data security on network. In Chapter (4), the design and implementation of the proposed system is expressed. In the final Chapter (5), the conclusions, advantages and limitations, and further extensions of the system are presented.

CHAPTER 2

BACKGROUND THEORY

This chapter describes what ARP is, how the protocol functions, and how ARP interacts with other systems. First, in a local-area network, the Address Resolution Protocol (ARP), also known as Media Access Control (MAC) address, links a dynamic Internet Protocol (IP) address to a fixed physical machine address (LAN). The primary function of ARP is to translate the 32-bit IP address to a 48-bit address because it is one of the most significant network layer protocols that aids in determining the MAC address given the system's IP address.

2.1 Related Work

PCs design authentic addresses (IP) to genuine addresses using the Address Resolution Protocol (ARP). ARP can withstand such a wide variety of attacks and is also a helpful design. It is a state-ful display that reduces the potential effects of various ARP attacks by maintaining the Request frame information in the ARP store. By distributing ARP Reply frame around the organization and taking care of pertinent areas in the ARP hold each time correspondence occurs, it is more practical and secure [1].

Undoubtedly, one of the fundamental components of the Internet and the majority of IP networks is the Domain Name System (DNS). Despite the fact that the Domain Name System is enormous, only a small percentage of people have even heard of it. Information confirmation is necessary in the majority of DNS trades. Given its crucial role, DNS is trapped in sophisticated Internet attacks that target both the actual system and other Internet resources. This structure impedes DNS and has flaws, as well as several attacks on the DNS framework [2].

2.2 Address Resolution Protocol (ARP)

As illustrated in Table 2.1 [15], the Open Systems Interconnection (OSI) model, which serves as the industry standard for association designing, has seven layers. The TCP/IP association plan is currently used by the majority of obvious

associations. Figure 2.1 juxtaposes the OSI model and the TCP/IP model to illustrate how the TCP/IP model's different layers fit into the OSI model's layering scheme. The picture also arranges the various shows according to the layer in which they operate within the TCP/IP paradigm.

From the base up, the layers are numbered 1 through 7. For instance, the application layer and the genuine layer both must be layers 1 and 7, respectively. An IP address, a 32-cycle number, is used to identify a host in the Network layer or layer 3 of the TCP/IP suite. In any event, the TCP/IP suite's Medium Access Control (MAC) layer, sometimes known as layer 2, follows a different pattern. A 48-piece MAC address recognizes an association point in the MAC layer.

Layer 3 validates the IP address of the goal machine when it receives a group from upper layers. The pack can be sent directly to the goal machine if it is in the same extremely near proximity as the sending machine; otherwise, the IP bundle needs to be coordinated through a switch. The association layer must comprehend the goal machine's MAC address in order to send the pack to it plainly. The Address Resolution Protocol (ARP) is used for this by the TCP/IP suite's association layer. ARP continually converts a machine's 48-bit MAC address from its 32-digit IP address.

Table 2.1: OSI Model Layers

Application Layer
Presentation Layer
Session Layer
Transport Layer
Network Layer
Logical Link Layer
Physical Layer

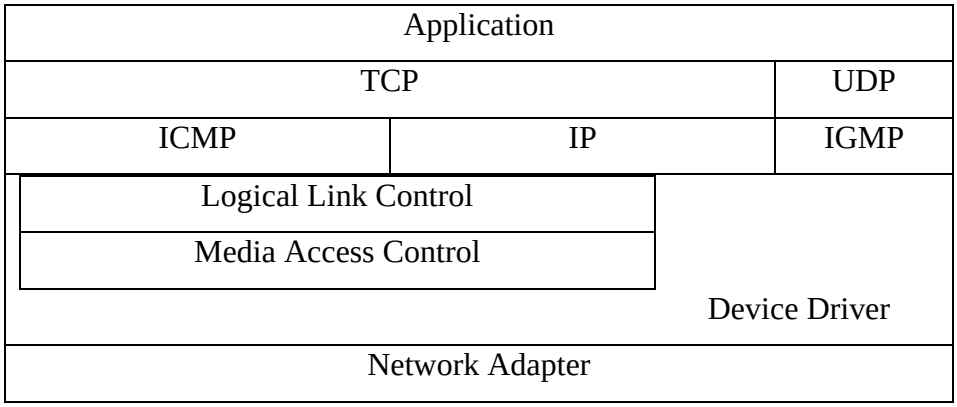

Figure 2.1: The Architecture of the TCP/IP Reference Model

Let's say we type the following order: ftp 10.40.68.22

The following activities take place:

1. The FTP client requests that the TCP layer establish a connection with the pending request.
2. TCP delivers an IP datagram including an affiliation request segment to the target IP address.
3. The IP address is converted into a 48-bit Ethernet address by ARP if the target IP address is on a nearby association.
4. Who owns 10.40.68.22? Tell 10.40.68.50 in an ARP interest sent over Ethernet to all of the hosts in its nearby association (Assuming 10.40.68.50 is the IP address of the referencing machine).
5. Every host that receives an ARP request checks to see if the target IP address is present.
6. The host with the IP address 10.40.68.22 will respond to an ARP request with the message, "10.40.68.22 is at 00:0f:d2:ce:43:12," along with its MAC address.
7. After receiving the ARP response from the sender machine, the IP datagram is delivered to the destination machine.

2.2.1 ARP Messages

There are four types of messages in the ARP protocol:

- ARP Request
- ARP Reply

- RARP Request
- RARP Reply

0	8	15 16	31
Hardware Type		**Protocol Type**	
HLEN	**PLEN**	**Operation**	
Sender HA (octets 0-3)			
Sender HA (octets 4-5)		**Sender IP (octets 0-1)**	
Sender IP (octets 2-3)		**Target HA (octets 0-1)**	
Target HA (octets 2-5)			
Target IP (octets 0-3)			

Figure 2.2: Format of an ARP Message

Coming up next are the fields of an ARP message:-

Equipment Type - Specifies what the hidden equipment is. Model, Ethernet

Convention type-Specifies the sort of convention over this layer

HLEN - Specifies the length of the equipment address

PLEN - Specifies the length of the Protocol (Example IP) address

Activity - Specifies what kind of ARP message it is.

Shipper HA-Hardware Address/MAC address of the sending machine

Shipper IP - IP address of the sending machine

Target IP - Target IP address of the objective machine

Target HA - Hardware Address/MAC address of the objective machine

- ARP Request - When a host sends an ARP request, it includes its IP address, the MAC address, the objective IP address, and the kind of ARP message. All hosts in a LAN that is similar to the sender host receive the ARP request. The host with the objective IP address is left to fill in the objective HA.
- ARP Reply - When a host receives an ARP request with its own IP address as the objective IP address, it enters its MAC address in the objective HA field. The transporter and target fields' potential gains are pivotal, and the operation field is set to the ARP reply's opcode when the host sends an ARP reply. The referenced machine is the only recipient of this package after that.

- RARP Request - Reverse Address Resolution Protocol (RARP) is the antithesis of ARP. When a device needs to find the IP address that links with its MAC address, it sends a RARP request. In the LAN, RARP requests are transmitted.
- RARP Reply - RARP servers transmit RARP Reply. A response is delivered with the corresponding IP address if the MAC address in the RARP request matches one of the clients the RARP server serves.

The IP address of the referring computer is obtained from the RARP request and RARP reply packets as they are delivered off. When RARP messages are transmitted or received, they have no effect on the ARP hold. This makes RARP messages fully incompatible with the ARP Cache Poisoning. Similar to how most organizations employ a static IP address plan or the Dynamic Host Control Protocol (DHCP), RARP usage isn't common.

Before they are transmitted over the network, ARP messages are sampled inside an Ethernet header.

2.2.2 ARP Request and ARP Reply in ARP

Machine A needs to send a package to machine D, but A main knows D's IP address. According to Figure 2.3, Machine A transmits an ARP request with IP address D.

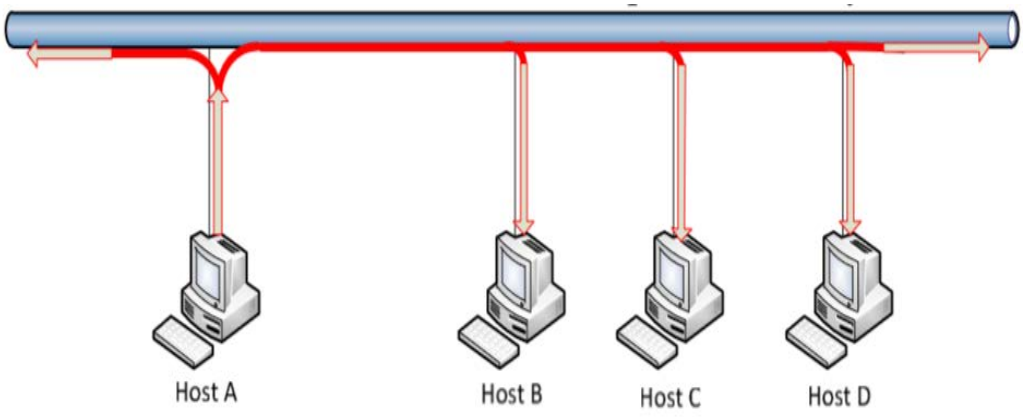

Figure 2.3: Host A Broadcasts Request for Host D

All machines inside the local organization receive the sent ARP Request. As seen in Figure 2.4, Machine D responds with its MAC address through a unicast ARP Reply and updates D's ARP save with MAC of A. D's MAC address is added to

Machine A's ARP hold. As of right now, Machine A can definitely send the group on to D.

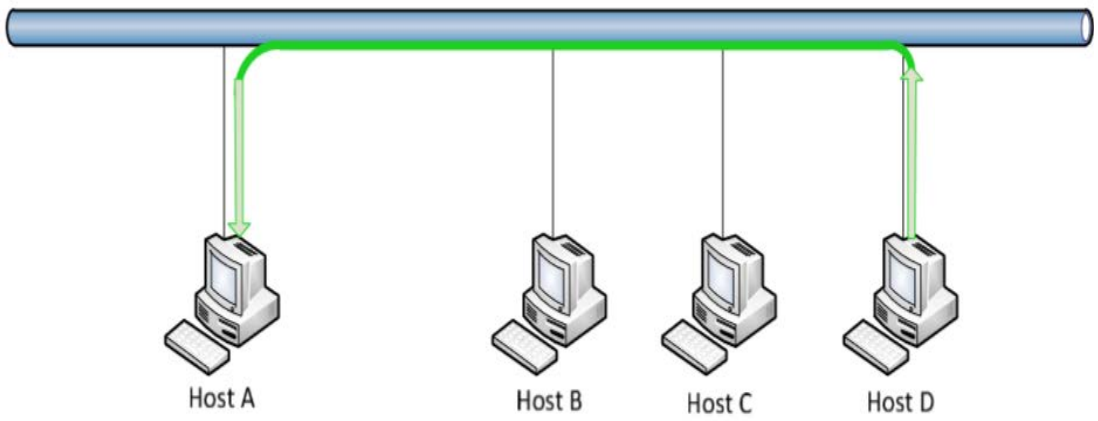

Figure 2.4: Host D Replies to Host A (unicast)

2.2.3 ARP Cache

Each host's ARP layer maintains a database of the conversion of IP address to MAC address for recently assigned IP addresses in an effort to reduce network traffic. Once more, this store is only briefly kept in mind, and when its break passes, the part is abandoned; if it is reached, the break is reinstated. In the following situations, a section in the ARP store is created or updated:-

- A host creates a segment in its ARP store for the preparation of the transporter's IP address to the source's MAC address just before sending an ARP reply to the machine that sent the ARP interest.
- Exactly when a host receives an ARP interest from another host, the segment will be revived if an entry connecting with the IP address of the sender host exists in its ARP store.

2.3 ARP Cache Poisoning

By delivering a fake ARP reply, an attacker can fraudulently alter the mapping of an IP address to its corresponding MAC address in another host's ARP cache. This technique is known as ARP cache poisoning. Therefore, this method is also known as ARP spoofing. The attacker in the following figure is Host C. By sending a faked ARP reply to Host A stating that IP address of Host B maps to MAC address of Host C and a spoofed ARP reply to Host B stating that IP address of Host A maps to MAC

address of Host C, it carries out the ARP Cache Poisoning attack. Since ARP is a stateless protocol, replies are not compared to open requests. A malicious host is vulnerable to the ARP cache poisoning attack, which has a significant impact on same network.

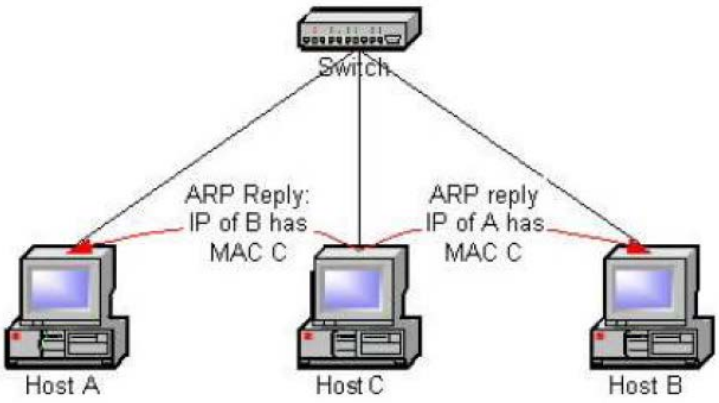

Figure 2.5: Host C Performing the ARP Poisoning Attack on Host A and Host B

A Denial-of-Service attack aims to prevent the intended users from accessing a computer resource. It typically entails the coordinated activities of one or more individuals to hinder the service's ability to operate effectively. When the attacker does not transfer the packets to the actual destination machine after reading them, it differs slightly from an MITM attack. The attacker in the following figure is Host C. After reading the packets, host C does not send them on to the destination node.

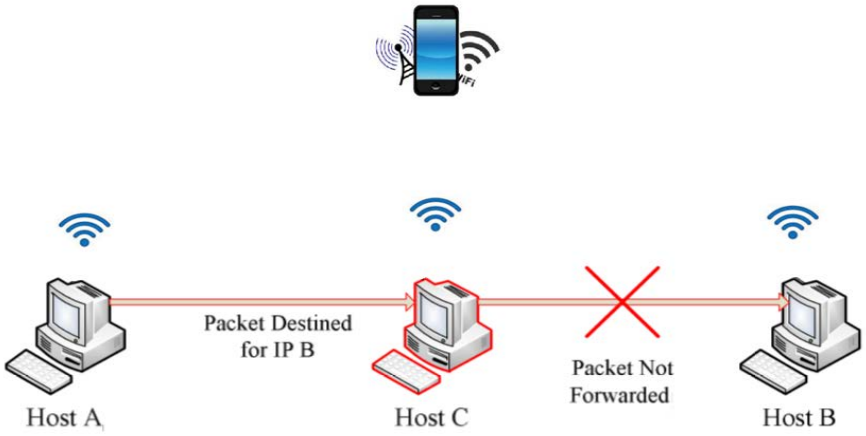

Figure 2.6: Denial-of-Service Attack

Host A and Host B won't even be aware that they are being attacked if Host C forwards the packets to the true destination machine after reading them. This is a Man-in-the-Middle attack, where the attacker can force traffic between two machines

to go through him instead of the other way around. Host C is the attacker in Figure 2.7. The traffic between two machines can be redirected to pass through Host C.

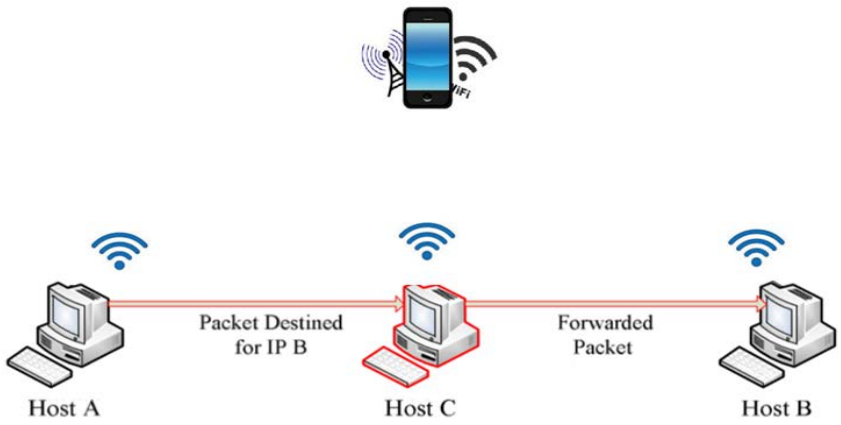

Figure 2.7: Man-in-the-Middle Attack

Once the ARP stores of Host A and Host B are hurt, Host A will send all the traffic headed for Host B, to Host C. Similarly Host B will send all traffic headed for Host A, to Host C. Have C can now examine all the traffic between Host A and Host B. If Host C advances the packages, resulting to grasping them, to the veritable goal machine, then Host A and Host B will not distinguish that they are being gone after.

2.3.1 ARP Cache Poisoning Methods

ARP Cache Poisoning can be avoided using any of the following two techniques: (1) Unsolicited response and (2) Request.

Unsolicited response:

- Any host may send an amusing ARP response, and the receiving host will update its ARP database.
- All hosts in the LAN could receive a mock ARP response, which would damage the ARP reserve of the comparatively large number of hosts with just one message.

Request:

- Whether or not a host had significant sales, the ARP layer in the host will reactivate its ARP hold in response to the arrangement indicated in

the source IP and source MAC address fields of the ARP request group [10]. To harm the security of the several hosts in a LAN, an attacker only needs to deliver a spoof ARP interest (naturally transmitted).

Response to a request:

- A malicious device in a LAN has the ability to transmit a mock ARP response in response to a certified ARP interest. The certified ARP reply and the inflated ARP reply can arrive at the referring host in a race circumstance. The most recent ARP response will be used to revive the ARP storage.

2.4 Wireless Networks

Radio waves are used by hosts in wireless networks, often known as Wireless LANs (WLANs).

2.4.1 Modes of Wireless LANs

There are two methods of WLANs:-

- Foundation mode - In this type of WLAN, each remote client communicates with a base station or a conduit (AP). The tunnel functions as a connection to the wired organization, which serves as the WLAN's skeleton.

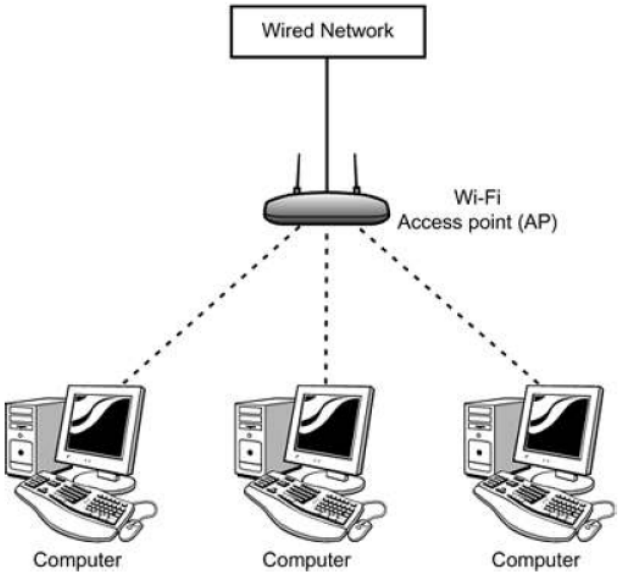

Figure 2.8: Infrastructure Mode

- Ad-hoc mode - In this mode, wireless clients can communicate with one another directly without using a centralized server.

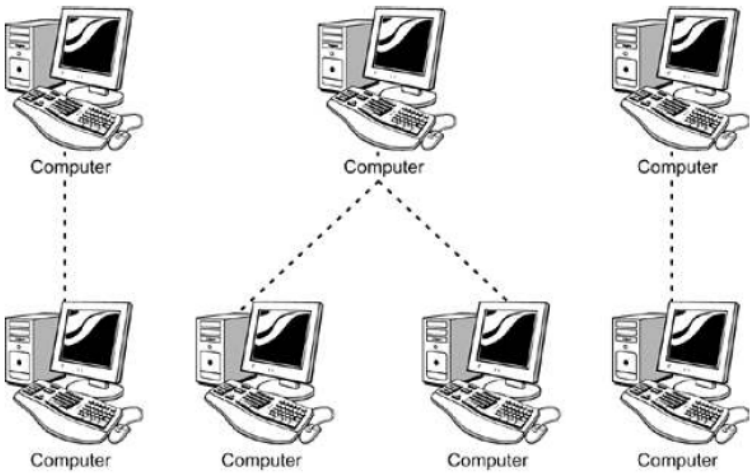

Figure 2.9: Ad-hoc mode

We might consider the WLAN foundation approach for this assignment. When a distant client tries to contact the wired clients via a remote AP or a remote switch to which they are fully connected, the risk of ARP Cache Poisoning increases. The remote hardware that the remote clients and wired clients are typically connected to is absent in specially assigned mode. Therefore, the problem is with the WLAN framework technique.

2.4.2 Wireless Access Point

The establishment mode allows for simple section-to-section communication between remote clients. The method decodes the radio waves received from distant clients and transmits them via an Ethernet connection to the Internet. In a similar manner, information obtained from a wired connection is converted into radio waves and sent to distant clients.

The search for open access points is made by a distant client who intends to join a distant association. Each access point consistently transmits messages to inform distant stations of its availability. The sign receives a Service Set Identification (SSID) from the access point that distinguishes one connection from another. The remote client sends a connection request to the access point after it has located the area it needs to connect to. The handshake communication between the remote client and the AP combines the exchange of data regarding the association and check. The

AP will verify the distant client and initiate network communication with the distant client from that point forward.

The client must cut off its connection to the AP once it has finished using the remote connection. The client's relationship will end if they don't detach and don't exclude the association for a set amount of time.

Items that make up the access point:-

- Facilitates communication between two distant stations that are conversing with one another.
- Serves likely as a platform between the wired 802.3 association and the 802.11 association.

2.5 ARP Cache Poisoning in Wireless Networks

ARP store harming is an attack that cannot be avoided on LANs; hence, all hosts connected to the same switch or focus as malicious hosts are defenseless against it. Ways function as hubs for remote associations and as extensions between those associations and wired networks. Figure 2.10 depicts the general strategy of a remote association connected to a wired LAN.

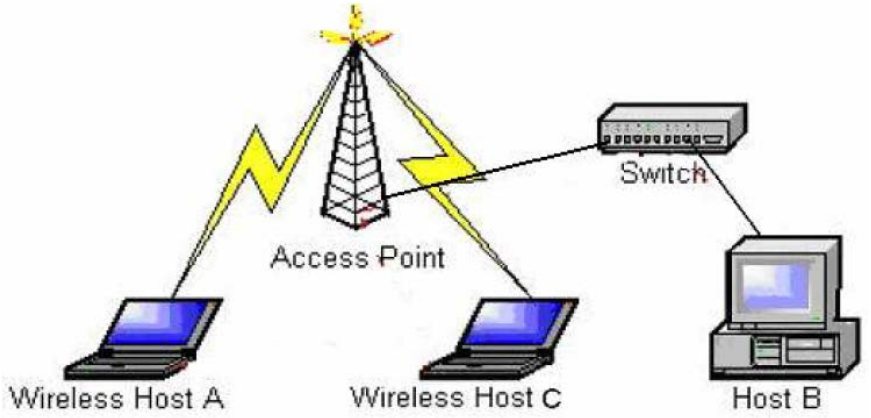

Figure 2.10: General Set-Up of Wireless Network with the Wired Network

The wired clients are connected to the exact switch that the access point is connected to, as shown in the plan in Figure 2.10. Every message sent from remote hosts A and C is received by wired host B. All of the machines connected to a switch are consolidated in an association's transmission space. Here, the AP and switch are connected, and any distant hosts associated with that AP have a place in the switch's transmission area. Additionally, the wired clients that are directly connected to the

switch are inside its transmission region. In a LAN, ARP requests are transmitted. As a result, the ARP requests are received by all the sites in the transmission region. As a result, the wired hosts connected to the same switch as the AP are rendered defenseless against an attack from distant clients.

In general, in troubled areas like bistros, car dealerships, etc. Clients with remote hosts will receive an access point to connect with the distant association. The overall strategy is such that the wired hosts in the bistro will also be related to the AP through a change. The wired hosts can be exchanging sensitive information. If a malicious distant client uses ARP Cache Poisoning in an MITM attack, it can be useful to examine this information.

Whether or whether the remote clients are in a remote association equipped with security mechanisms like Wired Equivalent Privacy (WEP) or Wi-Fi Protected Access (WPA), the ARP store damaging attack can still be carried out. The Layer 2 bundles are masked by WEP and WPA. ARP is a Layer 3 show because it is on the same layer as IP. In a remote association, the damaged ARP packs are therefore conveyed inside a WEP or WPA encoded frame. All packages transmitted by the remote clients who are conducting the ARP store damaging attack have recently joined the association, and as a result, all of their packages are intermingled. Since these packets are WEP or WPA encrypted with the first chosen key, the Access Point will recognize them and send them to the target distant machine. The box is opened as soon as the group arrives at the target machine, and the mocked arrangement is examined via the ARP frame. The counterfeit preparation revives the ARP hold, harming the ARP storage.

2.5.1 Attack Scenarios

ARP attacks are subject to a variety of situations. The following describes a few scenarios.

- **Attacking wired clients using a wireless client:**

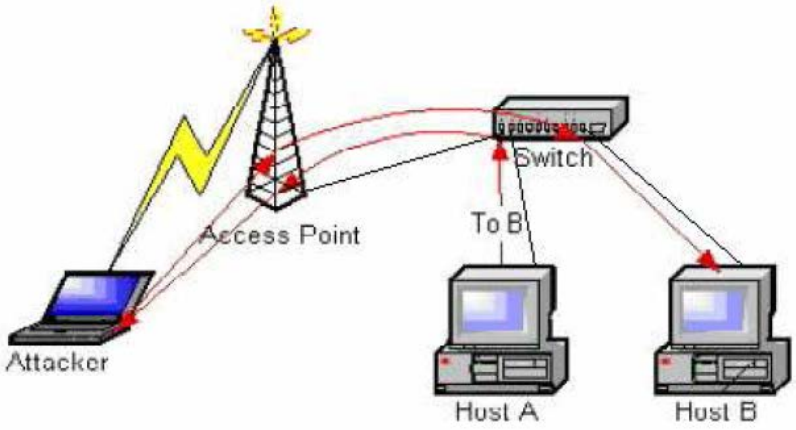

Figure 2.11: Wireless Client Attacking Wired Clients

In the current situation, a distant client called the Attacker sends a bogus ARP package to Host A informing it that the IP address of Host B is needed for the Attacker's MAC address. In relation to this, the Attacker informs Host B via a mocked ARP package that Host A's IP address contains the Attacker's MAC address. By damaging Hosts A and B's ARP stores in this way, the Attacker forces all traffic between them to pass via him.

- **Attacking a wireless client and a wired client:**

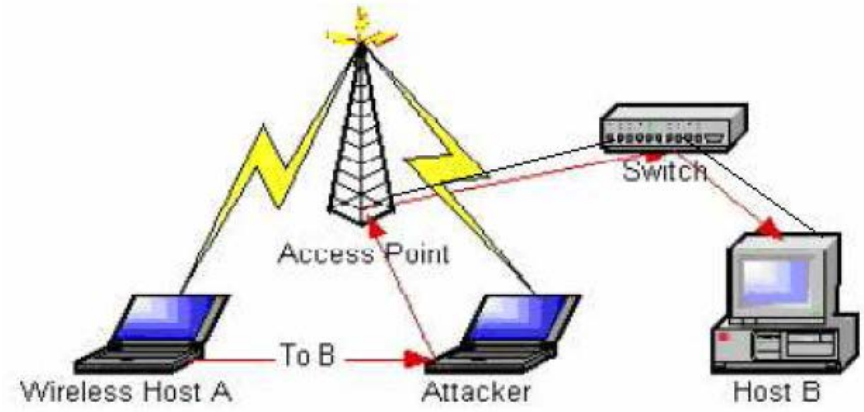

Figure 2.12: Wireless Client Attacking a Wired Client and a Wireless Client

In Figure 2.12, the Attacker damages the ARP storage of wired Host B and wireless Host A by sending parody ARP packets to those hosts. Due to the fact that both casualties are in the same area as the attacker, mock ARP bundles will eventually reach the target population.

- **Attacking wireless hosts:**

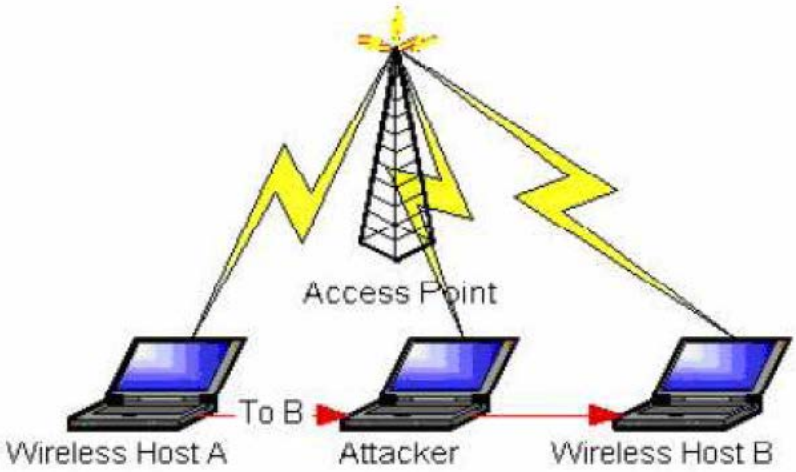

Figure 2.13: Attacking Wireless Clients

Two wireless hosts that are connected to the same AP as the attacker and are in its broadcast domain are also vulnerable to attack by the attacker.

- **Attacking roaming wireless hosts:**

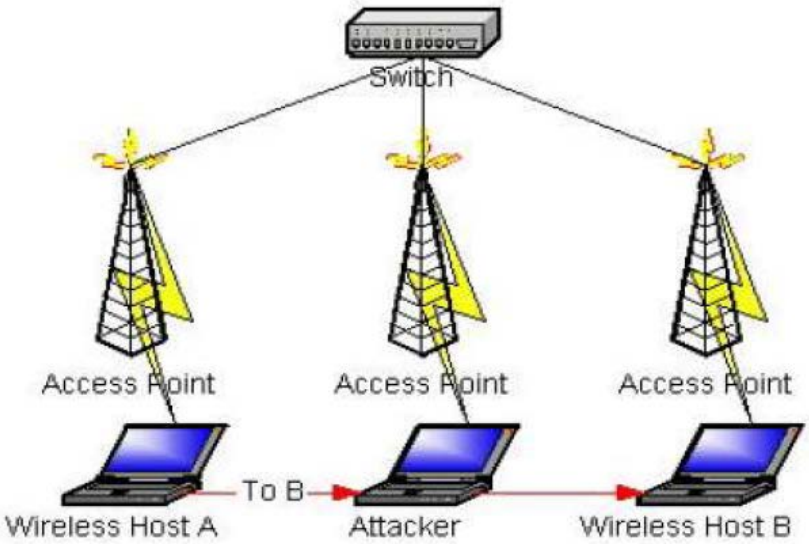

Figure 2.14: Attacking Roaming Wireless Hosts

Different APs are connected to a similar switch in Figure 2.14. The APs in 802.11b organizations need to be connected to a comparable switch in order to implement meandering. Due to this configuration, each remote host connected to these APs has a spot in a comparable transmission space. Any fake ARP bundle sent by the Attacker can therefore reach any remote host connected to any of these APs.

- **Attacking home networks:**

As shown in Figure 2.15, the majority of retailers sell a combined switch, switch, and passage in one device. In these devices, the AP is for remote hosts in the LAN, the switch is for wired clients in a similar LAN, and the switch is for the clients to connect to their Internet Service Provider (ISP). Such a device satisfies the criteria for a home network.

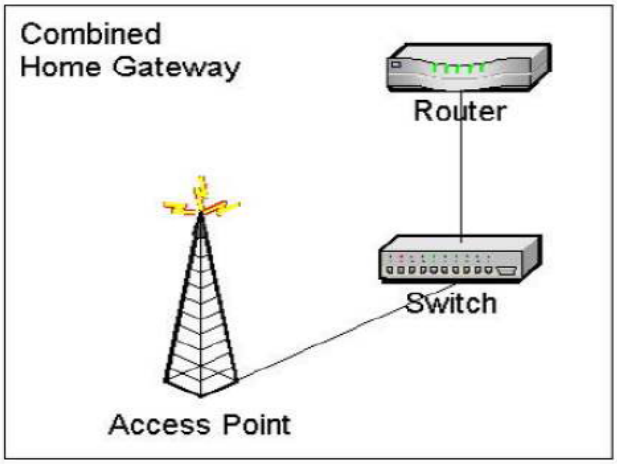

Figure 2.15: Combined Home Gateway Device

The AP is connected to the same switch as the wired clients in this hybrid device. As a result, wired clients are defenseless against a distant client's ARP Cache Poisoning attack. The previously indicated attack scenarios from 2.4.1.1 - 2.4.1.2 are also possible on home organizations with this combined house door device, as shown in Figures 2.16 and 2.17.

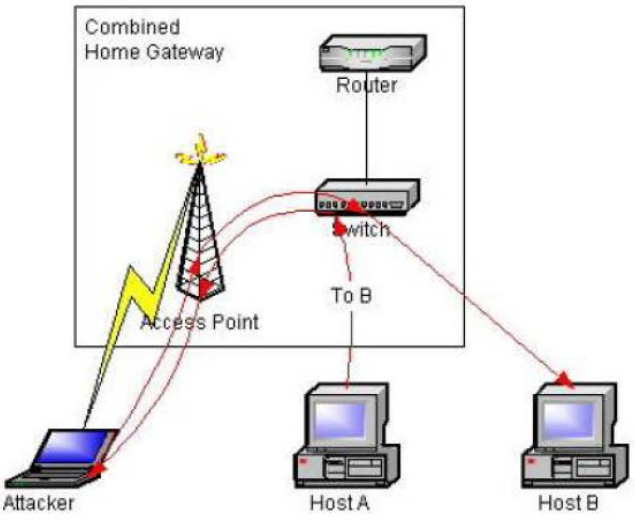

Figure 2.16: Attacking Two Wired Clients via a Wireless Client in a Home Deployment

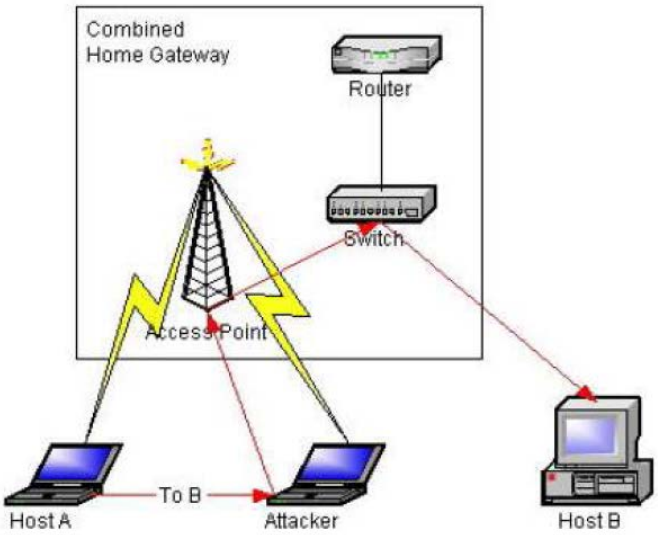

Figure 2.17: Attacking a Wired Client and a Wireless Client in a Home Network

CHAPTER 3

SECURE ADDRESS RESOLUTION PROTOCOL (S-ARP) AND DETECTION SCHEME ADDRESS RESOLUTION PROTOCOL (DS-ARP)

The 48-bit Ethernet address determines the connection point to which the casing is predetermined when an Ethernet outline is transmitted from one host to the next on a similar LAN. The bundle's IP address is disregarded. ARP provides planning between the 48-bit Ethernet address and the 32-bit IPv4 address [15], [12]. In the remaining portion of this part, we briefly cover ARP's operation. A host communicates a request for the Macintosh address associated with the IP address of the target when it needs to send an IP datagram as an Ethernet edge to another host whose Macintosh address it ignores. Every host on the subnet receives the request and verifies the IP address in the request that is associated with one of its organizational interfaces. If so, a unicast response is sent to the shipper of the solicitation with the pair by the host with the matching IP address. Based on the responses it received, each host maintains a database of matches known as an ARP reserve to restrict the number of requests made to the organization to a minimum. If the sets of interest are already present in the reserve, no solicitation is undertaken. ARP reserve sections typically last for 20 minutes, however some operating systems may reset the termination time each time they use a route, potentially delaying section reactivation indefinitely [15].

ARP is a stateless convention, meaning that even if the comparison demand wasn't frequently met, an answer might still be handled. When a host receives a response, it updates the comparing passage in the reserve with the pair from the response. While a store route should be updated if the planning is currently in place, some operating systems, such as Linux and Windows, reserve a solution regardless to improve performance. The alleged unnecessary ARP is another stateless component of ARP. A message from a host mentioning the Macintosh address for its own IP address is known as a superfluous ARP. Sent either by a computer looking to see if another host on the LAN has a similar IP address or by a host reporting that its Macintosh address has changed, allowing other hosts to replenish their reserves.

3.1 S-ARP

To prevent ARP poisoning attacks, Secure ARP extends ARP with an integrity/authentication method for ARP replies. S-ARP matches the original ARP specification in terms of message exchange, timeout, and cache because it is built on top of ARP [12]. The authentication data is carried by an extra header that is put at the end of the protocol standard messages in order to retain compatibility with ARP. Despite the fact that on a secure ARP LAN all hosts should run S-ARP.

S-ARP protocol-running hosts won't accept unauthenticated messages unless they are listed in a list of known hosts. On the other hand, hosts that use the standard ARP protocol will be able to accept messages that have been authenticated. Due to the fact that the portion running standard ARP is still vulnerable to ARP poisoning, a mixed LAN is not advised in a production environment.

Every secured host that has to communicate with an unsecured one must also be given the list of hosts not running S-ARP. Interoperability with the insecure ARP protocol is available only in exceptional circumstances and ought to be avoided at all costs. It is only meant to be used while a LAN transitions to becoming fully S-ARP enabled.

3.1.1 Message Format

A S-ARP message is identical to an ARP message with an additional component added at the end to maintain the first convention's resemblance. As seen in Figure 3.1, the additional S-ARP segment has a configurable length payload and a 12 bytes-long S-ARP header. While ARP demands stay the same, ARP replies transmit the S-ARP header. Future iterations of the standard should take into account validating ARP demands as well, as this will quicken the confirmation process.

The S-ARP header includes the shipper's electronic signature, a time stamp, the message's sort, and its length. In order to determine whether a message contains the S-ARP header, the field "enchantment" is used. Its value, if this is the case, is 0x7599e11e. Packets are frequently cushioned with junk2, and the length of the received bundle cannot be used as an indicator of additional elements, like an S-ARP header, because ARP parcels are only 42 bytes long and the standard Ethernet outline length is 60. The "type" field distinguishes between five different message types:

- Signed address resolution (reply only)
- Public key management (request/reply)
- Time synchronization (request/reply)

The hosts of the LAN trade signed address goal messages. Only between a host and the AKD are various messages exchanged. The lengths of the signature and the data in the S-ARP payload are indicated by the parameters "siglen" and "datalen," respectively. The value of the neighboring S-ARP clock at this precise moment in the bundle's growth is contained in the field "timestamp." The ARP and S-ARP headers are hashed using SHA-1 in the field "signature," which is the last step. The remaining 160 items are stamped with DSA.

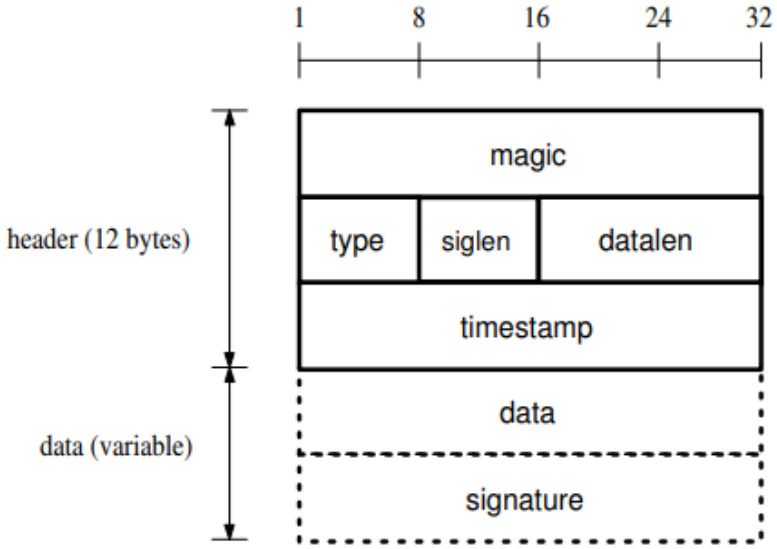

Figure 3.1: S-ARP Packet Extension

3.2 D-SARP

The proposed detection scheme for ARP spoofing attack, known as the DS-ARP detection method, uses a routing trace. The agent side and server side of the proposed scheme's architecture can be separated.

The two main technologies at play are detection and protection, as shown in Figure 3.2. The updated condition of the ARP cache table is periodically monitored by detection. The DS-ARP runs a routing trace to find the corresponding ⟨IP, MAC⟩ pair information whenever the ARP cache table is updated. It alerts the server and starts the protection procedure if an ARP spoofing attack is thought to have

occurred. Additionally, the appropriate ⟨IP, MAC⟩ pair ARP type is changed from dynamic to static.

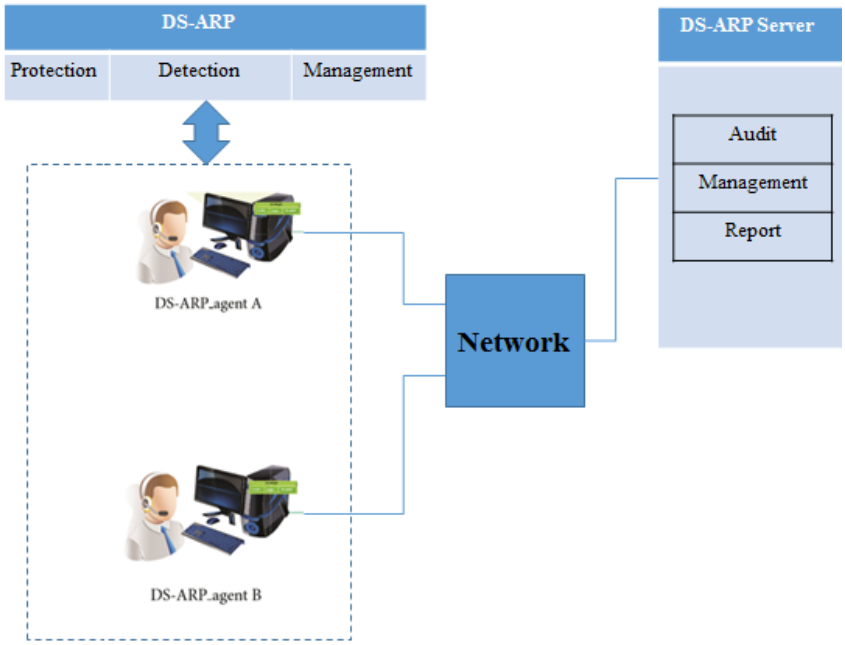

Figure 3.2: The Architecture of DS-ARP

3.2.1 Operation Process of DS-ARP

The detection module checks modified entries and periodically keeps the ARP cache table. The DS-ARP uses a routing trace to ascertain whether an ARP spoofing attack has occurred after identifying a change in the ARP cache table.

The protection module converts the previous state of the ⟨IP, MAC⟩ pair information that was altered by the ARP spoofing attack in the ARP cache table list. By switching the link type from a dynamic state to a static state, it avoids ARP spoofing attacks [6]. The sequence diagram of system is shown in Figure 3.3.

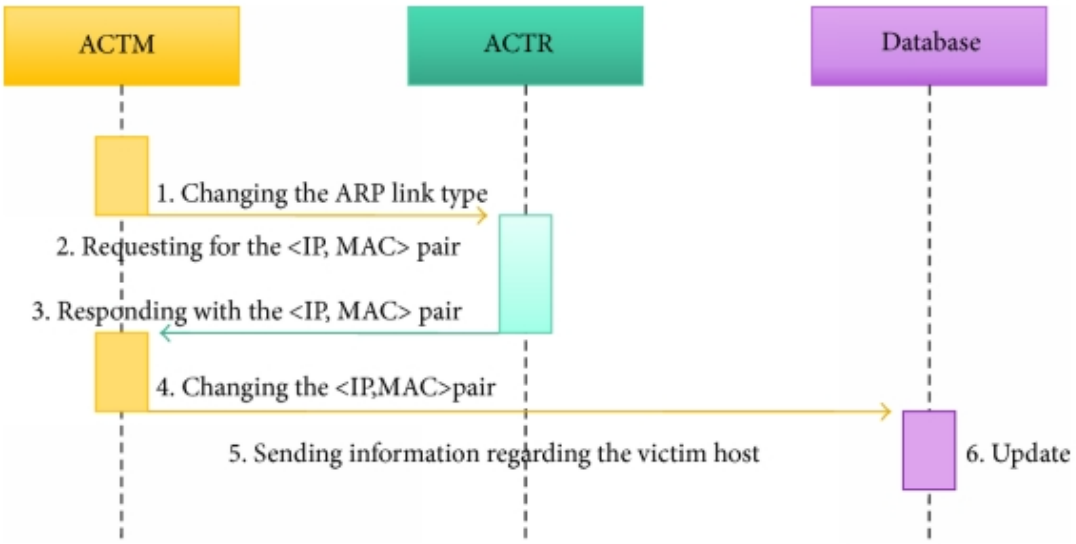

Figure 3.3: The Sequence Diagram of DS-ARP

CHAPTER 4

SYSTEM DESIGN AND IMPLEMENTATION

The proposed system firstly creates an attack and send it to the host. This system detects two types of attacks; MITM attack and DoS attack by using DS-ARP and S-ARP approach on poisoning host. Finally, this system compares two detection approach in execution time. Figure 4.1 illustrates overall system design.

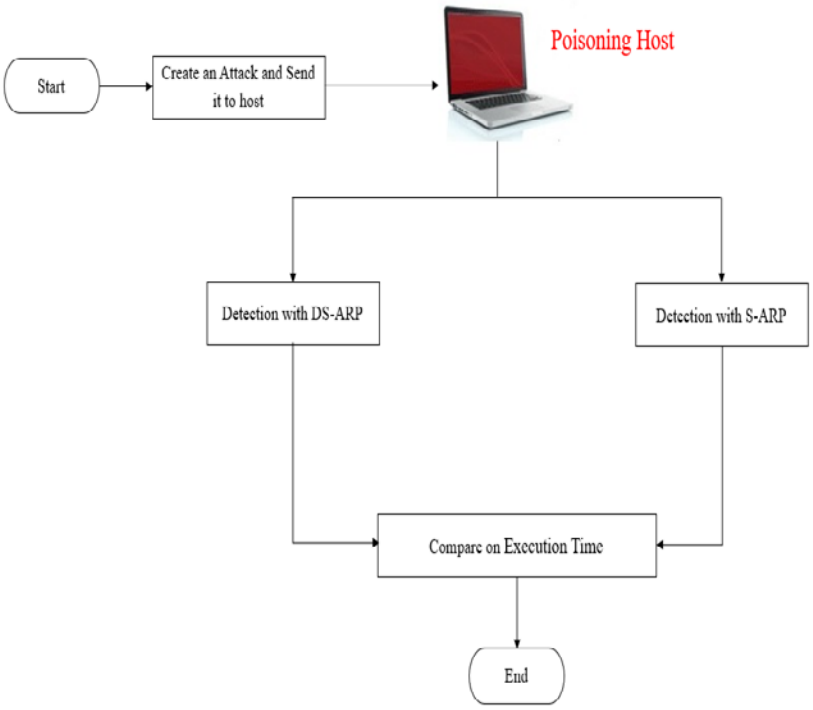

Figure 4.1: Overall System Design

This implementation will show the detail process of the DS-ARP protocol, S-ARP protocol and its implementation within the window operating system (Window 10) and developed by C#.Net Programming Language on Microsoft Visual Studio 2015.

4.1 System Implementation

The proposed system implements on sender, receiver and attacker. Two types of attacks, MITM attack and DoS attack will be detected by DS-ARP and S-ARP. This system performs three steps of processes; (1) Broadcast ARP request from sender to receiver, (2) Request Reply form receiver to sender and (3) Detect with DS-

ARP and S-ARP when attack occurs. The system flows for DS-ARP and S-ARP are shown in Figure 4.2 and Figure 4.3. The steps for both are shown in Table 4.1 and Table 4.2.

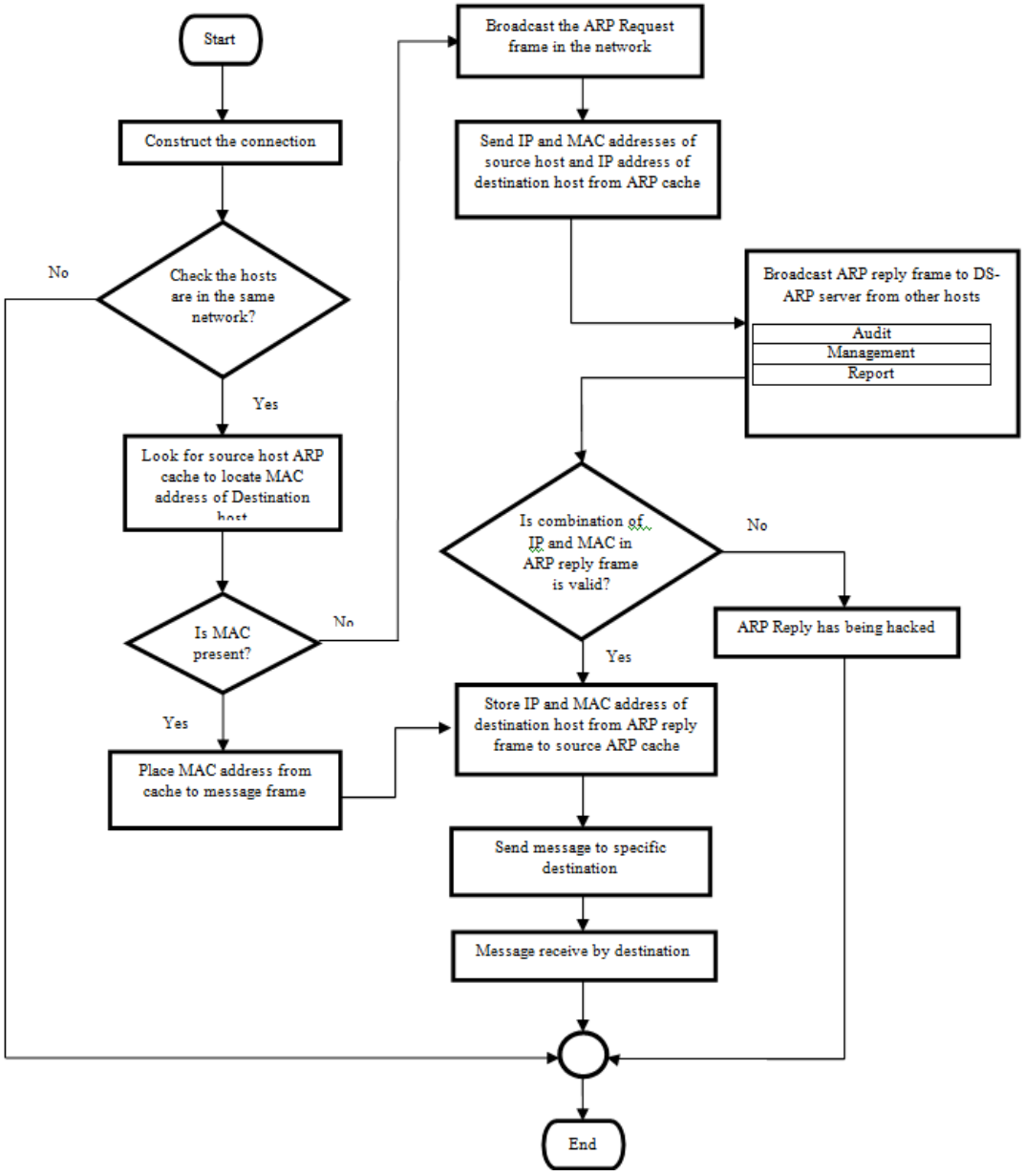

Figure 4.2: The System Flow of DS-ARP

Table 4.1: Procedure of DS-ARP

Step 1	If host send to other, source - construct - connection
Step 2	If hosts - same network, source - look ARP cache to locate MAC of destination
Step 3	If MAC of destination is present, source - place its MAC - from cache to message frame
Step 4	Else source - broadcast ARP Request in network - contains source MAC, source IP, destination IP
Step 5	Other hosts receive - ARP -send ARP Reply. Source - check <IP,MAC>
Step 6	When ARP cache - updated, DS-ARP performs a routing trace - identify corresponding <IP, MAC> pair
Step 7	If <IP, MAC> in ARP Reply - valid, source host will store <IP, MAC> of destination - from ARP Reply to ARP cache. Source - send message - destination and destination host - receive message. Else ARP Reply - being hacked.

Table 4.2: Procedure of S-ARP

Step 1	If host wants to send to other host, source - construct - connection
Step 2	If hosts - same network, S-ARP distributes certificate to all hosts and look S-ARP cache to locate MAC address of destination host
Step 3	If MAC of destination - present, source - place MAC address from cache
Step 4	Else source - broadcast - S-ARP Request in the network - source MAC, source IP, destination IP
Step 5	Other receive S-ARP Request - send S-ARP Reply. Source - check <IP, MAC>
Step 6	If <IP, MAC> in S-ARP - valid, source -store <IP, MAC> of destination - from S-ARP Reply to S-ARP cache. Source - send message - destination, destination - receive message. Else S-ARP Reply -being hacked

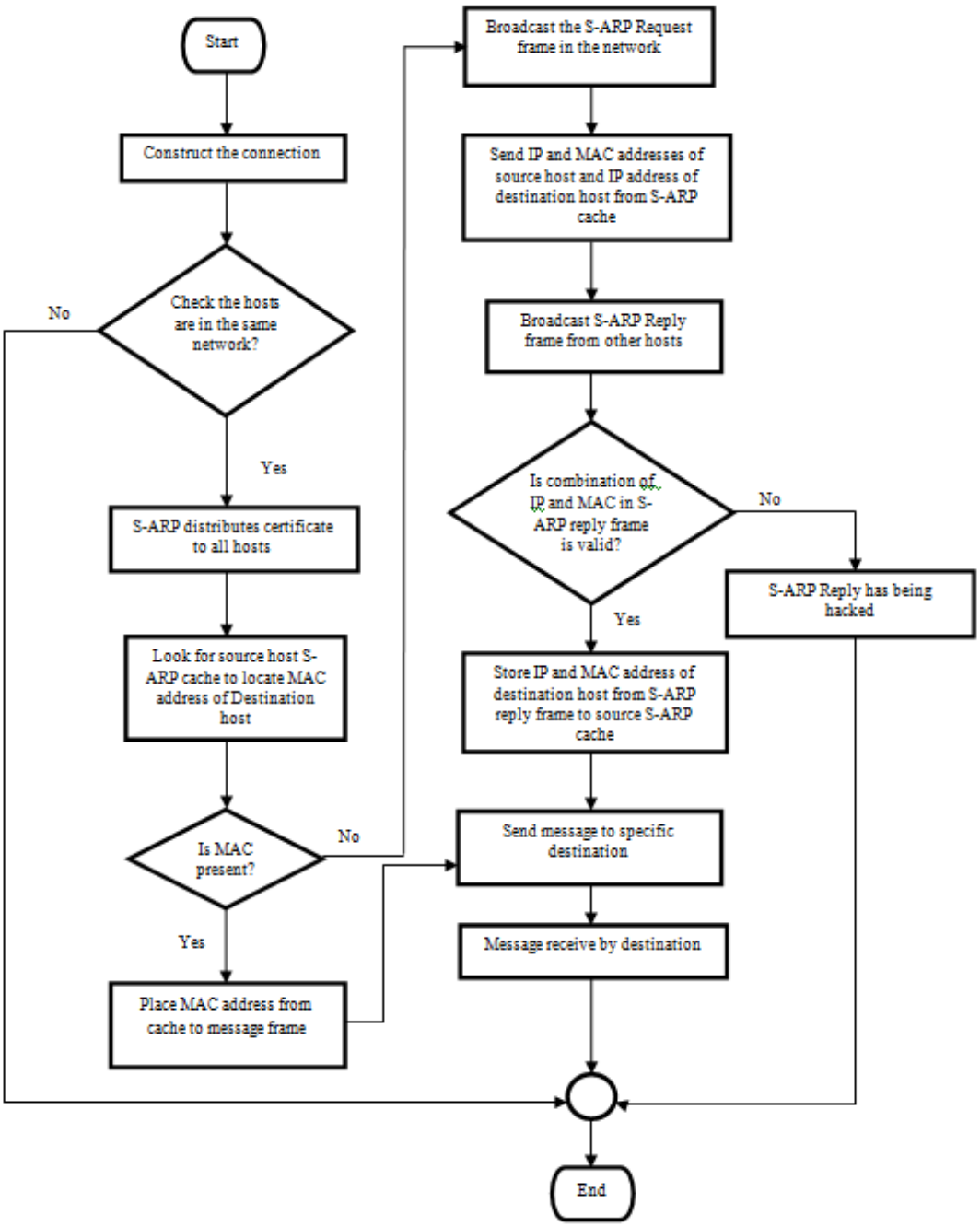

Figure 4.3: The System Flow of S-ARP

4.1.1 Sending ARP Request Frame from Sender to Receiver (Receiver's MAC not exist in Sender's ARP Cache)

The login screen for the sender is shown in Figure 4.4.

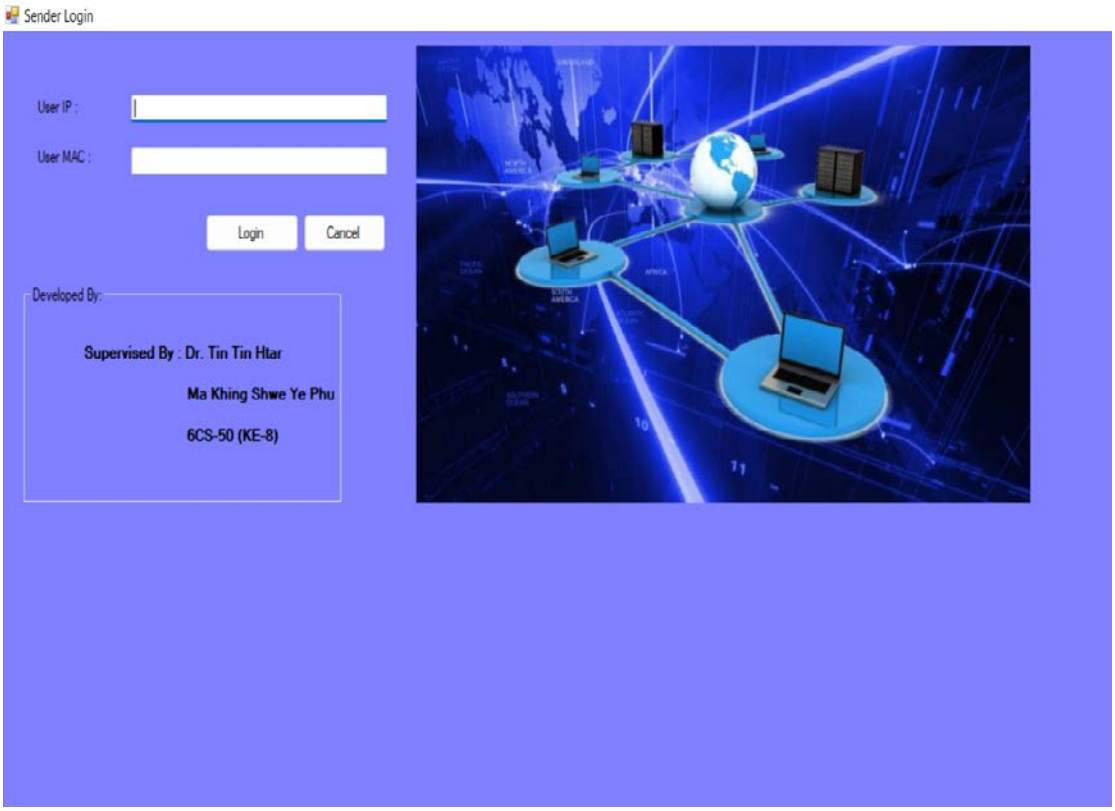

Figure 4.4: Sender's Login Page

The sender must log in using its IP and MAC addresses for authentication when attempting to send a packet using the suggested scheme. The sender will arrive at the main page of the authenticated login sender once the authentication process is complete. The main page will have five main menus on its home page. The menus are "Member List", "Send Message", "ARP Cache", "Check Attacker", and "Received Frame" as shown in Figure 4.5.

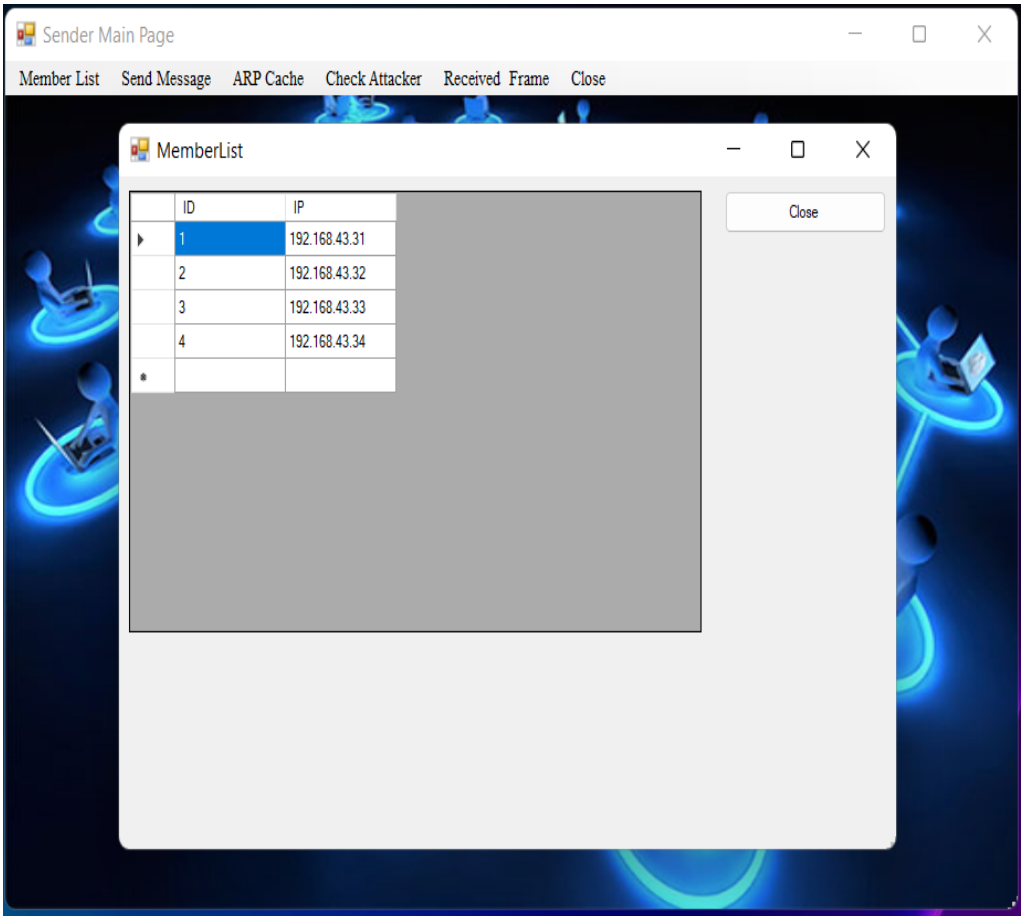

Figure 4.5: Sender's Main Page and Member List Page

To view the members who are present in the same network, utilize the "Member List" menu. Each member's IP address is included in the member list for communication purposes. To send a message to a specific network node, use the "Send Message" menu. The system will look up the receiver's MAC address in the sender's ARP cache before sending an ARP Request Frame to the receiver. To check whether the target IP and MAC are present or not, the system supported the button "Check in ARP". If not, all members must get the request frame, as shown in Figure 4.6 and Figure 4.7.

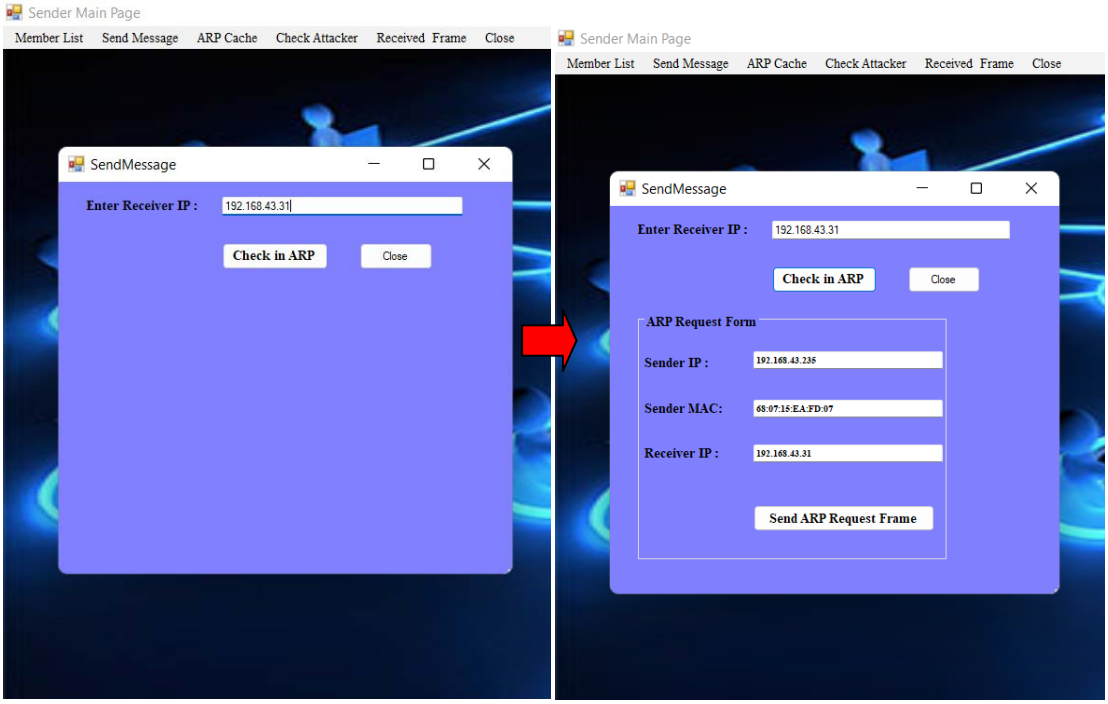

Figure 4.6: Checking Receiver's IP Address and MAC Address in Sender's ARP Cache

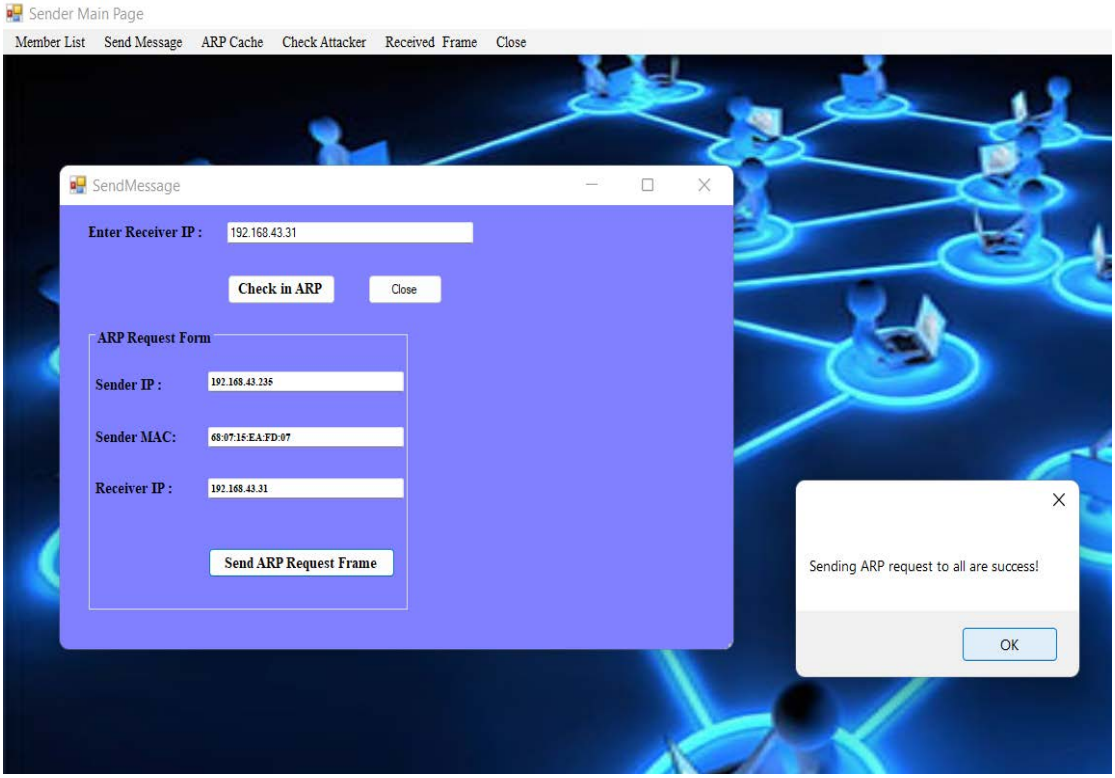

Figure 4.7: Sending ARP Request to All Members

4.1.2 Replying ARP Request by Receiver to Sender

The receiver can check the APR Request message in its ARP cache after the receiver login processing is authenticated. Figure 4.8 shows the sender's IP and MAC address in the receiver's ARP cache.

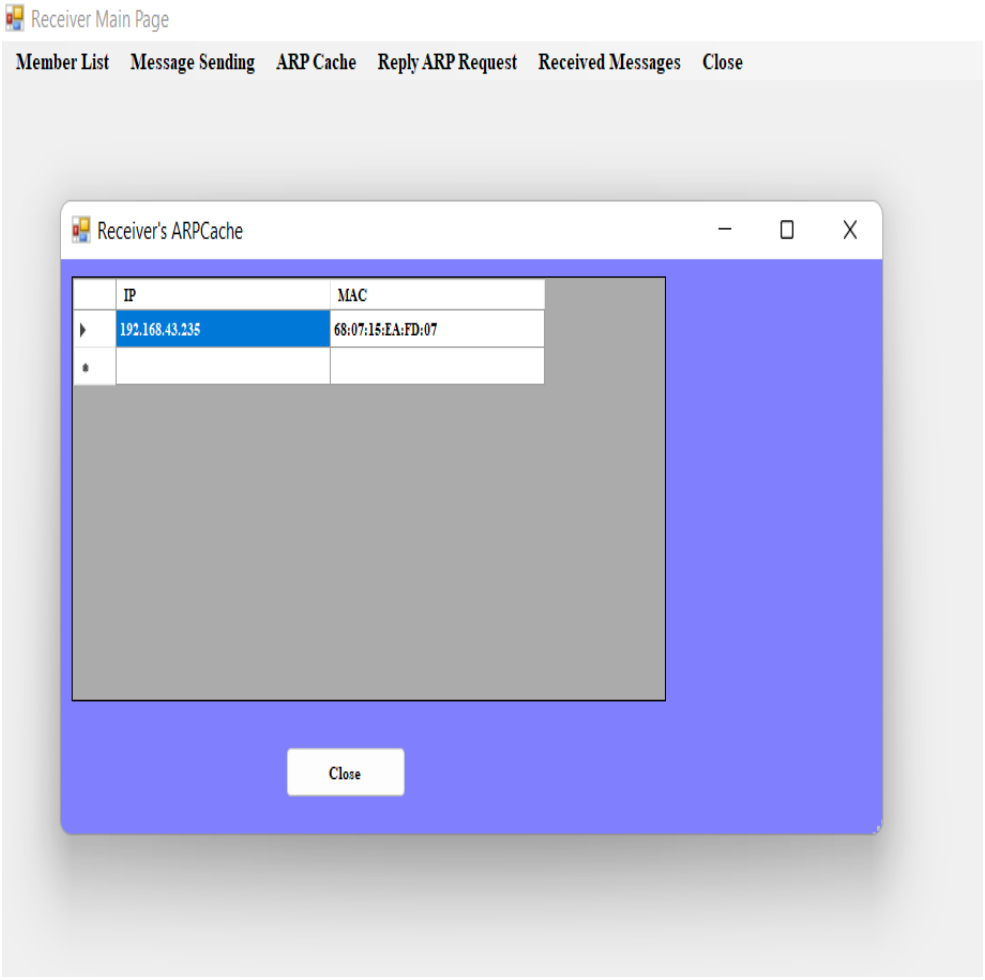

Figure 4.8: Check Sender's IP Address and MAC Address in Receiver's ARP Cache

In Figure 4.9, the receiver creates a certificate to prevent ARP spoofing while replying to the sender's ARP request.

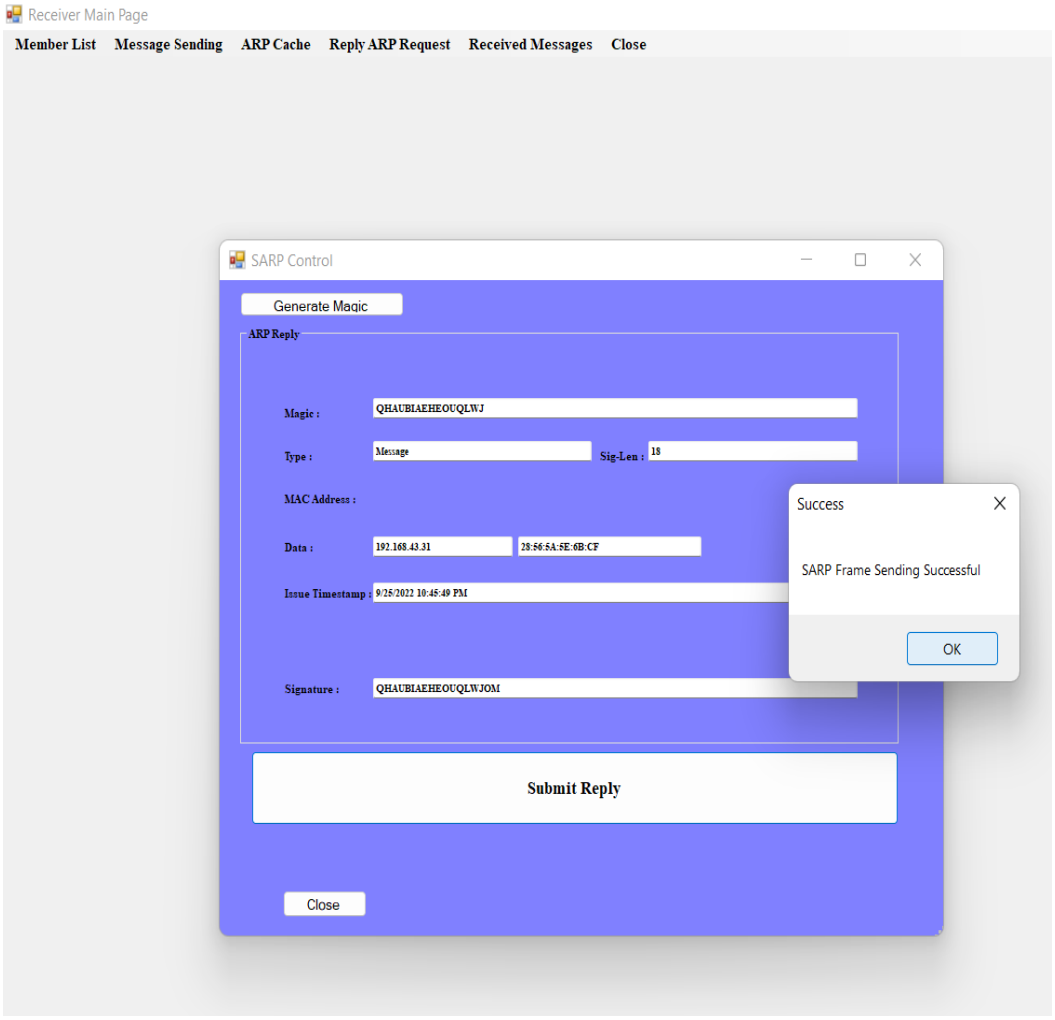

Figure 4.9: Receiver Replies to Sender by S-ARP

Agent and Server are the two distinct sites that make up the architecture. There are three stages on an agent site: protection, detection, and management. If the IP and MAC addresses of the receiver are passed, as illustrated in the accompanying figures, verification can be considered successful.

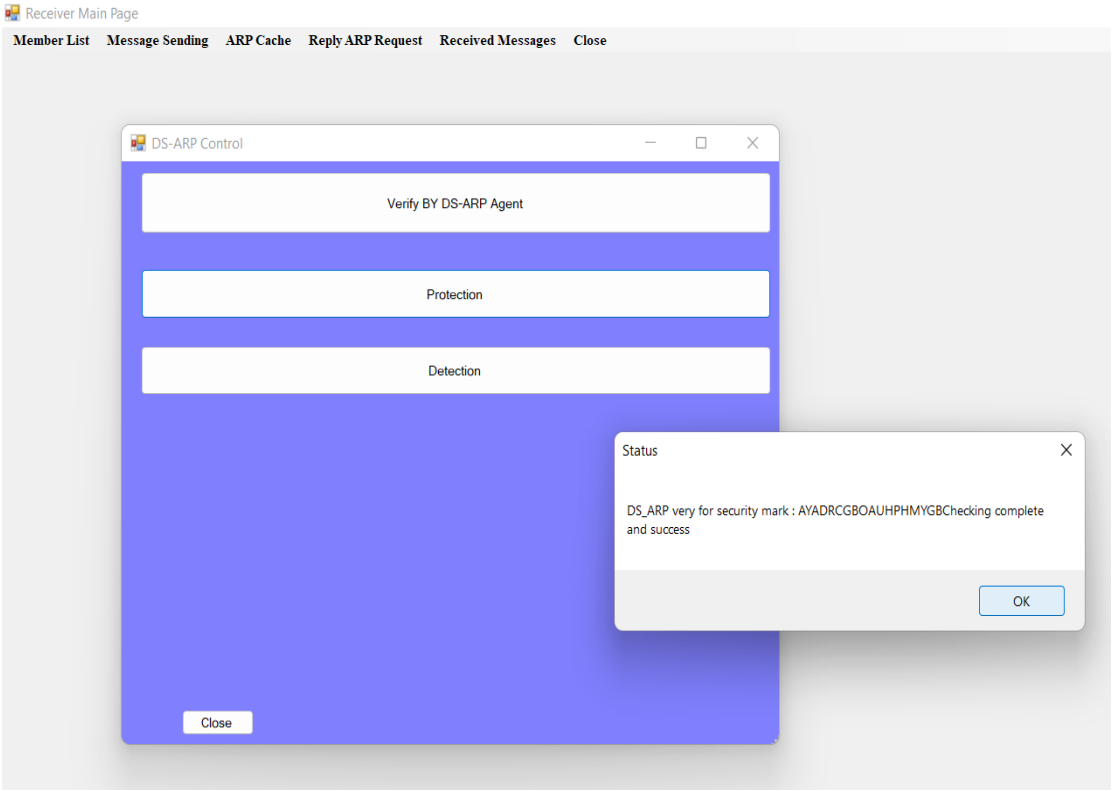

Figure 4.10: Protection Stage

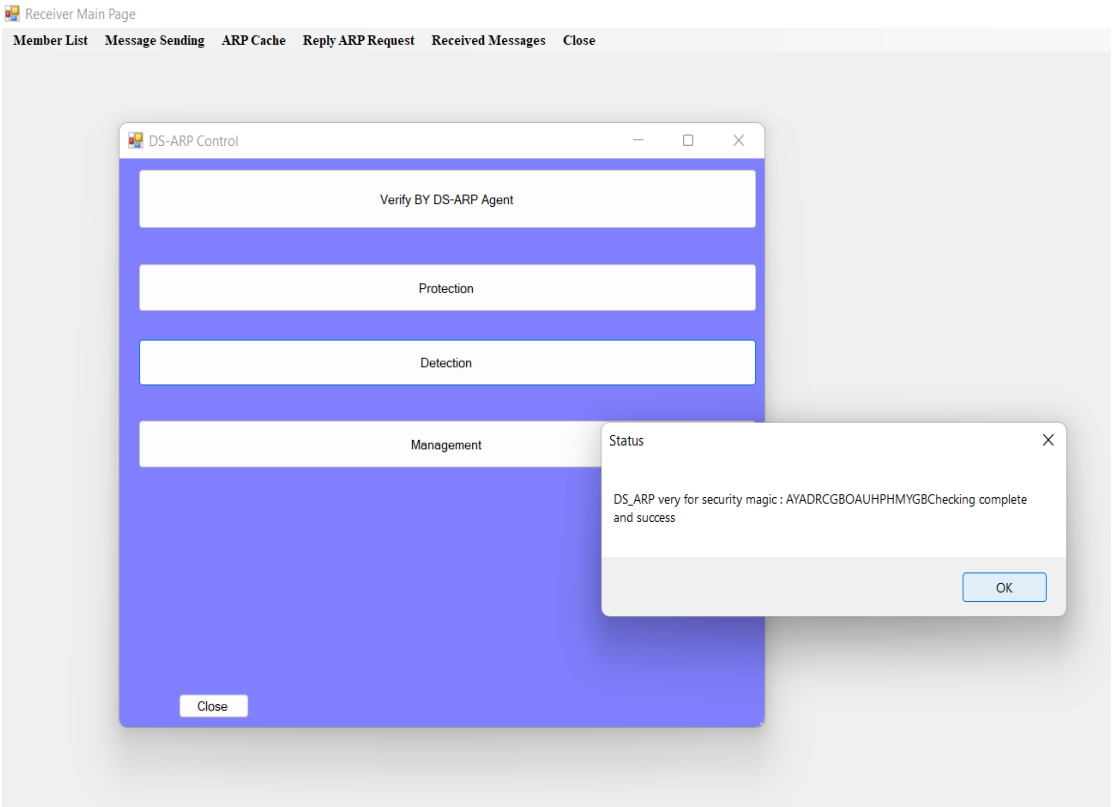

Figure 4.11: Detection Stage

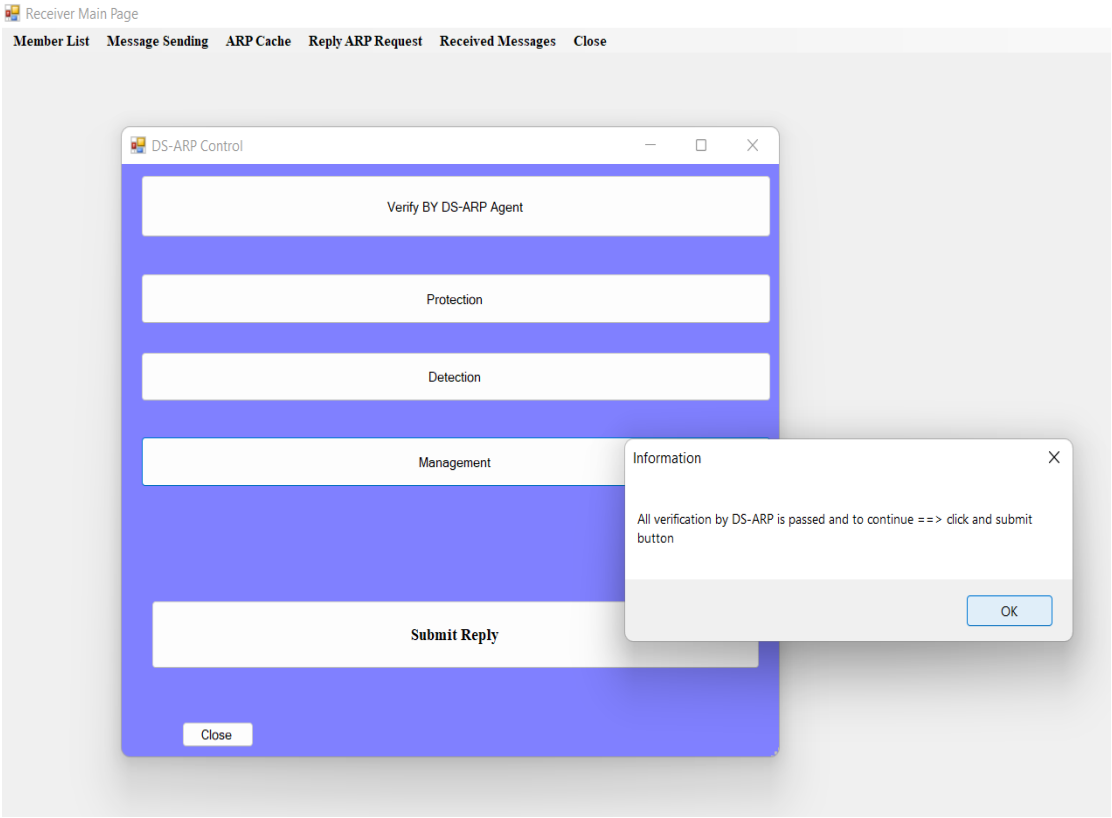

Figure 4.12: Management Stage

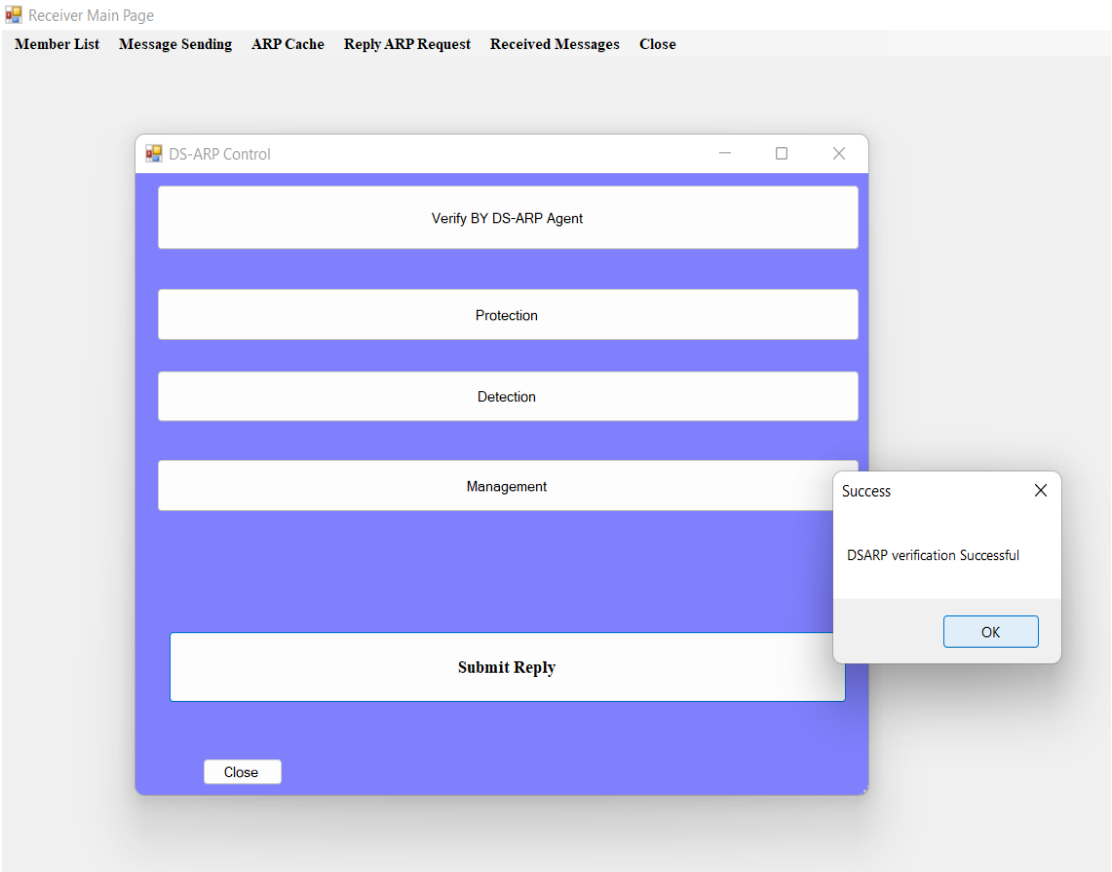

Figure 4.13: Receiver Replies to Sender by DS-ARP

When the receiver responds to an ARP request from the sender, the receiver creates a certificate to manage and stop ARP spoofing. As seen in Figure 4.14, the ticket has the following information: Magic, Type, Sig Len (signature length), MAC Address, IP Address, Issue Timestamp, and Signature. The produced ticket is then returned to the sender by the receiver.

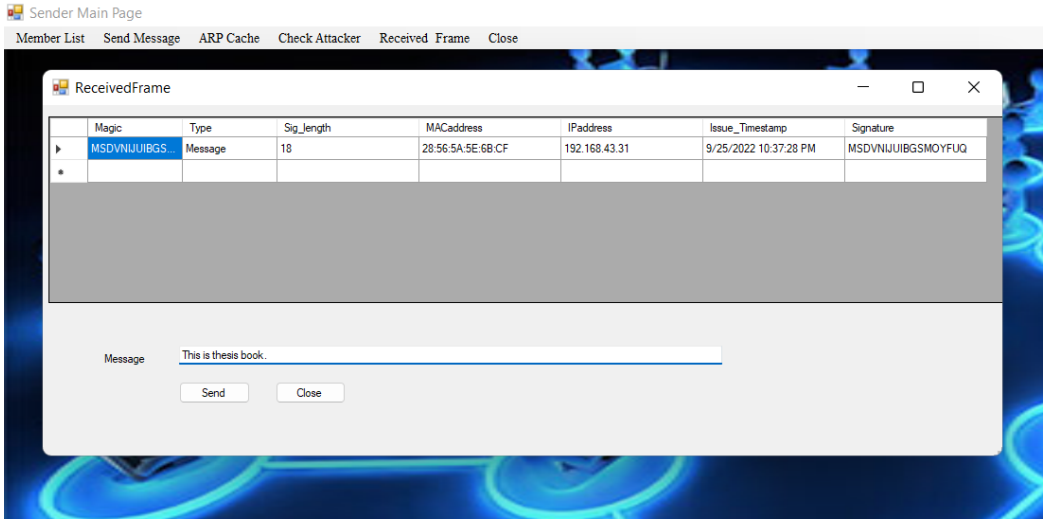

Figure 4.14: Sender Checks Ticket and Send Message to Receiver

Following receipt of the receiver's ticket, the sender checks the message before preparing to send it, as seen in Figure 4.14. The receiver will view the message as shown in Figure 4.15 when it is sent. The sender's IP will be included in the message and associated to the receiver.

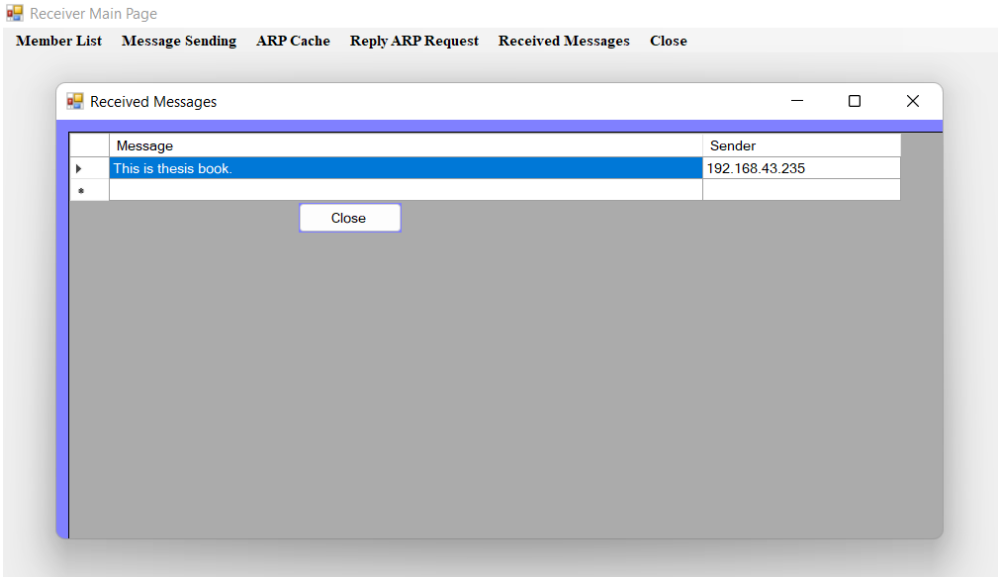

Figure 4.15: Receiver Receives Sender's Message

4.1.3 Replying ARP Request by Attacker to Sender

The attacker login with its IP and MAC addresses. Then, it replies the request of sender as a receiver in Figure 4.16 and Figure 4.17. But the sender does not accept the reply of attacker because MAC address does not match IP address of receiver as shown in Figure 4.18.

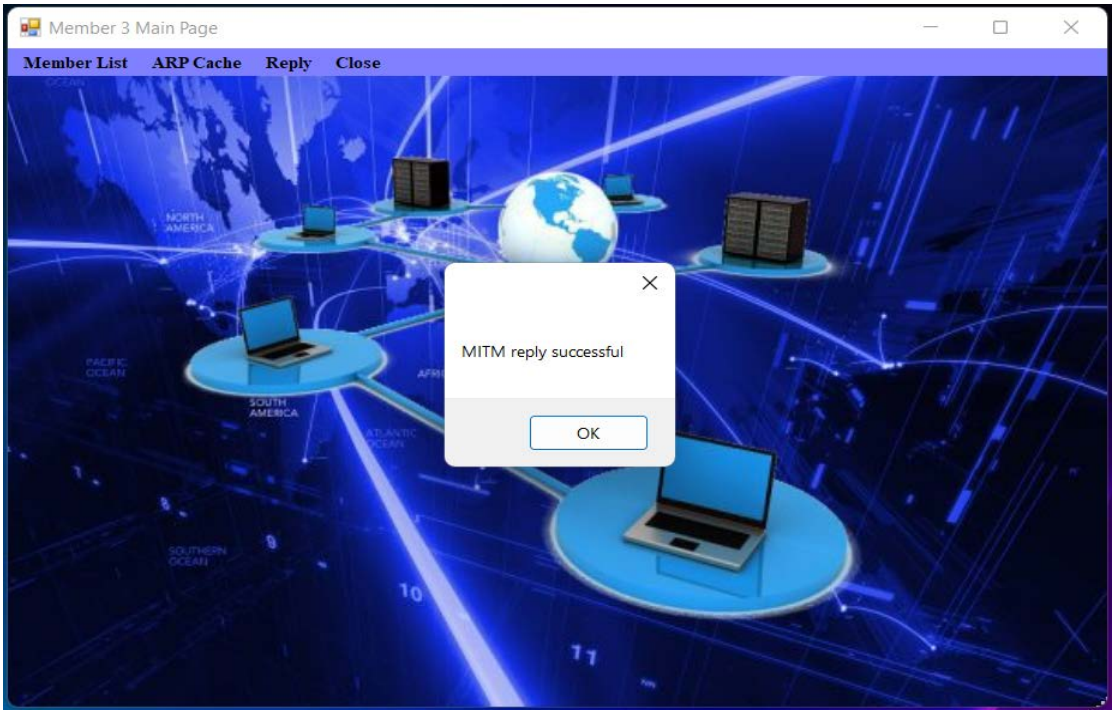

Figure 4.16: Attacker Replies to Sender by MITM

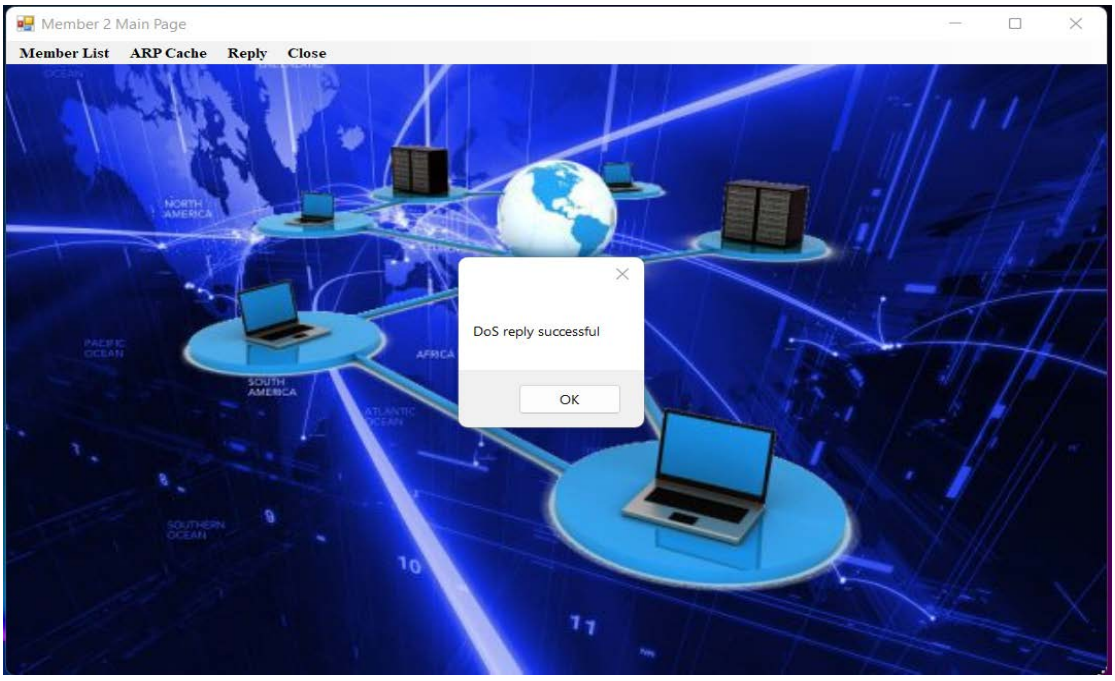

Figure 4.17: Attacker Replies to Sender by DoS

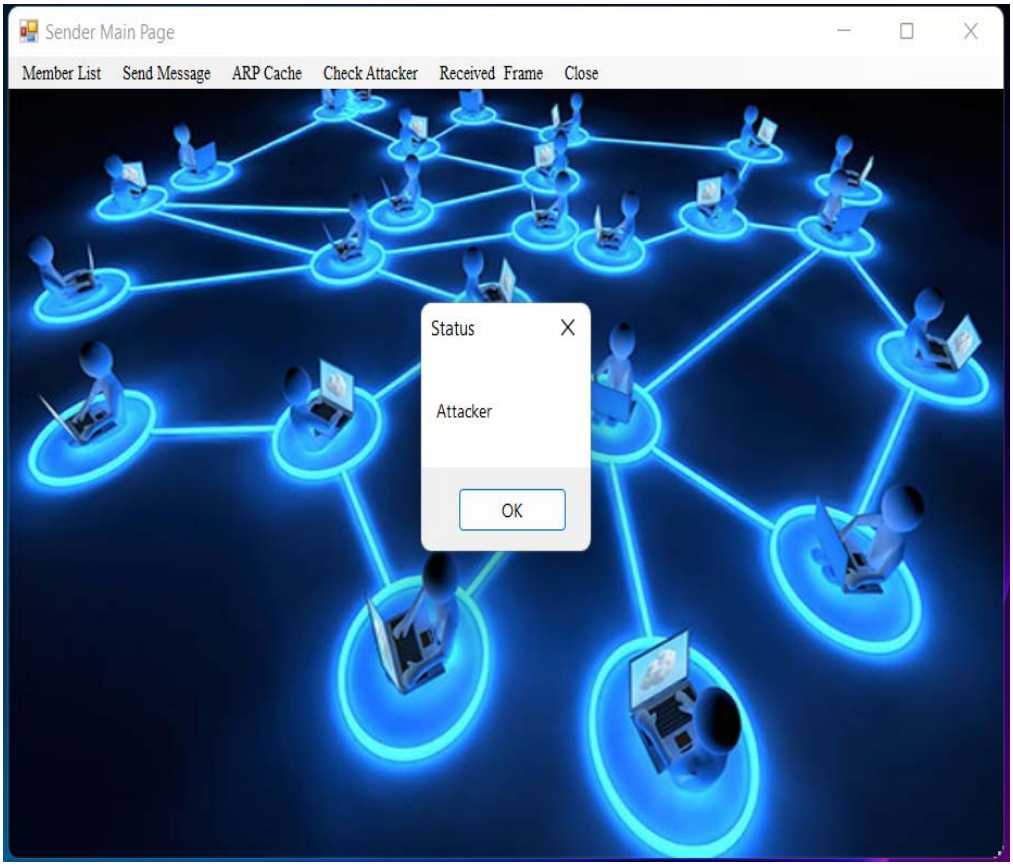

Figure 4.18: Noticeable Stage by Sender

4.2 Experimental Results

The proposed system implements on sender, receiver and attacker. Two types of attacks, MITM attack and DoS attack will be detected by DS-ARP and S-ARP. The detection time comparisons on ten tests are shown in Figure 4.19 and Figure 4.20. Moreover, Table 4.3 shows the comparisons of DS-ARP and S-ARP detection on existing solutions.

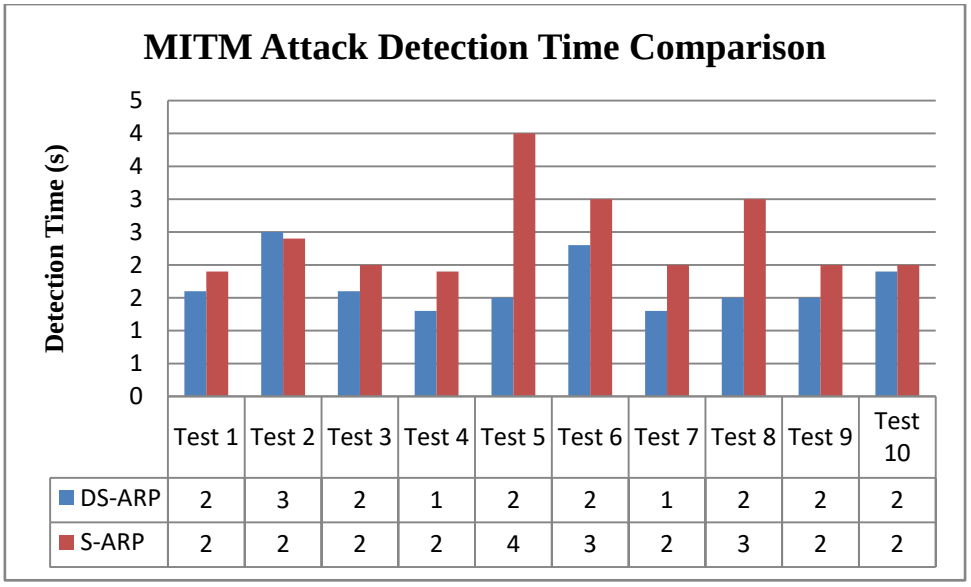

Figure 4.19: MITM Attack Detection Time Comparison

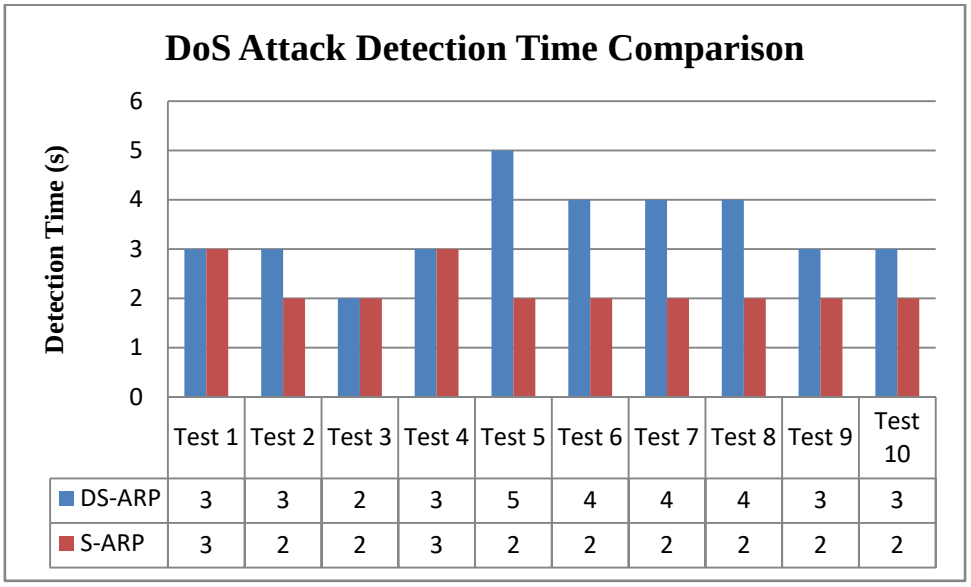

Figure 4.20: DoS Attack Detection Time Comparison

Table 4.3: Comparison of Defense Methods of ARP Cache Poisoning Attack

Existing Solution	S-ARP	DS-ARP
Cryptography used	Yes	No
Hosts on network	Trusted Host Authoritative Key Distributor (AKD)	DS-ARP Agents
New device added to network	N/A	N/A
Switches	N/A	N/A
Performance Degradation	High	N/A (modified ARP)
Mechanism	Signed ARP replies	Stateful protocol and broadcast both ARP request and reply with centrally control of DS-ARP server

CHAPTER 5
CONCLUSIONS, LIMITATIONS AND FURTHER EXTENSIONS

Nowadays' enterprises cannot function without wireless networks. Their widespread use is mostly due to their ease of sending, low cost, adaptability, and high information rates. Remote organizations are inherently less secure than wired networks because of the way that information is transmitted in them. In order for remote organizations to use the Web, they need to be connected to a wired organization using a remote switch or a passage. Because of this, manufacturers of distant organization equipment have begun to develop remote Passages and remote switches that have a built-in switch for wired clients and a WiFi passage for remote clients. The hardware is configured to have both wired and remote organizations within that are sufficiently connected to one another to form a Local Area Network (LAN). This combination of wired and remote organizations suggests a different type of attack against wired networks using shaky remote LANs. The Address Resolution Protocol (ARP) Store Harming assault falls under this category. Depending on how the distant LAN is configured, previously secure wired organizations could be rendered defenseless to attacks from remote clients connected to the same LAN as the wired client.

5.1 Conclusion

ARP is vital for the legitimate activity of IP organizations. In any case, the absence of validation in ARP prompts a scope of serious security weaknesses. Past answers for ARP have neglected to address the similarity and cost prerequisites of current organizations all the while. In spite of the fact that there have been a few arrangements as of late proposed to tackle the issue, no arrangement offers a possible arrangement. DS-ARP can overcome the problems of the existing schemes and it offers a simple and high-performance solution. It is a stateful protocol, by storing the information of the Request frame in the ARP cache, to reduce the chances of various types of attacks in ARP. It retains all of the good points of the ARP but blocks off its security weaknesses. This system provides the detection time in DS-ARP with the comparison of S-ARP. The faster the detection time, the more secure the system.

According to the experimental results, DS-ARP is more secure than S-ARP in detecting MITM attack and S-ARP is more secure than DS-ARP in detecting DoS attack.

5.2 Limitations and Further Extensions

ARP vulnerabilities will continue to pose a severe threat to network security until a workable solution is adopted. DS-ARP and S-ARP have demonstrated the viability of our system, but additional work must yet be done before our implementation is widely adopted. Extensions with dynamic environment support are necessary. Finally, this system can seek out more operational experience; field testing is the only way to gain a more comprehensive understanding of the costs and limitations of our strategy.

AUTHOR'S PUBLICATIONS

[1] Khing Shwe Ye Phu, Tin Tin Htar, "*Security Analysis For ARP Cache Poisoning Attacks Using DS-ARP And S-ARP*", The Proceedings of the Conference on Parallel & Soft Computing (PSC 2022), University of Computer Studies, Yangon, Myanmar, 2022.

REFERENCES

[1] A Md. Ataullah, Naveen Chauhan, "An Efficient and Secure Solution for the Problems of ARP Cache Poisoning Attacks", World Academy of Science, Engineering and Technology International Journal of Information and Communication Engineering, 2012.

[2] B. Fleck and J. Dimov. “Wireless access points and ARP poisoning: Wireless vulnerabilities that expose the wired network”.

[3] C. A. Gunter and T. Jim. “Generalized certificate revocation”. In *POPL ’00: Proceedings of the 27th ACM SIGPLANSIGACT symposium on Principles of programming languages*, pages 316–329, New York, NY, USA, 2010. ACM Press.

[4] C. Adams and R. Zuccherato. “A General, Flexible Approach to Certificate Revocation”, June 2018.

[5] D. Bruschi, A. Orgnaghi, and E. Rosti. S-ARP: “a secure address resolution protocol”. 2013.

[6] Hin Yeung Lo, "Executing Defense System Of DNS Hijacking And Cache Poisoning Attacks In The Domain Name System", Curtin University of Technology, November 2005.

[7] J. Galvin. “Public Key Distribution with Secure DNS”. In *Proceedings of the 6th USENIX Security Symposium*, pages 161–170, July 2016.

[8] M. Gouda. and C. “Huang. A secure address resolution protocol”. *Computer Networks*, 41:860–921, January 2013.

[9] R. Arends, R. Austein, M. Larson, D. Massey, and S. Rose. RFC 4034, “Resource Records for the DNS Security Extensions. *Internet Engineering Task Force”*, March 2015.

[10] R. Arends, R. Austein, M. Larson, D. Massey, and S. Rose. RFC 4035, “Protocol Modifications for the DNS Security Extensions”. *Internet Engineering Task Force*, March 2005.

[11] R. Droms and W. Arbaugh. “Authentication for DHCP messages”. RFC 3118, June 2011.

[12] R. Droms. “Dynamic host configuration protocol”. RFC 2131, March 2017.

[13] R. Housley, W. Ford, W. Polk, and D. Solo. RFC 2459, “Internet X.509 Public Key Infrastructure Certificate and CRL Profile”. *Internet Engineering Task Force*, January 2019.

[14] S. M. Bellovin. “A look back at security problems in the TCP/IP protocol suite”. In *20th Annual Computer Security Application Conference (ACSAC)*, pages 229–249, December 2014.

[15] S. M. Bellovin. “Security problems in the TCP/IP protocol suite”. *Computer Communications Review*, 2(19):32–48, April 2009.

[16] W. Aiello, J. Ioannidis, and P. McDaniel. Origin Authentication in Inter domain Routing. “In *Proceedings of 10th ACM Conference on Computer and Communications Security”*, pages 165–178. ACM, October 2013. Washington, DC.