Secure Mobile IP Communication

Diplomarbeit
der Philosophisch-naturwissenschaftlichen Fakultät
der Universität Bern

Vorgelegt von:

Marc Danzeisen

Leiter der Arbeit:

Prof. Dr. Torsten Braun

Forschungsgruppe Rechnernetze und Verteilte Systeme (RVS)
Institut für Informatik und angewandte Mathematik

2001

Table of contents:

1 Abstract

"Mobility is everything" seems to be the slogan of our society. Nowadays mobility means liberty and liberty needs mobility. Our society wants to be always online, always able to communicate. Since the future infrastructure for this communications seems to be based on IP networks, mobility needs IP mobility. To provide this IP mobility, a protocol called Mobile IP was created. But mobility alone is not enough. Sensitive data has to be protected against malicious attacks. Therefore, we need secure IP mobility. The aim of this work is to analyze different approaches to provide such a secured Mobile IP. Out of these different proposals an other concept that is based on IP standards has been developed and a prototype has been implemented to test its performance.

The sections two and three of this thesis give a brief overview to the Mobile IP protocol and its open security issues. Then, in section four the main components of the IPSec protocol suite are explained. Related works are analyzed in the paragraph number five. In section six and seven, the developed concept of the implemented SecMIP (Secured Mobile IP) prototype is described. Finally, the last section examines security and performance characteristics of this prototype.

2 Mobile IP (MIP) Overview

2.1 Introduction

The scalability of the global Internet depends on network-specific routing. So all nodes connected to the same link require to share a common network-prefix portion of their IP address. If a node changes its attachment point, it has to acquire a new, valuable address. This, in turn makes it impossible to maintain any ongoing communications without re-establishment of a TCP connection.

2.2 Mobility problems solved by Mobile IP

Mobile IP was designed to solve mobility problems of the Internet protocol. Mobile IP keeps the connectivity to the mobile node (MN) by redirecting IP packets through a tunnel that is dynamically established between the HA and the MN. Thus the scope of the Mobile IP solution is simply the specification of those mechanisms which are necessary to route packets to the MN at the network layer. Other technologies, including modifications to TCP and to applications, are specifically outside the scope of Mobile IP.

2.3 Functional Entities

This section briefly gives an overview of the functionalities of Mobile IP version 4 and a detailed description of the mechanisms used to secure the ongoing communication between a mobile node and its home network.

Mobile IP needs three functional entities where its mobility protocol must be implemented:

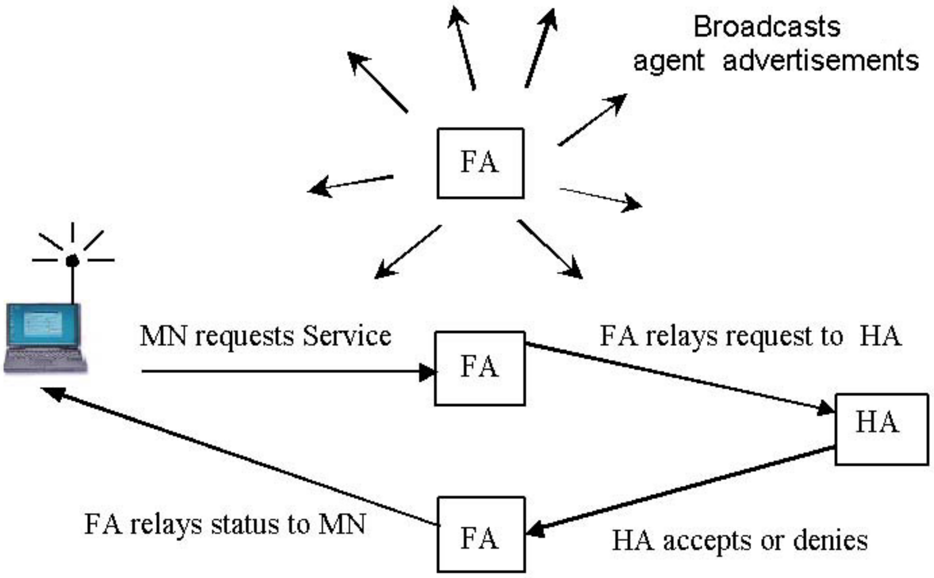
- **Mobile Node (MN):** A host or router, which can change its point of attachment from one network or sub network to another. This change of location may not concern its (home) IP address. All ongoing communications can be maintained without any interrupt.
- **Home Agent (HA):** A router on the mobile node’s home network that redirects any IP packets for the mobile node to its current location.
- **Foreign Agent (FA):** A router on a visited network providing routing services to the MN.

2.4 Protocol Overview (Mobile IP version 4)

The main functionalities of Mobile IP can be separated in Agent Discovery, Registration and Tunneling.

In the Agent Discovery phase, the mobile node discovers its new environment. This can be done in a passive or active way. The MN may listen to mobility agents (HA and FA) which advertise their availability on each link for which they provide service, or the mobile node can send a solicitation message to learn whether any agents are present.

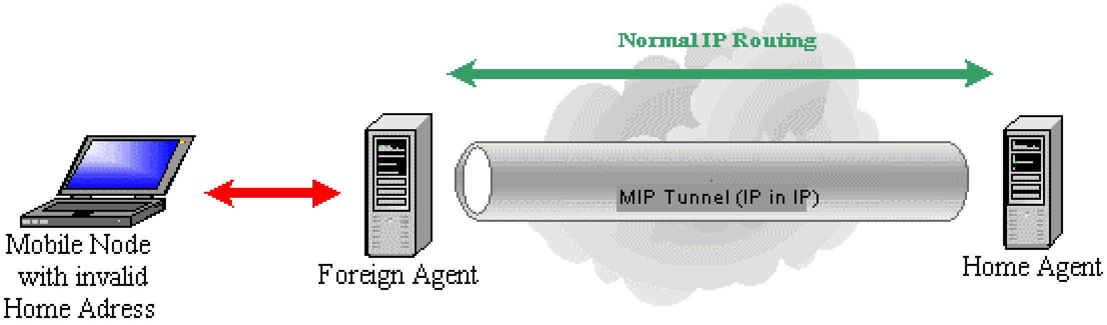
When the MN is away from home, it registers its new location with its HA. This registration is done by a registration request that communicates a valid IP address for the tunnel end point (also called care-of address (COA)) to the HA. When a HA accepts the request, it begins to associate the home address of the MN with the COA, and maintains this association until the registration lifetime expires. The triplet that contains the home address, care-of address, and the registration lifetime is called a binding for the mobile node. A registration request can be considered as a binding update sent by the mobile node. Depending on the method of attachment, the care-of address can be the foreign agent's address or a collocated care-of address.



(Figure 1 - Mobile IP)

2.4.1 FA decapsulation

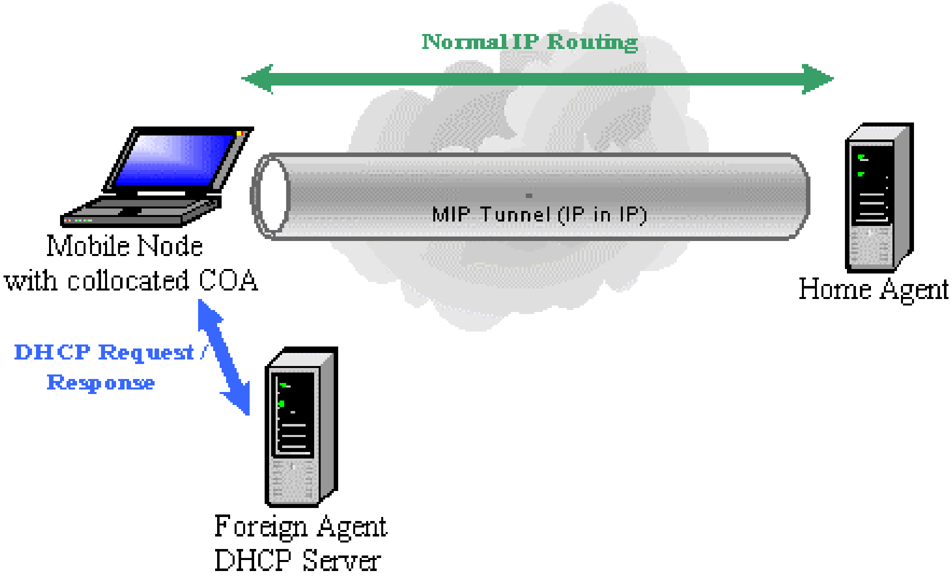
A foreign agent care-of address is provided by the foreign agent through its agent advertisement. This message includes several useful information for the visiting mobile nodes. Reading this agent advertisement, every MN is capable to send a registration request to the foreign agent, even if it does not have a valid IP address. The foreign agent, in turn, can communicate with the home agent and forward the MN's registration request. The main advantage of this method is that the MNs do not have to be reconfigured arriving to a new attachment point. Since the FA is responsible for all tunneling operations (encapsulation and decapsulation), such a method is called FA decapsulation.



(Figure 2 - FA Decapsulation))

2.4.2 MN decapsulation

A collocated care-of address is a care-of address acquired by the mobile node as a local IP address through some external means, which the mobile node associates with one of its own network interfaces. This address may be dynamically acquired, such as through a DHCP server or by the help of a foreign agent. After acquiring a routable IP address, the mobile node is now able to communicate directly with his home agent, without any help from a foreign agent. Using this method, the tunnel ends just at the mobile node and all decapsulation is done by the MN itself. Such a method is called MN decapsulation.

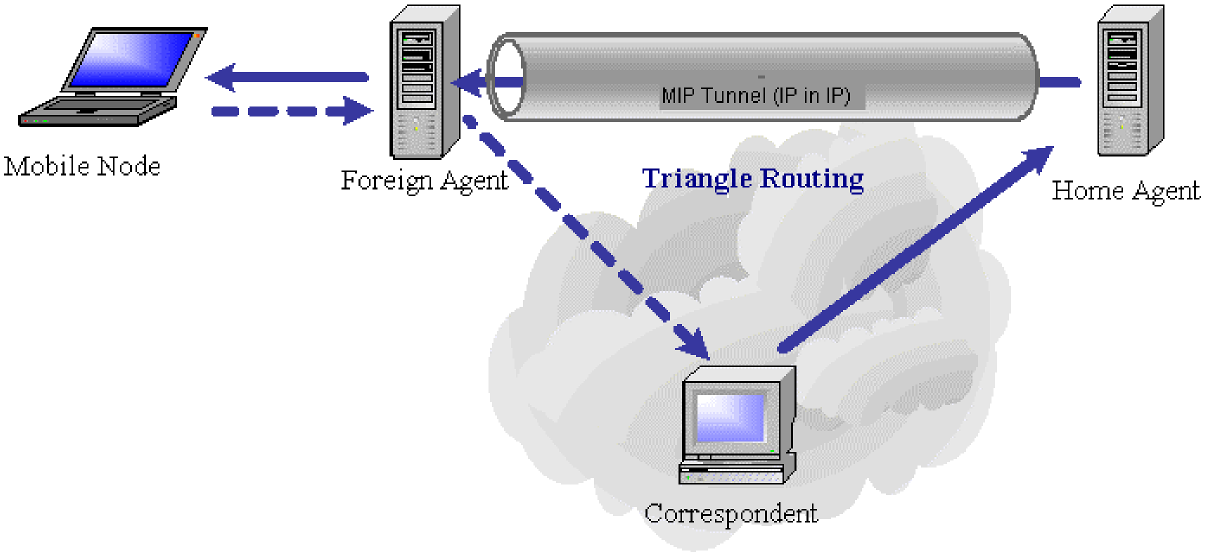


(Figure 3 - MN Decapsulation)

If the registration request is valid, Mobile IP uses a tunneling mechanism to hide a mobile node's home address from intervening routers between its home network and its current location. The mobile MN's care-of address, which must be a routable address, is used as tunnel end point. At this end point, the tunneled IP packets are decapsulated and delivered to the MN.

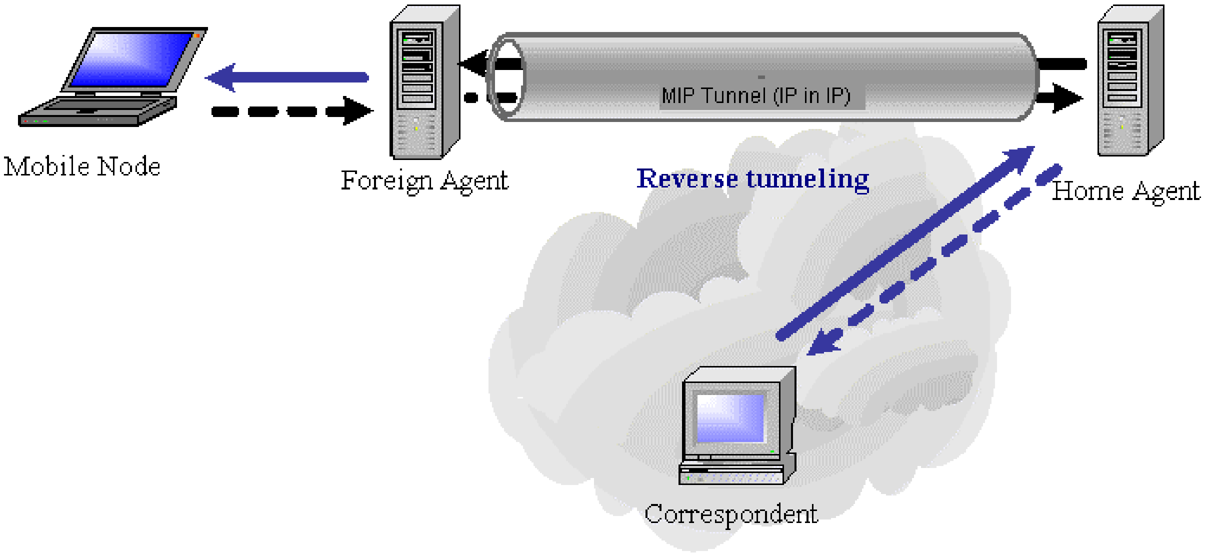
2.4.3 Triangle routing vs. optimized routing

In both, foreign agent and mobile node decapsulation mode, packets that are sent by a correspondent to a mobile node connected to a foreign link are routed first to the mobile node's home agent and then tunneled to the mobile node's care-of address. However, packets sent by the mobile node are routed directly to the correspondent, thus forming a triangle.



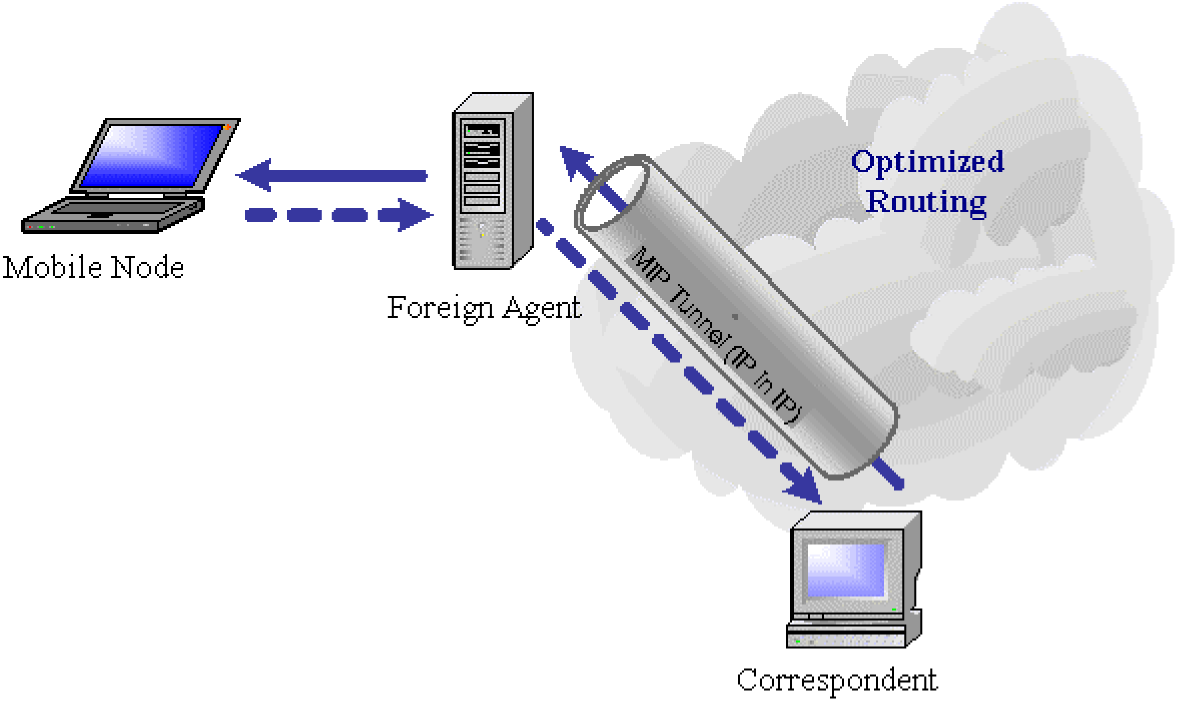
(Figure 4 - Triangle Routing)

One of the main problems deploying triangle routing appears when communicating with a correspondent, that is located inside the home network. Many routers and firewalls deploy a mechanism called ingress filtering. This filter drops packets, that appear to have arrived from the "wrong" place. The home firewall, for instance, drops packets with a source address belonging to the home subnet. In IPv4, tunneling of these packets is the only way to deal with such ingress filtering routers. The use of a topologically correct tunnel to the home network is called reverse tunneling. So the outer IP header has the foreign agent and the home agent addresses and the mobile node's home address in hidden in the inner IP header of the tunnel packet.



(Figure 5 – Reverse tunneling)

If the mobile node would inform correspondents about its care-of address and have them tunnel directly to the mobile node, bypassing the home agent, the route would be optimized. This optimized routing is potentially more efficient in terms of delay and resource consumption than is triangle routing, because, in general, the packets will have to traverse fewer links on their way to their destination.



(Figure 6 - Optimized Routing)

The main obstacle to route optimization relates to security. For a correspondent to tunnel directly to a mobile node, it must be informed of the mobile node's care-of address. Without strong authentication in the messages that inform a mobile node's correspondent of its current care-of address, trivial denial-of-service attacks would be possible to perform with respect to correspondents. These issues have to be considered by any attempts to optimize the routing in Mobile IP. It is conceivable that a network administrator could configure a secret key between a mobile node and its home agent, in order to protect the registration messages against forgeries. It is not practical, however, to distribute keys between a mobile node and every other node with which it might correspond. In the absence of automated mechanisms, distributing keys between a mobile node and its correspondents is simply not feasible.

That is why route optimization in Mobile IP (version 4) is "work in progress". Route optimization provides significant resource savings only when the mobile node is far from its home agent and near its correspondent. In most situations, the mobile node or the correspondent is close to the home agent, implying that the network resources to be saved by direct tunneling are small in comparison to the authentication and key distribution necessary to do it securely.

For detailed information about Mobile IP version 4, please consult these documents:

- RFC 2002 [1], which defines the Mobile IP protocol itself;
- RFC 2003 [2], 2004 [3], and 1701[4], which define three types of tunneling used in MIP;
- RFC 2005 [5], which describes the applicability of Mobile IP; and
- RFC 2006, [6] which defines the Mobile IP *Management Information Base (MIB)*
- Draft-ietf-mobileip-optim-xx.txt for route optimization in Mobile IP

2.5 Mobile IP version 6

The design of Mobile IP support in IPv6 (Mobile IPv6) represents a natural combination of the experiences gained from the development of Mobile IP support in IPv4 (Mobile IPv4) together with the opportunities provided by the design and deployment of a new version of IP itself (IPv6) and the new protocol features offered by IPv6. Mobile IPv6 thus shares many features with Mobile IPv4, but the protocol is now fully integrated into IP and provides many improvements over Mobile IPv4. This section summarizes the major differences between Mobile IPv4 and Mobile IPv6:

- Support for what is known in Mobile IPv4 as "Route Optimization" is now built in as a fundamental part of the protocol, rather than being added on as an optional set of extensions that may not be supported by all nodes as in Mobile IPv4. This integration of Route Optimization functionality allows direct routing from any correspondent node to any mobile node, without needing to pass through the mobile node's home network and be forwarded by its home agent, and thus eliminates the problem of "triangle routing" present in the base Mobile IPv4 protocol. The Mobile IPv4 "registration" functionality and the Mobile IPv4 Route Optimization functionality are performed by a single protocol rather than two separate (and different) protocols.

- Support is also integrated into Mobile IPv6 -- and into IPv6 itself -- for allowing mobile nodes and Mobile IP to coexist efficiently with routers that perform ingress filtering. A mobile node now uses its care-of address as the source address, allowing the packets to pass normally through ingress filtering routers. The home address of the mobile node is carried in the packet in a home address destination option, allowing the use of the care-of address in the packet to be transparent above the IP layer. The ability to correctly process a home address option in a received packet is required in all IPv6 nodes, whether mobile or stationary, whether host or router.

- The use of the care-of address as the source address in each packet's IP header also simplifies routing of multicast packets sent by a mobile node. With Mobile IPv4, the mobile node had to tunnel multicast packets to its home agent in order to transparently use its home address as the source of the multicast packets. With Mobile IPv6, the use of the home address option allows the home address to be used but still be compatible with multicast routing that may be based on the packet's source address.

- There is no longer any need to deploy special routers as "foreign agents" as used in Mobile IPv4. In Mobile IPv6, mobile nodes make use of IPv6 features, such as Neighbor Discovery and Address Autoconfiguration, to operate in any location away from home without any special support required from its local router. So foreign agents do not exist in MIPv6.

- Unlike Mobile IPv4, Mobile IPv6 utilizes IP Security (IPSec) for all security requirements (sender authentication, data integrity protection, and replay protection) for Binding Updates (which serve the role of both registration and Route Optimization in Mobile IPv4). Mobile IPv4 relies on its own security mechanisms for these functions, based on statically configured "mobility security associations".

- The movement detection mechanism in Mobile IPv6 provides bi-directional confirmation of a mobile node's ability to communicate with its default router in its current location (packets that the router sends are reaching the mobile node, and packets that the mobile node sends are reaching the router). This confirmation provides a detection of the "black hole" situation that may exist in some wireless environments where the link to the router does not work equally well in both directions, such as when the mobile node has moved out of good wireless transmission range from the router. The mobile node may then attempt to find a new router and begin using a new care-of address if its link to its current router is not working well. In contrast, in Mobile IPv4, only the forward direction (packets from the router are reaching the mobile node) is confirmed, allowing the black hole condition to persist.

- Most packets sent to a mobile node while away from home in Mobile IPv6 are sent using an IPv6 Routing header rather than IP encapsulation, whereas Mobile IPv4 must use encapsulation for all packets. The use of a Routing header requires less additional header bytes to be added to the packet, reducing the overhead of Mobile IP packet delivery. To avoid modifying the packet in flight, however, packets intercepted and tunneled by a mobile node's home agent in Mobile IPv6 must still use encapsulation for delivery to the mobile node.

- While a mobile node is away from home, its home agent intercepts any packets for the mobile node that arrive at the home network, using IPv6 Neighbor Discovery rather than ARP as is used in Mobile IPv4. The use of Neighbor Discovery improves the robustness of the protocol (e.g., due to the Neighbor Advertisement "override" bit) and simplifies implementation of Mobile IP due to the ability to not be concerned with any particular link layer as is required in ARP.

- The dynamic home agent address discovery mechanism in Mobile IPv6 uses IPv6 anycast and returns a single reply to the mobile node, rather than the corresponding Mobile IPv4 mechanism that used IPv4 directed broadcast and returned a separate reply from each home agent on the mobile node's home link. The Mobile IPv6 mechanism is more efficient and more reliable, since only one packet need be sent back to the mobile node. The mobile node is less likely to loose one of the replies because no "implosion" of replies is required by the protocol.

- Mobile IPv6 defines an Advertisement Interval option on Router Advertisements (equivalent to Agent Advertisements in Mobile IPv4), allowing a mobile node to decide for itself how many Router Advertisements (Agent Advertisements) it is willing to miss before declaring its current router unreachable.

- The use of IPv6 destination options allows all Mobile IPv6 control traffic to be piggybacked on any existing IPv6 packets, whereas in Mobile IPv4 and its Route Optimization extensions, separate UDP packets were required for each control message.

3 Security in Mobile IP

This section gives a brief overview to the security aspects using Mobile IP for mobile virtual private networks (MVPN). The issues mentioned here, will be examined in detail some later in this document. As the goal of this paper is to discuss approaches to secure Mobile IP, these security issues will serve as a guideline through the whole document.

3.1 Mobile IP open issues

Among the most important open issues in Mobile-IP, there are:

- Intrinsic security issues: The protocol acts as an “open-door” for hackers of all kind, there is no strong authentication of the visiting user, no data privacy and no data integrity protection between the MN and its home network. No network provider wants to give access to a unknown guest node, without having any protection of his network.
- Firewall traversal: No direct provision has been made in the protocol for coping with firewall-protected Virtual Private Networks (VPNs), although this is very frequent, especially in corporate VPNs. Redirected IP packets from the MN’s new location has to be authenticated and eventually accepted.

3.2 Security issues in Mobile IP based MVPNs

3.2.1 General Security Threats

In a mobile VPN, the access is often made through wireless and shared links. These shared access links are particularly vulnerable to following types of attacks:

- Passive eavesdropping, where the attacker is simply “listening” at the communication with some IP packet sniffer software. By that means, he may record entire remote access sessions and eventually get logon passwords if they were sent in clear text or only weakly encrypted (this is unfortunately too often the case). He may also keep the recordings as input for the next type of attack.
- Active replay attacks, in which the attacker uses portions of a previously recorded session, in order to gain access to the network via the recorded legitimate login session data, impersonating the legitimate user.
- Denial of service, where the attacker massively floods the servers with packets, such that the latter are not able to provide a normal service anymore. This is a very harmful attack for commercial providers whose services are dropping under such a flood.
- Session stealing attacks, where the attacker “hi-jacks“ the connection of a legitimate user, once it has been established. The legitimate user then thinks the server is down, while the attacker goes on using the service on behalf of the legitimate user.

Although these attacks are not specific to Mobile IP, this protocol really eases them significantly.

3.2.2 Security Issues In Mobile IP

While taking a closer look at the basic Mobile IP protocol specification (rfc2002 [1]), it appears that:

- The **registration procedure** is only provided with a very minimal tamper-proof protection. With the help of authentication methods (Keyed MD5 [RFC 1321]) the registration messages are protected against being changed during the transition. But there is no privacy for the registration information as the MN's current location or the HA's IP address.
- There are **ARP Cache** security concerns: It acts as a leaking pipe at the home network end! - After gratuitous ARP, there is a leaking pipe if the MN moves. Until timeout of the registration or re-registration.
- There is no real **key management** Strategy.

It is especially vulnerable to following attacks:

- **Replay attack**: An attacker records and replays the registration sequence later.
- **Denial of Service (DoS)**: An attacker overflows access server. This is possible because the sensitive IP addresses of the HA and the MN are not hidden in the registration messages.
- **Session Stealing**: An attacker hi-jacks session just after normal registration.
- There is no **transport integrity and privacy**: Encryption and tamper-proofing of content (authentication) is missing.
- **Tunnel spoofing**: The tunnel to the home network may be used to hide malicious IP packets and get them pass the firewall.
- The **Firewall Traversal Problem** is still open: Firewalls should not have to understand MIP. A good firewall is blocking insecure packets from carrying sensitive data outside the protected network. Also IP in IP packets which are used by Mobile IP to redirect packets to the MN are often filtered by firewalls.

3.3 Security models

To secure the protocol, two approaches may be used:

Weak security approach

Since the services are not primarily of commercial nature and/or of high added value, in typical "campus"-like environments, the user as well as the provider may agree on a weaker level of security characterized by:

- Available protection against malicious attempts such as:
  - ➢ HA has confidence that the care-of address of a MN is correct, because all allowed care-of addresses concern to well known IP address ranges in the campus network.
  - ➢ Foreign Mobile IP compatible nodes (guests) in the network need to authenticate bindings.
  - ➢ When a MN is migrating outside the protected campus network, it sends a registration request with password to the HA.

Strong Security Approach

However, in commercial environments, where a customer signs up a contract with a provider and where he pays for a given content with added value, given access facility and QoS, the weak security approach above is not suitable anymore. Both will now have to agree on a stronger level of security policy where:

- Mobile IP authenticates any binding notification messages or other information received about a mobile host
- Public and private keys and trusted servers are used, but in turn it slows down the operation

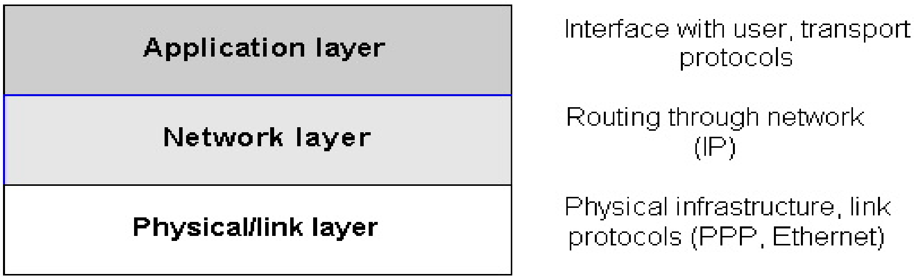
All these open issues shown in this section make it hard to deploy Mobile IP in a company's network environment that is used to transfer sensitive data. IPSec can solve nearly all of these security problems.

4 IPSec overview

4.1 Where does IPSec fit in?

Technologies securing Internet communications exist, but most of them are dedicated to specific software applications, for example PGP for mail encryption and browser-based authentication, and encryption between the browser and the web server (SSL) to protect sensitive web traffic. These restrictions do not get along with the requests of a large enterprise and the average Internet service provider that may never know precisely what applications may be running tomorrow over the networks they are building today.

The most effective way to fulfill such an application independent security is to place all security mechanisms below the application layer, i.e. in the network layer.


Application layer
Network layer
Physical/link layer
Interface with user, transport protocols
Routing through network (IP)
Physical infrastructure, link protocols (PPP, Ethernet)

(Figure 7 - Networking layers)

The lowest layer, namely the physical/link layer consists of the electrical, optical cables, network devices as network cards, radio links on which information travels, as well as the simple data carrying protocols that provide an interface for the higher level protocols.

Using the services provided by the physical layer, the network layer can transmit information between different nodes. Therefore it has its own routing logic to work out the most sensible subnets through which to send the data.

Above the network layer are a few higher level protocols that set up the links between nodes for different types of communications, and the application layer in which the applications run. Applications use the services of the network layer to determine how to move data from network node to network node and the network layer, in turn, uses the physical layer to get the data from one computer's network card to the next.

4.2 Securing the IP layer

An IETF working group has developed a method to secure the IP layer. They call it the IP security protocol suite (IPSec). This protocol suite adds security services to the IP layer keeping compatible with IP standard (IPv4).

Using IPSec where normally using IP, all communications for all applications and all users can be secured in a transparent way.

IPSec eases building secure virtual private networks (VPN) – a secure, private network that is as safe or safer than an isolated office LAN, but built on an unsecured, public network. Such VPNs can be build on demand, and with anyone else using the standard.

Because the IPSec protocol suite is compatible with the normal IP protocol, it is enough to support IPSec on the end systems. The rest of the network in between can work just as it works now.

IPSec promises to become the new international standard, allowing different networks around the world to interconnect and communicate securely. It also promises a very good scalability while providing quiet and reliable security services.

4.3 Security services offered by IPSec

Since this whole document is driven by security threats in the network environment, let us take a closer look at IPSec keeping the known attacks in mind.

Three things must be ensured for security in a network environment:

- The communicating persons must really be the persons they seem to be (authentication)
- No one shall be able to eavesdrop on communications (confidentiality, privacy)
- The received communication must not be altered in any way during transmission (integrity)

4.3.1 Spoofing – counterfeit IP addresses

The first difficulty of IP networks is that it is difficult to know where information really comes from. An attack called IP spoofing takes advantage of this weakness.

Since the source IP address of a packet has no influence to the deliverability, it can easily be changed. The attack – called spoofing – makes a packet coming from one machine appear to come from somewhere else altogether.

4.3.2 Session hijacking

Spoofing makes it possible to take over a connection. An IP source address is not trustable, since everyone can pretend to be the owner of this address. Even authentication that is done once for each communication is not a protection against session hijacking. Identifying the communicating person once, does not ensure that it will be the same person through the rest of the session. Each data’s source has to be authenticated throughout the transmission.

4.3.3 Electronic eavesdropping – Ethernet LANs and sniffing

A large part of most networks are based on Ethernet LANs. This technology has the advantages of being cheap, universally available, well-understood and easy to expand. But it has the disadvantage of making sniffing easy.

In Ethernet networks, every node can read every packet being transmitted over the subnet. Conventionally, each network interface card only listens and responds to packets specifically addressed to it. But it is easy to force these devices to collect every packet that passes on the wire (this operation mode is called promiscuous mode). Physically, there is no way to detect from elsewhere on the network, which network interface card is working in the promiscuous mode.

To get the most information out of the collected packets you can use commercial diagnostic tools called Sniffers. Such tools can record all the network traffic and are normally used to determine quickly what is going through any segment of the network. This often can drastically ease the error detection. However, in the hands of someone who wants to listen in on sensitive communications, a sniffer is a powerful eavesdropping tool.

4.3.4 The man-in-the-middle

The most obvious solution to all these IP security threats would be to use encryption to conceal and authenticate the data passed in IP packets. But there are complications in doing this.

First of all there are encryption keys to be exchanged between the communicating parties. Encryption keys are used with encryption algorithms to encrypt and decrypt data. Because of the much higher performance nearly all of those encryption algorithms are symmetric. That means that the same key is used to encrypt and decrypt data. If someone can intercept the unprotected packets used to exchange this key, he can introduce his own key and assure that he will be able to decrypt the upcoming communication. This attack is called man-in-the-middle attack.

4.4 IPSec protocol suite

The IPSec-Protocol-Suite consists of three main parts:

- **Authentication Header** (AH) - ties data in each packet to a verifiable signature that allows to verify both the identity of the person sending data and that data has not been modified.
- **Encapsulating Security Payload** (ESP) – encrypts data (and even certain sensitive IP addresses) in each packet – so a sniffer somewhere on the network doesn’t get anything usable.
- **Internet Key Exchange** (IKE) – a powerful, flexible negotiation protocol that allows users to agree on authentication methods, encryption methods, the keys to use, how long to use the keys before changing them, and that allows smart, secure key exchange.

With these three protocols it is possible to secure a connection on the IP level. After having exchanged all parameters with IKE, all packets are being encrypted and authenticated with AH/ESP.

4.4.1 Encapsulating Security Payload

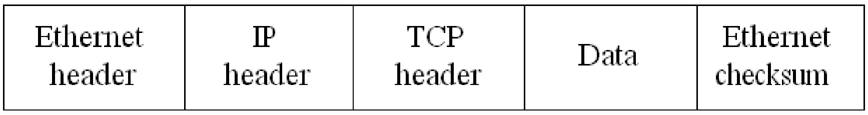
ESP supports nearly any kind of symmetric encryption. The default standard built into ESP that assures basic interoperability is 56-bit DES. ESP also supports some authentication (as can the AH – the two have been designed with some overlap).

To see what exactly happens to a TCP/IP packet on an Ethernet LAN, let us have a closer look at the packet before and after applying ESP in transport mode.

An Ethernet packet carrying TCP/IP data is built as follows:

- First, the TCP packet header is assembled and appended to the data.

- Then, the IP header is assembled and appended to the TCP header (in front of it).
- Then the Ethernet header is assembled and appended to the IP header (in front of it – though there is also a checksum on the end with Ethernet).

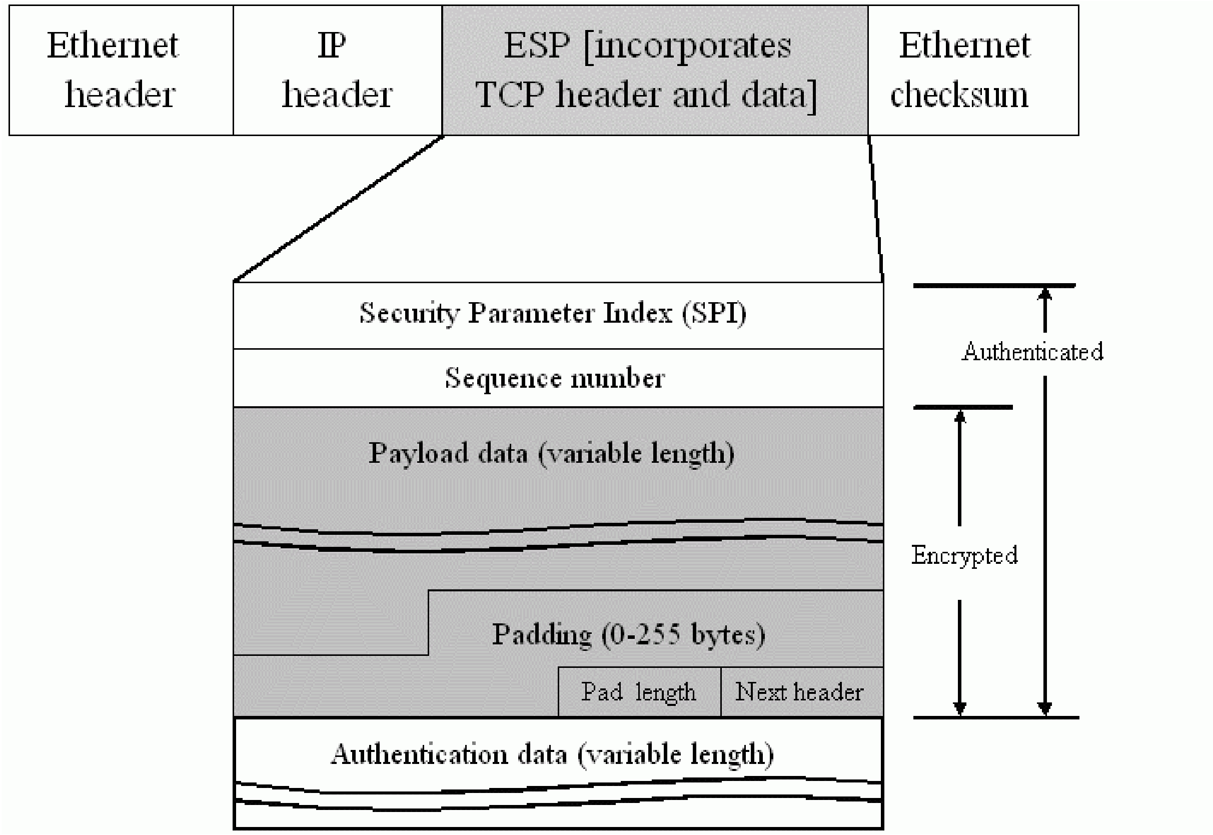


Ethernet header	IP header	TCP header	Data	Ethernet checksum

(Figure 8 - Ethernet packet)

With ESP the Ethernet packet is structured differently:

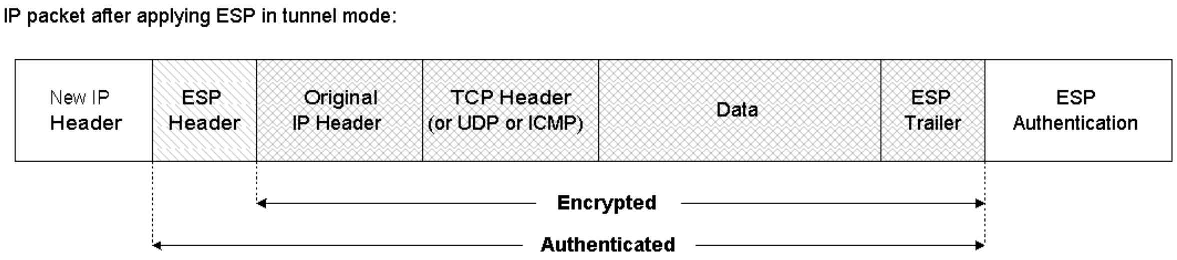
- First, the TCP packet header is assembled and appended to the data.
- Second, the ESP packet is assembled. With encryption, it encapsulates the TCP packet in totality, including the header.
- Third, the IP header is assembled and added to the front of this.
- Finally, the Ethernet header and checksum are assembled and tacked onto the front and the end.


Ethernet header
IP header
ESP [incorporates TCP header and data]
Ethernet checksum
Security Parameter Index (SPI)
Sequence number
Payload data (variable length)
Padding (0-255 bytes)
Pad length
Next header
Authentication data (variable length)
Authenticated
Encrypted

(Figure 9 - Ethernet packet with ESP)

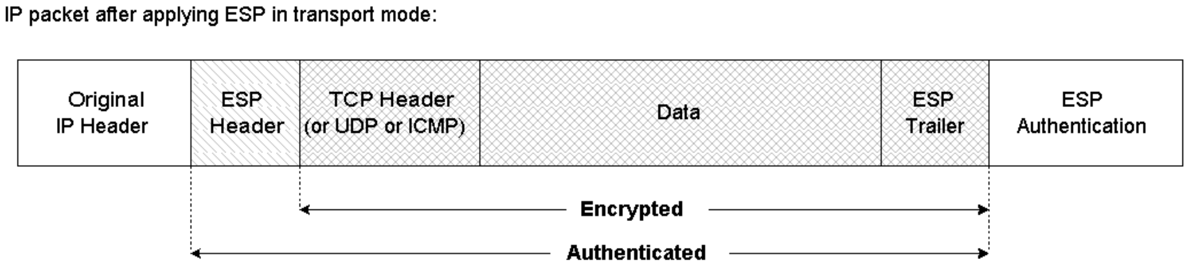
4.4.2 Tunnel and transport mode

IPSec was designed to be used in two different modes. The tunnel mode and the transport mode. Tunneling takes the original IP packet and encapsulates it within the ESP. Then it adds to the packet a new IP header containing the address of the IPSec gateways. This mode allows you to pass illegal IP addresses through a public network that otherwise would not accept them, as the private addresses of the inner IP header are hidden. Privacy is also given by hiding the original network topology.



(Figure 10 - IPSec tunnel mode)

The transport mode just encrypts and authenticates the payload and a part of the IP header.



(Figure 11 - IPSec transport mode)

ESP components

The security parameter index (SPI) and the sequence number are authenticated but not encrypted. The SPI is an arbitrary 32-bit number, which specifies the group of security protocols the sender is using for communication – which algorithms, which keys, and how long those keys are valid. All these information are stored in a so-called security association (SA).

A security association is a concept. Several secured connections can use the same SA. The connections are referencing the SAs through the SPI. The SPI together with the SA concept, makes keeping track of keys and protocols easy and automatic.

It works as follows: When a SA is being negotiated, the recipient node assigns an SPI it is not already using, and preferably, one it has not used in a while. It then communicates this SPI to the node with which it negotiated the SA. From then until the expiration of that SA, whenever that node wishes to communicate with yours using that SA, it uses that SPI to specify it.

As recipient, the node looks at the SPI to determine which SA it needs to use. According to the rules of that SA, it can decrypt and authenticate the received data.

The sequence number is a counter that increases each time a packet is sent to the same address using the same SPI. This sequence number helps to identify the packets and provides protection against replay attacks – in which an attacker copies a packet and sends it out of sequence, to confuse communicating nodes.

The parts, which are colored gray are encrypted. They are namely the payload data, the padding field, the pad length and next header fields.

The payload data is the actual data being carried by the packet. The padding supports types of encryption algorithms that require the data to be a multiple of a certain number of bytes. This prevents also sniffer to estimate the length of the transmitted data. The pad length field specifies how much of the payload is padding as opposed to data.

The next header field is, like in normal IP packets, indicating the type of the data carried and the protocol above. Finally, there is an authentication field, which is an optional field. It contains a value called an integrity check value (ICV) – essentially a digital signature computed over the remaining part of the ESP. Depending on the authentication algorithm used the length varies. It may also be omitted entirely, if authentication services are not selected for the ESP.

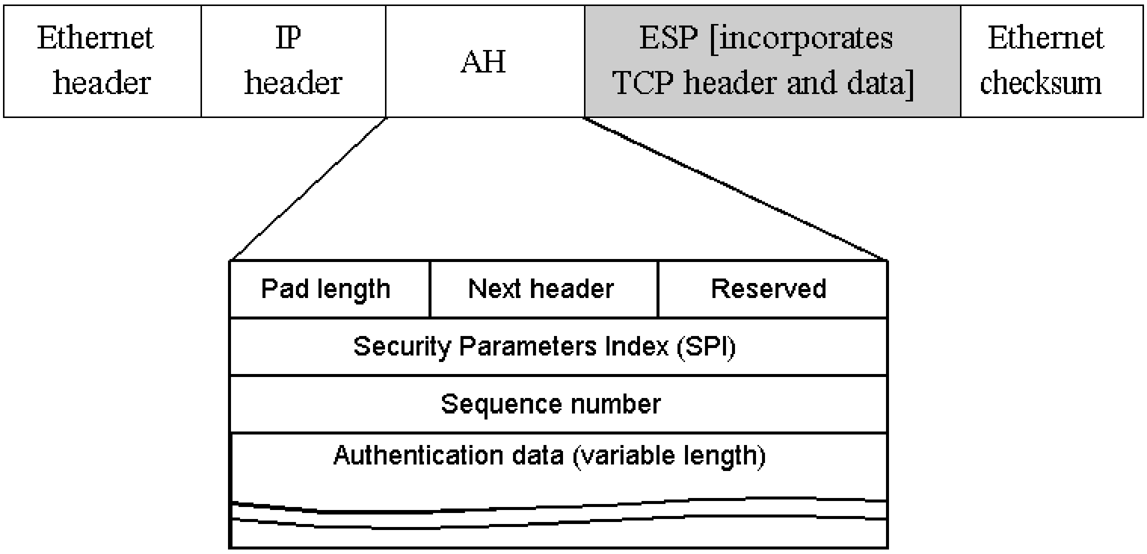
The main advantage of introducing the ESP as the payload of the IP packet is that this IPSec packets can also be routed by routers, which do not understand the ESP. This way the IPSec stays backwards compatible.

ESP can use any number of encryption protocols; it is up to the user to decide which ones to use. Per default it uses a basic DES-CBC (cipher block chaining mode) to guarantee a minimal interoperability among IPSec networks. It is to say, that ESP's encryption support is designed for use by symmetric encryption algorithms. To exchange this symmetric keys between the communicating parties, IPSec uses asymmetric algorithms. (*see 4.4.4 Internet Key Exchange (IKE)*)

4.4.3 AH – authentication header

The second protocol of the IPSec suite is the authentication header. As its name says, it offers just authentication of data and not confidentiality. In contrast to the authentication that is provided by ESP, this authentication protocol also authenticates parts of the IP header – specially the parts, which do not change during transmission.

The next figure shows how an Ethernet packet carrying an TCP/IP packet looks after applying AH and ESP.


Ethernet header
IP header
AH
ESP [incorporates TCP header and data]
Ethernet checksum
Pad length
Next header
Reserved
Security Parameters Index (SPI)
Sequence number
Authentication data (variable length)

(Figure 12 - Ethernet packet with AH/ESP)

The design of the authentication header protocol makes it independent of the higher level protocol. It can be used with or without ESP. The different fields of the AH are:

- The next header field that specifies the higher level protocol following the AH.
- The Pad length field is an 8-bit value specifying the size of the AH.
- The reserved field is reserved for future use and is currently always set to zero.
- The SPI identifies a set of security parameters to use for this connection.
- The sequence number increases for each packet sent with a given SPI.
- Finally, the authentication data is the actual ICV, or digital signature, for the packet. It may include padding to bring the length of the header to an integral multiple of 32 bits (in IPv4) or 64 bits (in IPv6).

To guarantee minimal interoperability, all IPSec implementations must support at least HMAC-MD5 (Keyed-Hash Message Authentication Code for the Message Digest 5 Algorithm) and HMAC-SHA-1 (Keyed-Hash Message Authentication Code for Secure Hash 1 Algorithm) for AH.

For the new IP protocol release, the IPSec group has developed protocols for flexible ranges of authentication and intelligent placing of the AH header in the IP packet so that it can work under either IPv4 or IPv6.

As it was mentioned before, IPSec uses symmetric encryption scheme to encrypt the transported data. The main problem now, is the ensure a confidential exchange of this shared key among the communicating parties. The next section is dealing with this problem taking a closer look at the key management and exchange.

4.4.4 Internet Key Exchange (IKE)

To communicate with someone using authentication and encryption services you need to:

- Negotiate with other people the protocols, encryption algorithms, and keys, to use.
- Exchange keys easily (this might include changing them often).
- Keep track of all these agreements.

Security associations are used to keep all the needed information about how to communicate securely with someone else.

Under IPSec, the SA specifies:

- The mode of the authentication algorithm used in the AH and the keys to that authentication algorithm
- The ESP encryption algorithm mode and the keys to that.
- The presence and size of (or absence of) any cryptographic synchronization to be used in that encryption algorithm.
- How to authenticate communications (using what protocols, what encrypting algorithm and what key).
- How to make communication private (again, what algorithm and what key).
- How often those keys are to be changed
- The authentication algorithm, mode and transform for use in ESP plus the keys to be used by that algorithm
- The key lifetimes
- The lifetime of the SA itself
- The SA source address
- A sensitivity level descriptor

So this SA can be imagined as a contract with someone at the other end of the secure channel.

IKE is the IPSec group's answer to protocol negotiation and key exchange through the Internet. It is actually a hybrid protocol which integrates the Internet Security Association and Key Management Protocol (ISAKMP)[8] with a subset of the Oakley key exchange scheme.

With IKE there are following services available:

- Negotiation services (which protocols, algorithms, and keys to use)
- Primary authentication services (ensure authentication from the beginning of the exchange)
- Key management (manage those keys after they have been agreed upon)
- Exchange material for generating those keys safely

IKE works in two phases. The first phase is dedicated to establish a secure channel for doing IKE. This first negotiation leads to the so called IKE SA, which gives the rules for this primer secure channel. In the second phase, general purpose SAs are negotiated.

An IKE peer is an IPSec-compliant node capable of establishing IKE channels and negotiating SAs. For example the desktop computer or a security gateway that negotiates security services for several computers.

4.4.4.1 IKE modes

For the phase one, the establishment of the primer secure channel, Oakley provides two modes of exchanging keying information and setting up IKE SAs.

- Main mode accomplishes a phase one IKE exchange by establishing a secure channel.
- Aggressive mode is another way of accomplishing a phase one exchange. It is simpler and faster than the main mode, because the negotiating nodes transmit their identities before having negotiated a secure channel. The price to pay for this gain of time is that there is no identity protection.

For the phase two, there is just one mode.

- Quick mode accomplishes a phase two exchange by negotiating an SA for general purpose communications.

To establish an IKE SA, the initiating node proposes several things:

- Encryption algorithms (to protect data)
- Hash algorithms (to reduce data for signing)
- An authentication method (for signing data)
- Information about the group type over which to do a Diffie-Hellman exchange (modulus length of 768 bit, 1024 bit, etc.)
- A pseudo-random function (PRF) used to hash certain values during the key exchange for verification purposes (this is optional, you can also just use the hash algorithm)
- The type of protection to use (ESP or AH)

The main difficulty, establishing such a secure channel, is to provide a shared secret key to both communicating nodes. This exchange is done using a scheme called Diffie-Hellman.

4.4.4.2 Diffie-Hellman

Two people independently and randomly generate values much like a public/private key pair. Each sends their public value to the other (using authentication to close out the man-in-the-middle). Each then combines the public key they received with the private key they just generated, using the Diffie-Hellman combination algorithm.

Mathematically, this is like:

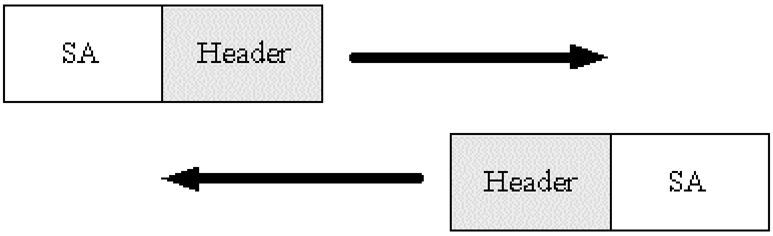
1. The two persons, let us call them Alice and Bob, select together a large prime number p as well as one concerning p primitive number of g. These numbers p and g are not secret.
2. Alice chooses a big, secret number x<p and transmits to bob the remainder X from the equation:
   $X = g^x \bmod p$
3. Similarly Bob selects a large number y<p and transmits to Alice the remainder Y from the equation:
   $Y = g^y \bmod p$
4. Alice calculates the remainder $s = Y^x \bmod p$.
5. Bob calculates the remainder $s' = X^y \bmod p$.

The remainders s and s' are equal, because $s = s' = g^{xy} \bmod p$. This value can be used for fast symmetric encryption by both parties. But no one can come up with the same value from the two public keys (*X* and *Y*) passed through the net, since the final value (*s*) also depends on the private values, which remain secret.

Let us now have a closer look to the structure of the packets being exchanged during the main, aggressive and quick mode of IKE.

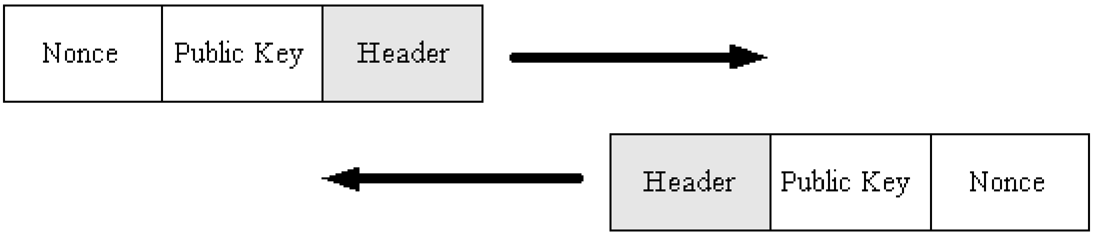
4.4.4.3 Main mode

The first step, securing an IKE SA using main mode, occurs in three two-way exchanges between the SA initiator and the recipient. In the first exchange, the two agree on basic algorithms and hashes.



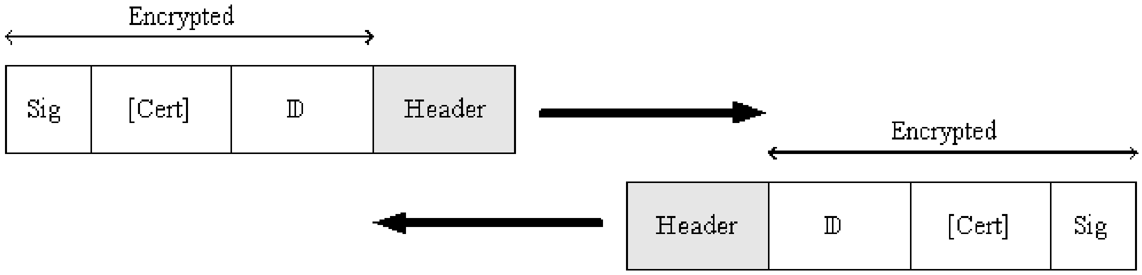
(Figure 13a - IKE main mode)

In the second step, they exchange public keys for the Diffie-Hellman exchange, and pass each other nonces – random numbers the other party must sign and return to prove their identity.



(Figure 13b - IKE main mode)

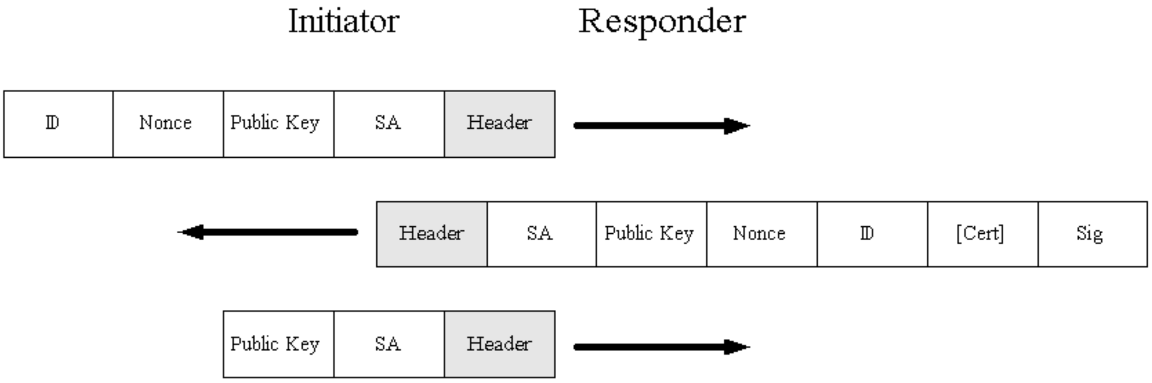
In the third step, they verify those identities.



(Figure 13c - IKE main mode)

4.4.4.4 Aggressive mode

Aggressive mode provides the same services as main mode. Here, the proposing party generates a Diffie-Hellman pair at the beginning of the exchange, and does as much as is practical with the first packet – proposing an SA, passing the Diffie-Hellman public key value, sending a nonce for the other party to sign, and sending an ID packet which the responder can use to check their identity with a third party. The responder then sends back everything needed to complete the exchange.



(Figure 14 - IKE aggressive mode)

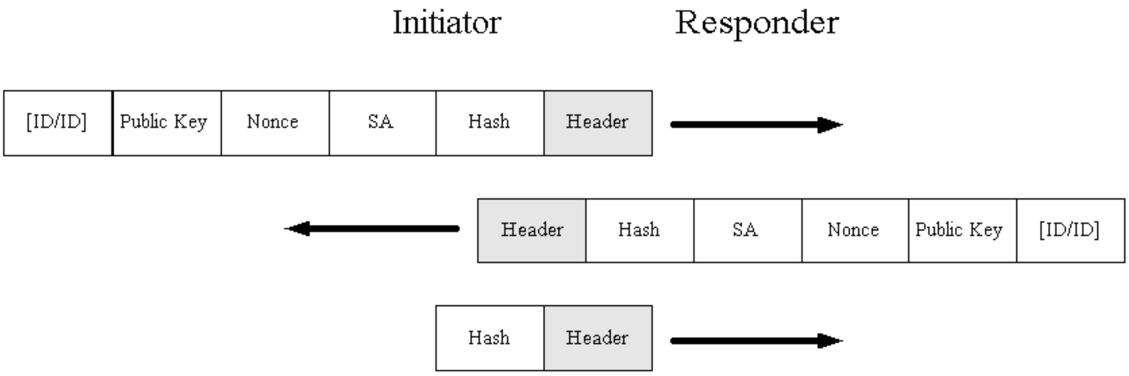
The main advantage of the aggressive mode is speed. But there is no identity protection for the communicating parties.

4.4.4.5 Quick mode

After having established an IKE SA, two communicating parties can use quick mode to negotiate general IPSec security services or generate fresh keying material.

Quick mode is less complex than either main or aggressive mode. Since it is already inside a secure tunnel (every packet is encrypted), it can also afford to be a little more flexible.

Quick mode packets are always encrypted, and always start with a hash payload. The hash payload is composed using the agreed-upon PRF and a derived authentication key for the IKE SA. The hash payload is used to authenticate the rest of the packet. Basic quick mode is a three packet exchange, like aggressive mode.



(Figure 15 - IKE quick mode)

4.4.4.6 Negotiating the SA

After having built a secure channel with the IKE SA, the general purpose SA can be negotiated. Therefore the initiator sends a quick mode message requesting the new SA. A single SA negotiation actually results in two SAs – one inbound, to the initiator, and one outbound. Each IPSec SA is one way and the node on the receiving end of that SA always chooses its own SPI to ensure it is the only SA using that reference.

Each SPI, in concert with the destination IP address and the protocol, uniquely identifies a single IPSec SA.

5 Related work

This chapter regards different existing concepts for the integration of IPSec and Mobile IP. For securing Mobile IP, the following features of IPSec are especially of interest:

- Tunnels to be established by using an automatic key and a security association management protocol.
- IPSec ESP protocol used in mobile IP to protect the redirected packets against both passive and active attacks launched.
- IPSec should also help these packets to go through firewalls.
- IP-Security and Mobility Integration.

The integration of both protocols (IPSec and Mobile IP) is still an open topic, which needs to be investigated. The major advantages can be summarized as follows:

- The key focus of this work will be to tie **Mobile IP** and **IPSEC** together as far as possible.
- IPSec may include both the link layer (by being at the network layer), the transport layer or run router to end system, router to router, etc.
- There should be no point in considering separate security mechanisms for the last virtual link tunneling scheme when IPSec can be used in all places.

Mobile IP needs IPSec by default as all packets between a remote MN to/from the home network should be made secure.

At the time this document was written, there were no standards for this merging. It seams that the work in progress focuses rather to the integration of security in the Mobile IP version 6. Nevertheless, mobility in IP version 4 has to be evaluated, because it will take some years to introduce the new IP version to the whole internet community. In the meantime nobody wants to work without mobility.

5.1 Internet draft 'Use of IPSec in Mobile IP'

The only draft dealing with the use of IPSec in Mobile IP was written in 1997 by John K. Zao and Matt Condell from BBN Technologies [9]. This draft was never proposed to become a RFC and is not valid anymore. It discuses the use of IPSec over Mobile IP for the HA-MN, HA-FA, CN-HA, CN-FA and the MN-CN connections. The IPSec is used in place of the normal IP in IP tunneling. Adaptations to the Mobile IP messages are proposed for coping with the IPSec tunnel establishment. There are special IPSec tunnel extensions added to the advertisements and the registration messages.

5.2 Secure Mobile Networking, Portland State University

This approach to integrate IPSec and Mobile IP is based on the IETF draft "Mobility Security Considerations" [10] written by Jim Binkley, Portland State University and John Richardson from Intel. The focus of this document is on how a secure enclave (firewall protected area) may tolerate Mobile IP or simple mobility systems (for example, DHCP used standalone) and remain secure.

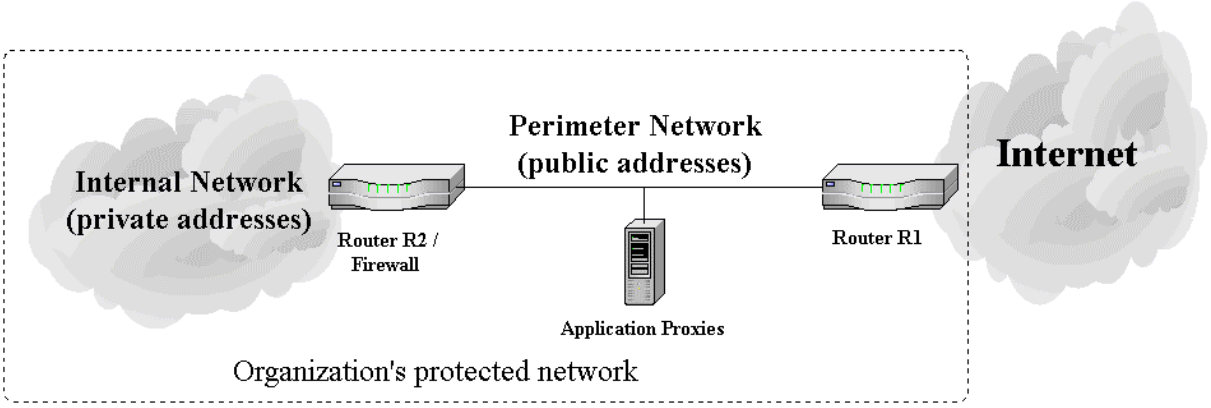
The draft discusses the security issues from two topological points of view. First they look at the situation from the mobile node abroad's point of view. It actually wants to get packets home and not compromise home security. Thus this point of view necessarily includes the mobile node's home enclave. They then look at the situation from the foreign security enclave's point of view, which wants to allow mobile service but protect itself.

To protect the mobile nodes in a foreign network, they propose to use DHCP to acquire "local" IP addresses, thus the mobile nodes can get by the anti-spoofing measures in the firewall router. This suggestion originally comes from Glass and Gupta [12]. Further, the mobile nodes can use IPSec with two-way tunnels between the home agent as a classic bastion host and the mobile node, as it is described in the "Secure Mobile Networking" document written by James R. Binkley and John McHugh from the Portland State University [19]. In this document, a secure mobile networking concept is presented that is based on ad-hoc networking secured with IPSec two-way tunnels. The main part concerning the integration of Mobile IP and IPSec is the replacement of the Mobile IP proposed IP in IP tunnel with IPSec. With their Ad-hoc routing concepts, the standard Mobile IP scenario is treated as a special ad-hoc routing case where the HA and the MN build a secure ad-hoc network.

5.3 Secure and mobile networking, Sun Microsystems, Inc.

Vipul Gupta and Gabriel Montenegro from Sun Microsystems [12] describe enhancements that enable Mobile IP operation in a network which is protected by some combination of source-filtering routers, sophisticated firewalls, and private address space. These enhancements should allow a mobile user, in the public Internet, to maintain a secure virtual presence within his firewall-protected office network. This constitutes what we call a Mobile Virtual Private Network (MVPN).

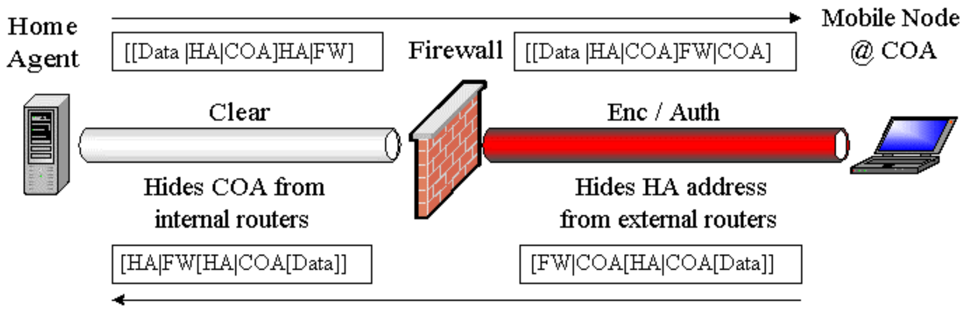
The first part of their paper describes the deployment of a security architecture which allows a separation of an organization's network into two sub networks with different security guidelines. The interior network is insulated from the Internet by a perimeter network (also known as De-Militarized Zone (DMZ)) and two packet filtering routers R1 (exterior or access router) and R2 (interior or choke router).



(Figure 16 - DMZ)

As an additional security measure internal network topology is hidden using application relays and private address space. Outside routers are unaware of internal addresses and inside routers (such as R2) are unaware of outside addresses. Inside routers, however, are aware of addresses on the perimeter network. All routers drop packets with an unknown destination address.

In the proposed deployment of a secure Mobile IP, the mobile nodes work in MN decapsulation mode with collocated COA. Two tunnels are used to pass the perimeter network (i.e. MIP registration messages). The tunnel between the home agent and the firewall hides the care-of address from inside routers and that between the firewall and the mobile node hides the home agent address from outside routers. The second tunnel can be used to provide encryption and authentication (*see Figure 17*).

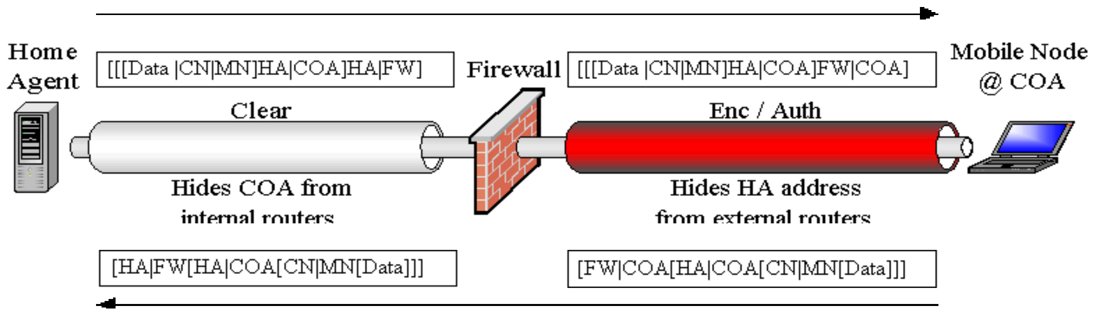


(Figure 17 – Tunnels for firewall traversal)

The authors propose to use SKIP[21] for the key management, the authentication and the encryption. The reason why they choose to take SKIP instead of the more recently used ISAKMP/Oakley [8], is the ability of SKIP to look up the sender's public key based on alternate names. With ISAKMP/Oakley, in turn, a receiver uses the source address of an incoming datagram to look up the sender's public key.

In their paper, the tunneling depends on the location of the mobile nodes. While roaming within the protected network, a mobile node can send datagrams without any SKIP processing. However, upon acquiring an outside care-of address, it should prepend a new IP header with the mobile node's care-of address as source and the home agent as destination on all packets sent using its home address. This establishes a reverse tunnel from the mobile node to its home agent. Then it should enable SKIP processing on all packets destined for the home agent. So the mobile node must be able to determine when its care-of address does not belong to the protected domain.

Being outside the protected network, all data exchanged between the MN and the HA is sent through these two tunnels. So even the registration messages of Mobile IP are protected by SKIP processing. After a successful registration the established Mobile IP tunnel is built between the MN and HA, passing through the other two tunnels. This looks like this:


Home Agent
[[[Data |CN|MN]HA|COA]HA|FW]
Firewall
[[[Data |CN|MN]HA|COA]FW|COA]
Mobile Node @ COA
Clear
Enc / Auth
Hides COA from internal routers
Hides HA address from external routers
[HA|FW[HA|COA[CN|MN[Data]]]
[FW|COA[HA|COA[CN|MN[Data]]]

(Figure 18 – Firewall traversal and Mobile IP tunnels)

5.4 Comparison of the different concepts

The first discussed draft with the title “Use of IPSec in Mobile IP” uses IPSec ESP protocol in the Mobile IP packet redirection tunnels to protect the redirected packets. For the establishment of these tunnels they propose to use automatic key and security association management protocols such as ISAKMP. In today’s network infrastructure the problem of a global key management is still not solved. So if SAs have to be built with foreign hosts it first has to be ensured that the same authentication mechanisms are used. That is why, today, proposals which are more independent of intervening hosts, have better chances to be deployed. This missing public key infrastructure (PKI) is also the main reason why existing proposals to fully integrate IPSec and Mobile IP are not really feasible.

The other two approaches are rather suggestions how to make Mobile IP and IPSec work together. This leads to redundant processing such as double authentication or tunneling of tunnels. At the other hand these approaches use Mobile IP and IPSec without changing them. Full integration of these two protocols is not possible without changing them.

The work called “Secure Mobile Networking”, describes a much more general approach to the IP mobility problem. The authors introduced a new protocol called *Multi-hop Multicast Ad Hoc Routing (MADRP)*[19] which allows a mobile node to do an expanding ring search for another destination ad-hoc host across any number of participating mobile hosts acting as routers. So they propose the look at the IP mobility problem as a part of the general ad-hoc networking problem. This is obviously a good idea, but much too complicated if the aim is to secure a Mobile IP environment.

Gupta and Montenegro’s realization of a secured Mobile IP seems to be the easiest and also most efficient way to solve Mobile IP security problems. Building a secured channel to the home firewall allows authentication of each packet entering the secure enclave. The main advantage of such a secure channel through the insecure Internet is that all Mobile IP messages traverse encapsulated. So known strong authentication and encryption of the IPSec protocol suite is used. It is important to see that this way even privacy for the registration information such as MN and HA IP addresses is guaranteed. It would be even possible to omit all authentication proceeding provided by Mobile IP.

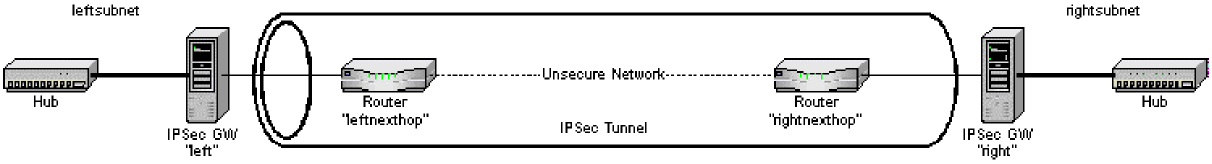
6 SecMIP: a Secured Mobile IP Implementation

After knowing the most important proposals how to secure Mobile IP with the help of strong authentication and strong encryption, the idea was to design a new deployment architecture taking the best out of the existing concepts. The result was called SecMIP, which stands for Secured Mobile IP.

6.1 Deployment Architecture

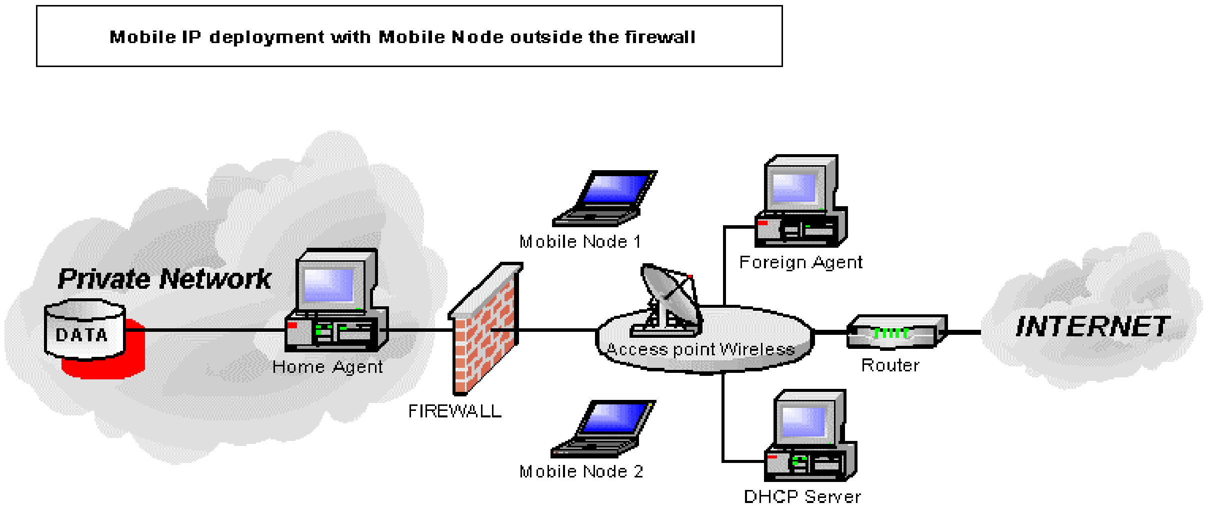
Like V.Gupta and G.Montenegro proposed in their paper "secure and mobile networking" [12], a so-called screened-subnet firewall architecture has choosen, where the organization's interior network is isolated from the Internet by a DMZ. This particular architecture was chosen for its popularity and superior security characteristics. The firewall between the DMZ and the private interior network is the only entry point to the organization's private network.

Later in this text, it will be shown that this simplifies the security management significantly, since all traffic must pass this firewall, Mobile IP included. As an additional security measure, private addresses are used for the internal network. This hides the topology of the private part of the network, even if packets are tunneled (i.e. with IPSec in tunnel mode) through a public network. This private network is then called a virtual private network (VPN). To ensure privacy of such VPNs, normally encryption mechanisms are deployed to the hide the tunneled data passing insecure parts of the Internet.



(Figure 19 - VPN)

The main requirement driving our deployment of Mobile IP, and the topological placement of home and foreign agents with respect to the firewall is that the corporate network must not be exposed to any new security threats. The easiest and most effective way to fulfill this requirement is to place all Mobile IP devices (except own HAs) outside the private network, i.e. placing them in the DMZ. This placement of the foreign agents allows a non-restricted Internet access by the guest mobile nodes, since they can be handled like any host in the public Internet. Of course the mobile node itself should be protected from attacks coming from other Internet nodes. This can be done with a firewall software on the MN.



(Figure 20 - MIP device deployment)

In the mobile node decapsulation mode, the mobile nodes receive their IP addresses from a DHCP server as described above. All mobile nodes are always outside the firewall, i.e. in the DMZ, even those owned by the corporation. This means that the mobile nodes are never located in the same subnetwork as the HA, while using wireless LAN and thus also never registered at home. Mobile nodes that become attached to the physically secured wired network inside the firewall, stop Mobile IP tunneling. Despite of speed reductions resulting from authenticating and encrypting data being sent from the organizations own DMZ to the firewall, the benefits concerning the security of the VPN justify this concept. It is even possible to reduce the traffic on the interior private network, as the home agent advertisements would not be needed regularly. If the organization's security policies allow the own mobile nodes to be attached inside the interior network, all Mobile IP functionalities should be disabled. This allows to ensure that wireless attachment points are only used with a secured Mobile IP.

6.2 IPSec in SecMIP

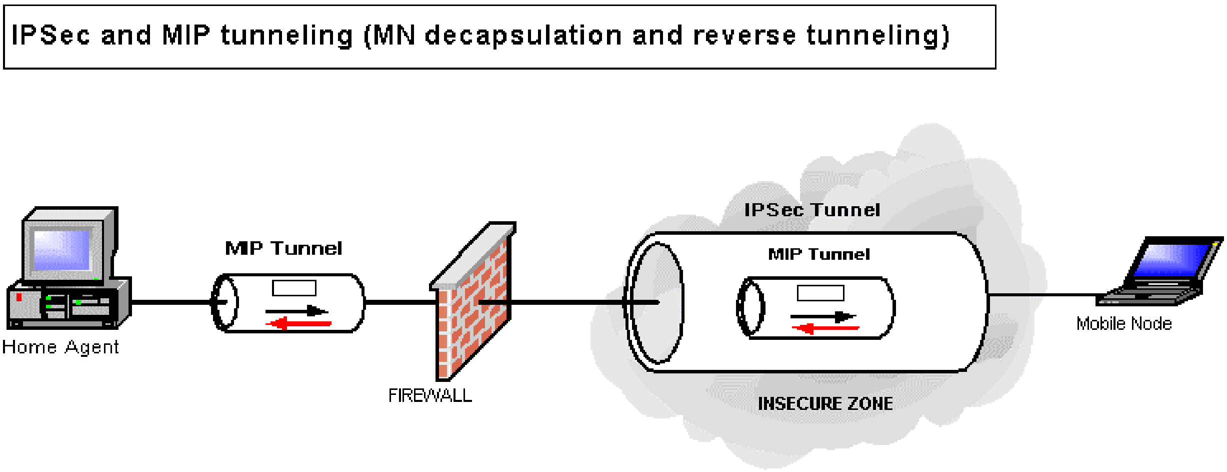
As the mobile nodes that belong to the corporation have to traverse the firewall to access the VPN, they have to authenticate themselves to the firewall. This authentication is realized with IPSec. Since there is a real end-to-end authentication between the corporation's own mobile nodes and the firewall, they can easily be configured with a shared secret or even RSA keys. The establishment of a secure IPSec tunnel between the mobile node and the firewall makes it possible to use a lightweight (without security mechanisms) implementation of Mobile IP, since all packets traversing the public network are encrypted and authenticated by IPSec. We will discuss the security mechanisms added by IPSec for each phase of Mobile IP as registration, tunneling, re-registration later in this document (*see 6.3 Security Aspects using SecMIP*).

Similar to the tunneling proposed by Sun, SecMIP uses an IPSec tunnel to protect the Mobile IP tunnel passing the insecure parts of the Internet. Within the private network, however, the Mobile IP tunnel is sufficient.

For SecMIP, ISAKMP/Oakley was chosen. ISAKMP/Oakley and SKIP are quite similar, both offer security for transported data. But there are some little differences, which favour ISAKMP:

- After having negotiated the SA, packets do not contain a key management header as in the SKIP case.
- An attacker has no knowledge of which algorithms are being used for encryption and authentication, unlike in SKIP.
- With ISAKMP there is less overhead for keying in every packet exchanged after having negotiated all security parameters.

There is work in progress for optimization of both SKIP and ISAKMP to reduce key management overhead. For more information, please consult the ietf Internet drafts.



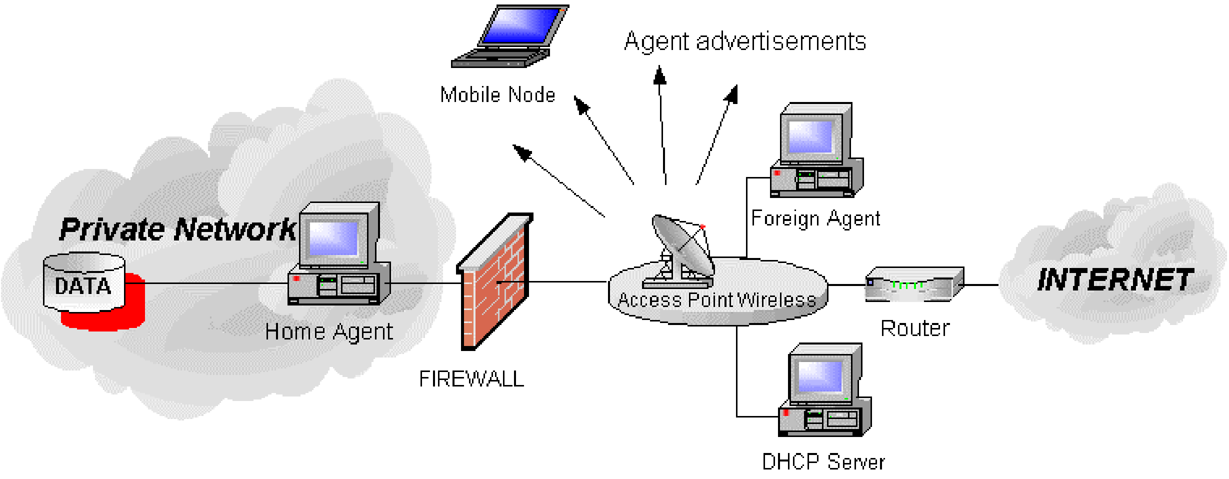
(Figure 21 - SecMIP tunneling)

6.2.1 SecMIP operation

In this section the operation mode of SecMIP is regarded in detail. This is done by going step by step with a mobile node which changes its point of attachment.

1. **Network detection**

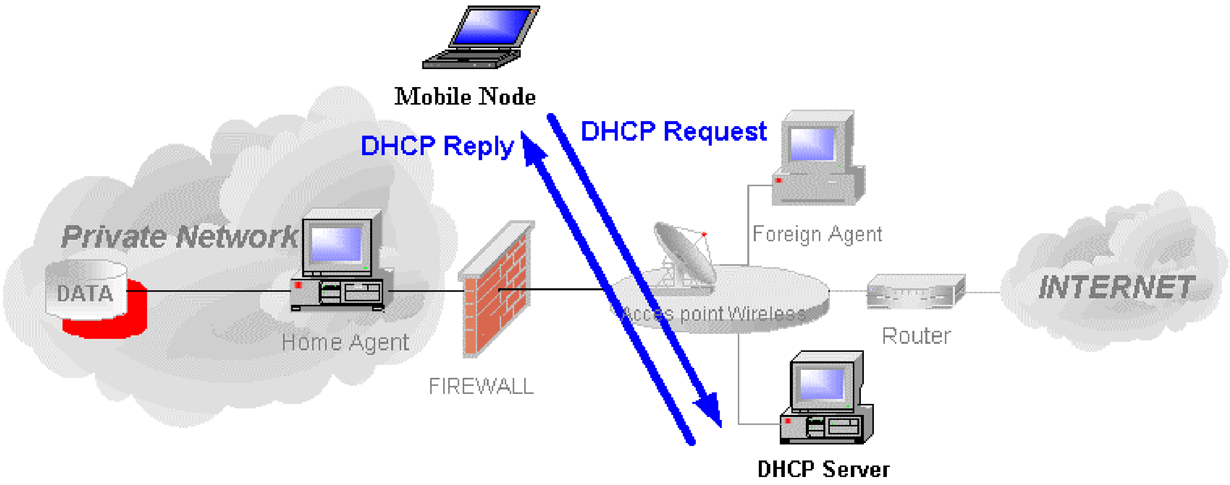
Entering a conference room, a mobile node has to be connected either to a wireless network (with access point – see *Figure 22*), or to a conventional network medium like Ethernet. On this demilitarized network, foreign agent advertisements are broadcasted regularly. Catching such an ICMP message, a MN learns that it just has entered a new network. The mobile node can also send an agent solicitation to provoke an agent advertisement. Then, the MN stops the old IPSec tunnel, which was been established from an older location (with an old collocated care-of address).



(Figure 22 - SecMIP Network detection)

2. Acquiring a routable IP address

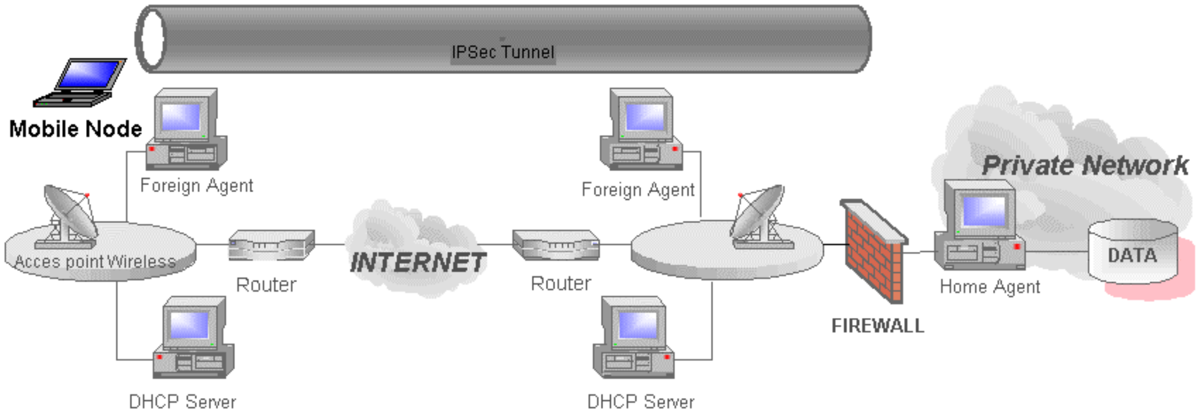
In MN decapsulation mode, the mobile node needs to acquire a collocated care of address through a DHCP server. It is also possible to read available collocated care-of addresses from the foreign agent advertisements. But in this case the foreign agent has to keep track on the used addresses.



(Figure 23 - SecMIP acquiring a collocated COA)

3. Establishment of a bi-directional IPSec tunnel between MN and Home Firewall

As shown in *Figure 24*, data packets pass an insecure, public network between MN and Home-Firewall. So it is by far the best approach to establish an IPSec tunnel between the MN's COA and the home firewall before any Mobile IP messages are exchanged between these two entities. The IPSec tunnel ensures **authentication, integrity and privacy** of every IP packet sent by the Mobile IP registration procedure.



(Figure 24 - IPSec tunnel MN-Home firewall)

4. Home Agent and MN negotiation: Mobile IP registration (light)

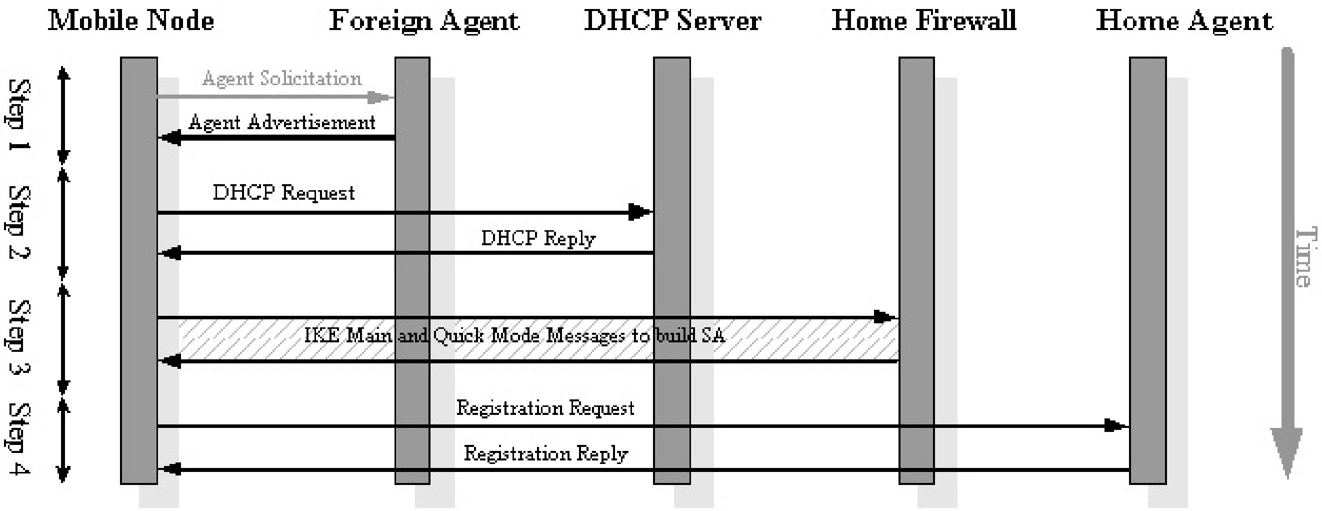
Since all Mobile IP negotiation between HA and MN pass the IPSec tunnel to the home site's firewall, the registration messages needs neither to be authenticated nor encrypted by the Mobile IP protocol. The security in the private network behind the firewall is supposed to be ensured. So the whole MIP registration proceeds in a secure way.

5. Data transfer from the MN to the whole Internet including its home network

Until the next movement, MN can communicate with any other CN. If the mobile node changes its location, the procedure begins at step 1.

6.2.2 Exchanged messages

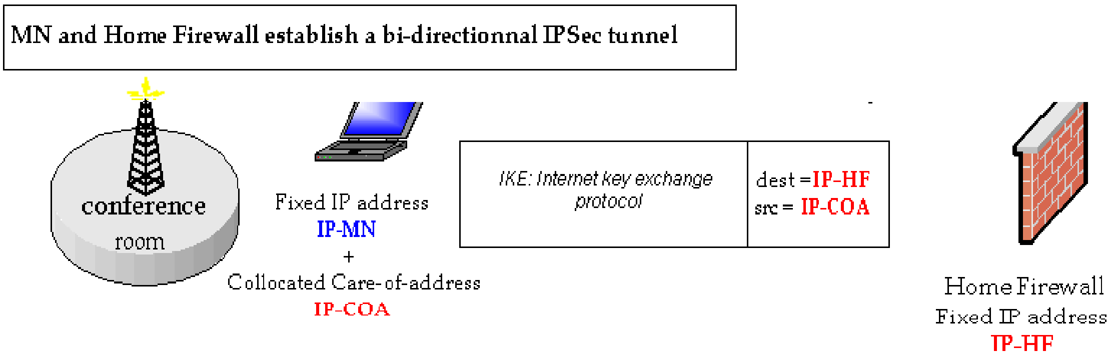
The next figure shows which messages are exchanged between the involved SecMIP entities during the described steps of SecMIP.



(Figure 25 - Exchanged messages)

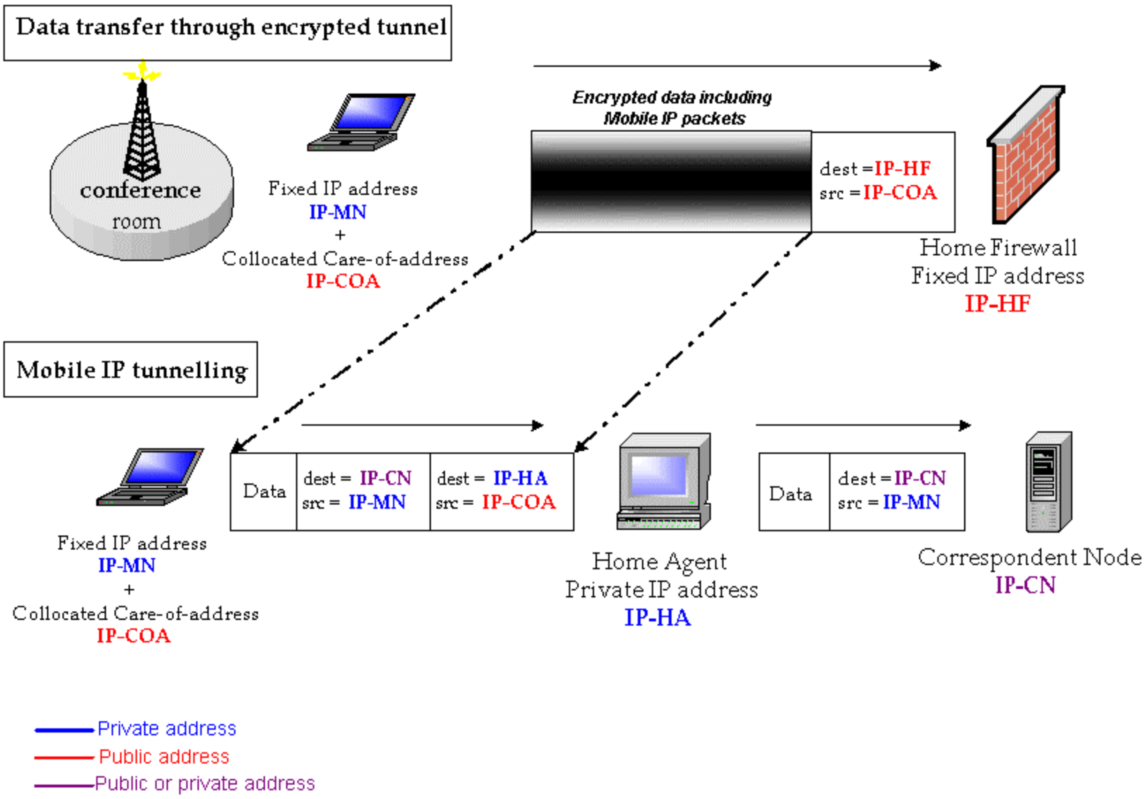
6.2.3 SecMIP packets

The figure below shows how the exchanged IP packets are built. The packets exchanged in the first two steps are not really important for the understanding of SecMIP and therefore not described explicitly. (For detailed information please consult RFC 2002 for structure of Agent Advertisements and RFC 2131 for the DHCP). In step three, IPSec packets are exchanged between the mobile node's collocated care-of address and the Home Firewall (HF). These packets carry the information for the main and quick mode of IKE in the payload (As described in *4.4.4 Internet Key Exchange (IKE)*).


MN and Home Firewall establish a bi-directionnal IPSec tunnel
conference
room
Fixed IP address
IP-MN
+
Collocated Care-of-address
IP-COA
IKE: Internet key exchange protocol
dest = IP-HF
src = IP-COA
Home Firewall
Fixed IP address
IP-HF

(Figure 26 - IPSec packets)

After having set up a secure channel with the IPSec protocol suite, Mobile IP packets can pass the insecure Internet. These encrypted and authenticated Mobile IP packets are decrypted and decapsulated by the Home Firewall and delivered to the HA. The home agent finally decapsulates these Mobile IP packets and delivers them to the appropriate receivers, the correspondent nodes.



(Figure 27 - SecMIP packets)

6.3 Security Aspects using SecMIP

This section takes a closer look to the security aspects using a secured Mobile IP solution in a company's network. The different attacks where already shortly discussed in a previous section (*3.2.2 Security issues in Mobile IP*). Here, these attacks are regarded especially for the use of SecMIP.

6.3.1 Denial-of-Service (DoS)

Generally spoken, a DoS attack is something that an attacker does in order to prevent someone from offering a service. Usually this happens by sending a tremendous number of packets to a server that brings the host's CPU to its knees attempting to process all of the packets. So there is no capacity left for serving the Good Guy. Another possibility is to disturb the connection between the client and the server. For example where an attacker prevents packets from flowing between two legitimate nodes.

Specifically to Mobile IP the registration request has to be protected against manipulations by an attacker. Adding a cryptographically strong authentication in all registration messages normally does this. Mobile IP allows a mobile node and home agent to use whichever authentication algorithm(s) they choose. However, all implementations must support the default algorithm of Keyed MD5. With this algorithm authentication and integrity is provided to the registration messages.

In an IPSec tunnel, all traffic is encrypted and authenticated. Establishing such a secure channel prior to exchanging Mobile IP control messages makes it possible to protect the whole Mobile IP protocol against attacks from the public internet. As a security increase IPSec provides also privacy since all packets are encrypted flowing through the insecure network.

6.3.2 Replay attacks

Imagine a MN registering with its HA. If an attacker could obtain and store a copy of a valid registration request, it could “replay” it at a later time and registering a bogus collocated care-of address. Such an attack is called “replay attack”. How to prevent it?

The Mobile node generates a unique value for the identification field in each successive attempted registration. Each value is generated in such a way that the home agent can determine what the next value should be. This way, the replay attack of an attacker will be considered as out of date. Mobile IP implements two methods: timestamps and nonces. With timestamps, the MN uses its current date and time in the identification field. Then the HA compares it to its own current date and time. If the two values are not sufficiently close, the HA refuses the registration and provides enough information in the reply to allow the MN to synchronize its clock (tolerance usually admitted: 7s). With nonces, the MN specifies to the HA the value to be placed in the lower half of the identification field in the next registration reply and conversely the HA specifies the value to be placed in the upper half of the identification field in the next registration request. In case of a failure, a special error code allows the MN to synchronize to the HA.

In our solution SecMIP, the registration negotiation occurs in the IPSec tunnel between the MN and the Home Firewall (see *Figure 24*). Outside the home private network, if an attacker can obtain a copy of a valid registration request, he can neither decrypt nor use it.

Theoretically, the home private network is considered as secure. If this is true, the replay protection of MIP is not useful anymore.

6.3.3 Passive eavesdropping

Theft of information can occur when somebody has physical access to the network whose packets are sent over. As it is nearly impossible to detect eavesdropping the only protection against it is to make the stolen information useless. The most efficient way to do this is the encryption of the information.

Again, when using IPSec to encrypt all Mobile IP messages there is no information to be stolen by an attacker. Even the IP addresses of the mobile node and the home agent are hidden inside the encrypted IPSec security payload.

6.3.4 Session-stealing attacks

If an attacker has been able to connect to the mobile node’s Ethernet link, a session–stealing attack can occur as follows: the attacker waits for a mobile node to register, eavesdrops to see any interesting conversations and IP addresses, then floods the MN with spoofing packets, and steals the session by sourcing packets that appear to have come from the MN and by catching packets destined to MN.

Such an attack may occur when an attacker is physically connected in the home private network if there is no link-layer encryption. However, it is not a threat specific to Mobile IP but concerns the internal home network security. But SecMIP is not threatened by session stealing attacks due to end-to-end encryption with IPSec between MN and Home Firewall. Outside the home network, an attacker can not execute these attacks.

6.4 Implementation of SecMIP

In this paragraph a prototype of SecMIP is explained in detail. As mentioned in section 5.3 (*Secure and mobile networking*), SecMIP uses two tunnels. One for providing mobility and the other for encrypting all communication.

6.4.1 Dynamics Mobile IP and FreeS/Wan IPSec

Dynamics Mobile IP[15] has been implemented by the Helsinki University of Technology (HUT). This implementation consists of three executable programs. One for each entity in Mobile IP, for the HA, FA and the MN. The programs are coded in C and all features are RFC compliant. The configuration of the entities is very simple, there is one configuration file for each of them.

In the SecMIP implementation, Dynamics Mobile IP is taking over the following functions:

- Handling agent advertisements (home and foreign)
- Establishing Mobile IP tunnels between HA and MN
- Capturing and redirecting packets for MN on the home network

FreeS/Wan[16] stands for “free secure WAN” and is the result of a project started by John Gilmore, who wanted to make an IPSec implementation for Linux available for free. FreeS/Wan works with RSA and is easy to configure. For each IPSec node a RSA key pair has to be created and the allowed connections have to be described in a configuration file.

FreeS/WAN does:

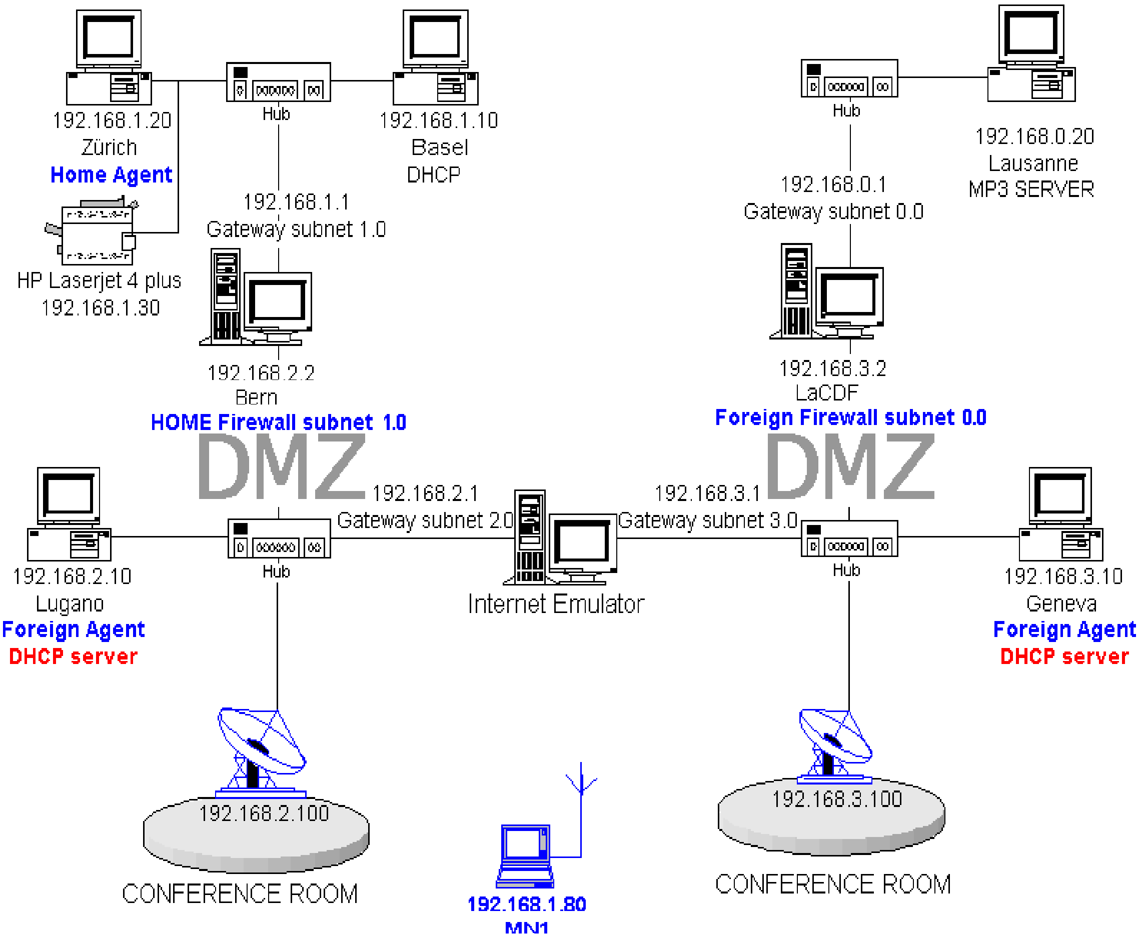
- Negotiating keys between MN and Home Firewall
- Establishing secured tunnels between MN and Home Firewall
- Encrypting and authenticating all data between MN and Home Firewall

Dynamics Mobile IP and FreeS/Wan have been chosen, because of their open source code. It has to be mentioned, that these implementations are not thought to be merged. Many adaptations were to be done, before they worked successfully together as an SecMIP prototype. In a fact, being used as the Mobile IP protocol part in a SecMIP implementation, dynamics Mobile IP is much too heavy, since a “light” MIP without any strong security would be enough. Also the design of FreeS/Wan is not flexible enough, as all IPSec devices are just initiated once starting up the IPSec daemon. These two main disadvantages had limiting effects on the delay minimization during a handover, since FreeS/Wan has to be restarted after each location update and dynamics provides strong authentication for each registration message.

In the next section the SecMIP environment and the implementation itself are explained in detail. The main part of the prototype is designed to handle the communication and the timing conditions between IPSec and Mobile IP. For that, shell scripts were written and placed into the source code of Dynamics. These scripts are shortly explained and a timing diagram shows the interaction between the main processes of SecMIP.

6.4.2 Test bed SecMIP

The figure below shows network that was installed for the development of SecMIP. On the left side there is the home network, where the MN normally belongs and where the HA keeps track of the MN's movements. On the right side the foreign network is situated. Both networks are built with a DMZ (*see 5.3 Secure and mobile networking*), where a conference room might be attached. In this DMZ it is secure to deploy wireless Access Points, because the interior network is protected by a firewall. To enable mobility services, a foreign agent with DHCP services is set up in this perimeter network.



(Figure 28 - SecMIP test bed)

The test environment is based on Linux PCs. All machines are equipped with SuSE's Linux distribution. Dynamics HUT implementation of Mobile IP and FreeS/Wan's implementation of IPSec are supposed to follow IETF standards.

6.4.3 SecMIP scripts

As already mentioned before, the main part of the merging work was to manage the interoperability between the functional entities, i.e. Dynamics MIP, FreeS/Wan and the operating system. Therefore, the following scripts have been written, which are then executed at the right time. All these scripts are running on the mobile node to ensure that Mobile IP uses always a well configured and if needed secured network interface to communicate with the home network.

Disconnect executes a Dynamics Mobile IP API call, which sends a deregistration message to the HA and disconnects the MN from the HA. In fact, this command destroys an existing tunnel between the MN and the HA.

Connect executes a Dynamics Mobile IP API call that sends a registration message to the HA and establishes a direct tunnel between MN and HA. Before doing that, the MN has to be disconnected.

DhcpSecure sends a DHCP request and updates the network interface configuration and the routing table. Afterwards an IPSec connection to the home firewall is built. This script causes that all outgoing IP packets on the MN are secured.

UpdateLocation1 (on a foreign network), UpdateLocation2 (on the home network): By the API call 'update *interface*' the process **dynamics_admin** can be forced to update the collocated COA. Therefore the actual configuration of the *interface* is used. If the mobile node is at home (UpdateLocation2), the COA is deactivated and the home IP configuration is taken by the 'update' command.

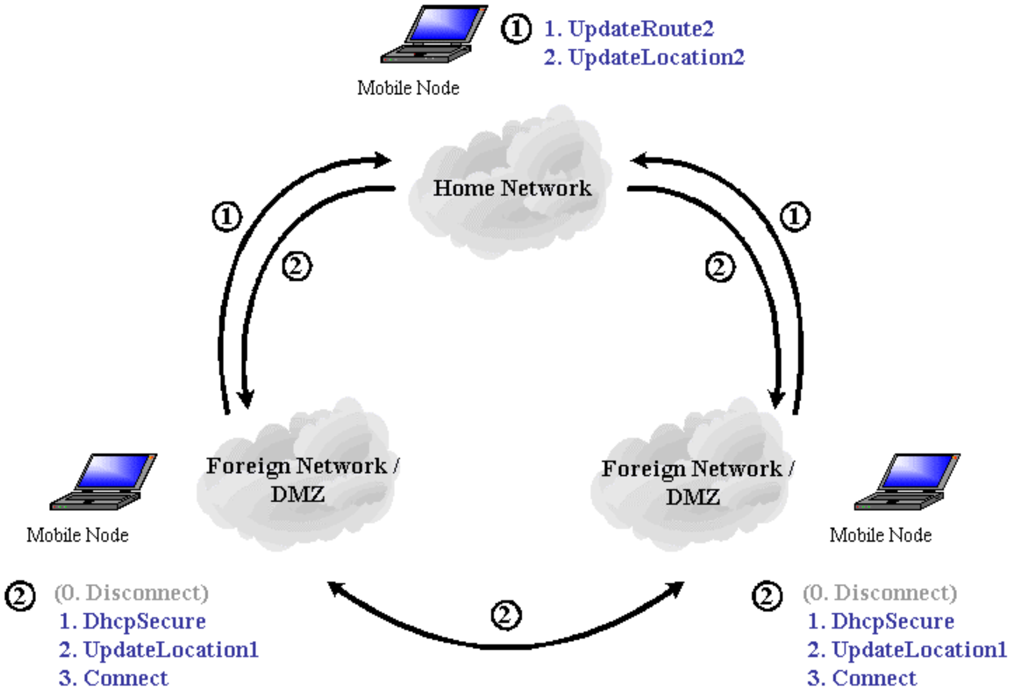
UpdateRoute1 updates the routing table of the MN when it is connected to a foreign network and when the Mobile IP tunnel between MN and HA is established.

UpdateRoute2: When the MN arrives at home, the IPSec and Mobile IP tunnels have to be stopped and the routing table updated.

Firewall.rc: To control the incoming and outgoing network traffic of the MN, an IP-Filter is initialized. In a Linux environment *ipchains* is the most well known filter (see *Linux Firewall Howto*). Three rule chains are created to control the Output, Input and Data traffic on the MN's network interface (*see Annex*). The mobile node has a default firewall configuration which protects it against intruders. This protection is always enabled. When not attached to the home network, the MN is only allowed to communicate through a secured IPSec device. This guarantees the privacy of sensitive data. The script Firewall.rc is enabling this additional security measure.

6.4.4 Temporal operational sequence

Keeping the different scripts in mind, let us have a closer look at the timing of the individual actions. Once Dynamics Mobile IP and FreeS/Wan's IPSec is started, the scripts are executed as followed.



(Figure 29 – Scripts timing)

6.4.5 Implementation details

To make it possible for the MN to detect its attachment point, agent advertisements are broadcasted on the network. These advertisements are either foreign agent advertisements on foreign networks or home agent advertisements on home network. Dynamics Mobile IP manages these agent advertisements:

- On the home network, the HA broadcasts home advertisements
- On each conference room (foreign network), FAs broadcast foreign advertisements
- The mobile node has to handle these advertisements to detect a new attachment point

In our secure Mobile IP solution, the Mobile IP must establish a direct bi-directional tunnel to the Home Agent. In dynamics source code, the variable **API_TUNNEL_FULL_HA** defines this operation mode. Unfortunately, dynamics Mobile IP is supposed to ignore all foreign advertisements in this mode, because it assumes that there are no foreign agents available at all. So two modifications had to be performed in the source code:

In **mn.c**, in the procedure called "find_agent", which decides what to do with the received advertisements:

```
//---------------------- SECMIP-----------------------------------

 //The 3 lines below give the current (foreign) advertisement the value
NULL
 //In our scenario, we don't want to ignore such advertisements
 //That's why, we suppress this operation by ignoring these 3 lines


            //if (mn.current_adv != NULL) {
            //mn.current_adv->in_use = 0;
            //mn.current_adv = NULL;
            //}

//---------------------END OF SECMIP----------------------------
```

- In **mn_agentadv.c**, in the procedure "find_fa_with_priority", which decides which foreign network to join:

```
//-----------------------SECMIP-----------------------------------------

 //DYNAMICS consider that in mode "direct connection to the HA", FA agent
 //advertisement are ignored. NOT FOR SECMIP!!

      /* if we are using direct connection to the HA, do not try to change
       * the FA */
/****************************************************/

      /*if (mn.tunnel_mode == API_TUNNEL_FULL_HA) {
            DEBUG(DEBUG_AGENTADV, "Direct connection to the HA - ignoring "
                  "FA agent advertisement\n");
            return FA_GET_NO;
            }*/

//-----------------------END OF SECMIP-----------------------------------
```

Running SecMIP

1st step: Dynamics mobile IP is running on the mobile node in order to handle agent advertisements. The initial state is 'disconnected'.

Depending on received advertisements, the good decision must be taken by the mobile node. In the source code of Dynamics, the file which handles the advertisements is called **mn_agentadv.c** (see Annex). Obviously, this is where the scripts have to be placed.

2nd step: If the mobile node receives foreign advertisements.

The function 'get_fa(current advertisement)' decides what has to be done after receiving an advertisement:

```
/* Get a FA
 * Returns:
 *   0 = FA_GET_NO = FA not found or HA agentadv still valid => do not try
to register
 *   1 =  FA_GET_CHANGED = new FA found
 *   2 = FA_GET_SAME FA found, but it is the same as the current FA */
```

When the mobile node changes its attachment point, this function returns FA_GET_CHANGED. Depending on the MN's actual state (disconnected, request_tunnel, connected…) and the returned value of 'get_fa', the procedure 'handle_fa_adv' defines the further behavior of the MN. With the simple command 'system("*script*")', the *script* can be invoked.

```
switch (mn.state) {
        case MN_DISCONNECTED:

//----------------------SECMIP------------------------------

 //If a (new) FA agent advertisement is received, 3 scripts are
 //executed: the first for DHCP request and IPSec establishement,
 //the second for updating dynamics_admin location
 //the third for establishing the tunnel between MN-COA and HA

        chg = get_fa(adv);

            if (chg == FA_GET_CHANGED){
              system("DhcpSecure");
              system("UpdateLocation1");
              system("Connect");

//-------------------END OF SECMIP----------------------------

            break;


        case MN_REQUEST_TUNNEL:
            /* FIX: check that the advertised data is ok (tunnel mode etc.)
             * FIX: if the real tunnel is not yet up and the MN gets a
             * flood of agentadvs from different FAs, there might not be
             * enough time for the reply to arrive and MN might try to
             * register to yet another FA.. */

              chg = get_fa(adv);

//----------------------SECMIP-------------------------------------

 //If a new FA is detected, the MN disconnects "from its old CAO",
 //then makes a new DHCP request, establishes a new IPSec Tunnel,
 //updates its location and connects again to the HA

            if (chg == FA_GET_CHANGED){
              system("Disconnect");
              system("DhcpSecure");
              system("UpdateLocation1");
              system("Connect");
            }

//---------------------END OF SECMIP-------------------------------

                break;
        case MN_CONNECTED:

            chg = get_fa(adv);
            /* start requesting the tunnel if the current FA's seq#
             * indicates that the FA has rebooted or if the FA has been
             * changed */

//--------------------SECMIP---------------------------

            if (chg == FA_GET_CHANGED){
              system("Disconnect");
              system("DhcpSecure");
              system("UpdateLocation1");
              system("Connect");
            }

//-----------------END OF SECMIP---------------------
```

After being successfully connected to the HA, the MN's routing table has to be changed to force all IP packets to pass the secured path home. This is done at the end of the procedure called 'connected' in the main file **mn.c.** Therefore the **UpdateRoute1** is executed just before that the MN prints "Connected".

3rd step: If the mobile node receives home advertisements

Dynamics uses other procedures to handle home agent advertisements, especially 'handle_home_adv' in **mn_agentadv.c**. So at the end of this procedure, the scripts **UpdateRoute2** and **UpdateLocation2** are executed.

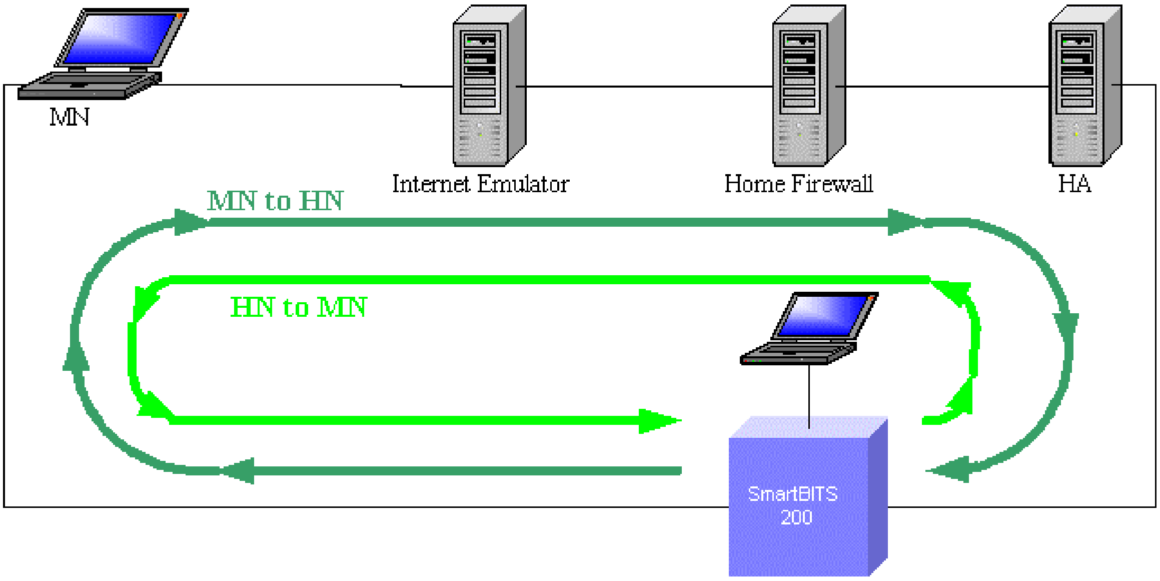
```
//-------------------------SECMIP----------------------------------

 //The MN is about to go back home and the two following system calls
 //update the routing table (home) and the location (dynamics_admin
updated)


            system("UpdateRoute2");
            system("UpdateLocation2");
            close_for_home(STATE_INIT);
      }
}

//-----------------------END OF SECMIP-------------------------------
```

7 Experimental results

The described SecMIP implementation has been tested to evaluate the effectiveness of the proposed way to protect Mobile IP communication. To estimate the performance impact due to reverse and IPSec tunneling, different scenarios were set up to compare the latency and frame loss rates.

7.1 Test network

All these tests were done with the help of a SMARTBITS 200 network testing tool. This tool has up to four Ethernet interfaces on which traffic can be generated and statistics can be evaluated. In order to lead the test packets through the SecMIP infrastructure, network devices were added to the HA and the MN (*see Figure 30*). To separate the performance impact due to encoding/encapsulation and decapsulation/decoding, unidirectional flows were defined.



(Figure 30 – Test network configuration)

7.2 Test scenarios

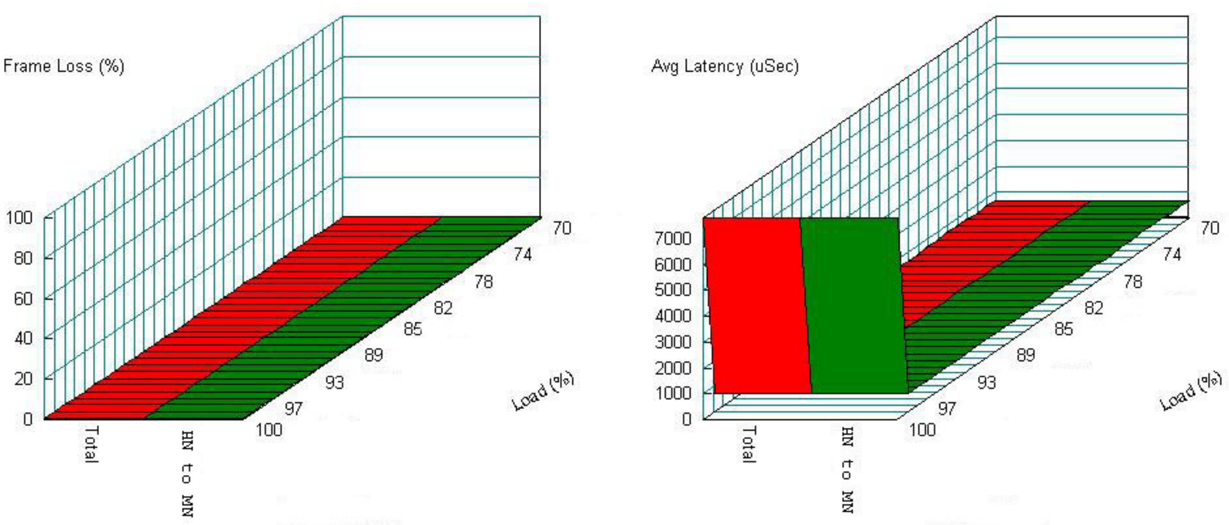
In the first scenario the routing through the network was measured. That means without any tunneling or additional processing due to Mobile IP or IPSec. The estimated performance in this scenario will then be compared with the values estimated in the next scenarios deploying Mobile IP and IPSec.

The next diagram shows the latency and the frame loss as functions of the load. All Ethernet devices on the test infrastructure support 100Mbit/sec in full duplex mode. So the traffic generator generates unidirectional flows of IP packets up to 100Mbit/sec. These unidirectional flows were generated successively to clearly separate the performance impact on the mobile node and the home firewall due to encoding/encapsulation and decoding/decapsulation.

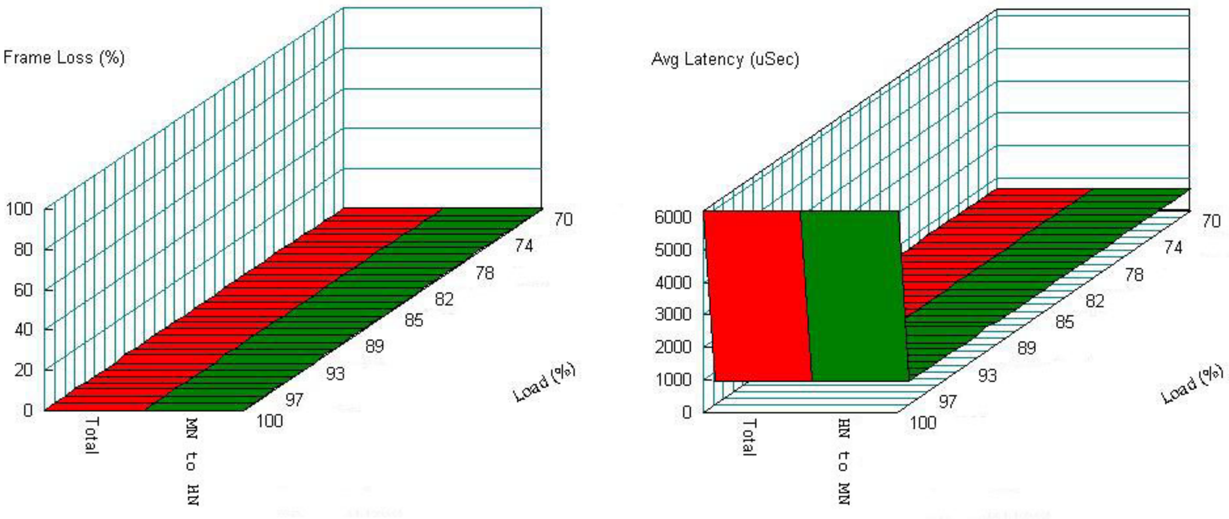
Two different frame sizes were tested, 64Bytes and 1400Bytes. The smaller packets were transporting IP/UDP as often used in streaming applications or Voice over IP (VoIP), and the bigger ones IP/TCP data simulating ftp data transfer. In the different test scenarios, these IP packets were then transported in different manners. In the first one, they were just routed by the intervening hosts. In the second scenario, as it will be shown later, these packets were encapsulated by the Mobile IP tunnel (IP in IP), which extends the frame sizes by an additional IP header (20Bytes). In the third scenario there is also the additional IPSec information to be carried. This overhead depends on the transported data in the ESP and its encryption and authentication.

7.2.1 Test scenario one – network performance

The first measurements estimated the performance of the test infrastructure. The only processing done by the intervening hosts is the routing of the IP packets. So it is not surprising that the estimated performance depends strongly on the packet size of the generated traffic.

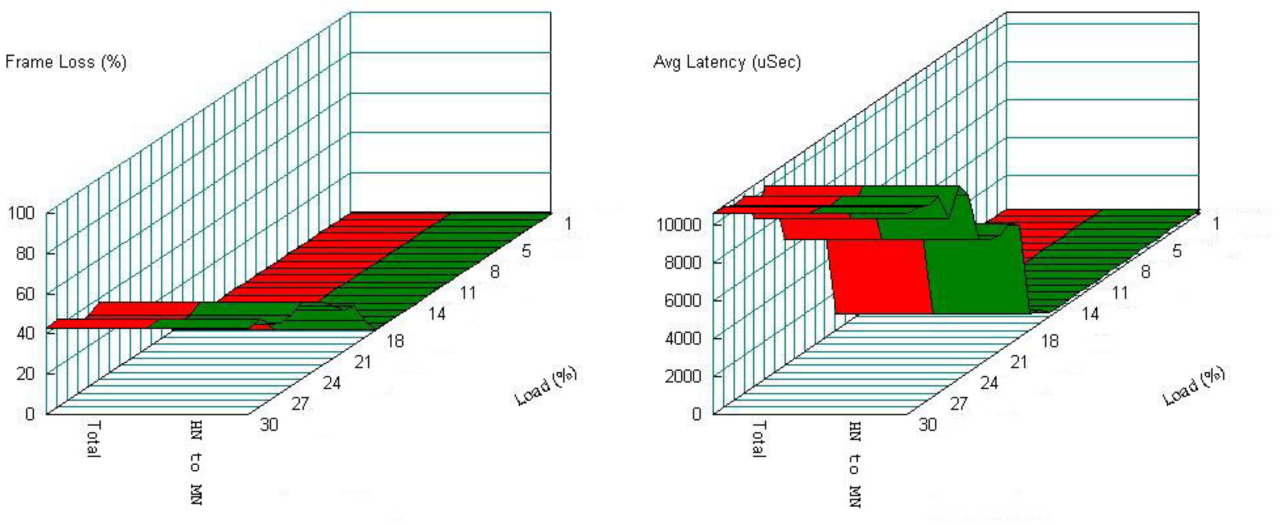


(Figure 31 – frame loss rate and latency in the test network HN ⇒ MN (1.4kBytes packets))

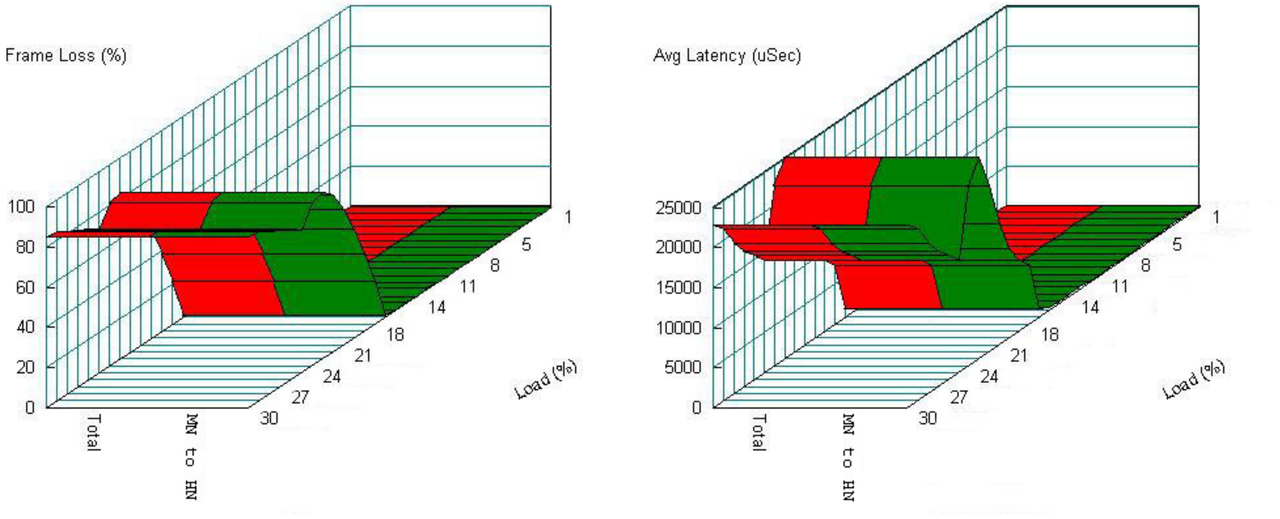


(Figure 32 – frame loss rate and latency in the test network MN ⇒ HN (1.4kBytes packets))

When small packets with a size of 64Bytes are generated, the impact on routing performance is much bigger. This is very interesting as streaming applications often use small packets carrying UDP. Also VoIP uses small packets to keep the delay as small as possible.



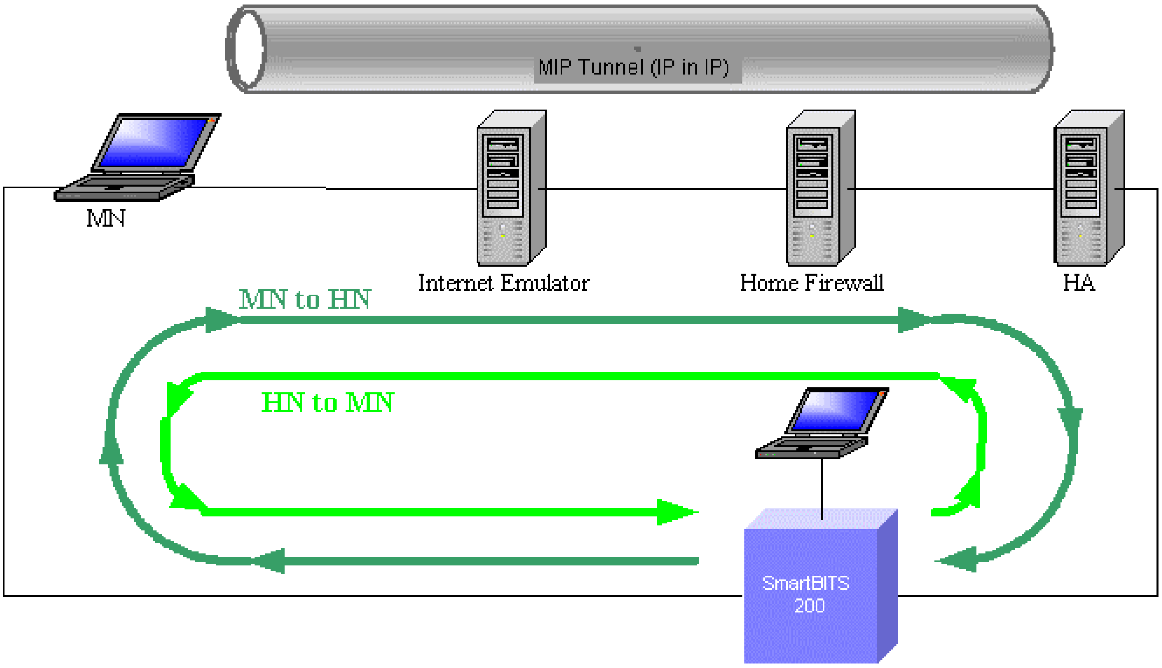
(Figure 33 – frame loss rate and latency in the test network HN⇒MN (64Bytes packets))



(Figure 34 – frame loss rate and latency in the test network MN⇒HN (64Bytes packets))

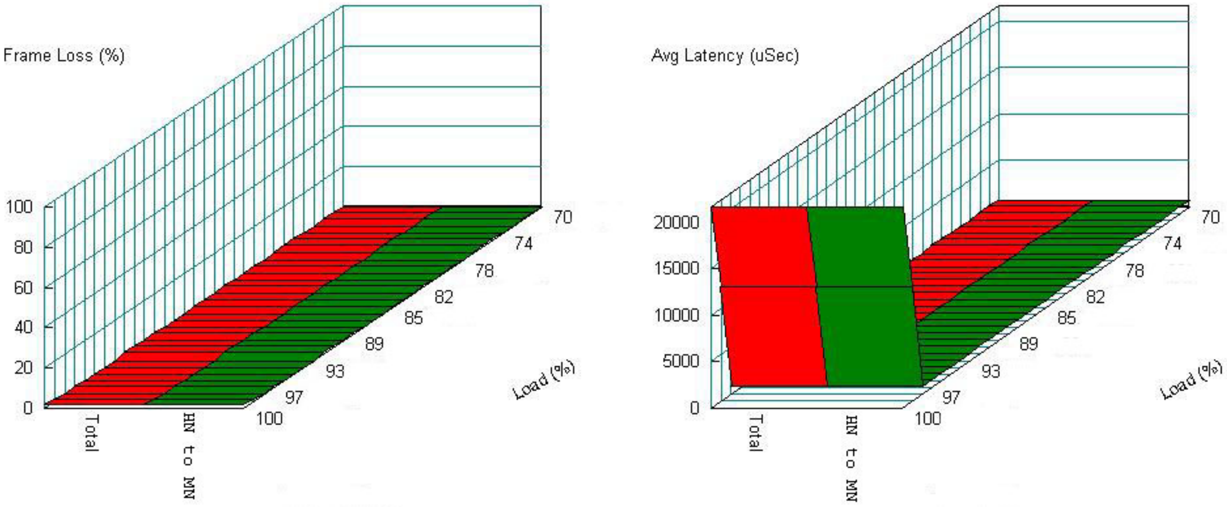
7.2.2 Test scenario two – Mobile IP tunneling

The second test scenario was set up to estimate the performance impact due to the Mobile IP tunnel established between the mobile nodes collocated CoA and the home agent. The network infrastructure is the same as by the first scenario. Only Dynamics Mobile IP agents were started on the mobile node and the home agent. As before, the MN is attached on a foreign network and communicating with the acquired collocated CoA. This leased IP address is used as the Mobile IP tunnel endpoint.

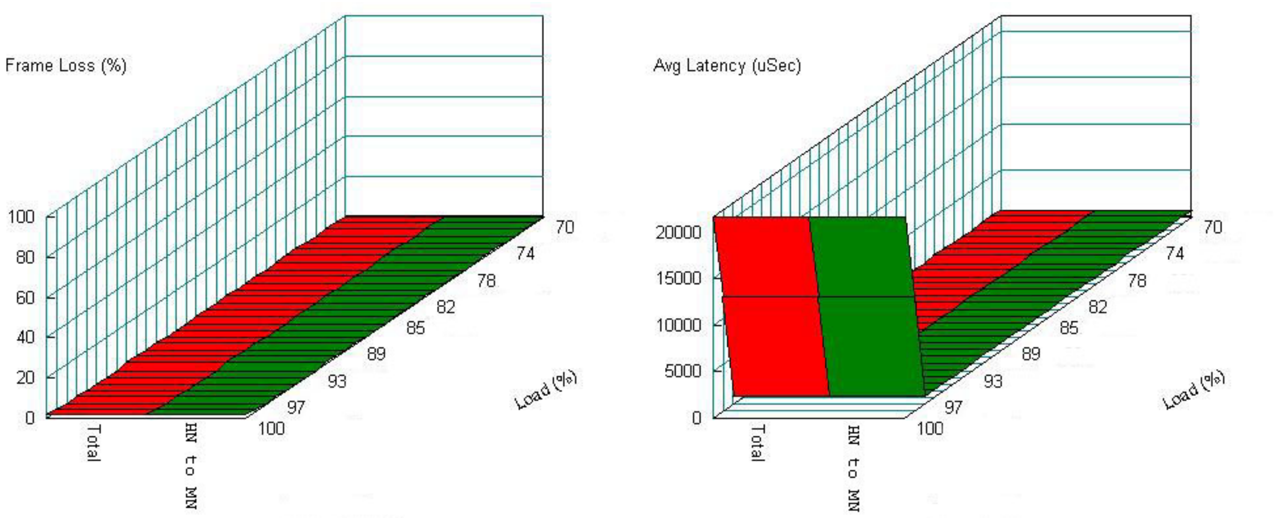


(Figure 35 – test network for Mobile IP tunnel (IP in IP))

The next few diagrams show the estimated frame loss rate and latency of the sent packets. Like before, two flows for each direction have been generated, one with small and one with big packet sizes.

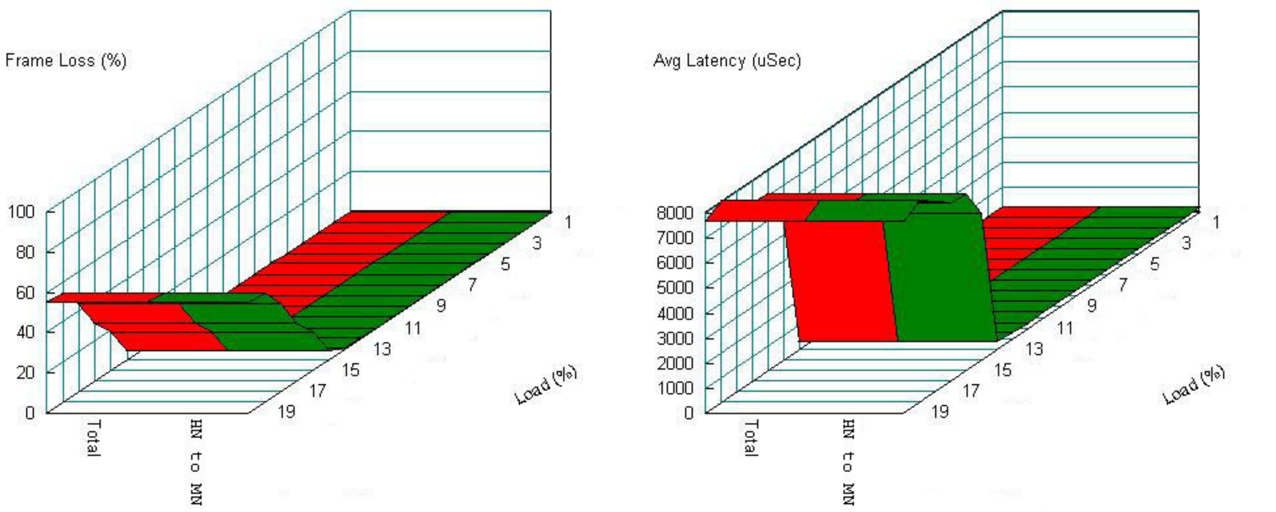


(Figure 36 – frame loss rate and latency with Mobile IP MN⇒HN (1.4kBytes packets))

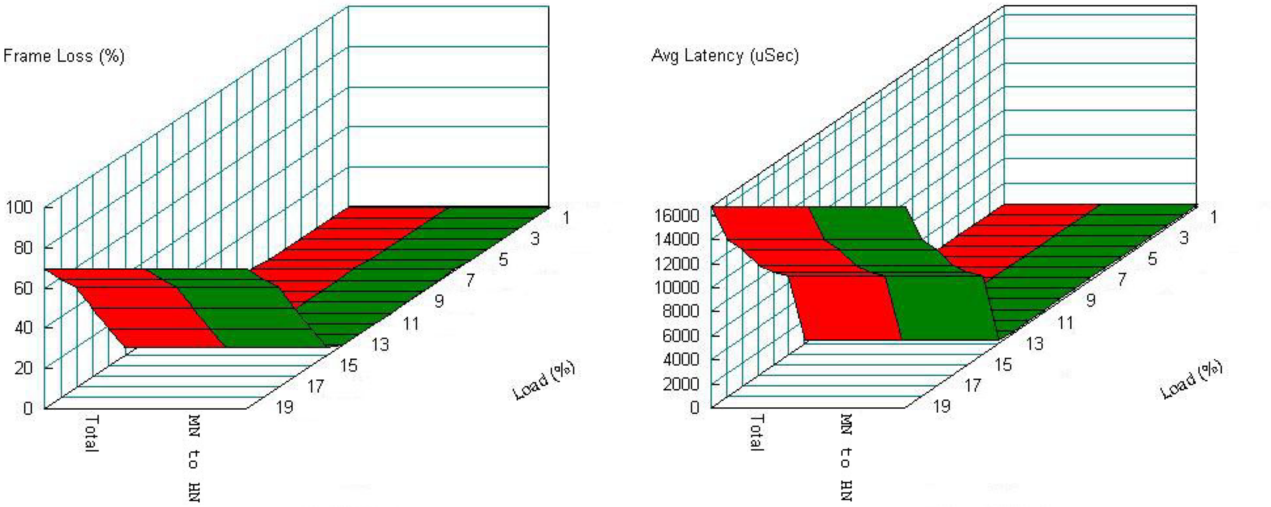


(Figure 37 – frame loss rate and latency with Mobile IP HN⇒MN (1.4kBytes packets))

There is nearly no performance impact due to the IP in IP tunnel. The IP in IP encapsulation and decapsulation is the only added processing. Again, when the packet size is being reduced, this processing take more time and reduces dramatically the maximum transfer rate.



(Figure 38 – frame loss rate and latency with Mobile IP HN⇒MN (64Bytes packets))

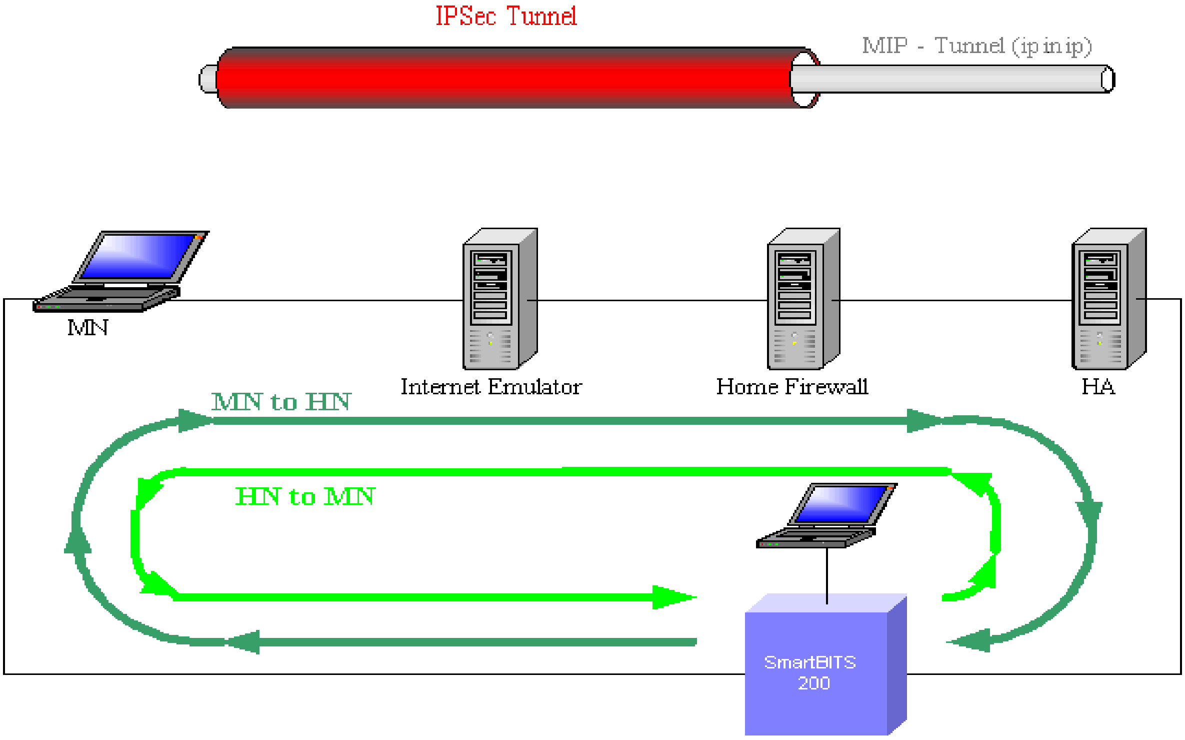


(Figure 39 – frame loss rate and latency with Mobile IP MN⇒HN (64Bytes packets))

7.2.3 Test scenario three - SecMIP

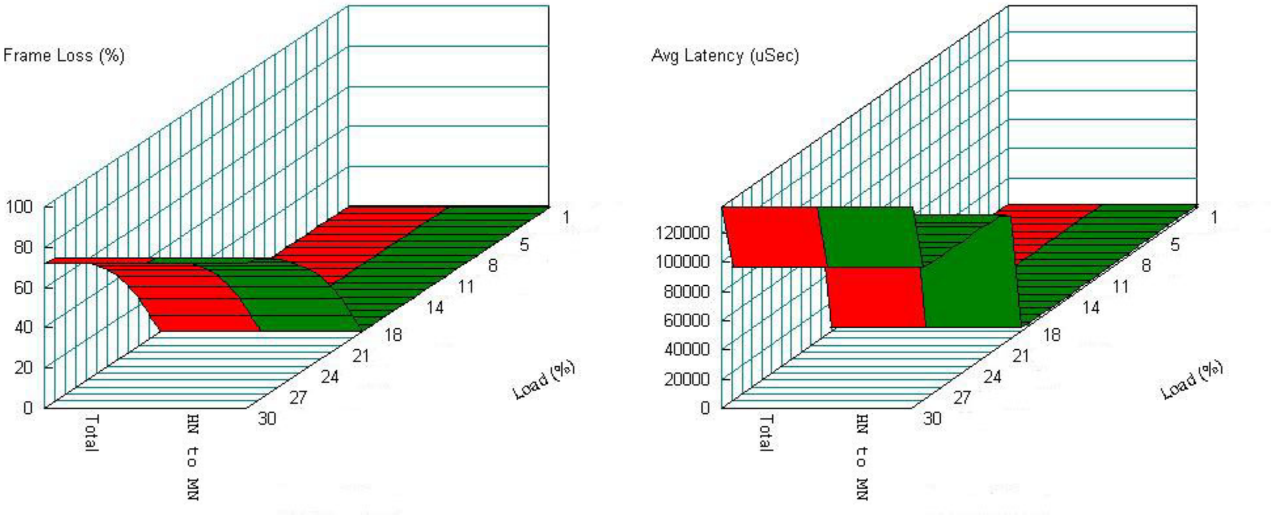
In the next scenario SecMIP was enabled. Compared with the precedent set up there is the additional IPSec tunnel between the mobile node and the home firewall. So both machines have to encode and decode the Mobile IP tunnel packets and tunnel them in new IP packets. The performance tests have been done after the IKE tunnel establishment. The session key life time was set to infinity so no IKE messages were exchanged during the test phase.

The next figure shows the network configuration for the last performance test with SecMIP running on the mobile node, the home firewall and the home agent.

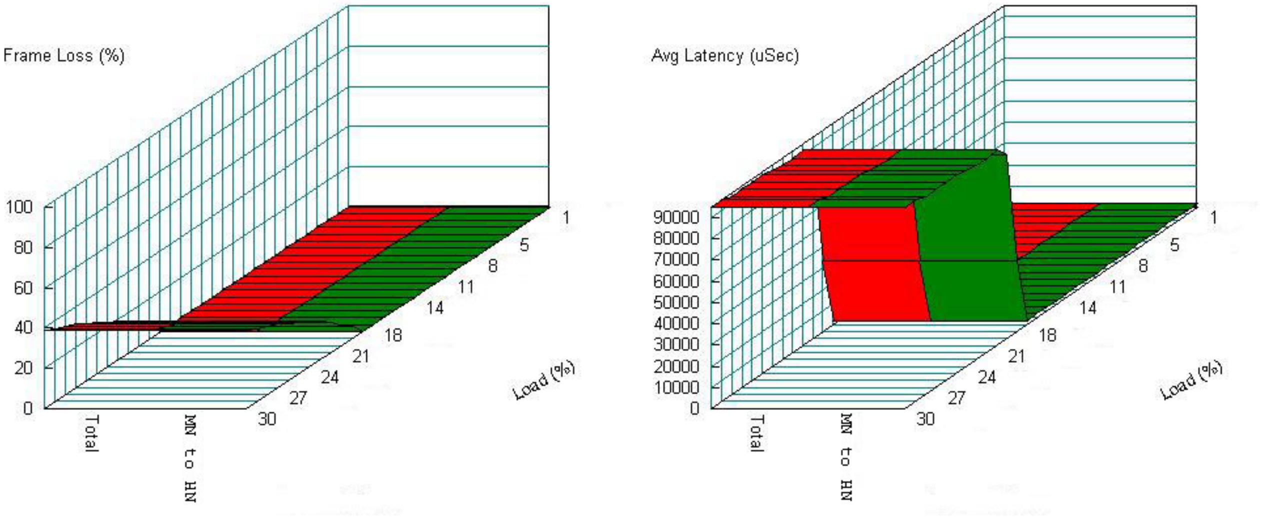


(Figure 39 – test network for SecMIP)

The first traffic stream with the big packets begins to break up when using a transfer rate bigger than 18 Mbit/sec. This will probably be the usual deployment of SecMIP for data transfer, where big TCP/IP packets are used.

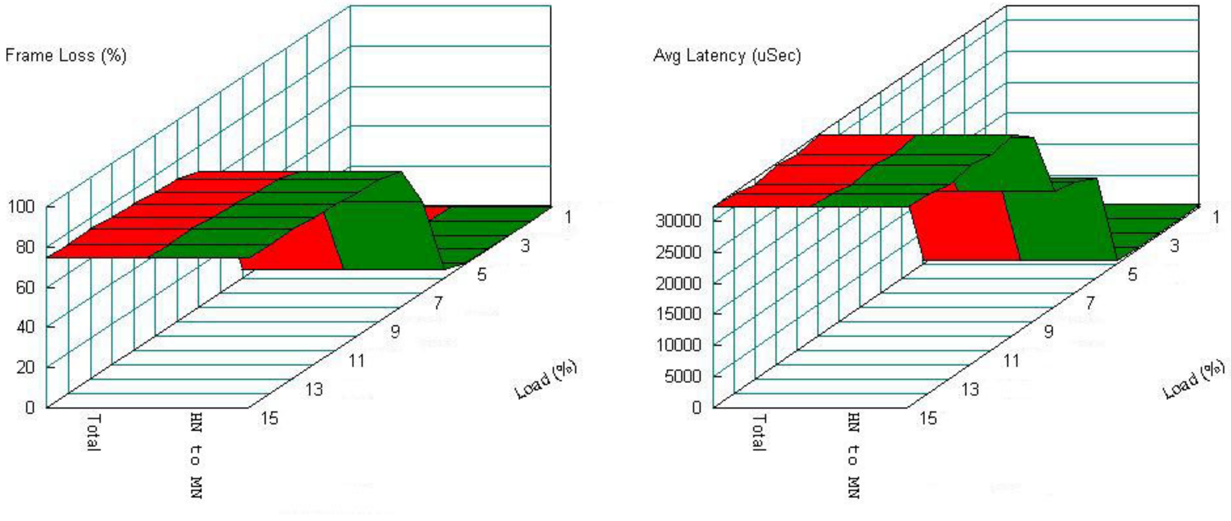


(Figure 40 – frame loss rate and latency with SecMIP HN⇒MN (1.4kBytes packets))



(Figure 41 – frame loss rate and latency with SecMIP MN⇒HN (1.4kBytes packets))

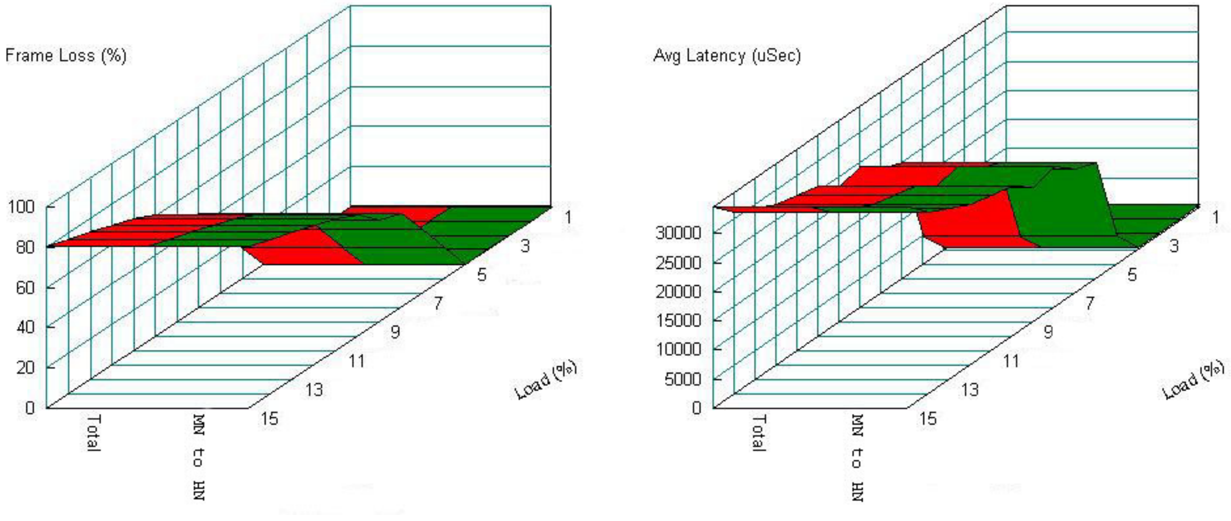
For small packets, the performance is worse, because the IPSec overhead for the stream is much bigger (IPSec has to make a SA lookup for every packet). Since a lot of streaming applications use small UDP/IP packets, the SecMIP scenario has to be tested with such small data packets.



(Figure 42 – frame loss rate and latency with Mobile IP HN⇒MN (64Bytes packets))

Without optimization of the FreeS/WAN IPSec module the maximum usable bandwidth using small packets is about 4 Mbit/sec due to encryption and authentication. If the traffic exceeds this value the IPSec module is not fast enough and begins to drop packets.

For the traffic flow passing the other way round (from the MN to the HN), the performance is approximately the same.



(Figure 43 – frame loss rate and latency with SecMIP MN⇒HN (64Bytes packets))

7.3 Performance conclusion

All these tests have been made to see which processes have which impact on the performance. Having a closer look at the results leads to the conclusion that security has its price. The deployment of IPSec realized as a software module has to be paid with up to 80% of performance impact. At the home network side a hardware IPSec device would be a solution to minimize this delays due to encryption.

The handover from one foreign network to an other takes about 7 seconds. That means that all connections are interrupted for this handover. The most of this delay comes from the FreeS/Wan IPSec module since the generated IPSec device has to be destroyed and rebuild after receiving a new IP address. This restart of the IPSec module takes about 4 seconds on the test PCs. The TCP congestion avoidance reacts to this interruption and takes about 20 seconds to increase the transfer rate to its original value. There is work in progress to adapt TCP to better cope with wireless environments were packets often get lost without any congestion on the medium.

Using a more dynamic IPSec module could decrease this handover delay up to 3 seconds, since the system just would have to wait for the DHCP procedure to configure the network interface to work in the new network environment. This needs a fast network neighborhood detection. In SecMIP this neighborhood detection is done with the help of the broadcasted agent advertisements. So the time in-between the broadcasted advertisements influences the handover delay.

To reach a seamless handover the mobile node has to be in the range of more than one access point. If the mobile node has several access points at the same time, multiple tunneling between the MN and its HA through different foreign networks could enable seamless handover. This way data packets could be sent through more than one tunnel and so increase the probability that they reach their destination node.

Looking at the available bandwidth of today’s mobile networks as Wireless LAN, GPRS or even Bluetooth, the estimated performance of SecMIP is acceptable for the moment. Of course optimizations have to be considered to keep up with new technologies.

8 Summary and Outlook

This study of security aspect in Mobile IP and development of a prototype for a secured Mobile IP enabled a lot of visions on future services for mobile units. The integration of different network devices seems to be the next step toward full connectivity. This SecMIP prototype was tested with Wireless LAN, Ethernet and HSCSD devices and worked fine. Tests with GPRS and Bluetooth are already planned. Further work is also being planned to minimize the handover delays. The Mobile IP topic becomes hot nowadays, every body wants to have full connectivity all the time. Most of the operators networks become IP networks. The need for the Mobile IP is undisputed.

The development on this sector is amazing. Research institutes and even manufacturers present nearly every week new results on how to communicate faster and new product that have more and more features included. The market for mobile devices and mobile services seems already to be endless and growing faster and faster.

The development of SecMIP is going on. In combination with a middleware that manages the different communication devices (GPRS, Wireless LAN, etc.) a mobile node will be able to maintain all connections without any interruption and without any user intervention. The mobile node will always choose automatically the best network device to connect to the home network (*see Portable Office, Swisscom project BROWSER*). When airports and hotels will offer wireless access points mobile nodes will connect to the Internet and VPNs with much higher bandwidth than mobile networks as GPRS or UMTS will ever offer. With upcoming ad-hoc network technologies, the visiting mobile nodes will be able to use locale infrastructure as printers, beamers and so on. – But there is still a lot of work till this visions will be reality.

9 Acknowledgments

To work on this subject was very interesting and to see that this work is going to be used by future projects justifies the effort.

I would like to thank Swisscom AG for the great support that I had during my work and for the provided network equipment. Special thanks also to Prof. Dr. T. Braun for the care during my Diploma work at the University of Bern (IAM), and to Florent Blot for his patient cooperation. Further thanks to Jan Linder, Stephan Robert, Pierre Jung, Alexander Dobreff, Erich Zahnd and Beat Perny for their great support and motivation during my work in Swisscom.

10 References

RFCs (On ftp://ftp.ietf.org/rfc/)

[1] *C. Perkins "IP Mobility Support", October 1996, rfc2002.txt.*
[2] *C. Perkins "IP Encapsulation within IP", October 1996, rfc2003.txt*
[3] *C. Perkins "Minimal Encapsulation within IP", October 1996, rfc2004.txt*
[4] *S. Hanks "Generic Routing Encapsulation (GRE)", October 1994, rfc1701.txt*
[5] J. *Solomon "Applicability statement for IP Mobility support", October 1996, rfc2005.txt*
[6] *D. Kong, "The Definitions of Managed Objects for IP Mobility Support using SMIv2", October 1996, rfc2006.txt*
[7] *D. Harkins, D. Carrel "The Internet Key Exchange (IKE)", rfc2409.txt*
[8] *D. Maughan, M. Schneider, M. Schertler, J. Turner „Internet Security Association and Key Management Protocol (ISAKMP)", November 1998, rfc2408.txt*

Internet Drafts

[9] *John K. Zao, Matt Condell "Use of IPSec in Mobile IP", November 1997*
[10] *Jim Binkley, John Richardson "Security considerations for Mobility and Firewalls, November 1998*
[11] *Charles Perkins, David B. Johnson "Mobility Support in IPv6", November 2000*
[12] *V. Gupta, G. Montenegro, Secure and mobile Networking, Mobile Networks and Applications 3 (381-390), Baltzer Science Publisher BV, 1998*
[13] *J. Zao, M. Condell, "Use of IPSec in Mobile IP", ftp://ftp.ietf.org/internet-drafts/draft-ietf-mobileip-ipsec-use-00.txt, November 1997*
[14] *S. Kelly, S. Ramamoorthi, "Requirements for IPSec Remote Access Scenarios", ftp://ftp.ietf.org/internet-drafts/draft-ietf-ipsra-reqmts-01.txt, November 1997*

Other documents

[15] *Dynamics Mobile IP documentation, http//www.cs.hut.fi*
[16] *Linux FreeS/Wan documentation, http://www.freeswan.org*
[17] *Alcatel Technical paper, "Understanding the IPSec Protocol Suite", March 2000*
[18] *C. Perkins "Mobile Networking Through Mobile IP, Tutorial", http://www.computer.org/internet/v2n1/perkins.htm*
[19] *James R. Binkley, John McHugh, Portland State University "Secure Mobile Networking Final Report", June 1999*
[20] *Mika Loukola, Helsinki University of Technologie "Internet Protocol Version 6 (IPv6)", 1997, http://www.tml.hut.fi/Opinot/Tik-110.501/1997/ipv6.html*
[21] *A. Aziz and M. Patterson, Design and Implementation of SKIP, available on-line at http://skip.incog.com/inet-95.ps.*
[22] *J. Linder, "Bericht für Dienstzwecke", Magic24 project, Swisscom-CIT-CT-ATS, May 2000*