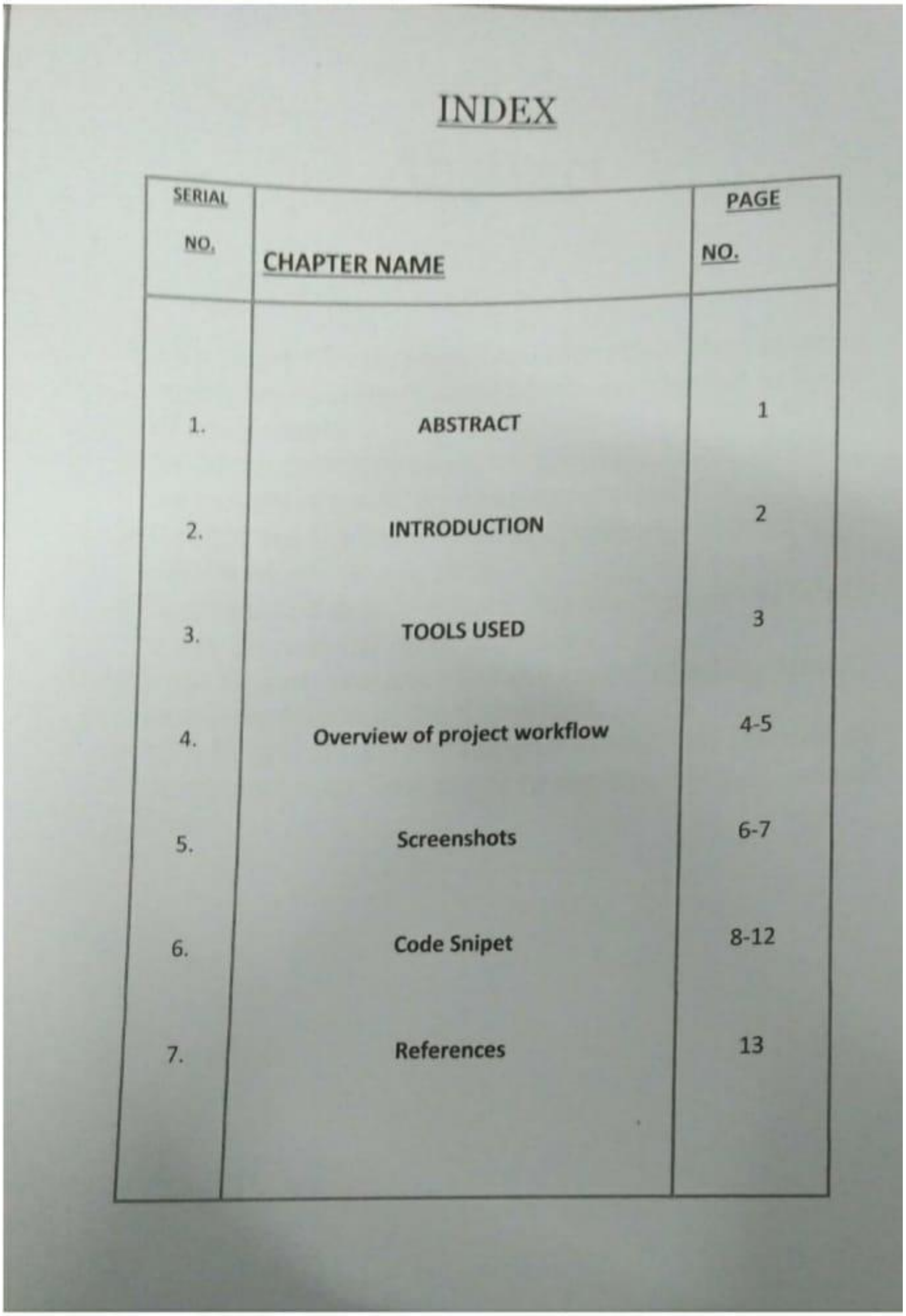
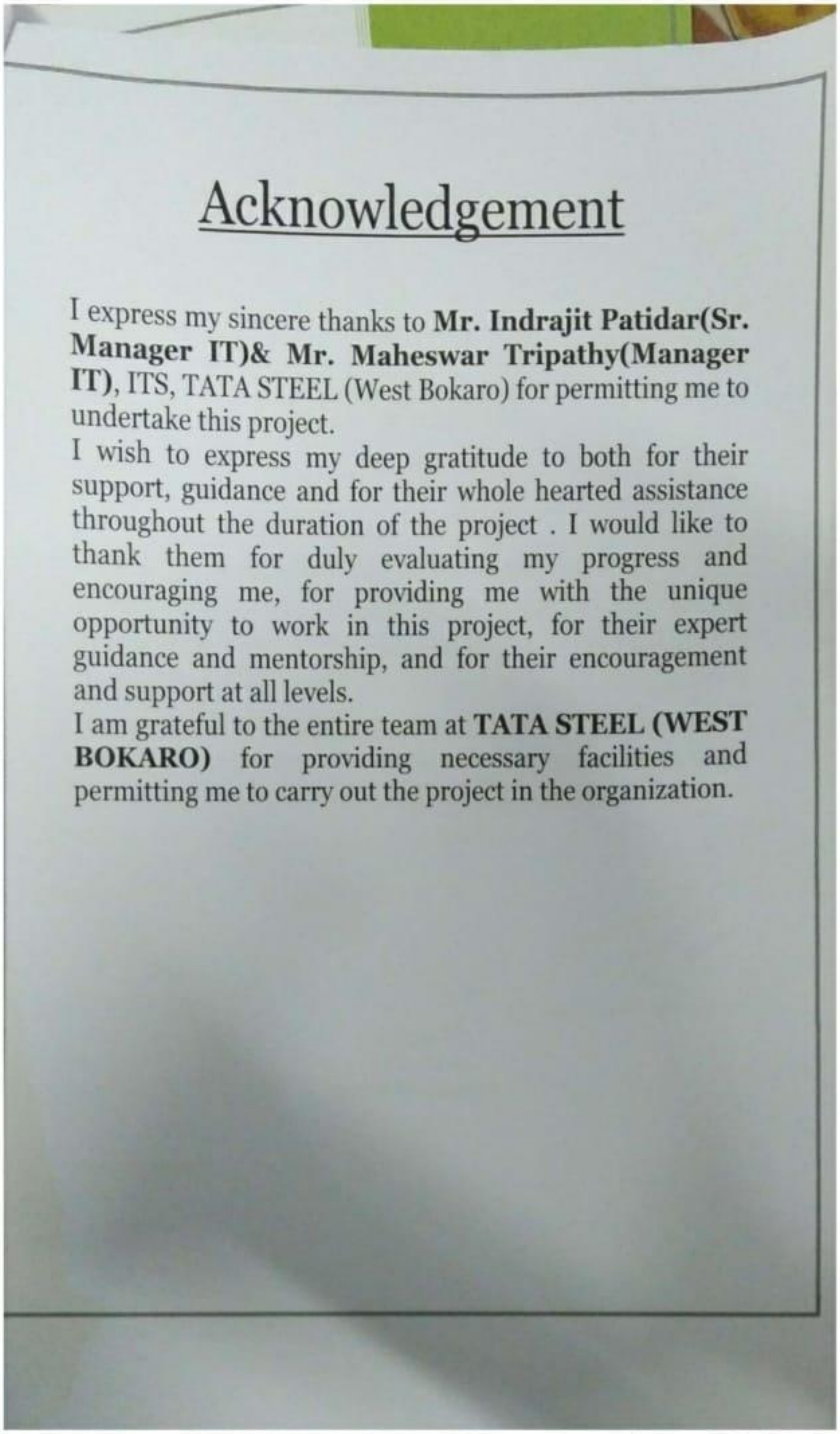


INDEX

[redacted]



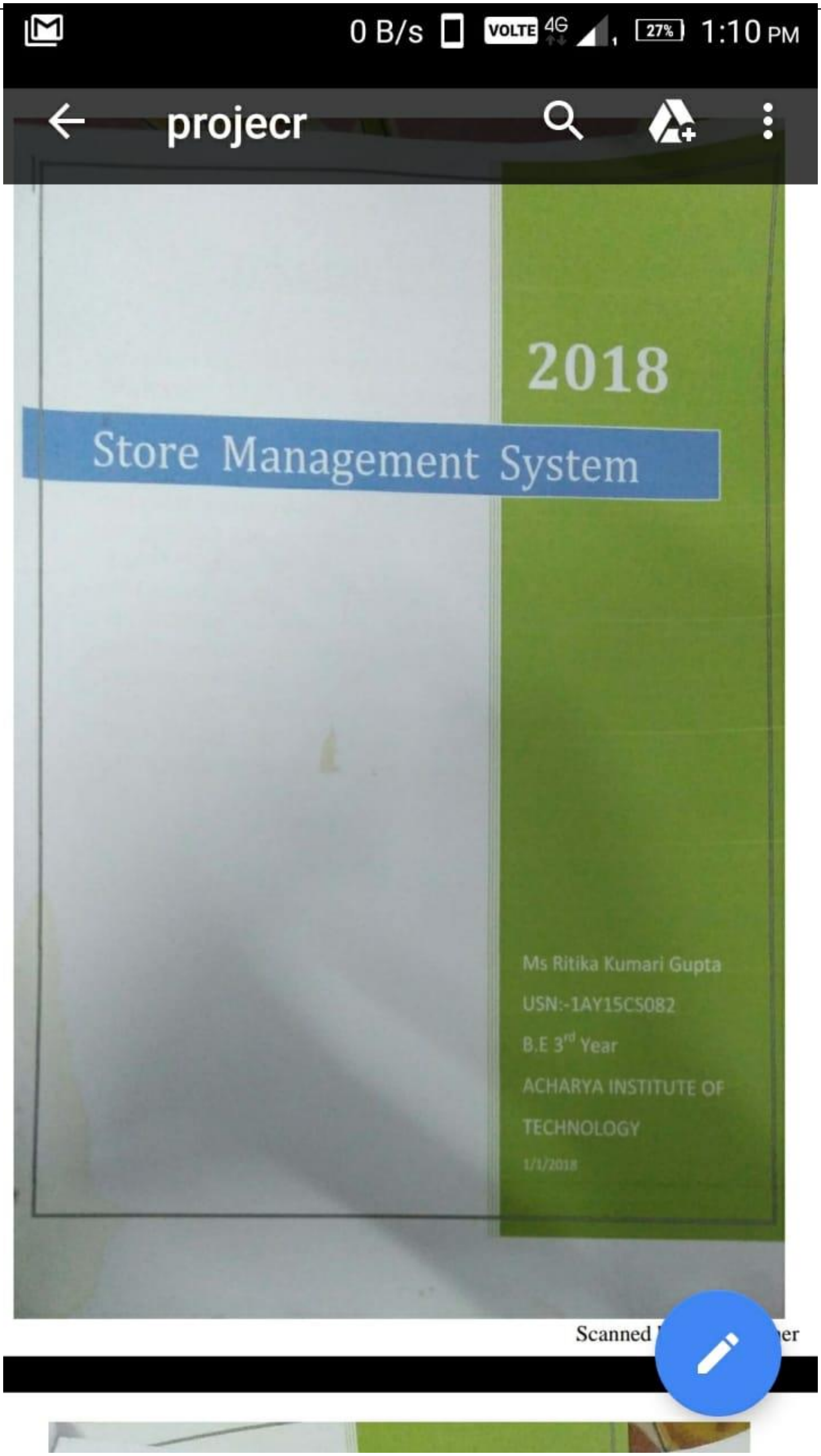
Acknowledgement

I express my sincere thanks to **Mr. Indrajit Patidar(Sr. Manager IT)& Mr. Maheswar Tripathy(Manager IT)**, ITS, TATA STEEL (West Bokaro) for permitting me to undertake this project.

I wish to express my deep gratitude to both for their support, guidance and for their whole hearted assistance throughout the duration of the project . I would like to thank them for duly evaluating my progress and encouraging me, for providing me with the unique opportunity to work in this project, for their expert guidance and mentorship, and for their encouragement and support at all levels.

I am grateful to the entire team at **TATA STEEL (WEST BOKARO)** for providing necessary facilities and permitting me to carry out the project in the organization.

[redacted]



2018

Store Management System

Ms Ritika Kumari Gupta

USN:-1AY15CS082

B.E 3rd Year

ACHARYA INSTITUTE OF TECHNOLOGY

1/1/2018

Scanned [illegible] er

Abstract

- This project is developed to store value of equipment which are coming to store or we can say that in & out of equipments.
- In this project equipment entry page is there where we can entry a new equipment details.
- Equipment Update:- we can update equipment details whenever required.
- Equipment delete:- we can delete a equipment which is not there in the store any more.
- View Report:- we can view the report of all equipment details by selecting the dropdown.
- New Registration:- For the admin who will operate all the project work flow needs to register himself/herself first.

Project Title:Security issues with Mobile IP

Preface

I would like to thank our supervisor **VIKASH KUMAR (ASSISTANT MANAGER IT)** for lots of ideas, his great inspiration and comments on this thesis. I would like to thank Mentor of ITS TATA STEEL for their assistance and positive attitude.

Finally, I wish to express our greatest thanks to our family, friends and colleagues, who have supported us during our study.

Abstract

With a rapid growth in wireless technology in recent years, Mobile IP has become very important for consumers and businesses by providing mobility based on IP addresses using several applications, which keep the employees connected with each others with critical information. In mobile IP the node can change its location by maintaining the same IP address and keep connected to the internet, which solves the issue of terminating the communication once it moves.

Since Mobile IP uses open airwaves as a transmission medium, it is subject to the many security threats that are routed in mobile IP network .Protecting mobile IP from threats and attacks is one of the most challenging task now days. IPSec is a standard security protocol solution for TCP/IP network that provides security through Authentication, Encryption and data integrity services. Mobile IP data traffic can be secured by combining with IP Security (IPSec) protocol.

This thesis describes Mobile IP operations, security threats, different existing methods for securing mobile IP and then IPSec standard, how it works and why IPSec is the best solution. This thesis also describes how to combine IPSec with a mobile IP to provide a solution called (SecMIP) that protects the mobile device's communication from any threats. Finally it describes Mobile IPv6, binding update and associated security concern.

Contents

1 Introduction

1.1 Background

Wireless communication has witnessed a growth number of users in the recent years; one of the main advantages of wireless technology is mobility, which allow mobile users to move from one network to another whilst maintaining their permanent IP address. This keeps transportation and high level connections whilst moving [1]. Mobile IP is a standard protocol established by the

Internet Engineering Task Force "IETF", to provide an efficient and scalable mechanism for mobile nodes within the internet. Mobile IP environments mostly exist in wireless networks where users need to carry their devices across several networks with different IP address. This can also be used in network 3G to provide transparency when user x of the internet migrates between cellular towers [2]. Cellular phones, PDAs, GPS and handheld devices are examples of wireless devices which have been developed rapidly. Cell phones allow users freedom of movement and Personal Digital Assistance "PDA" offers users to access email in any location. Global Positioning System (GPS) has the capability to pinpoint the location of the device anywhere in the world [3].Wireless technology promises to offer more features and functions in the coming few years.

Mobile IP is built on the IP protocol for internet infrastructure. As Mobile IP is a layer 3 solution for IP mobility, it will suffer from security problem in the same way as IP. As such the issue of securing Mobile IP has become the most significant point with increasing demand on Mobile IP [1]. The main goal of network security is to provide confidentiality, availability and integrity for data communication. In general confidentiality protects data so that it is not disclosed from unauthorized persons. Availability protects data from any attempts to withhold information and integrity protects data from unauthorized modification.

Since the internet is designed to interconnect computer and share information all over the world, it is subject to security attackers and threats such as session hijacking, denial of service, eavesdropping, address impersonation and so on. In order to protect against the attackers, firewalls, authentication and cryptography are used to secure communication [35][36].

The main differences between wireless networks and wired networks are mobility and medium. Wired network uses wire to connect the devices rather than radio waves to transmit data. Less wiring always mean more flexibility, portability and less installation cost. Since the airwaves are open to attackers the loss of integrity and confidentiality and threat of denial of service are most dangerous in wireless networks. Since Mobile IP is deployed in a wireless network it has the same characteristics as wireless network [4], we need to find away to secure mobile IP.

IPSec (Internet Protocol Security) was introduced by IETF as an open standard for ensuring private communication over IP networks protected by providing confidentiality, data integrity, authentication and replay protection. IPSec is different from other security standards as it is not limited to a single authentication method or algorithm. Over IPSec operates at the network layer. IPSec is designed in order to work with the protocol IPv6.The IPSec protocol suite was adapted for the current IP protocol (IPv4) and succeeds by routing message through an encrypted tunnel; this can be done by inserting AH and ESP header right after the IP header in each message.

Mobile IP can be integrated with IPSec to establish a solution called Secure Mobile IP (SecMIP) that protects Mobile IP devices and users from any security threats while they are accessing their organization‟s firewall through a virtual private network [37]. IPSec is applied to Mobile IP in both data tunnelling and registration process places.

Today, with a fast growth in the numbers of mobile devices, such as mobile phones, that are connected to the internet there is a shortage of numbers on current IPv4 that is not able to serve all these mobile users. IPv6 has been developed to cover the shortage of addresses. Mobile IPv6 is developed to allow mobility in IP networks combined with the mandatory features of IPSec protocol to achieve the demand of secure Mobile IPv6 [34].

1.2 Motivation

The number of the mobile devices such notebook computers, (PDA) personal digital assistants and mobile phones are increasing rapidly. Nowadays organizations are more dependent on information, thus employees need to be connected not only from their organization‟s premises, but also from elsewhere and in addition they required working remotely and access their business information using these mobile devices with appropriate security services.

Globally, mobile data will increase year on year until 2014, increasing 39 times between 2009 and 2014 reaching 3.6 exabytes per month or 40 exabytes per year by 2014 [5].

Mobile IP uses the standard TCP/IP protocol that routes datagrams to their destinations according to IP address. All the devices such as laptops, iPhones and PDAs are assigned IP address. The figure 1.1 shows overall mobile data traffic is expected to grow to 3.6 Exabyte‟s per month by 2014, and over 2.3 of those are due to mobile video traffic[5].This is because higher usage of the laptops and suitability of mobile broadband handset for high speed.

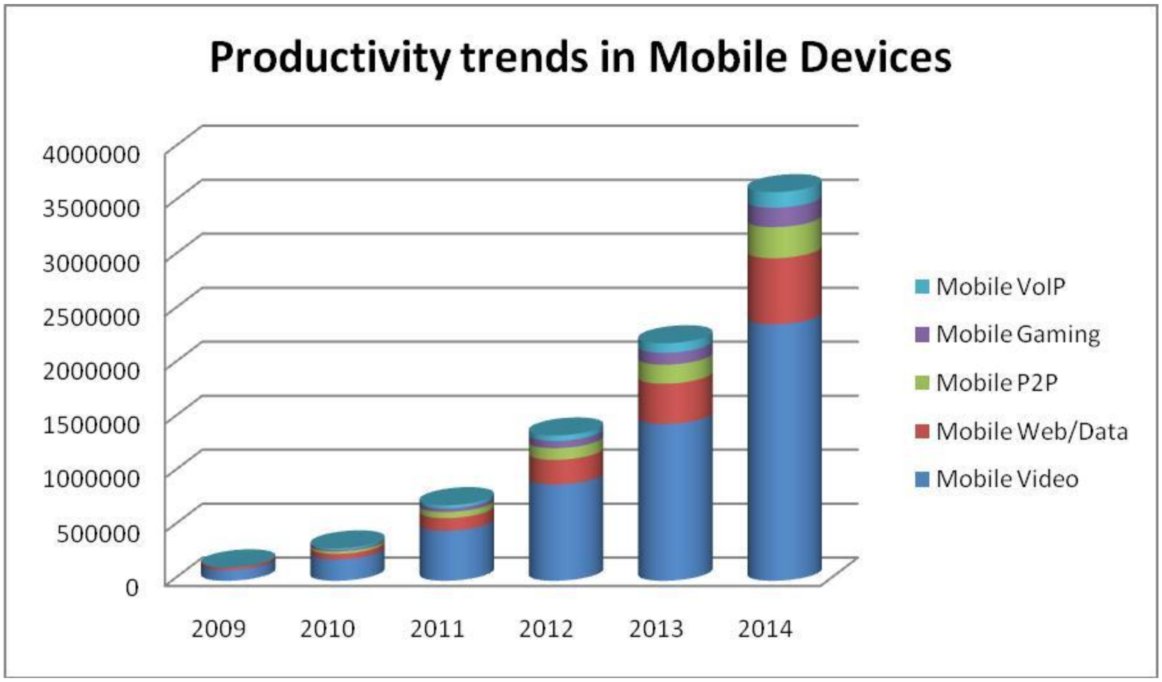


Figure 1.1- Productivity trends in Mobile Devices

1.3 Problem Description and Thesis questions

Security is always important in any network communication, especially with mobile IP networks, because mobile devices are using wireless communication that is less secure than a wired network.

The problem investigated in this thesis is about the security issues with mobile IP, especially due to using a registration system process and then forwarding the messages across an unsecured network.

In this thesis we hope to answer the following questions:

- How does Mobile IP work?
- What are the common security threats that faced mobile IP networks?
- What are the methods and suggestions to improve the security performance of Mobile IP?
- What is IPSec? How does it work? What issues does it handle?
- How does the secure MobileIP (SecMIP) work?
- What are the differences between MIPv4 and MIPv6?

1.4 Goal and Methodology

The methodology of this thesis is theoretical investigation, by studying different articles and comparing different approaches in how to combine IPSec with mobile IP to come up with the best solution to secure mobile IP.

Our goal in this thesis is to achieve a good solution to secure mobile IP. In order to accomplish this, it involves first hand analysis of the security issues that face mobile IP networks, the operation of the mobile IP and find out which points the attackers might break through.

1.5 Structure of thesis

This thesis is divided into eight chapters. The topic and main terms are introduced in the introduction. Chapter two provides an overview of wireless network security and continues with discussing internet vulnerabilities and secure technology. Chapter three describes mobile IP technology, entities of mobile IP, operation, registration and tunnelling. Chapter four detects the security issues with mobile IP and suggests solutions on how to improve security in Mobile IP. Chapter five introduces the IPSec protocols including security association, AH, ESP and IKE continuing with the combination of mobile IP and IPSec to establish a solution of (SecMIP). Chapter six describes the development of mobile IPv6 and differences between that and mobile IPv4 and describes mobile IPv6 security objectives and threats. Chapter seven contains discussion of our thesis work. The last chapter contains conclusion and suggestion to future work.

2 Internet Vulnerabilities and Secure Technology

In the beginning, the internet was created as an Advanced Research Projects Agency Network (ARPANET), it was essentially designed to share information between ARPA researchers. So it was designed as an open and flexible network but not to be secure. When the internet was exposed to the public, connecting millions of computers, it is inevitably subject to security threats such as denial of service, replay attack and session hijacking. For this reason security technologies such as cryptography, authentication and firewalls were developed to defend against the threats.

The known security threats can be classified in several types: denial of service, packet sniffing, address impersonation and session hijacking [10].

2.1 Internet Vulnerabilities

Packet sniffing

Packet sniffing is computer software or computer hardware which connects to the network and eavesdrops on the traffic. The sniffer captures the packets and tries to analyze and decode them [10] Packet sniffing can be used in a good way, where it is used by the network administrator to monitor the network and analyze the network traffic.

Information confidentiality is compromised if IP packets are caught in clear text. Many services and protocols on the internet such as FTP, Telnet and POP send data in clear text (plain text). The packet sniffer also can do what is called a replay attack where it replays the sniffed packets to a computer at the same connection [11].

Denial Of service

In this type of attacks the attacker sends and floods a huge number of requests to the computer server which causes an overload to the server. The server will not be accessible to the legitimate users, so this makes the server no longer functional [12]. A new type of Denial of Service attacks has been developed, known as Distributed Denial of Service (DDoS). In this attack the attacker uses multiple computers to flood a huge number of requests. (DDoS) is hard to stop because the attack is coming from a vast number of computers [12].

Address Impersonation

Impersonation attacks happen when the attacker can use some modifying tools to set any desired IP address in the packet .Every host on the network has unique IP address which identifies it. In the IP packet, two parts of information that must be in clear text, which are the source and destination IP addresses.

Therefore the IP address is the identity in network layer for which no authentication is provided for these network addresses [13].

Session Hijacking

The attacker gains unauthorized access to a session between two nodes and intercepts the packets it between them where it usually flows in clear text. The attacker sniffs the packets and then it can easily be altered and discarded. In the end the attacker can take over the whole session [13].

2.2 Security Technologies

A various number of technologies have been developed to defend networks from security threats. These technologies provide confidentiality, integrity and authentication. The classic technologies are cryptography, key management, authentication, auditing and firewall. These technologies are considered the basic blocks for the current security solutions.

Cryptography provides privacy and confidentiality to the information exchange by using encryption. Encryption is the transformation of data from readable form (Plaintext) to unreadable form (ciphertext). This process ensures privacy by keeping the information hidden to any intruder. Decryption is the reverse process of encryption which is transforming back the ciphertext to plaintext.

There are two methods of cryptosystems: symmetric and asymmetric. In symmetric cryptosystems, one key (public key) is used to encrypt the data for example DES, 3DES, AES.

In asymmetric cryptosystems two key are used, one key is used to encrypt the data (public key) and another one to decrypt the data (private key) for example RSA [14].

A symmetric key is usually used to encrypt messages while an asymmetric key is used for digital certification and key management. The two methods can be combined to provide cryptographic operation.

Authentication

Authentication is the process of making sure that the message is coming from an authentic source and going to an authentic destination.

Key Management

Key management is the process of managing the cryptographic keys. It includes the key generation, key exchange and key distribution. Keys should be changed frequently to ensure security.

The known key exchange algorithm that is usually used the Diffie-Hellman key algorithm which allows two nodes to exchange a secret key over an insecure network.

Firewall

A firewall is either hardware or software that used to enforce access control policy between networks. The firewall simply filters the incoming packets, where it rejects any unauthorized packets. Another type provides proxy services, data verification and authenticates service requests [15].

Auditing

Auditing is a mechanism used to log system activities. It has become an important technology in network security. Intrusion detection system (IDS) is one of these technologies, IDS is software or hardware device passively listens to the network traffic and when the IDS detects malicious traffic, it sends an alert to the management station [16].

2.3 Related works

Recently, several studies have been concentrated on ways of securing mobile IP. The author of Use IPSec in Mobile IP [6]; focused on how to use IPSec integrated with Mobile IP for (Home Agent-Mobile Device), (Home Agent-Foreign Agent), (Correspondent Node-Home Agent), (Correspondent Node-Foreign Agent) and (Mobile Device-Correspondent Node). The author of Secure and mobile Networking [7]; with an emphasis on how to improve Mobile IP operation that is protected by a combination of private address space , firewalls and source filtering routers. This improvement will help the mobile user in the public network such as the internet to keep a secure connection through the firewall organization network.

The author of packet filtering firewall and tunnel configuration to compatible mobility support in IP networks [8]; enhance a special gateways that has security such as firewall and foreign agent criteria in the same device and how IPSec provides authentication, encryption and integrity for data being sent from DMZ to the firewall. The author of considerations for Mobility and Firewalls research [9] explain how to use IPSec tunnels between mobile device and its home agent and using firewall with mobile IP and keeping DHCP secure.

3 Mobile IP

IP routing is based on the IP address, which uniquely identities a node‟s point of attachment to the internet [17]. When a device moves from its home network and enters a new network (foreign network), it has to change its IP address and re-establish a new TCP connection. If communication with this moving device occurs at that time, the communication has to be disconnected until a new IP address of a moving device is obtained. To solve this mobility issue, a working group within the Internet Engineering Task Force (IETF) proposed a solution, which is called Mobile IP Protocol.

3.1 Mobile IP Overview

Mobile IP is a standard protocol established by Internet Engineering Task Force (IETF) and designed to enable mobile users to move from one network to another whilst maintaining their permanent IP address.

The idea of mobile IP is similar to postal service delivery: once you move to a new location, you ask your home post office to send your mail to your new location‟s address by the local post office there [18]. Thus, a mobile device first leaves its home network and connects to a foreign network. The agent then sends packets locally to the mobile device visiting that network.

Mobile IP provides transparent Routing of IP datagram over Internet. Each mobile node is identified with its home address regardless of where its current location is. When a node is moved outside its home network as the node associated with a Care-of Address (CoA), which provides information on its current position.

Mobile IP specifies how a mobile‟s device registered with their home agent and how home agent routers connects to the mobile device through a tunnel. Mobile IP provides an efficient and scalable mechanism for roaming over the internet. When using Mobile IP, the devices can change their connection to the internet without changing its IP address. This means that the device can maintain a connection to the transport layer or a higher layer when the device moves and changes its location.

A mobile node may have two addresses, a permanent (home) address and a temporary address (care-of address), that changes at each new point of attachment. By using both addresses a mobile computing device can change its location and move to a new network without changing its home IP address and without loosing existing connections. The traffic redirects automatically between the home address and care-of address [18]. There are two versions of mobile IP, Mobile IPv4 and Mobile IPv6. Mobile IPv4 will be described in more detail in this chapter.

When IP packets are exchanged between a host and mobile device the following steps occurs that are shown in the figure 3.1:

1. Server x tries to connect to mobile device by sending IP packet with A‟s home address in the IP header. The IP address is routed to the home network.

2. The home agent intercepts the incoming packet and encapsulates the entire datagram inside a new IP care-of address and transmits the datagram as tunnelling to the foreign agent.

3. The outer IP header is removed by the foreign agent and sends the original IP datagram to A through the foreign network.

4. A mobile device receives the message and sends an IP packet to X using X‟s IP address to the foreign agent across the foreign network.

5. The foreign network routes the IP packet to the X server directly across the internet using X‟s IP address.

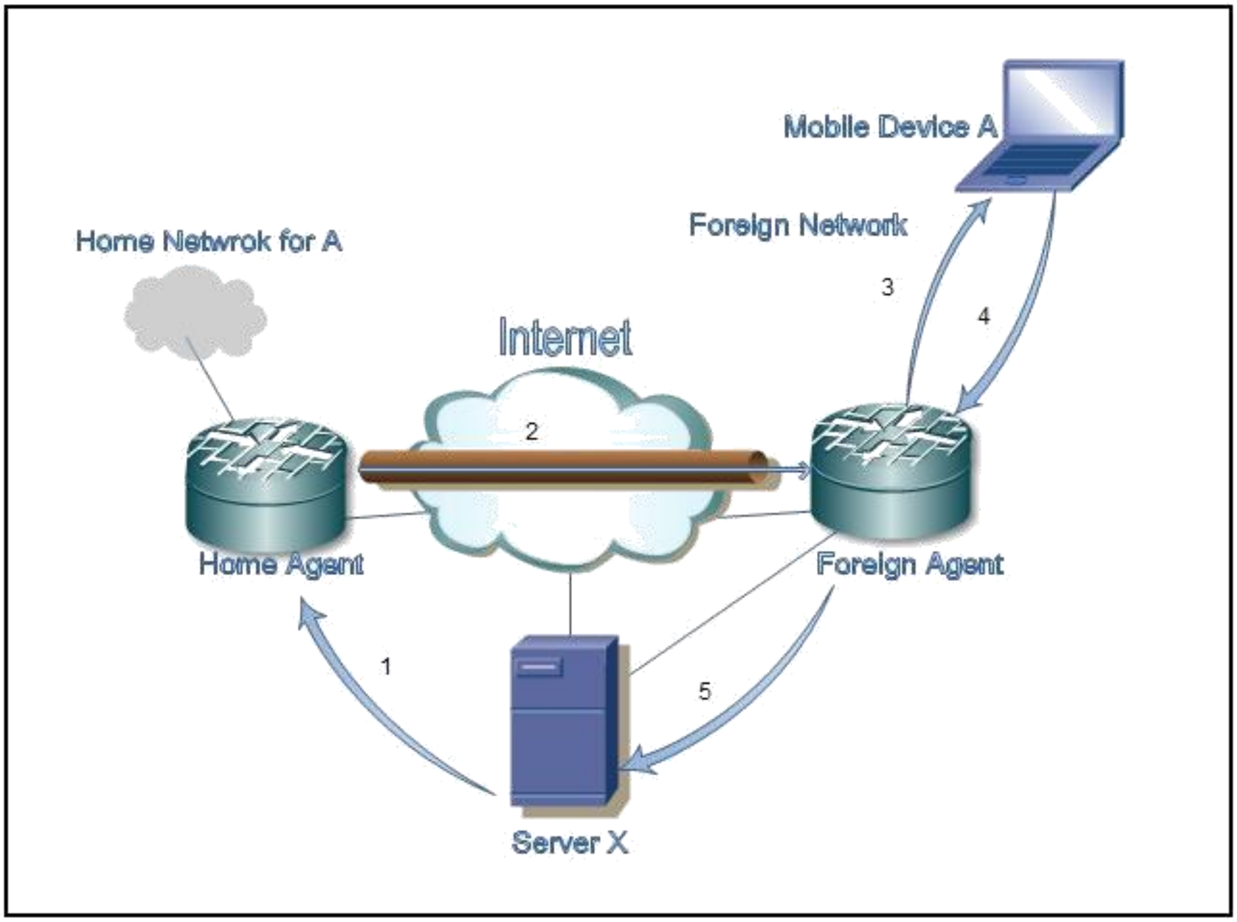


Figure 3.1- Mobile IP Operations

3.2 Mobile IP Terminology

Mobile IP has the following elements and entities that are required for optimum functionality [18][19] figure 3.2:

- Mobile Node (MN): is a moving internet connected device on which the location and point of attachment to the internet can be changed whilst keeping ongoing communication without interruption using its home fixed address. This kind of device is usually IP phone, laptop computer or router.

- Home Address: An IP address assigned to Mobile device within the network for extended period of time. It remains the same regardless of where the device is attached to the internet.

- Home Agent (HA): is a router on the mobile device‟s home network. It tracks the mobile device location (care of address), intercept and tunnels packets to the mobile device when it is away from home, and maintain s current location information for the mobile device.

- Home Network: is the network within which a device identifies as its home IP address. The IP routing mechanism will deliver packets destined to mobile device‟s home address to the mobile device‟s Home Network.

- Foreign Agent (FA): is a router on the mobile device‟s visited network. It provides the care-of-address to the mobile device and routing service to the mobile device whilst registered and acts as a default router for datagram generated by the mobile device. The foreign agent de-capsulates and delivers datagram to the mobile device that are encapsulated by the mobile device‟s home agent

- Foreign Network: Any network other than the mobile device‟s home network, on which the mobile device can operate successfully when away from its home network.

- Care-of-address: is a temporary IP address assigned to a mobile device while it is away from home network.

- Correspondent Node (CN): A device that sends or receives packets to or from the mobile device; the correspondent device may be another mobile device or a non mobile internet device.

A mobile device may have two addresses, a permanent home address and a care-of address (CoA).A care-of address is a temporary IP address that identifies a mobile device‟s current point of attachment to the internet and allows it to connect from different locations by keeping its home address. When a mobile device is leaving its home network and connects to any foreign network, it is assigned a care-of address. This may be a "foreign agent care-of address" which is a static address of a foreign agent with which the mobile device is registered, and a "co-located care-of address" which is a temporary IP address assigned to the mobile device. A co-located care-of address is assigned by Dynamic Host Configuration Protocol (DHCP), Point –to Point IP control protocol (PPP), or manual configuration.

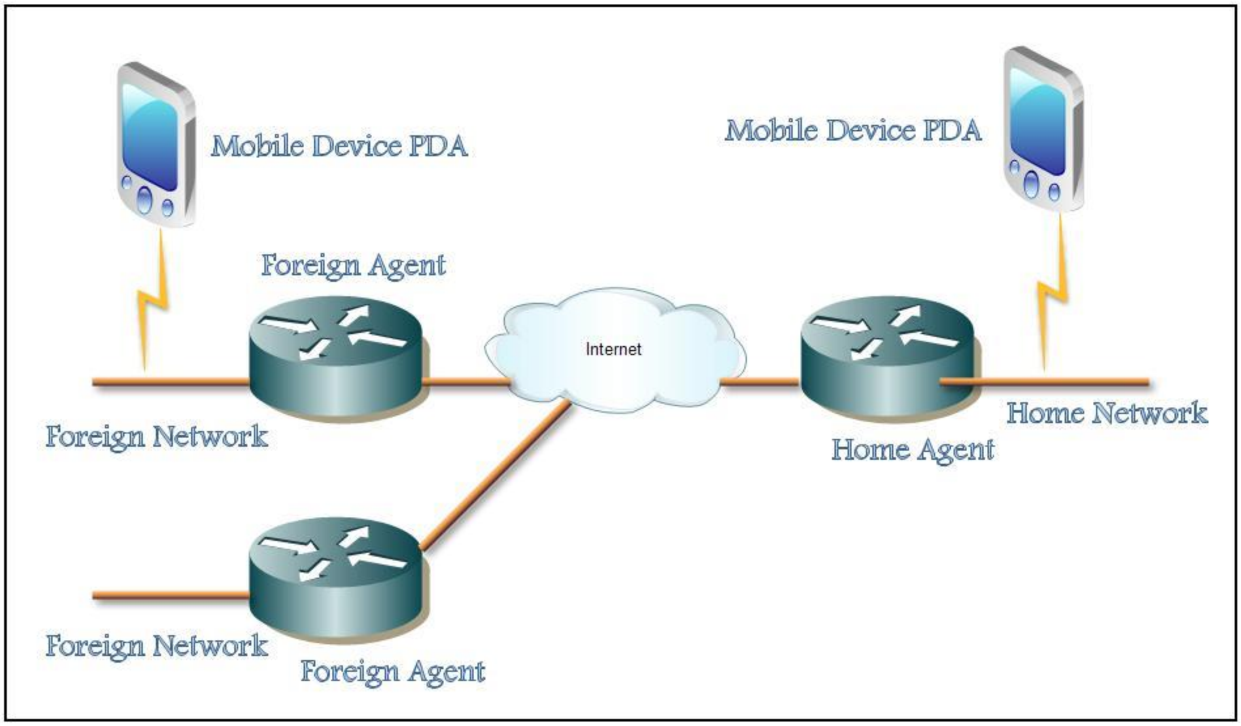


Figure 3.2- Mobile IP Components

3.3 Mobile IP Functionality

Mobile IP function can be divided using three mechanisms [19]:

- Discovering the Care-of Address;
- Registering the Care-of Address;
- Tunnelling to the Care-of Address;

3.3.1 Discovering the Care-of Address

The discovery process in Mobile IP is based on the ICMP (Internet Control Message Protocol). The mobile device is responsible for the discovery process by determining if it is attached to its home network or a foreign network. Because handoff from home network to the foreign network occurs at the physical layer, a transition between those two different networks can happen at any time without notification to the upper layer (network layer, i.e. the IP layer). The discover y process for mobile device is continuous. A special message called Agent Advertisement is periodically broadcasted by the home agent or foreign agent to advertise their availability to any attached links. A mobile device listens to these agent advertisement messages and compares the network portion of the router‟s IP address with the network portion of its own home address. If the network portions match, then the mobile device is on a home network; but if it does not match, then the mobile device is on the foreign network. If the mobile device stays in its home network, then it will work without Mobile IP functionality.

If the mobile device gets a foreign agent care of address, then the foreign agent will be the end of the tunnel and will perform the de-capsulation and will deliver the message to the mobile device. In the other case, if the mobile device gets a co-located care-of address, then the mobile device it self will perform the de-capsulation for the tunnelling.

3.3.2 Registering the Care-of Address

Once the mobile device gets a care of address and recognizes that it is on a foreign network, it needs to tell the home agent where it is and request home agent to forward its IP traffic. This is done according to the following process that is shown in (Figure 3.3):

1. The mobile device requests forwarding process by sending a registration request to the foreign agent that the mobile device moved to. This request contains the home address of the mobile device, care-of address of the mobile device and the registration lifetime.

2. The foreign agent passes this request to the home agent of the mobile device. In some cases, the mobile device may register directly with the home agent.

3. Home agent receives the registration request, it either accepted or denied. If the request is accepted, the home agent updates its route table associated the home IP address of the mobile device with its care-of address. The home agent keeps the association until the registration lifetime expires.
4. The foreign agent forwards this reply to the mobile device

Registration in Mobile IP must be secured so that malicious registration can be detected and rejected .Otherwise, attackers on the internet could disrupt communication between the home agent and the mobile device. However Mobile IP provides some authentication methods like identification field and timestamp.

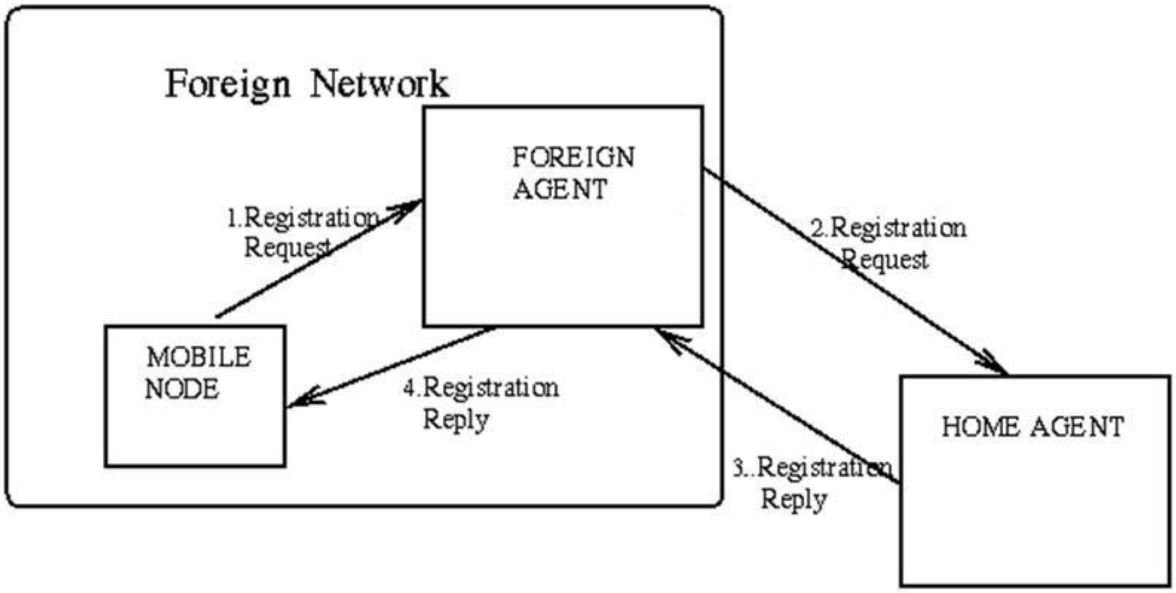


Figure 3.3- Registration process

The registration operation has two types of messages. The registration request message figure 3.4 consists of the following fields [18]:

Type: 1 this is related to a registration request.

S: Simultaneous bindings. The mobile device requests form home agent to maintain its prior binding mobility.

B: Broadcast datagram clarifies that the mobile device can receive a number of broadcast messages.

D: De-capsulation by mobile device. The mobile device is using a collocated care-of address and will de-capsulate its own tunnelled IP message.

M: Clarify that the minimal encapsulation will be used by home agent.

V: Clarify Van Jacobson header compression will be used.

G: Clarify that GRE encapsulation should be used by home agent.

Lifetime: The time in seconds before the registration is considered to be expired.

Home address: An IP address assigned to a mobile device within the network for an extended period of time. It remains the same regardless of where the device is attached to the internet.

Home agent: The IP address of the mobile device home agent. This tells the foreign agent of the address to which this request should go.

Care-of address: The IP address at this end of the tunnel. The home agent should forward the IP datagram that it receives with the mobile device home address to this destination address.

Identification: A 64-bit number generated by the mobile device.

Extensions*:* authentication extension.

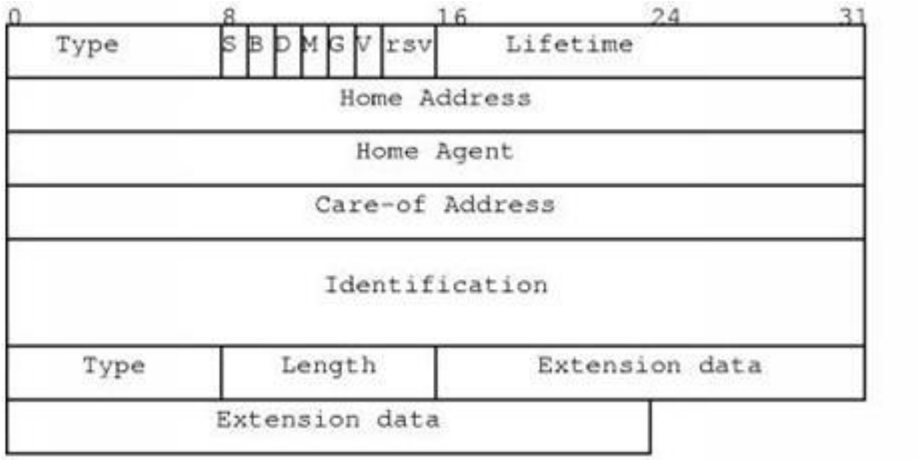


Figure 3.4- The registration request message.

The registration reply message in the figure3.5 consists of the following fields [18]:

Type: 3, this is related to a registration reply.

Code: Indicates result of the registration request.

Lifetime: is the time in seconds before the successful registration is expired.

Home address*:* The home IP address of the mobile device.

Home agent: The IP address of the mobile device home agent.

Identification: A 64-bit number used for matching to registration replies registration requests.

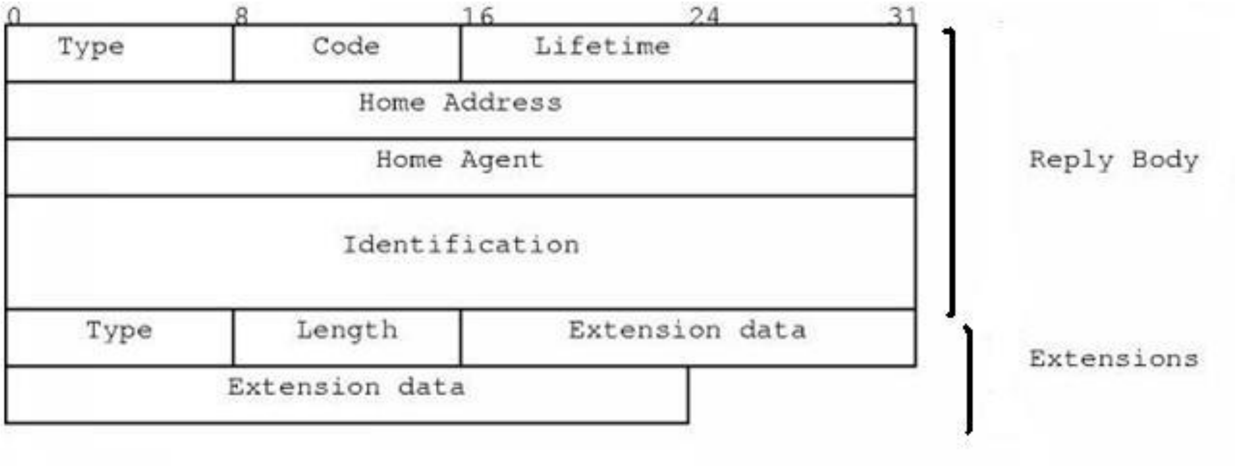
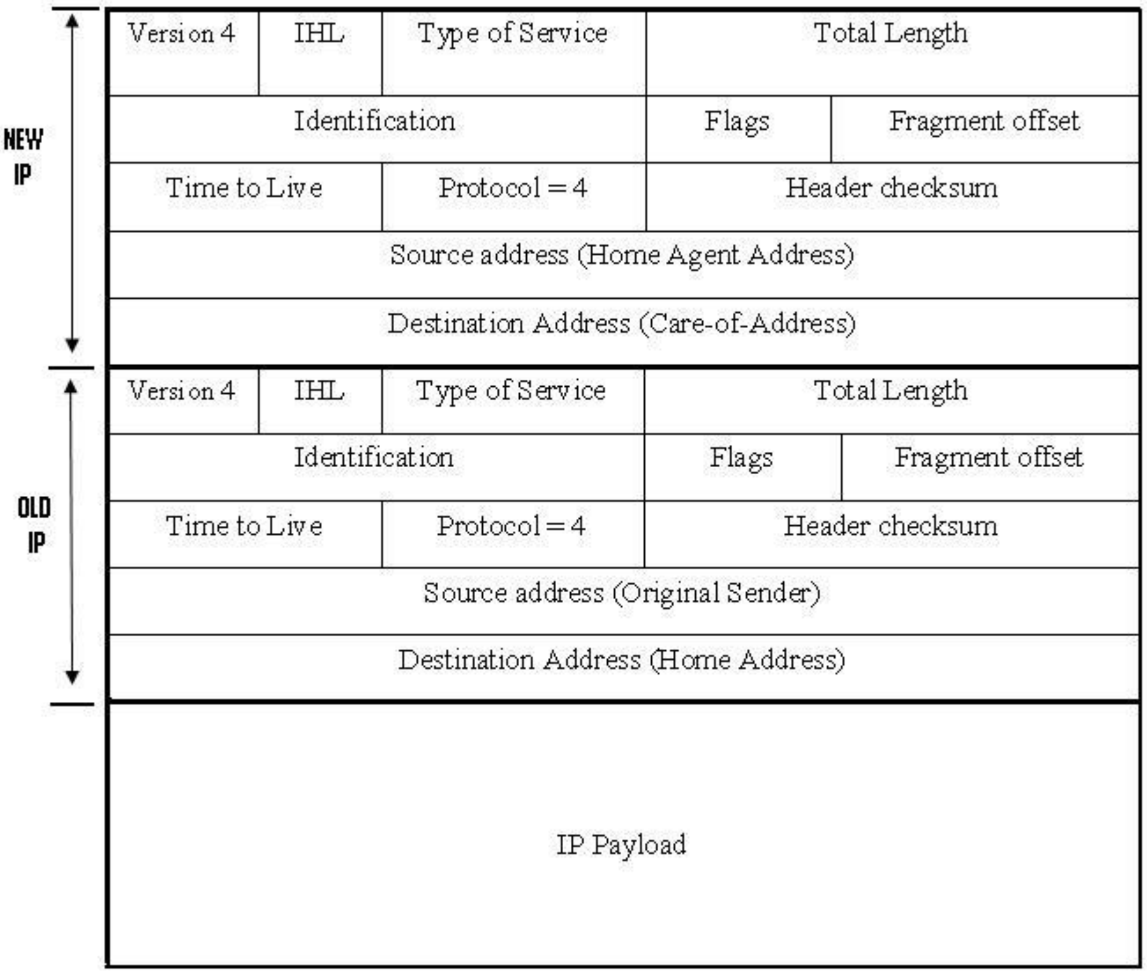


Figure 3.5- The registration reply message.

3.3.3 Tunnelling to the Care-of Address

Once the mobile device registers to its home agent, the home agent will be able to intercept the IP packets that send to the mobile device"s home address so that these packets can de transmitted using tunnelling. An encapsulation mechanism is used to forward the IP datagram to the care-of-address by inserting the entire IP datagram into an outer IP datagram by the home agent. Three different type of encapsulation are used in Mobile IP: IP-within IP Encapsulation, Minimal Encapsulation and Generic Routing Encapsulation (GRE).

- **IP-within-IP Encapsulation,** in this scenario the entire original IP packet becomes the payload in the new IP packet (figure 3.6). In the old IP header, the source address refers to the corresponding device that sends the original message and the destination address is the home address of the mobile device. In the new IP header the source address refers to the IP address of the home agent and the destination address refer to the care-of address for the mobile device.



<table>
<tr><td>Version 4</td><td>IHL</td><td>Type of Service</td><td colspan="2">Total Length</td></tr>
<tr><td colspan="3">Identification</td><td>Flags</td><td>Fragment offset</td></tr>
<tr><td colspan="2">Time to Live</td><td>Protocol = 4</td><td colspan="2">Header checksum</td></tr>
<tr><td colspan="5">Source address (Home Agent Address)</td></tr>
<tr><td colspan="5">Destination Address (Care-of-Address)</td></tr>
<tr><td>Version 4</td><td>IHL</td><td>Type of Service</td><td colspan="2">Total Length</td></tr>
<tr><td colspan="3">Identification</td><td>Flags</td><td>Fragment offset</td></tr>
<tr><td colspan="2">Time to Live</td><td>Protocol = 4</td><td colspan="2">Header checksum</td></tr>
<tr><td colspan="5">Source address (Original Sender)</td></tr>
<tr><td colspan="5">Destination Address (Home Address)</td></tr>
<tr><td colspan="5">IP Payload</td></tr>
</table>

Figure 3.6- IP within IP encapsulation

- **Minimal Encapsulation,** in this scenario the new header is inserted between the original IP header and the original IP payload (figure 3.7) this can be used if both home and foreign agent accepted to do so. Minimal encapsulation results in less overhead.

Home agent encapsulates the datagram as it shown in the (figure 3.7) through tunnelling and sends it across the internet to the case-of address. This minimal header is de-capsulated to the original header by either foreign agent or the mobile device itself. It includes the following fields [7]:

Protocol: This field specifies the protocol type of the original IP payload and also specifies the type of header that starts the original IP payload.

S: If 1, the original source address is exist. If 0, the original source address does not exist.

Header checksum: Calculated over all the fields of this header.

Original destination address: Is the same of Destination IP Address in the original IP header.

Original source address: Is the same of the Source IP Address in the original IP header.

The next fields in the original IP header are modified to form the new outer IP header:

Total length: Increased by the size of the minimal forwarding header (12 or 8).

Protocol: 55; this is the protocol number relied to minimal IP encapsulation.

Header checksum: Calculated over all the fields of this header.

Source address: The encapsulated IP address, mostly the home agent.

Destination address: This is the care-of address and may be either the IP address of the mobile device or IP address of the foreign agent.

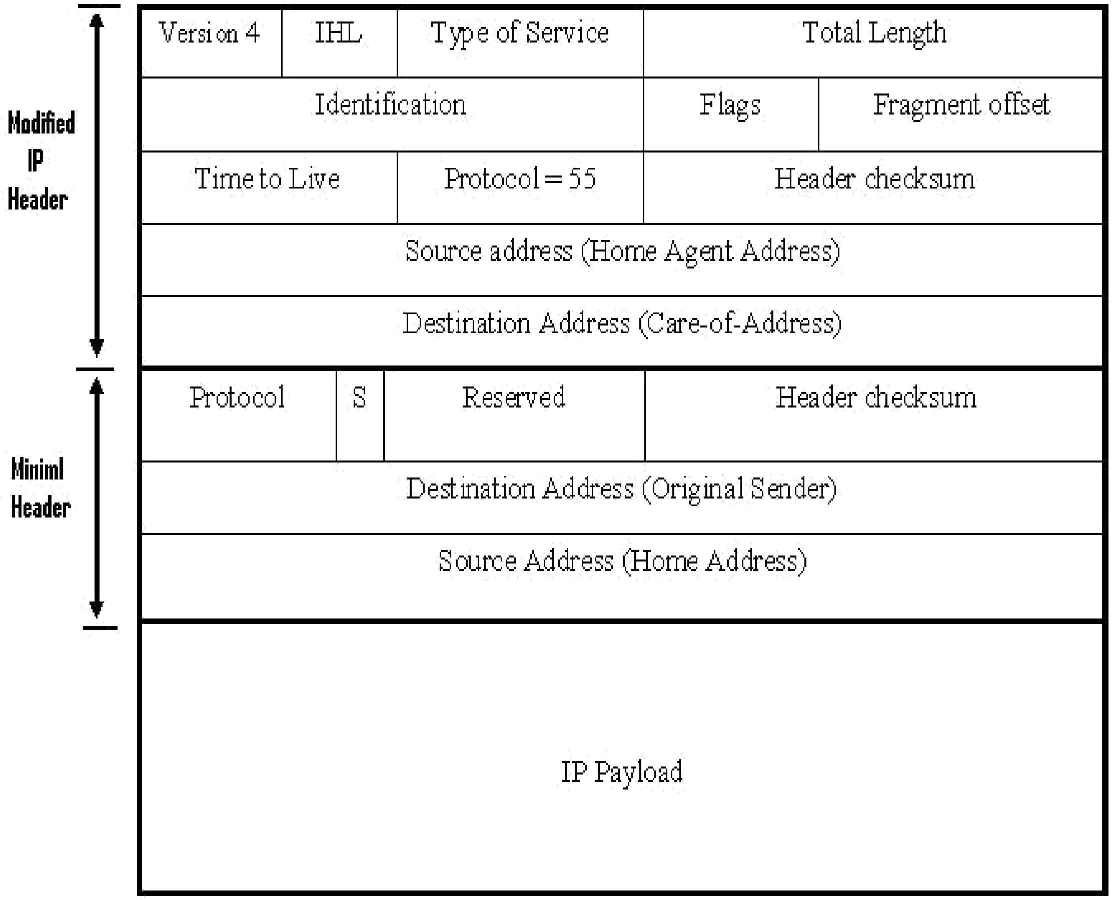


Figure 3.7- Minimal Encapsulation

- **Generic Routing Encapsulation (GRE)** is an optional tunnelling method used by mobile IP. GRE tunnel builds a virtual point-to-point link between two routers at remote point over an IP internetwork. GRE is good in certain applications because it supports multiprotocol and provides prevention of recursive encapsulation.

4 Security issues with mobile IP

4.1 Introduction

Security is one of the most challenging tasks in mobile IP network. Mobile IP allows mobile users to change their network attachment frequently without losing their connection, which gives many advantages to users. However, the mobility of communication devices and characteristics of the wireless channel introduce many security issues. Security issues for Mobile IP are considered when the mobile device registers its care-of address to the home agent, this registration messages requires an authentication. This chapter will introduce the common security threats that face mobile IP networks as well as the method and suggestion to improve the security performance of mobile IP.

4.2 Security issues with mobile IP

4.2.1 A Denial-of-Service Attack

A Denial-of-service attack (DoS) is raised up once the attackers prevent the authorized users from getting their work done [20]. This kind of attack usually takes the following steps:

1. By sending a large number of requests over the internet. These many requests make the target device to run below the optimum speeds till it become unavailable.

2. The other way is to intercept the communication between two devices on the network directly. For example, attacker can use the techniques of redirection to make the data not reach the authorized user.

In the case of Mobile IP, the denial of service attack happens once the attacker starts to manipulate the registration of a care of address for particular mobile device, figure 4.1 illustrated Denial of Service‟s manipulated registrations. Such a manipulation of registration leads to two issues:

- The Mobile device is no longer connected

- The attacker gets all the traffic directed to the original mobile device.

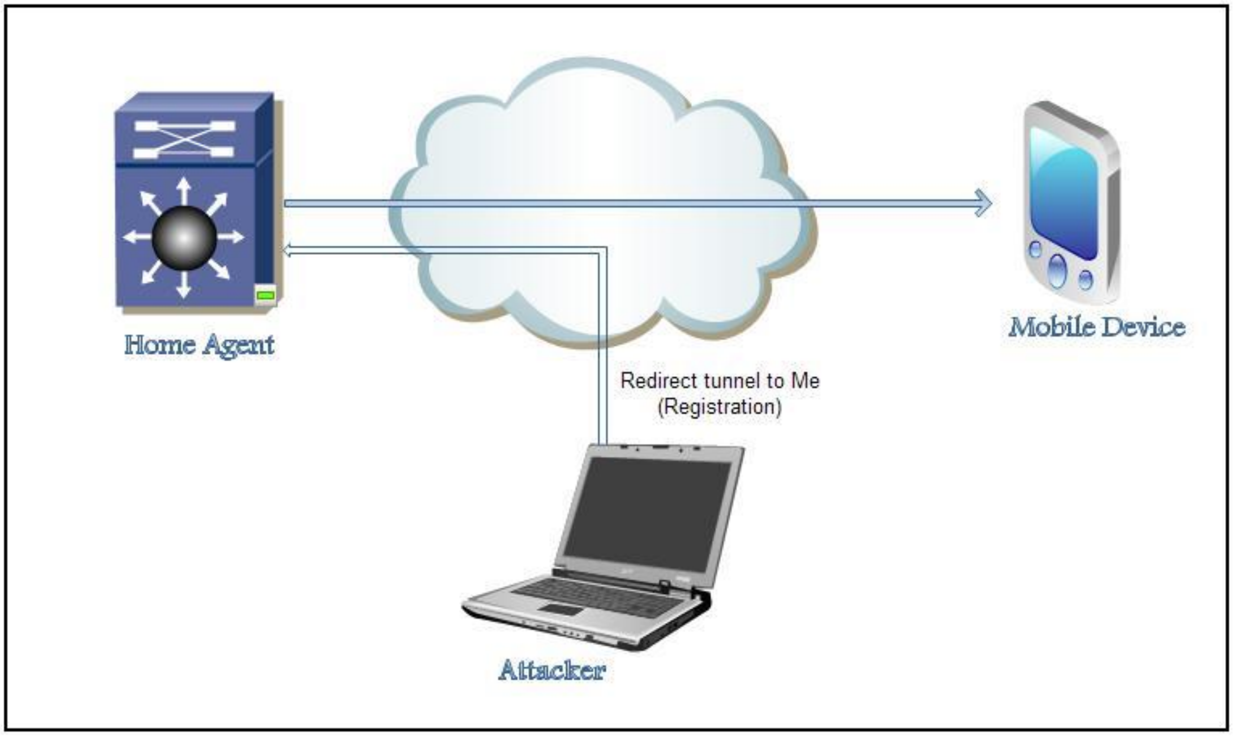


Figure 4.1– Denial of Service attack to a Mobile IP network

In this kind of attack, the attacker generally needs to be in the middle between the two corresponding hosts in order to cut off their traffic. With a Mobile IP network, the attacker can attack the network from anywhere, if a mobile device is connected on the foreign network, it is mandatory to use the registration method to inform its home agent of its current care-of address to which home agent will intercept and tunnel all the traffic destined to the mobile device‟s home address. So the attacker can generate a manipulated register request message declaring with its own IP address as the care-of address for a mobile device to the home agent. So all traffic transmitted to the Mobile device goes to the attacker instead. In order to protect the Mobile network from this kind of attacks, strong authentications are required in all registration traffic exchange by a mobile device and its home IP agent.

Authentication mechanism insures that that traffic is going to the mobile device that should receive it, not anybody else. Mobile IP allows a mobile device and home agent to use and agree with any authentication algorithms they agreed. However, all implementation of mobile IP supports the default algorithm MD5 which can provide the strong authentication that is needed.

4.2.2 Passive Eavesdropping

Passive Eavesdropping is type of a theft of information attack. A passive eavesdropping attack happens when an attacker start to listen to the traffic that is transferred between mobile device and its home agent.

The attacker in passive eavesdropping needs to access to the traffic in order this to happen; this can happen in different ways. An attacker can get access to a network and connect a host to the network. In case of a shared Ethernet, all traffic on the same segment may be a victim of eavesdropping. Sometimes a thief is able to receive packets transmitted by radio signals if he is close enough to the wireless network.

In order to prevent eavesdropping in mobile IP it is required to use encryption method to encrypt all ongoing traffic information. This can be done in several ways. Traffic should be encrypted on the foreign link, so the attacker can‟t decode and understand the cipher text and eavesdropping can no longer happen on the foreign link. Although, the traffic still might be a victim of eavesdropping on the rest of end to end connection.

The best solution would be to use the end to end encryption method on all traffic, this makes eavesdropping attacks impossible.

4.2.3 Reply Attack

Using Authentication, a mobile device can prevent the denial of service attack as we mentioned in previous sections. However it cannot protect mobile devices from a reply attack, because the attacker can have a copy of the valid registration request message, buffer it, and then reply it later on by registering a manipulated care-of address for the mobile device.

To prevent this kind of attack, the mobile device has to generate a unique value for identification field of each successful attempt of registration. As such, the stored registration request message by the attacker will be defined as out of date from the respective home agent. Mobile IP defines two ways to set identification field. The first one uses timestamp, where the mobile device uses an estimate date and time of day in the identification field. The second method uses a random number. In this method, the mobile device and home agent declare the value which is entered in the identification field accordingly. A message will be rejected if either device receives a registration message with identification field that not match the expected value and this message will be ignored in the case of the mobile device [9].

4.2.4 Session Stealing

Session Stealing is a type of theft of information attacks the same as passive eavesdropping, but in different steps:

- The attacker waits for the mobile device to authenticate and register with its home agent and starts application sessions.
- The attacker eavesdrops on the mobile device to see if any interesting conversation traffic comes through.
- The attacker then floods the mobile device with malicious packets.
- The attacker steals the session by intercepting the packet that is going to the mobile device then the attacker send their own packets that appear to have come from the mobile device.

The user of the mobile device might not notice that the session has been stolen because there is no sign that something like this has happened. The protection against session stealing is the same as passive eavesdropping by providing end to end encryption with authentication.

4.2.5 Tunnel Spoofing

The tunnel to the home network or foreign network may be used to hide malicious packets and get them to pass through the firewall.

As registration method is a key role of Mobile IP, Mobile IP has some basic security solutions. Mobile IP requires authentication for registration methods between the mobile device and the home agent. Moreover, Mobile IP uses identification fields and timestamp to protect registration from any attacks.

4.3 Security Models

In order to secure the protocol, two approaches can be used [35]:

4.3.1 Weak Security Approach

Weak levels of security may be used between users in environment such as “campus”, since these services are not high added value or not primarily of commercial nature. A protection against manipulated attempts could be:

- Home Agent assures the care-of address of mobile device is correct, because the allowed care-of address relates to a well known IP address.
- The mobile device in the foreign network has to authenticate bindings.
- When a mobile device attaches to the foreign network, it sends a registration request with password to the home agent.

4.3.2 Strong Security Approach

The weak security approach that was discussed in the previous section is not suitable any more. Both now have to agree on a stronger level of security policy where mobile IP authenticates any binding message or authenticates information received about a mobile device. Trusted servers and private and public keys are used, but they slow down the operation.

4.4 Security Improvements of Mobile IP

4.4.1 Using Tunneling instead of Source Routing:

The main purpose of using tunneling techniques instead of source routing is that tunneling relates to fewer security threats. Attacker can use a manipulated care-of address as a destination in a loose source route. This will make the correspondent node reverse the source route and send the message to the manipulated care of address. So the mobile device is disconnected from communicating with his correspondent node. This issue can be solved by proper use of authentication [21].

4.4.2 Avoiding Route Optimization:

When a mobile device is communicating with a correspondent node from a foreign network, all its packets must be forwarded through its home agent, this is called triangle routing which can results in significant degrading of performance.[22]Route optimization to mobile IP has been recently proposed, allowing the home agent to inform the correspondent node with the mobile device‟s care of address, thus correspondent node can communicate directly with mobile device without passing the home agent, which results in less delay and resource consumption. However the main issue with route optimization is security. A network administrator configures a secret key to authenticate between the mobile device and its correspondent node, but with a large numbers of mobile devices, it is not practical to configure keys between a mobile device and every other correspondent node. In the case of triangle routing, it‟s conceivable to configure a key between mobile device and its home agent.

4.4.3 Using Firewall:

A firewall is used to prevent unwanted access to network services. The firewall monitors the traffic going through the network and decides on the basis of defined rules whether certain packets are allowed through or not. In this way it tries to prevent unauthorized access. Typically, a firewall can not prevent the exploitation of vulnerability in the network service if the communication partner can access it [15]. There are several kinds of firewall, mainly in the following three categories:

- **Packet filtering**: It is the oldest network filtering device, introduced on routers. The simple filtering data packet uses the network addresses as basic function of the firewall. It looks at each packet independently and compares it to a list of preconfigured rules. The issue with packet filtering is that it is hard to configure correctly and they cannot keep private IP address invisible to public IP addresses.
- **Stateful Inspection:** This stateful filtering is an advanced form of packet filtering. It has two main improvements over packet filtering, session table to track all connections and recognition of dynamic application. This make statetful inspection better in protect the internal network from unwanted external access.
- **Proxy filter:** A proxy firewall is a firewall which is based dedicated proxy and circuit level proxy recourse as filter modules. These filter modules implement rules by deciding what data is transferred to the actual communication party. In this way it tries to proxy firewall its own network (segment) to protect against unauthorized access, but can also make a conversion of the data cache of certain content, and exercise all other functions that are particular to a proxy.

In summary, we can say that firewalls provide good security and flexibility for mobile IP by using the firewall categories described above.

4.4.4 Implementing IPSec as a solution to security issues in Mobile IP:

IPSec (Internet Security protocol) is defined by IETF as a framework of open standards for ensuring private communications over IP networks protected by the use of cryptographic security services·

In the next chapter we will discuss in detail how IPSec works and what the issues does it handle and how can it solve these problems

5. IPSec with Mobile IP

5.1 IPSec overview

The IPSec suite is an end-to-end security scheme working in the IP layer, used to provide privacy and authentication services. IPSec suite provides security algorithms with general framework that allows using the appropriate security algorithms for the communication. IPSec is widely used as a means of secure communication through the internet [23].

IPsec developed by the Internet Engineering Task Force (IETF) to secure the packet exchange.

It contains three main protocols: the ESP Protocol, AH Protocol and the IKE Internet Key Exchange, where they provide confidentiality, data origin Authentication, connectionless Integrity to the communication [24]

5.2 IPSec components

IPSec suite is an open standard contains three protocols [10]:

- Authentication Header (AH): The IP Authentication Header (AH) is used to provide integrity and data origin authentication, and protection against replays but it does not provide confidentiality protection.
- Encapsulating Security Payload: is designed to provide a combination of security services integrity, confidentiality, and authentication of data for both IPv4 and IPv6. ESP may be applied alone, or with the IP Authentication Header (AH).
- Internet Key Exchange (IKE): Is a key management protocol where it provides a security association to handle the negotiation of authentication algorithms, encryption algorithms, which keys to use and the key‟s lifetime.

The Figure 5.1 shows the IPSec architecture

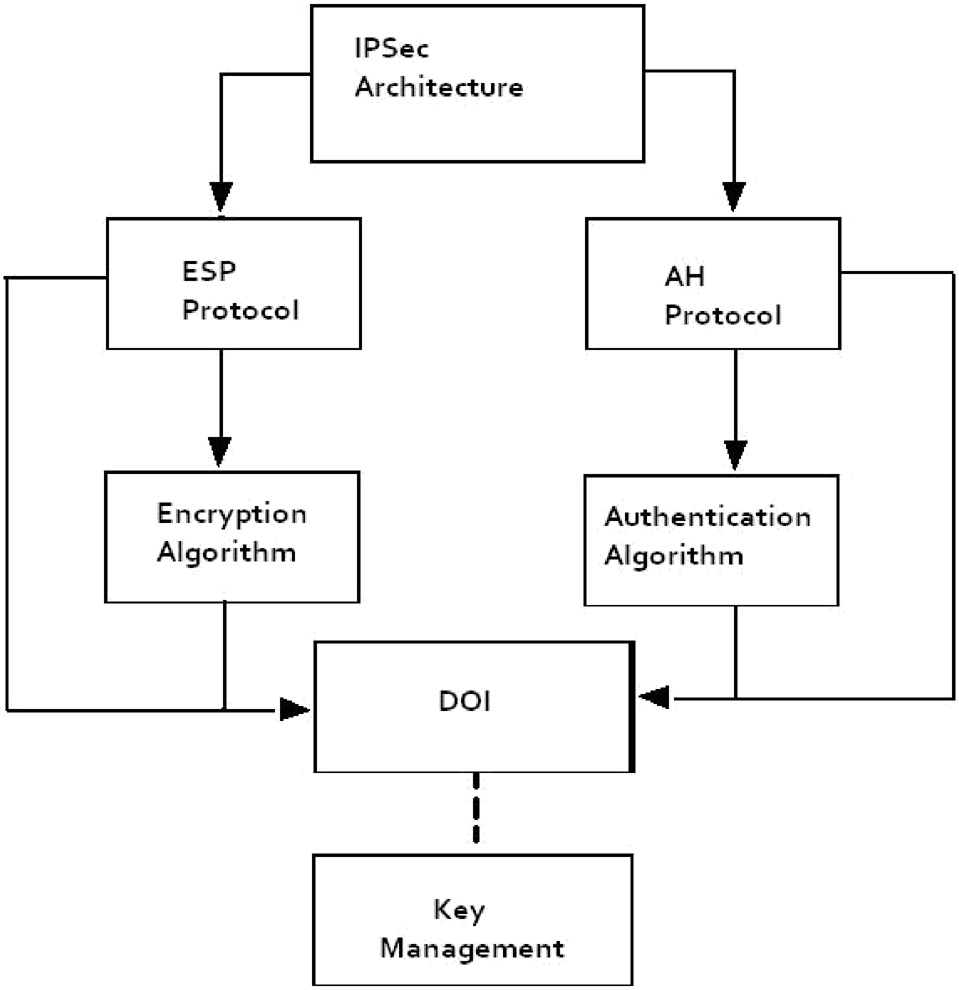


Fig 5.1- IPSec Architecture

5.3 Security association (SA)

A security association is a set of algorithms and keys that is used for encryption and authentication in a one-way directional agreement it is like a contract which specifies the particular security mechanisms that are used for secure communications between the two[26].

The actual choice of encryption and authentication algorithms (from a list) is the job for IPSec administrators.

The security association‟s concept is fundamental to IPSec.

SA manages the following policies under the IPSec [26]:

- The authentication algorithm‟s mode that is used in the AH and the authentication algorithm keys.
- How to secure the communication (which algorithms and keys).
- How many times the keys are changed.
- Cryptographic synchronization size that is used in the encryption algorithm.
- The encryption algorithm mode and keys of ESP.
- The key lifetimes.
- The authentication algorithm and mode and transform for use in ESP and the key that used by the algorithm.

There are two databases used to manage the SA‟s in the IPSec: the Security Po licy Database (SPD) and the Security Association Database (SAD).

The SPD specifies the orders and types of SAs and provide them to the SAD; the SAD specifies the parameters for the SA [27].

IPsec operates as the following: when communication between two ends need protection, first the two ends negotiate the SAs to decide the security parameters with IKE, after that, when one end sends a packet, first it looks up the SA in the database where it looks at SPD first then the SAD.

To specify which protocol is used, ESP or AH or both it inserts an SPI (Security Parameter Index) in the IPsec header. When the receiver receives the packet, it looks up the SA in its database SPD and then SAD by the destination address and the SPI [27].

5.4 IPSec modes

There are two modes used by IPSec to forward data: Tunnel mode and Transport mode [28].

Tunnel mode

In tunnel mode the whole IP packet is encrypted and protected, in this case the IP header is hidden because the tunnel mode encapsulates it, a new IP header will be added to be forwarded. These IP addresses that are inserted in new headers will be configured in the two end devices.

Tunnel can be used with either AH or ESP or both, and in tunnel mode an additional 20 bytes will be added to the original packet (the new IP header) [28].

Transport mode

In this mode only the IP payload is encrypted, and the IP header is left without encryption

The disadvantage of this mode is that the source and destination addresses are visible and not protected whereas the advantage is that a few bits are added to the packet. Transport mode can be used with ESP or AH or both [28].

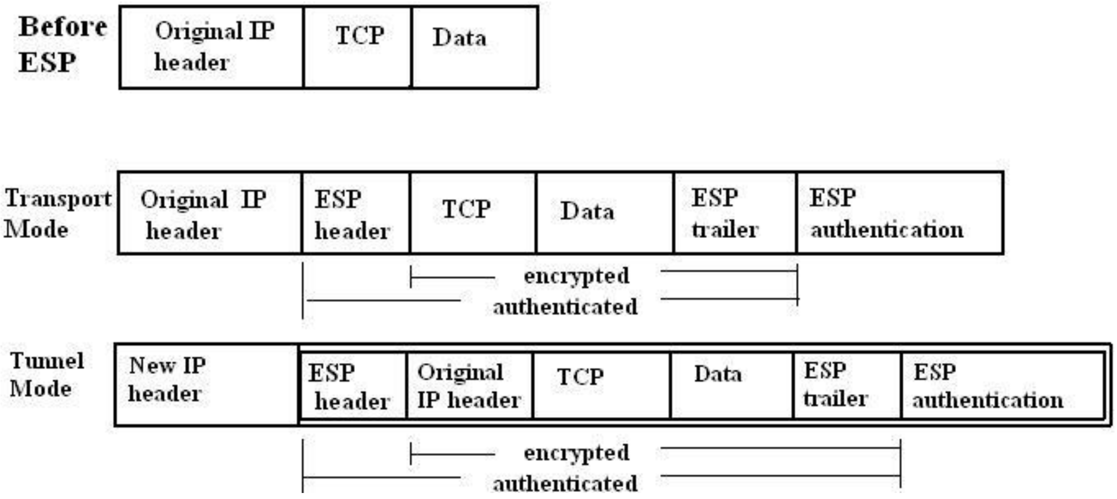


Figure 5.2- ESP in Transport Mode and Tunnel Mode

5.5 IPSec Technologies:

IPSec provides confidentiality, authenticity and integrity by using a combination of different security technologies [10]:

- Diffie-Hellman key exchange to create key material between the two peers.
- Algorithms used for encryption like DES, IDEA and RC4.
- Keyed hash algorithms like HMAC in combination with traditional one-way hash algorithms such SHA and MD5.
- Public key cryptography to sign the Diffie-Hellman exchange.
- Digital certificates.

5.5.1 Authentication Header Protocol (AH)

Provides authentication, integrity and optional anti-replay protection AH protocol does not protect the packet but it protects only the data portion, therefore it does not provide confidentiality. AH protocol should not be used alone when data confidentiality is required [10].

AH is an IP protocol and is assigned the protocol number 51 and supports SHA-1 and MD5 algorithms.

The Figure 5.3 shows the AH header which is inserted after the IP header and before the upper layer TCP, UDP, ICMP.

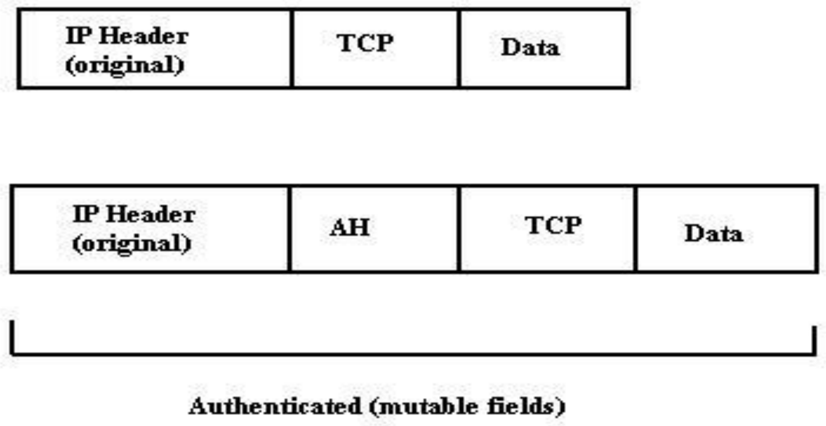
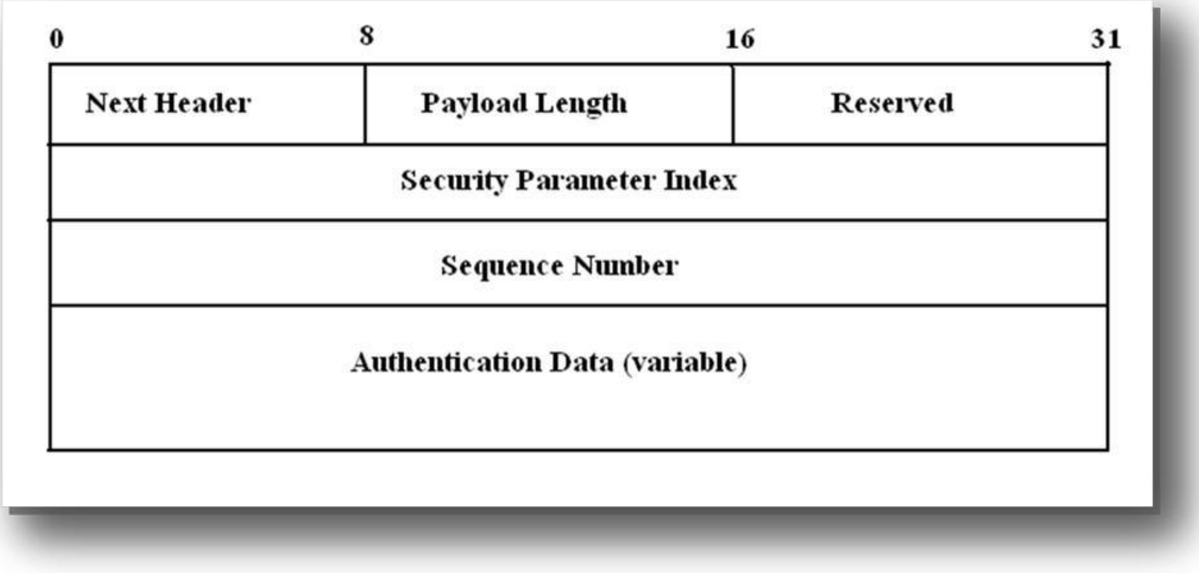


Figure 5.3- AH header is inserted after the IP header and before the upper layer

The Figure 5.4 shows the IP Authentication Header Format:



0	8	16	31
Next Header	Payload Length	Reserved	
Security Parameter Index			
Sequence Number			
Authentication Data (variable)			

Figure 5.4- IP Authentication Header Format

Next Header (8 bits): identifies the -type of next payload after the AH.

Payload Length (8 bits): identifies the AH length.

Reserved (16 bits): for future use.

Security Parameter Index (32 bits): An arbitrary value uniquely identifies the SA of the connection.

Sequence Number (32 bits): contains a counter value that is incremented by 1 every packet sent used for anti-replay protection.

Authentication Data (variable): contains the integrity check value (ICV) of the packet.

5.5.2 Encapsulating Security Payload (ESP)

It is used to provide confidentiality, connectionless integrity, data origin authentication, and an anti-replay protection. The difference between ESP and the AH is that ESP provides encryption by using encryption algorithms and cryptographic key. ESP supports symmetric encryption algorithms DES-CBC and integrity algorithms HMAC-SHA1, and can be used alone or a combination with AH [10].

The set of services provided are selected at the time of (SA) establishment and implementation.

The Figure 5.5 shows the ESP Header that is inserted before the IP header and after the upper layer protocol.

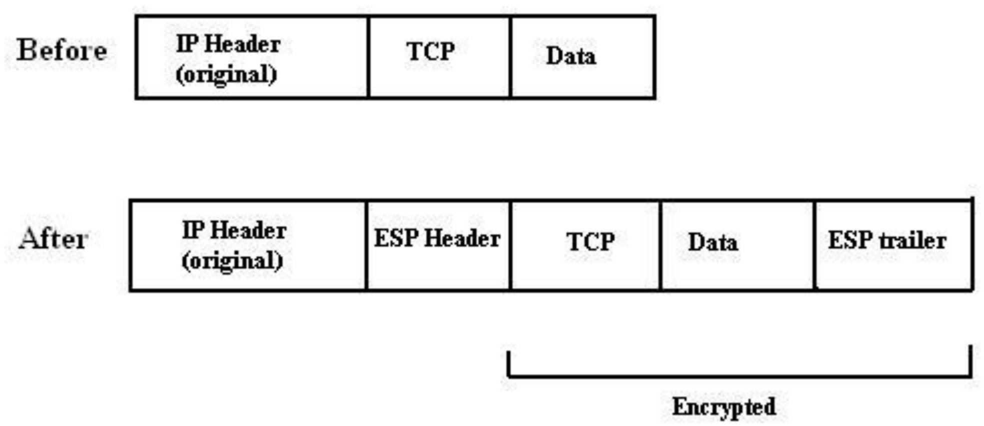


Figure 5.5 -ESP Header inserted before the IP header and after the upper layer protocol.

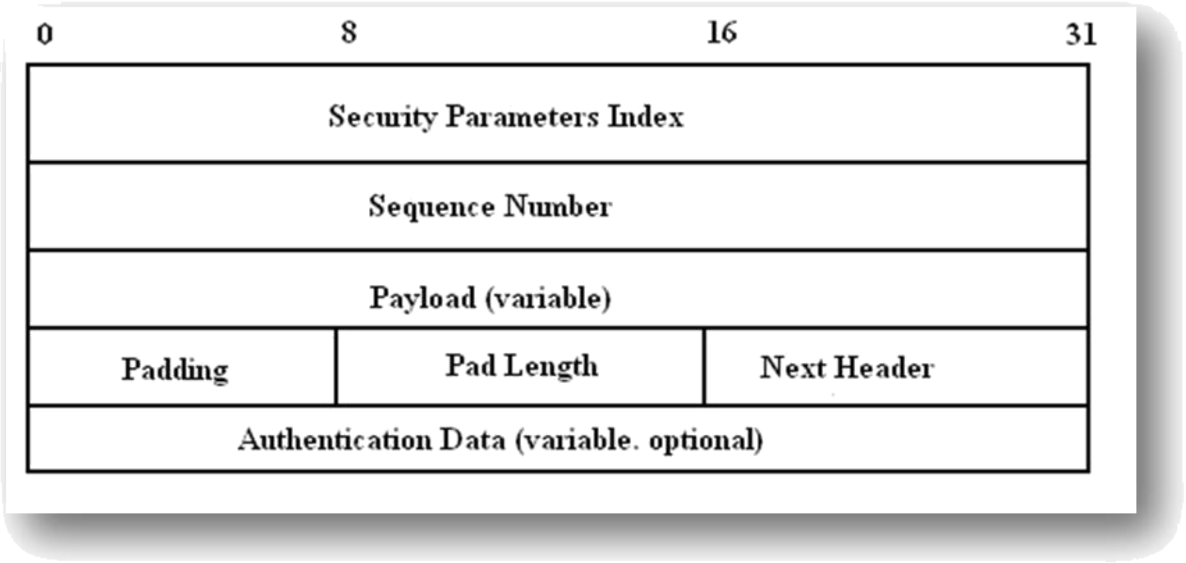
ESP has two fields beside the ESP header:

- ***ESP Header:*** It contains two fields, the SPI and the sequence Number, where it comes before the encrypted data. It is used to indicate whether ESP is used in tunnel mode or transport mode.

- ***ESP Trailer:*** This field is inserted after the encrypted data. It contains padding which used to align the encrypted data, it is also contains the Next Header.

- ***ESP Authentication Data:*** This field contains the Integrity Check Value (ICV).

The Figure 5.6 shows the IP Encapsulating Security payload format



0	8	16	31
Security Parameters Index			
Sequence Number			
Payload (variable)			
Padding	Pad Length	Next Header	
Authentication Data (variable. optional)			

Figure5.6 -IP Encapsulating Security payload Format

Security Parameters Index (32 bits): An arbitrary value uniquely identifies the SA of the connection.

Sequence Number (32 bits): contains a counter value that is incremented by 1 every packet sent used for anti-replay protection.

Payload (variable): a variable-length field contains data described by the Next Header field.

Padding: padding for encryption.

Pad Length: indicates the number pad bytes ranging between 0-255.

Next Header (8 bits)**:** identifies what type of data in the next payload field.

Authentication Data: a variable-length field contains an Integrity Check Value (ICV)

5.5.3 Internet Key Exchange (IKE)

IKE is a key management protocol used to establish and negotiate the security association (SA). It is a hybrid protocol which uses the Oakley key exchange and the Skeme key exchange with the Key Management Protocol (ISAKMP) framework. (Oakley, ISAKMP, SKEME are security protocols implemented by IKE)[10].

The usage of IKE allows devices to exchange information required for secure communication. As the name indicates, it includes cryptographic keys used to encode authentication information and performing payload encryption. IKE‟s main job is to allow IPSec-capable devices to exchange (SAs) [10].

IKE works in two Phases [28]:

Phase 1: is where the two devices initially negotiate the SAs to establish secure channel to exchange information phase 1 occurs in two modes: main mode or aggressive mode.

Phase 2: is the establishment of non-IKE SAs ESP and AH services, there is only one mode in Phase 2 which is the quick mode.

Phase 1 to establish the primer secure channel.

- Main mode: accomplishes a phase 1 IKE exchange by establishing a secure channel.
- Aggressive mode: simple and fast comparing to the main mode, because the peers transmit their identities before negotiating a secure channel. The disadvantage of this mode is that there is no identity protection.

For the phase 2, there is only one mode.

- Quick mode is the negotiation of SA for general purpose communications

To establish an IKE SA, the node proposes these police:

- Encryption algorithms (for data protection)
- Hash algorithms (integrity)
- An authentication method
- Information about the group type over which to do a Diffie-Hellman exchange
- The type of protection to use (ESP or AH)

5.5.4 Diffie-Hellman

The Diffie-Hellman protocol is a method for two parties to generate a shared private key used to encrypt and decrypt data across an insecure communication. In Diffie-Hellman, the two users generate a public and private key pair. The private will be kept secret and never shared. The public key is created from the private key and is exchanged over the insecure communication. After that, each user combines the public key of the other user with its own private key and calculates the same shared secret number. The shared secret number will be converted into a shared secret key. The operation is shown in Figure5.7. This shared secret key is never exchanged over the insecure communication [10].

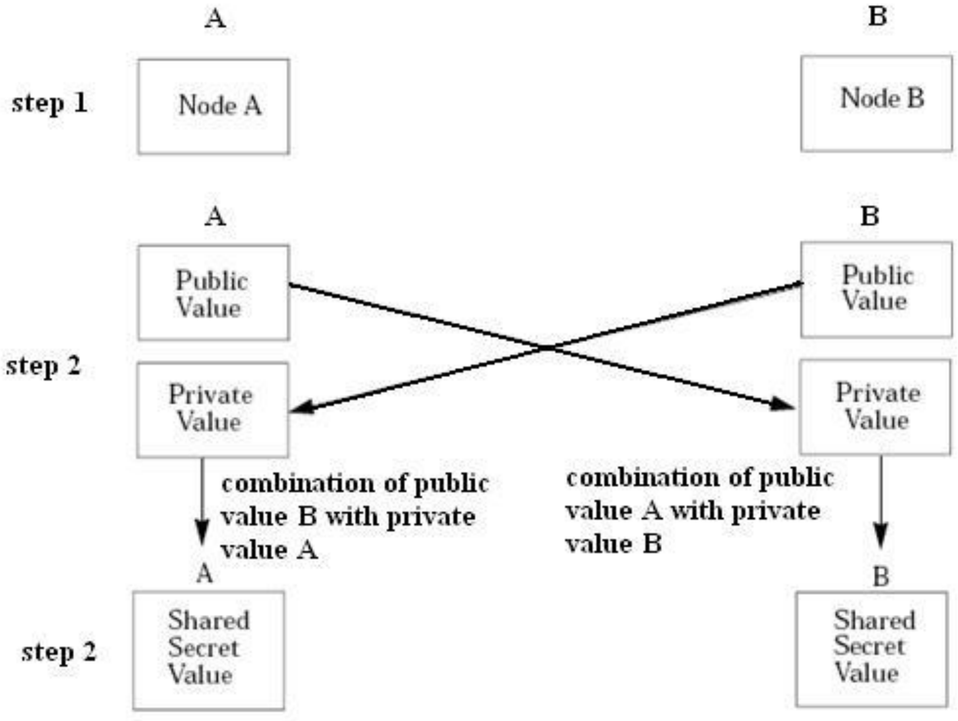


Figure 5.7- Diffie Hellman (key exchange)

5.6 Use of IPSec in Mobile IP

There is more than one proposal and development that investigates the issue of IPsec mobility and security. Zao and Condell proposed a solution to use of IPSec with Mobile IP for connections HA-MN, HA-FA, CN-HA, CN-FA, and MN-CN .IP-IP-tunnelling is replaced by IPSec and also some small adaptations or extensions to the advertisements and registration messages to cope with the IPSec tunnel [24].

Binkley and Richardson, proposed a way to secure firewall protected area that tolerates Mobile IP or simple mobility systems like DHCP. In this paper they discuss how to use bi-directional

IPSec tunnels between the MN and HA. This scenario is considered as special ad-hoc case where the MN and the HA create a secure ad-hoc network [30].

Another proposal is suggested by V.Gupta and G.Montenegro which considers deployment architecture that describes some enhancements to enable secure Mobile IP operation in the network [29]. These enhancements give the mobile user secure connection in the public network within the firewall-protection. ISAKMP is chosen for key management.

Torsten. B and Marc. D proposed a solution called Secure Mobile IP (SecMIP) [25]. They suggest that the interior network is protected by a firewall which acts as the only gate to enter the network. IPSec tunnel will be established between the Mobile IP node and the firewall. The use of SKIP is proposed for key management authentication and encryption [25]. This proposal will be discussed in details later as we consider it as a good solution.

In Mobile IP security, IPSec following features are provided:

- A Tunnel will be created between the two end pairs by using an automatic key and the security association management protocol.
- The use of IPSec ESP protocol in mobile IP by protecting the redirected packets against passive and active attacks.
- IPSec helps the packets to go through firewalls.
- IP-Security and mobility integration.

5.6.1 SecMIP (Secured Mobile IP)

Torsten. B and Marc suggest that the idea is to design a new deployment architecture taking the best features of the existing protocols. SecMIP is one of these designs, which stands for Secured Mobile IP. This design is called screened-subnet firewall where the private network is isolated from the outside network (internet) by a demilitarized zone (DMZ). The firewall between the DMZ and the private network is the only entry to the private network [31].

This architecture simplifies the security management where all the traffic will pass through the firewall, the home agent device is placed inside the private network and all mobile IP nodes must be placed outside (in the DMZ).This provides privacy and protection to the internal network from attacks coming from the internet.

The mobile IP node has to authenticate itself to the firewall and this authentication is done by the IPSec protocol. This authentication can be configured with a shared secret or RSA keys. SecMIP uses IPSec tunnel by protecting the mobile IP tunnel where it passes through the insecure outside network (Internet), whereas inside the private network the tunnel is not important. SecMIP uses ISAKMP/Oakley and SKIP, the two are used to provide security for key exchange [29].ISAKMP is preferred over the SKIP.

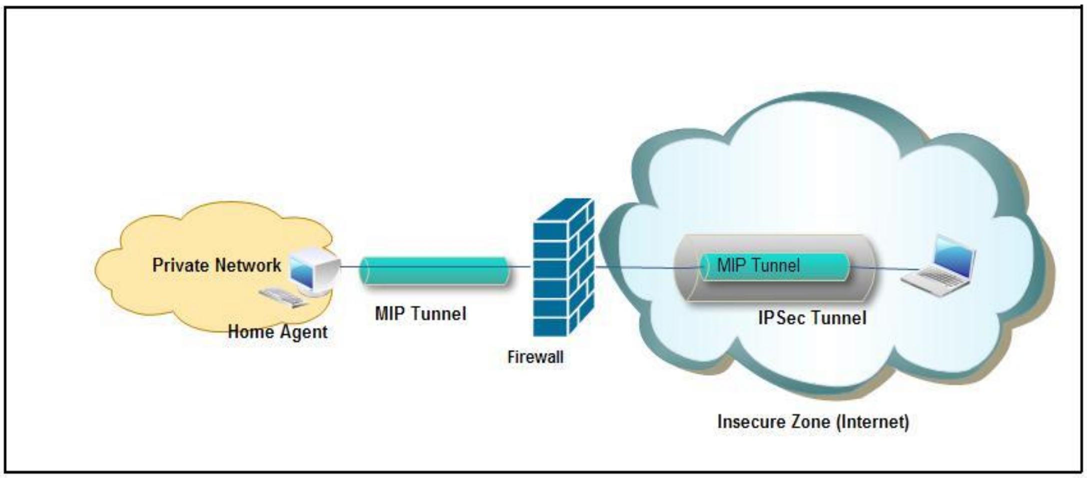


Figure 5.8-SecMIP tunneling

5.6.2 SecMIP Operation

1. Network detection

This step is the first step when the mobile node enters a new network and starts connecting via the wireless access point [25].

The foreign agent broadcast advertisements regularly inside the new network. The mobile IP receives these advertisements. For example ICMP messages make the mobile IP learn that it is in a new network. The mobile node can also send request messages to trigger an agent advertisement. The mobile node will stop the old IPSec tunnel if there is one established in another network where an old collocated care-of-address was used [25].

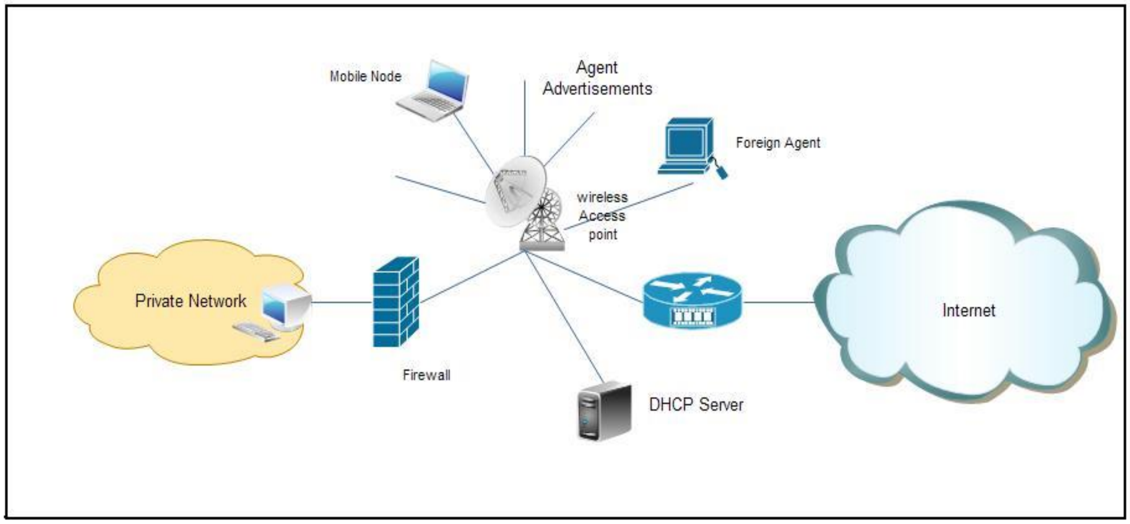


Figure 5.9-Network detection

2. Acquiring a routable IP address

In this step the mobile node acquires a collocated care-of-address from a DHCP server or the foreign agent. The mobile node sends a request message to the DHCP server and receives reply message containing a care-of-address [25].

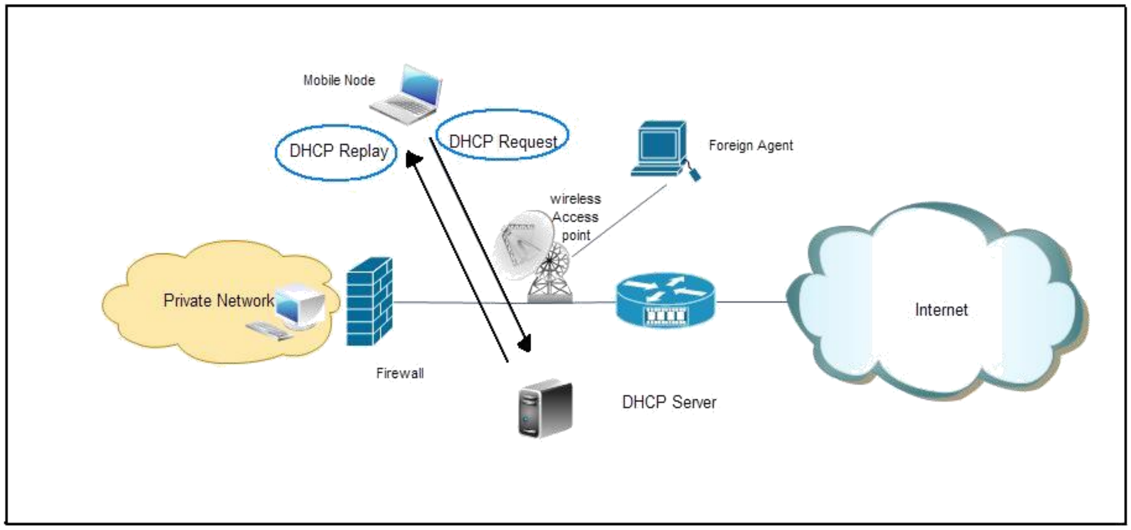


Figure 5.10- Acquiring a routable IP address

3. Establishment of IPSec tunnel between MN and Firewall

In this step an IPSec tunnel should be established between the MN"s COA and the home firewall before any messages are exchanged between them. The IPSec ensures a secure connection in a insecure public network and also provides authentication, integrity and privacy to the connection [25].

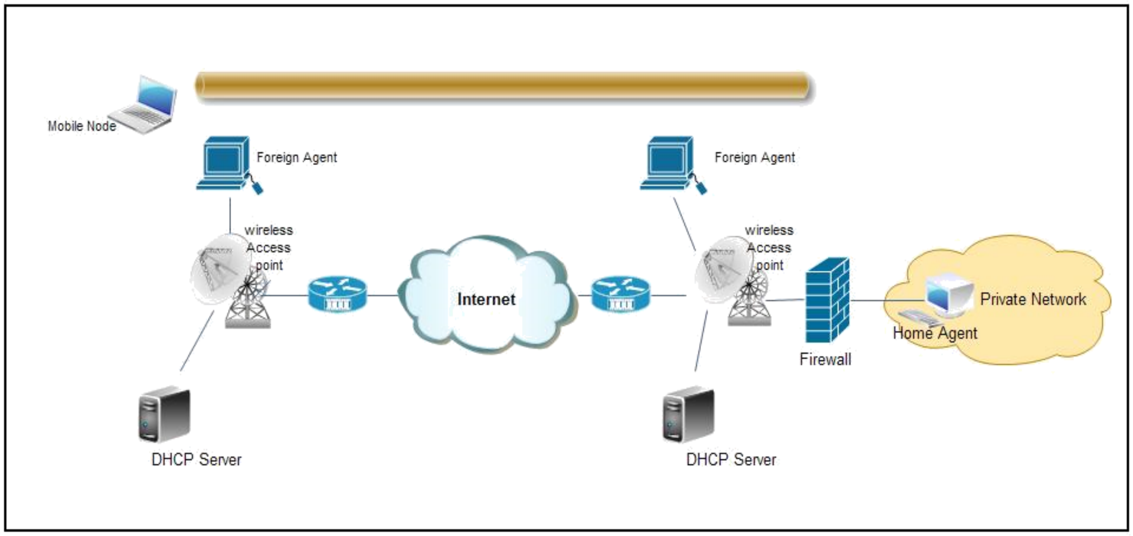


Figure 5.11- Establishment of IPSec tunnel

4. Mobile IP Registration at Home Agent

The mobile node makes registration at the home agent, the register messages that will be negotiated don‟t require authentication or encryption because it will pass through the IPSec tunnel to the firewall, behind the firewall the private network is supposed to be totally secure [25].

5. Data transfer

In this step the MN can communicate and transfer data with CN inside or outside the private network. The communication between the MN and the CN will be via the home agent to provide security. All the mobile IP packets sent to the CN were authenticated and encrypted [25].

The figure 5.12 shows all the steps and messages that are exchanged between all devices involved in the SecMIP.

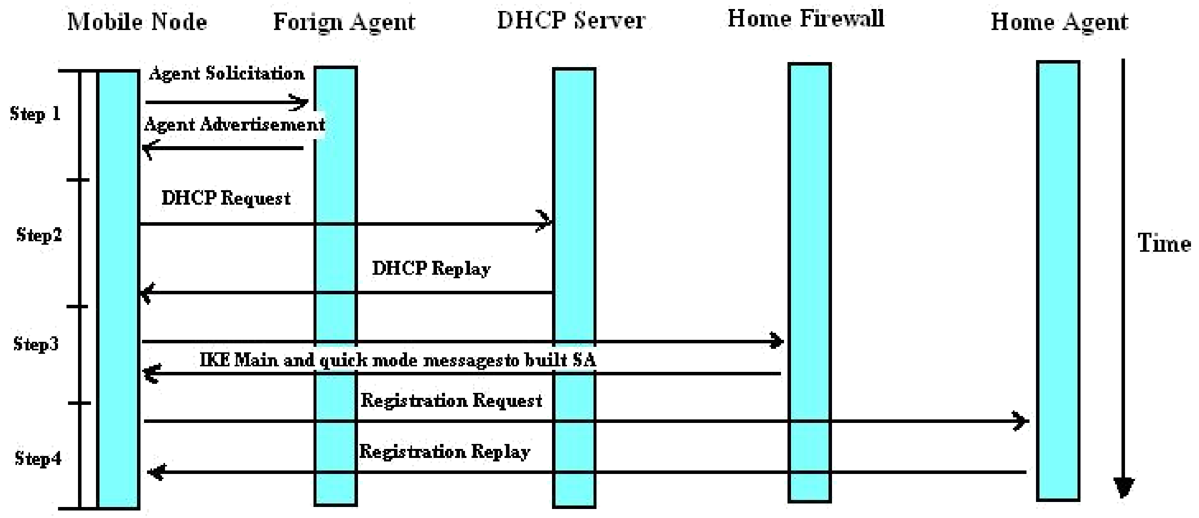


Figure 5.12- exchanged messages

Chapter 6 Mobile IPv6

6.1 Mobile IPv6 Overview

With the fast growth in the numbers of the mobile and handheld devices that are connected to the internet, the current IPv4 protocol is not able to cover the growth in the number of IP addresses. This is why Internet Protocol IPv6 has been developed.

Mobile IPv6 is an essential mandatory feature of the IPv6 that has been built to enable mobility for mobile devices in IP networks. Mobile IPv6 specification is still uncomplete, so the protocol will most likely have some changes in the future. Security of mobile IPv6 is a essential; it will be discussed in detail in this chapter.

In addition to the mobility features of mobile IPv6, IPSec is also a mandatory feature that is required for IPv6 to provide data security and services for communication in IP networks and application layer protocols of TCP/IP. IPSec is used to protect Mobile IPv6 from the security threats, but there are still some issues that need to be resolved.

6.2 Differences between MIPv4 and MIPv6

MIPv6 is the next generation standard for Mobile IP after MIPv4, the following is the main differences between MIPv4 and MIPv6:

- **Foreign agent,** MIPv6 rely on DHCP (dynamic host configuration protocol) server or router advertisements on the foreign network to get a care-of address (CoA), this scenario makes the mobile device able to operate in any place without requiring any additional support from the local router, because it does not depend on the foreign agent to issue the care-of address as with MIPv4.
- **Home agent address discovery,** IPv6 is has a feature called any cast that sends data to the nearest or best receiver. With this feature, mobile devices can send updates to the home agent through cast address. In this case, if there are multiple home agents on the network, the nearest home agent will send the response to the mobile device. By using this feature, scalability and redundancy can be provided to the network by keeping track of several home agents.

- **Security,** Both Mipv6 and Mipv4 provide data security by using a Virtual Private Network (VPN) solution. Once the mobile device travels outside its home network and connects to the foreign network; Mipv4 uses IPSec v4 (Internet Protocol Security) and the VPN Solution. Mipv6 uses IPSec v6 and the VPN solution.
- **Route Optimization,** When the mobile device leaves its own network and connects to another network , it gets a new care-of address and then informs the home agent of this address, then the home agent records the new Care-of address in its binding table. MIPv6 has a direct routing packet feature that routes between mobile device and the correspondent nodes that existed on the IPv6 network. All packets destined to the mobile device home address will be intercepted by the home agent which then tunnels them to its Care-of address. In the case of MIPv4 traffic between correspondent nodes and the mobile device must go through the home agent. In the case of MIPv6 the correspondent node caches the Care-of address by using route optimization MIPv6 and then transfers the packets directly to the mobile device as it shown in the figure 6.1 [32].

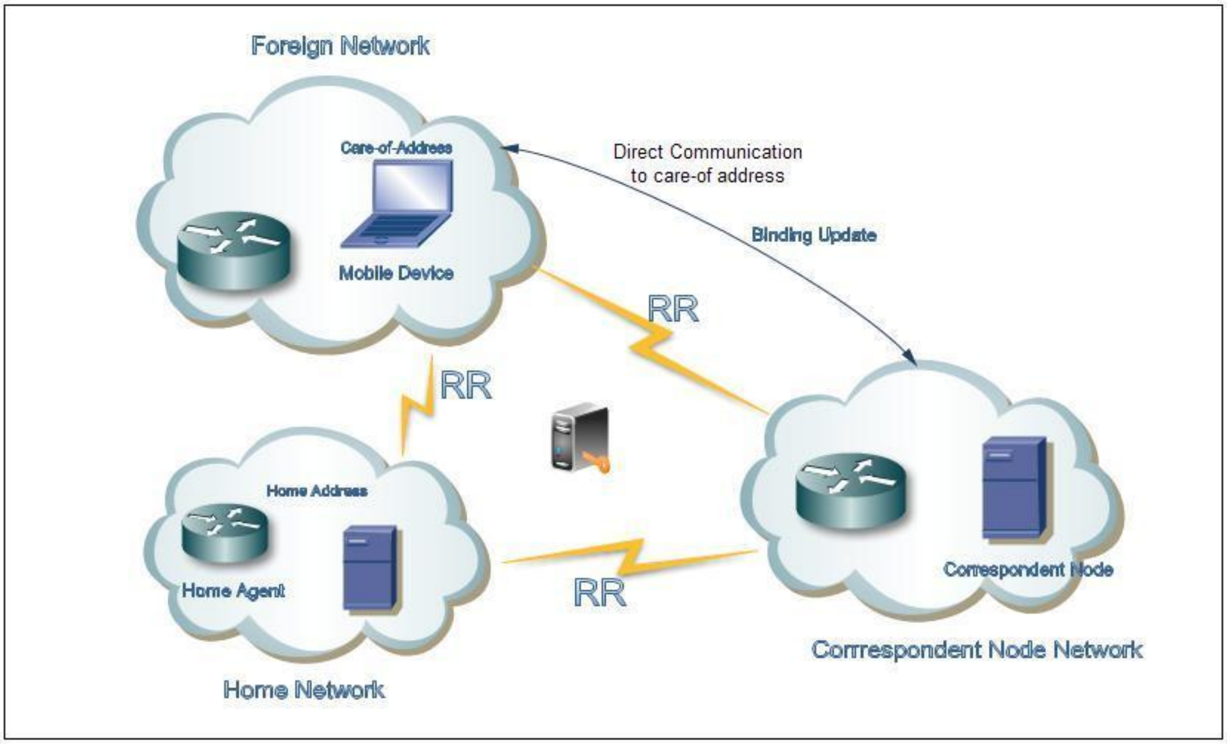


Figure 6.1- Route Optimization in MIPv6

6.3 Mobile IPv6 Security Threats

Mobile IPv6 has been developed to provide mobility and security for IPv6 with the same features as MIPv4. MIPv6 introduces different security threats as following [33]:

1. Threats against binding updates sent to home agents: an attacker might advise that a certain mobile device is currently at a different location than it really is. Then the home agent accepts the information sent to it as is. The mobile device may not get the message directed to it, and other nodes might get messages they did not want.

2. Threats against route optimization with corresponding nodes.

3. Threats where MIPv6 correspondent node functionality is used to launch reflection attacks against other parties. The response traffic against a node, whose IP address appears in the option, will be directed using the home address option without giving a possibility for ingress filtering to catch the forged.

4. Threats where the tunnels between the mobile device and the home agent are attacked to make it appear that the mobile node is sending traffic when it is not.

5. Threats where IPv6 Routing Header which is employed in MIPv6 is used to circumvent IP-address based rules in firewalls or to reflect traffic from other nodes. The generality of the Routing Header allows the kind of usage that opens vulnerabilities, even if the usage that MIPv6 needs is safe.

6. The security mechanisms of MIPv6 may also be attacked them, e.g. in order to force the participants to execute expensive cryptographic operations or allocate memory for the purpose of keeping state.

6.4 Securing the Binding Update:

MIPv6 is a host routing protocol, developed to modify the normal routing for a specific host, as it changes the way of sending packets to the host [34]. The binding update tells a correspondent node of the new care-of address, a correspondent node authenticate the binding update and verifies that it does not come from the manipulated node . In order to successfully authenticate the update the mobile device and the correspondent node need to establish security association and share a secret key.

IPSec in transport mode is used between home agent and its mobile device in order to secure the MIPv6 message such as binding update.

6.5 Summary

Mobile IP is used to maintain communications while the IP address is changing. Mobile IPv6 is much more optimized and deployable than Mobile IPv4, such as direct communication between the correspondent node and mobile device, even though Mobile IPv6 is still uncomplete; the issues have been with the security of the protocol.

7 Discussion

In this discussion section we describe our thoughts and analysis of the security issues that introduced with mobile IP and comparing different existing methods for securing mobile IP. Mobile IP solved the mobility problem of internet protocol by enabling mobile users to move from one network to another whilst maintaining their permanent IP address. Securing mobile IP is one of the more challenging tasks in mobile IP networking, especially when mobile devices register their care-of address to the home agent. Denial-of-Service attack, passive eavesdropping, reply attack and session stealing are different types of security threats that facing mobile IP campus intranets.

Since denial of service attacks happen once the attacker starts to manipulate the registration process for a particular mobile device. Strong authentication in all registration traffic between mobile devices and their home IP agent will be a good solution because it ensures that the messages come from an authentic source and go to an authentic destination. In case of passive eavesdropping and session stealing, the attacker starts to listen to the traffic that is transferred between a mobile device and its home agent. The best solution would be to use the end to end encryption method on all traffic, as this makes eavesdropping attacks impossible. In a reply attack, an attacker can have a copy of valid registration request message, buffer it, and then reply to it later on by registering a manipulated care-of address for the mobile device. Due to this, using authentication only can-not protect a mobile device from a reply attack. Generating unique value for an identification field of each successful attempt of registration by a mobile device will prevent this kind of attack.

In a Mobile IP internet world wide environment, additional security threats are facing mobile IP network. Using tunnelling instead of source routing, avoiding routing optimization, using firewall and integrate IPSec with mobile IP are different methods for improving security of Mobile IP.

The main purpose of using tunnelling techniques instead of source routing is that tunnelling relates to fewer security threats because it is built based on an authentication and encryption mechanism. Route optimization is an alternative recently proposed solution to replace triangle routing which results in degrading of significant performance. In route optimization, correspondent node can communicate directly with a mobile device without passing through the home agent, which results in less delay and resource consumption. However applying security with route optimization is a difficult task because a secret key has to be configured between mobile device and every other correspondent node. In the case of triangle routing, it‟s enough to configure a key between mobile device and its home agent. So for this reason we suggest to keep using triangle routing.

Using a firewall prevents unwanted access to network services by monitoring the traffic going through the network and deciding on the basis of defined rules whether certain network packets are allowed through or not. Packet filtering, stateful inspection and secure tunnel firewall strengthen security for mobile IP network.

IPSec is a framework of open standards for ensuring private communications over IP networks protected by the use of cryptographic security services .It is a set of protocols using algorithms to secure data transport over a network IP. IPSec is different from previous security standards as it is not limited to a single authentication method or algorithm and that is why it is considered a part of open standards. IPSec operates at the network layer (layer 3 OSI) Contrary to the standards that operated in application layer (layer 7 of OSI), which makes it independent of the applications, and means that users do not need to configure each application to standard IPSec. The integration of IPSec and mobile IP is an-effective solution to secure the communication of mobile IP network. There are different proposed solutions in how to combine IPSec with mobile IP.

In this part, an evaluation of the deployment of Mobile IP in combination with IPSec is presented. Two different solutions are presented to represent this combination. The two proposed solutions “Secure and Mobile networking” and Secure Mobile IP (SecMIP) choose the same architecture so-called “screened-subnet firewall”. The two solutions use IPSec with Mobile IP protocol which provides protection and security to the Home Network.

Analysis of the existing solutions

The two solutions use the same architecture “screened-subnet firewall”. In this architecture the home network is isolated from the internet by Demilitarized Zone, known as “DMZ”. A firewall is located between the DMZ and the home network. This design provides an extra protection and superior security characteristics.

The advantages of “screened-subnet firewall “architecture can be summarized:

- A firewall provides perfect isolation to the home network where the firewall is the only entry to the home network.
- The communication path between the Home Agent and the Mobile IP node is split by the intermediate firewall. An additional bi-directional tunnelling is created on the two halves. An IP-in-IP tunnel is used between the Home Agent and Foreign Agent to provide privacy where it hides the Care-of-address from the inside routers. An IPSec tunnel is used between the Firewall and the Mobile IP node to provide encryption and authentication and to hide the Home Agent address from outside routers.
- An attacker that manages to break into the DMZ will not be able to launch attacks against the home network because the filter point (firewall) will filter all the entering and exiting traffic.

.

To make the IPSec mechanisms practical, a scalable key management standard is needed. Two popular standards are chosen by the IETF for the IPSec. The first standard ISAKMP/Oakley is mandatory-to-implement, and the second standard SKIP is optional.

Secure Mobile IP (SecMIP) solution uses internet key exchange ISAKMP/Oakley protocol. The ISAKMP/Oakley is defined as a combination of ISAKMP (Internet Security Association and Key Management Protocol) and Oakley protocol. ISAKMP/Oakley provides secure exchange of the cryptographic keys between the two IPSec enabled nodes.

The second solution “Secure and Mobile networking” uses simple key management (SKIP) as a key management standard to provide secure key exchange. A special header is inserted before the IPSec header in each packet. The Diffie-Hellman key exchange or shared secret based key exchange can be used with SKIP. The inserted header causes an overhead about 20 to 30 bytes added in each packet.

In our prospective, ISAKMP/Oakley is preferred over SKIP for several reasons:

- After the SA negotiation, the packets will not contain a key management header as in SKIP.
- The attacker has no idea of which algorithms are used for encryption and authentication.

- Overhead size that is used for keying in every packet exchanged after SA negotiation is less in ISAKMP/Oakley.

An AH authentication header and ESP encapsulating security payload were suggested to provide authentication and data integrity.

There are some drawbacks that can be seen when SecMIP is used. There is only one path that is secured, which is the one between where mobile IP node and the firewall where the IPSec is created. Therefore it is not possible to transfer data directly from mobile IP node to the correspondent node or from the correspondent node to the mobile IP node without passing through a firewall.

For this reason the following problems will occur:

- The home agent will overload.
- Traffic will increase.

Nevertheless the combination of IPSec and mobile IP is an efficient solution to provide security for the mobile IP environment.

8 Conclusion and Suggestions to Future Work

Mobile IP provides network mobility solution over the internet. This paper‟s study focus on the security aspect in mobile IP and provides a lot of suggestions and methods to improve security in mobile IP. In this report we firstly described wireless network security threats and security technology, we also investigated mobile security threats and different security solutions that can be applied to Mobile IP with emphasis on IPSec to provide the security solution for Mobile IP. Mobility feature and IPSec were not built on IPv4 protocol; they were designed as an extension to IPv4 standard. Mobile IP was an extension of the IPv4 standard under the name “Mobile IPv4” to support mobility.

IPSec manages connections and can guarantee both encryption and data integrity through protocols of Authentication Header (AH), Encapsulated Security Payload (ESP) and Internet Key Exchange (IKE). The powerful way to secure mobile IP is by combining it with IPSec protocol; even though there are some limitations such as, IPSec does not stop traffic analysis and it use strong authentication for machines, not users. These limitations can be studied in future work.

IPSec is not the only protocol that deal with securing mobile IP, there are several security protocols such as AAA protocol (Authentication, Authorization and Accounting) and Public Key Infrastructure protocol that provide strong management. With a combination of these protocols with IPSec, we get more security and protection for mobile IP.

IPv6 was developed because the number of possible address entries in IPv4 is limited. In mobile IPv6, IPSec is a mandatory feature that is required to provide data security and services for communication in IPv6 network. The main difference between Mobile IPv4 and Mobile IPv6 is that Mobile IPv6 is not an add-on feature of IPv6, it is built into the base of IPv6 which makes it more efficient and easier to implement. Mobile IPv6 introduces different security threats that continue to get attention and should be studied in future work.