Secure Mobile IP Communication

Torsten Braun and Marc Danzeisen
Institute of Computer Science and Applied Mathematics, University of Bern
Neubrückstrasse 10, CH-3012 Bern, Switzerland
Email: [braun|danzeis]@iam.unibe.ch

Abstract

This paper describes a solution called Secure Mobile IP (SecMIP) to provide mobile IP users secure access to their company's firewall protected virtual private network. The solution requires neither introducing new protocols nor to insert or modify network components. It only requires a slight adaptation of the end system communication software in order to adapt Mobile IP and IP Security protocol implementations to each other. The paper describes the concept, prototype implementation, and initial performance measurement results.

1. Introduction

The Internet Protocol (IP) will be the dominant protocol for any future communication. In the mobile world, however, Mobile IP is not very frequently used yet, but with the increasing popularity of wireless LANs this will probably change.

Since business people are the driving market force for mobile communication services, security becomes extremely important in those wireless LAN / Mobile IP scenarios. Attackers can spoof packets transmitted over wireless links and mobile users must be authenticated safely when roaming from one wireless access point to another. A natural way to provide security to Mobile IP users is to use the IP Security protocol suite. A particular problem when using Mobile IP is the firewall traversal problem. In this case, a campus network or a virtual private network (VPN) of an organization such as a university or a company is protected by a firewall from the global Internet. Only authorized users shall get access to that private network.

This paper reviews proposed solutions developed by other researchers in Section 2 and presents our SecMIP architecture in Section 3. Section 4 describes the SecMIP implementation and Section 5 discusses performance measurements. Finally, Section 6 concludes the paper.

2. Related Work

Zao and Condell discuss the use of IPSec over Mobile IP for HA-MN, HA-FA, CN-HA, CN-FA, and MN-CN connections (HA: home agent, FA: foreign agent, CN: correspondent node, MN: mobile node) [2]. IPSec is used to replace IP-IP-tunneling. Adaptations to Mobile IP messages are proposed for coping with IPSec tunnel establishment. Special IPSec tunnel extensions are added to advertisements and registration messages.

Binkley and Richardson [3] describe how a secure firewall protected area may tolerate Mobile IP or mobile systems using DHCP only and remain secure. They propose to use bi-directional IPSec tunnels between the home agent as a classic bastion host and the mobile node [8]. A secure mobile networking concept has been proposed that is based on ad-hoc networking and secure bi-directional IPSec tunnels. The standard Mobile IP scenario is treated as a special ad-hoc routing case where home agent and mobile node build a secure ad-hoc network. Considering the IP mobility problem as a special case of the general ad-hoc networking problem is a nice idea, but may be too complex for the goal to secure a Mobile IP environment only.

Gupta and Montenegro describe enhancements enabling Mobile IP operation in a network, which is protected by a combination of source-filtering routers, sophisticated firewalls, and private address space [5]. These enhancements should allow a mobile user in the public Internet to maintain a secure virtual presence within his firewall-protected office network. The authors propose to use SKIP [9] for key management, authentication and encryption. The reason why they chose SKIP instead of ISAKMP/Oakley [1], is SKIP's ability to look up the sender's public key based on alternate names, while this is done with source addresses in the case of ISAKMP/Oakley. The concept of a secured Mobile IP seems to be an easy and efficient way to solve Mobile IP security problems, but it requires introducing new protocols.

Pählke et al. propose the deployment of special gateways that include any security (e.g., firewall) and foreign agent functionality in the same node [10]. IPSec tunnels are established among those nodes in order to achieve security. The approach allows leaving mobile nodes unchanged but requires the presence of those nodes in any visited network. In addition, securing a wireless link requires link-level mechanisms leading to possibly duplication of encryption.

3. Secured Mobile IP (SecMIP)

3.1 SecMIP Scenario

Similar as proposed in [5] we have chosen a so-called screened-subnet firewall architecture, where the organization's interior network is isolated from the Internet by a de-militarized zone (DMZ). The firewall between the DMZ and the private interior network is the only entry point to the organization's private network (Figure 1). This simplifies the security management significantly, because all traffic must pass this firewall. In addition, private addresses are used for the private network hiding the topology of the private network when packets are tunneled (e.g., with IPSec in tunnel mode) through a public network. To ensure privacy of such virtual private networks (VPNs), encryption mechanisms are usually deployed.

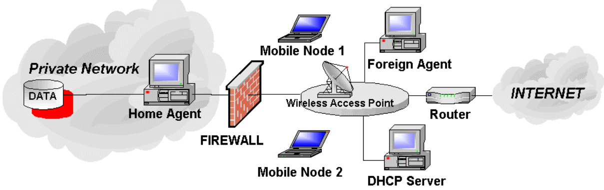


Figure 1 : SecMIP Scenario

The main requirement driving our deployment of Mobile IP is that a private 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 home agents) outside the private network, i.e. placing them within the DMZ. This placement of foreign agents allows non-restricted Internet access by guest mobile nodes, because 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, e.g. with an end system firewall software on the mobile node.

We assume that mobile nodes receive their IP addresses from DHCP servers. All mobile nodes are always outside the firewall, i.e. in the DMZ, even those owned by the corporation. This means that while being connected to a wireless LAN, mobile nodes are never located in the home agent's subnet and never register at home. Mobile nodes that become attached to the physically secured wired private network stop Mobile IP tunneling.

Despite of speed limitations resulting from authentication and encryption data being sent from the organization's own DMZ to the firewall, the security benefits justify this concept. It is even possible to reduce the traffic on the interior private network, because home agent advertisements are not required any more. 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 to ensure that wireless attachment points are only used with a secure Mobile IP.

3.2 IPSec in SecMIP

Since the mobile nodes belonging to the corporation have to traverse the firewall to access the private network, they have to authenticate themselves to the firewall using 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 secret or public keys. The establishment of a secure IPSec tunnel between mobile node and firewall (Figure 2) allows using a lightweight Mobile IP implementation without security mechanisms, because all packets traversing the public network are encrypted and authenticated by IPSec.

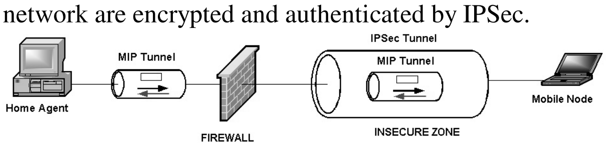


Figure 2 : SecMIP tunneling

Similar to the proposal by Gupta and Montenegro, 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. ISAKMP/Oakley has been chosen for SecMIP. ISAKMP/Oakley is similar to SKIP but has a few advantages:

- After having negotiated the security association, packets do not contain a key management header as in SKIP.
- An attacker does not know which algorithms are being used for encryption and authentication, unlike in SKIP.
- ISAKMP causes fewer overhead for exchanging security parameters. While many parameters are contained in every SKIP packet, in the case of ISAKMP those parameters are stored in security associations established prior to data exchange.

3.3 SecMIP Operation

This section describes the SecMIP operation in more detail. This is done step-by-step considering a mobile node changing its point of attachment.

Step 1: Network detection. After entering a new network area, a mobile node has to be connected via a wireless network access point (Figure 3). Foreign agent advertisements are broadcasted regularly into this demilitarized network. By receiving such an ICMP message, a mobile node learns that it just has entered a new network. The mobile node can also send an agent solicitation to trigger an agent advertisement. Then, the mobile node stops the old IPSec tunnel, which was established in another network using an old collocated care-of-address.

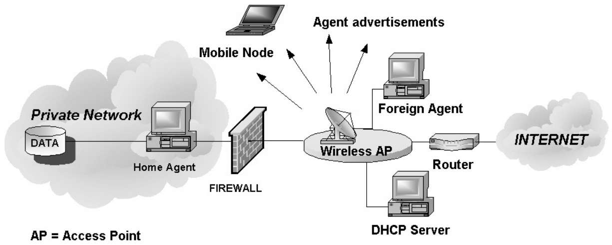


Figure 3 : SecMIP Network detection

Step2: Acquiring a routable IP address. The mobile node needs to acquire a collocated care-of-address from DHCP servers (Figure 4) or foreign agents. However, it is rather common nowadays to get care-of-addresses from DHCP servers, which are commonly deployed in wireless LAN environments. This also avoids the existence of foreign agents, which is the case in IPv6 anyhow.

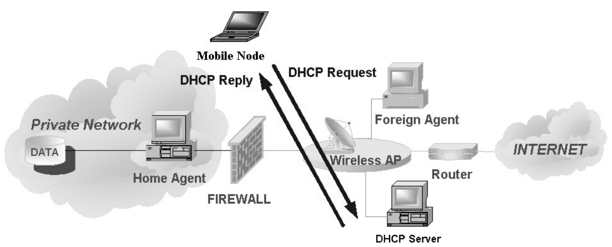


Figure 4 : SecMIP acquiring a collocated Care-of-Address

Step 3: Establishment of a bi-directional IPSec tunnel between mobile node and home firewall. As shown in Figure 5, data packets pass an insecure, public network between mobile node and home firewall. Therefore, a logical approach is to establish an IPSec tunnel between the mobile node's care-of-address and the home firewall before any Mobile IP messages are exchanged between the mobile node and its home network. The IPSec tunnel provides authentication, integrity, and privacy of each IP packet sent during the Mobile IP registration procedure. Figure 6 shows the packets exchanged in step 3 between the mobile node's collocated care-of address and the home firewall. The packets payload carry the information for main and quick mode of the Internet Key Exchange (IKE) protocol [13].

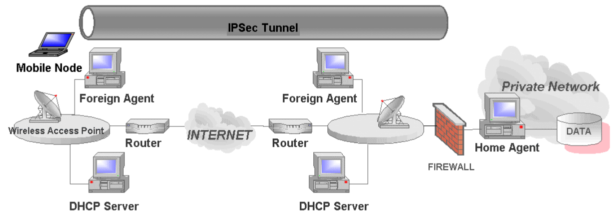


Figure 5 : IPSec Tunnel Mobile Node - Home Firewall

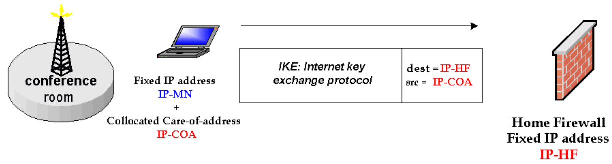


Figure 6 : IPSec packets

Step 4: Mobile IP Registration at Home Agent. In this step, the mobile node registers at the home agent. Since all Mobile IP negotiation between home agent and mobile node pass the IPSec tunnel to the home firewall, there is no need for another authentication / encryption of Mobile IP registration messages. We assume that the private network behind the firewall is secure. Figure 7 summarizes the message exchange during steps 1- 4.

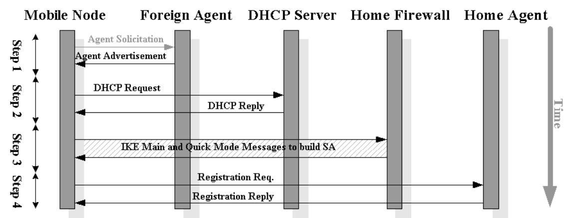


Figure 7 : Message Exchange

Step 5: Data transfer. Until the next movement, the mobile node can communicate with any other correspondent node independent whether this is inside or outside the private network. Any data transfer between the mobile node and any other correspondent node is relayed via the home agent for security reasons. It is also possible to communicate directly to correspondent nodes outside of the private network directly using the care-of-address, if that connection does not need to be secured. It can be configured easily by modifying the mobile node's routing table, whether packets have to be relayed via the home agent or not. Figure 8 shows Mobile IP packets sent from a mobile node to a correspondent node. The encrypted and authenticated Mobile IP packets are decrypted and decapsulated by the home firewall and delivered to the home agent. The home agent finally decapsulates these Mobile IP packets and delivers them to the appropriate receivers, the correspondent nodes.

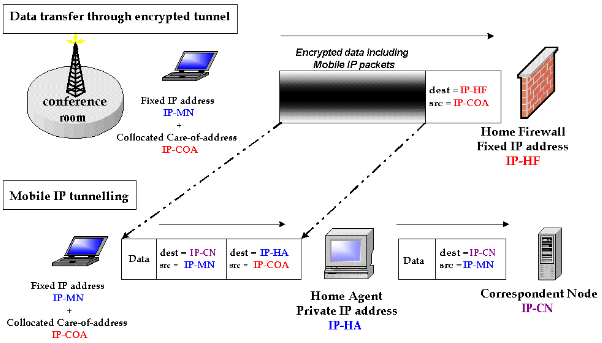


Figure 8 : SecMIP packets

4. SecMIP Implementation

4.1 Dynamics Mobile IP and FreeS/Wan IPSec

SecMIP has been implemented on Linux-based end systems and routers. It uses two tunnels: one for supporting mobility and the other one for IPSec.

Dynamics Mobile IP [6] developed by the Helsinki University of Technology (HUT) has been selected for Mobile IP. The implementation consists of three executable programs: one for each Mobile IP component, i.e. home agent, foreign agent and mobile node. The source code is available in C and all features are RFC compliant. The configuration of the components is rather simple. There is one configuration file for each of them. In the SecMIP implementation, Dynamics Mobile IP handles agent advertisements (home and foreign), establishes Mobile IP tunnels between home agent and mobile node, captures and redirects packets for the mobile node at the home network.

FreeS/Wan [7] (Free Secure WAN) works with RSA and for each IPSec node a RSA key pair has to be created. The allowed connections have to be described in a configuration file. FreeS/WAN negotiates keys between mobile node and home firewall, establishes secured tunnels between mobile node and home firewall, and encrypts / authenticates all data between mobile node and home firewall.

Dynamics Mobile IP and FreeS/Wan have been chosen because of their source code availability, but these implementations are not intended to be merged. Therefore, we had to perform many adaptations, before they worked successfully together in SecMIP. Dynamics Mobile IP is too heavy and a lightweight Mobile IP implementation without strong security support would have been sufficient for our purposes. Also the design of FreeS/Wan is not flexible enough, because all IPSec devices are just initiated once by starting up the IPSec daemon. These two disadvantages had limiting effects on the delay minimization during a handover, because FreeS/Wan must be restarted after each location update.

4.2 Script Implementation

The main part of the implementation work was to achieve interoperability between Dynamics Mobile IP, FreeS/Wan, and the operating system. For that reason, the following scripts have been developed.

Disconnect executes a Dynamics Mobile IP API call that sends a deregistration message to the home agent and disconnects the mobile node from the home agent.

Connect executes a Dynamics Mobile IP API call that sends a registration message to the home agent and establishes a direct tunnel between mobile node and home agent.

DhcpSecure sends a DHCP request and updates the network interface configuration and the routing table. Then, an IPSec connection to the home firewall is built.

UpdateLocation1 (on a foreign network) and **UpdateLocation2** (on the home network): By the API call 'update interface' the process *dynamics_admin* can be forced to read the actual IP configuration of the interface. If this configuration is identical with the home configuration, the mobile node is at home and sends a deregistration message to the home agent (UpdateLocation2). Otherwise, a new registration procedure is invoked (UpdateLocation1).

UpdateRoute1 updates the routing table of the mobile node when it is connected to a foreign network and when the Mobile IP tunnel between mobile node and home agent is established. When the mobile node arrives at home, the IPSec and Mobile IP tunnels have to be disabled and the routing table must be updated again (**UpdateRoute2**).

Firewall.rc: To control incoming and outgoing network traffic of the mobile node, an IP-Filter is initialized using *ipchains*. 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 mobile node is only allowed to communicate to nodes of the private network through a secured IPSec device. This guarantees data privacy.

The scripts are running on the mobile node to ensure that Mobile IP uses always a secured network interface to communicate with the home network. Once Dynamics Mobile IP and FreeS/Wan's IPSec have been started, the scripts are executed as shown in Figure 9. All script calls were placed in the Dynamics Mobile IP source code. Since no changes were necessary within the FreeS/WAN source code, we can also use alternative IPSec implementations. The use of any other home agent and IPSec gateway is possible in the home network, because only the code of the mobile node needed to be modified. For more implementation details see [11].

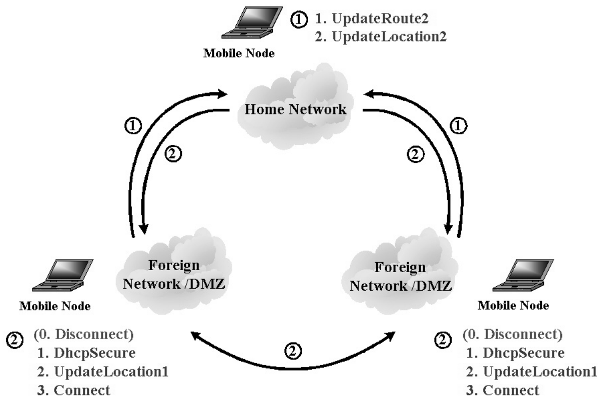


Figure 9 : SecMIP Scripts

5. Performance Evaluation

The performance of the SecMIP implementation has been evaluated in order to prove the effectiveness of the proposed approach for Mobile IP communication protection. The tests have been performed with the help of a SMARTBITS 200 network test box, which has up to four Ethernet interfaces on which traffic can be generated and statistics can be evaluated. All Ethernet devices of the test infrastructure support 100 Mbps in full duplex mode. The traffic generator generated unidirectional flows of IP packets up to 100 Mbps. Figure 10 shows the network scenario used for the various tests. No tunnel has been established for test scenario 1, the Mobile IP tunnel has been used for scenarios 2 and 3, while the IPSec tunnel has been established for scenario 3 only.

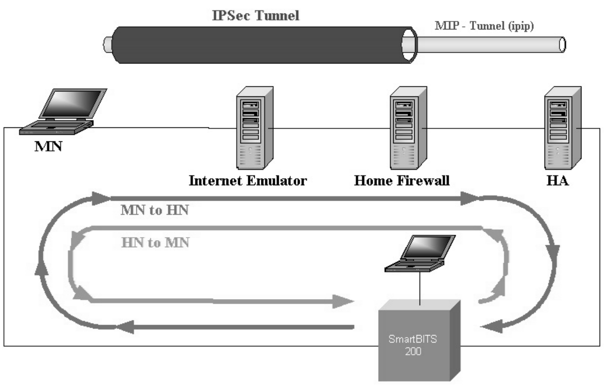


Figure 10: Test Network Configuration

Two different frame sizes have been tested: 64 bytes and 1400 bytes. The smaller packets were transporting UDP/IP as frequently used in streaming applications or Voice over IP, and the bigger ones have been used for TCP/IP data simulating bulk data transfer. In the different test scenarios, these IP packets were then transported in different manners. In the first scenario, the intermediate routers have just routed them. In the second scenario, the packets were encapsulated by the Mobile IP tunnel (IP in IP), which extends the frame sizes by an additional IP header (20 bytes). In the third scenario additional IPSec information is carried.

5.1 Test 1: Performance without SecMIP

In the first scenario the performance without any tunneling or additional processing due to Mobile IP or IPSec has been measured (Figure 11). The only processing by intermediate routers is packet forwarding. This allows evaluating the performance of the test infrastructure. The diagrams show the latency and the frame loss dependent on the traffic from the mobile node to the home network. Measurements for the opposite direction have been very similar. It is not surprising that the performance depends strongly on the generated traffic's packet size. The impact on routing performance is much stronger for smaller packets (Figure 12).

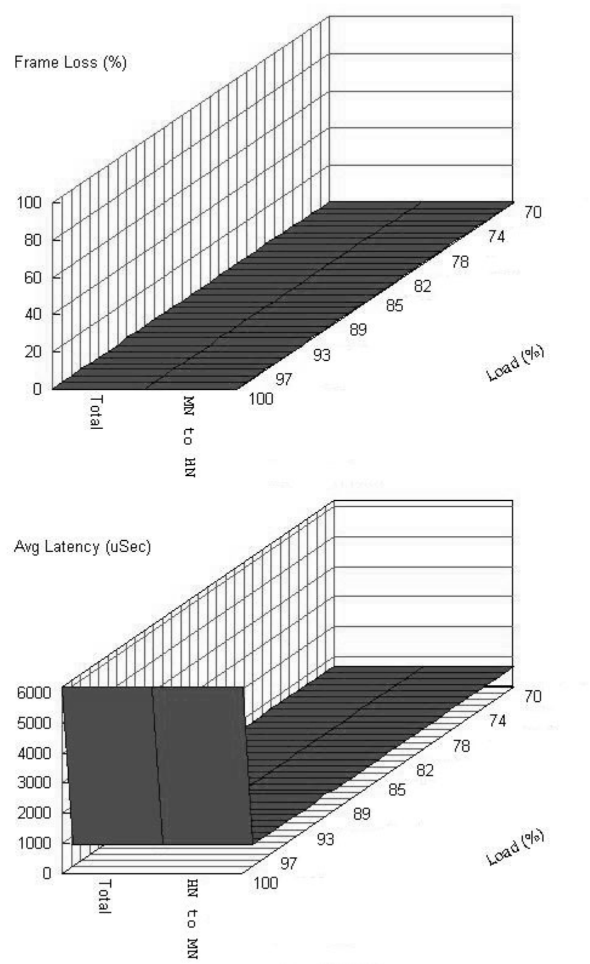


Figure 11: Performance for 1.4 kB packets

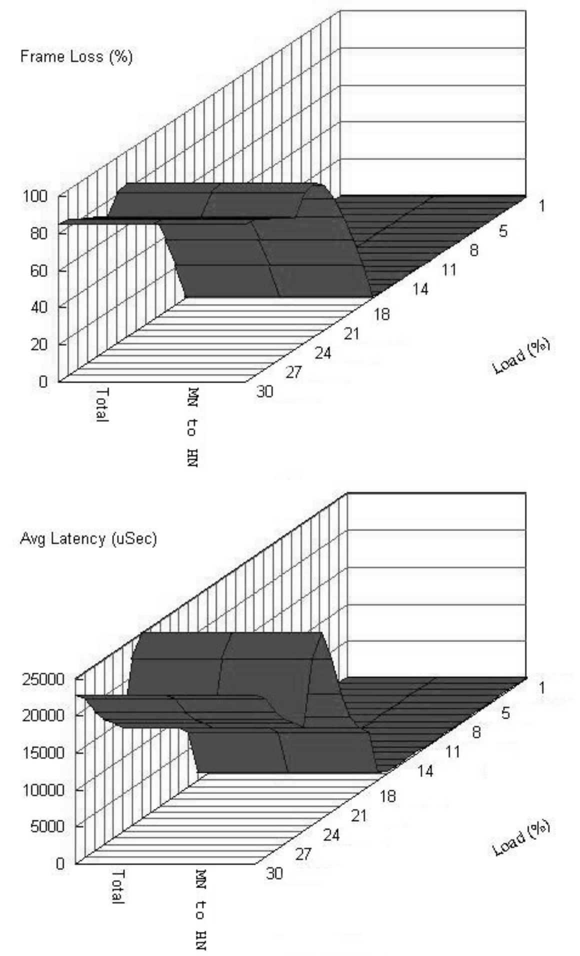


Figure 12: Performance for 64 byte packets

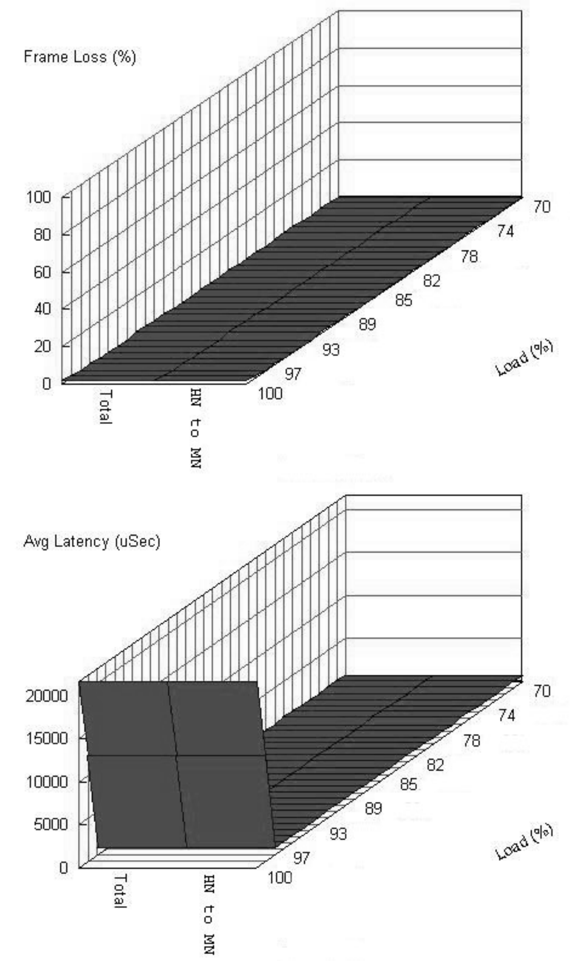


Figure 13: Mobile IP performance with 1.4 kB packets

5.2 Test 2: Mobile IP Tunneling

The second test scenario was established to estimate the performance impact of the Mobile IP tunnel between the mobile nodes collocated care-of-address and the home agent. Dynamics Mobile IP agents were started on the mobile node and the home agent. The mobile node is again attached on a foreign network and it uses the acquired collocated care-of-address as the Mobile IP tunnel endpoint. IP-in-IP encapsulation and decapsulation is the only additional processing. There is nearly no performance impact due to the IP-in-IP tunnel (Figure 13). Again, the maximum data rate is dramatically lower for small packet sizes (Figure 14).

5.3 Test 3: Secure Mobile IP

Compared with the previous scenario there is an additional IPSec tunnel between the mobile node and the home firewall in order to enable SecMIP. Home firewall and mobile node have to encode and decode the Mobile IP tunnel packets and tunnel them. The performance has been measured after IKE tunnel establishment. The session key lifetime was set to infinity to avoid IKE message exchange during data transfer. The traffic stream with large packets begins to break down for transfer rates over 18 Mbps (Figure 15). For small 64 byte packets, the performance is worse, because the IPSec overhead for the stream is much bigger (Figure 16). IPSec has to perform a security association lookup for every packet. The FreeS/WAN IPSec limits the maximum usable bandwidth to approximately 4 Mbps due to encryption and authentication. If the traffic exceeds this value the IPSec module is not fast enough and begins to drop packets.

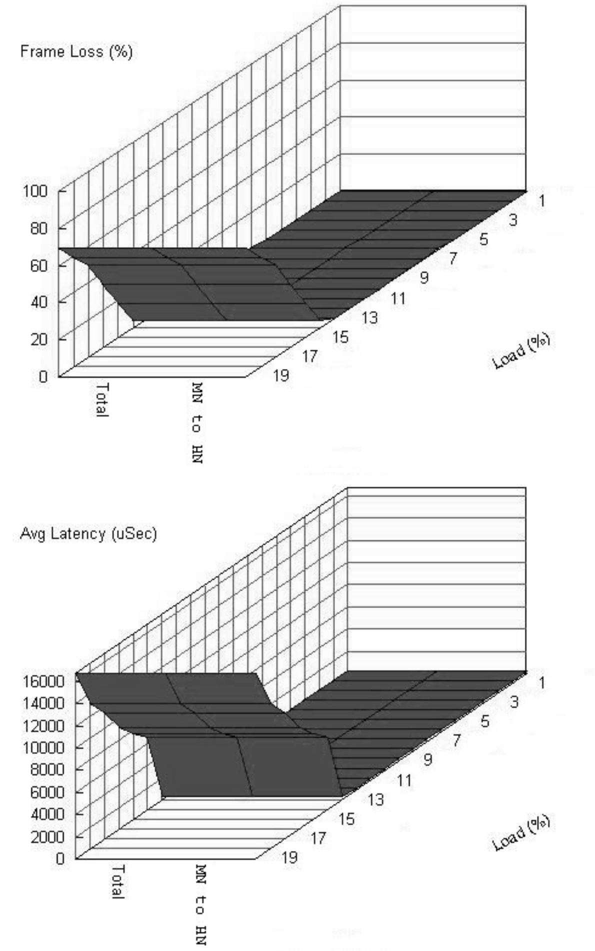


Figure 14: Mobile IP performance with 64 byte packets

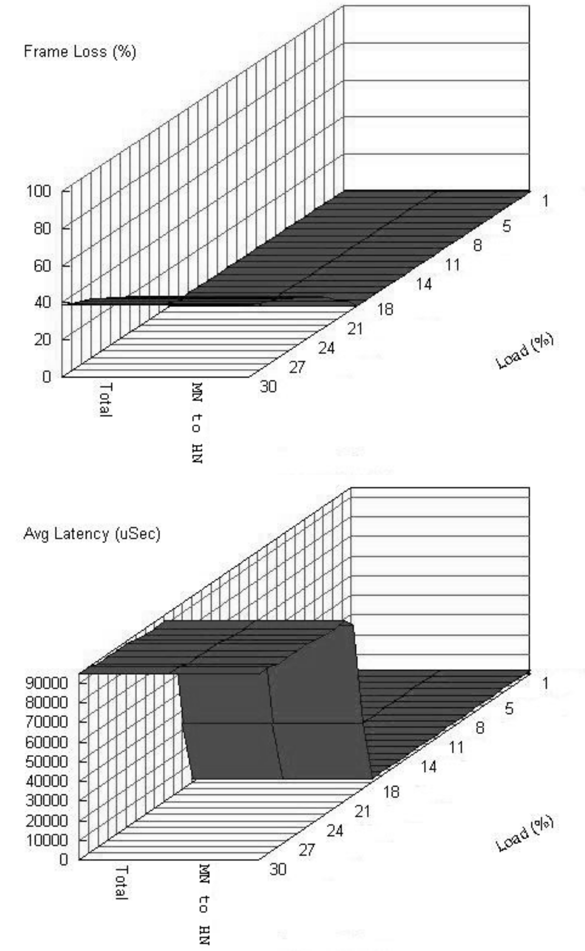
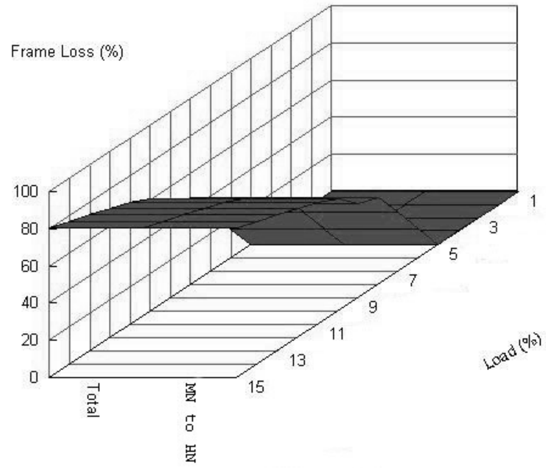


Figure 15: SecMIP performance with 1.4 kB packets

5.4 Performance Summary

The tests have been performed in order to investigate the performance impact of the various SecMIP processes. The IPSec implementation as software modules has to be paid by a performance impact of up to 80 %. A hardware IPSec device at the home network would be a solution to minimize performance degradation by encryption. The handover from one foreign network to another takes currently up to 7 seconds. Most of this delay comes from the FreeS/Wan IPSec module, because the generated IPSec device has to be shut down and restarted after learning a new IP address. This restart of the IPSec module takes about 4 seconds on the test PCs. Using a more dynamic IPSec module could decrease this handover delay to max. 3 seconds. That delay is caused by DHCP to configure the network interface to work in the new network environment.

Another performance improvement can be achieved by establishing two simultaneous IPSec tunnels and two Mobile IP registrations for an overlapping period of time during handovers in order to achieve seamless handovers without service disruption. Those performance optimizations are subject for future research. This is in particular important since the TCP congestion control algorithm reacts to this handover interrupt and takes about 20 seconds to increase the transfer rate to its original value. We, therefore, see a strong need to adapt TCP to better cope with wireless environments where packets often get lost without any network congestion but due to handovers.



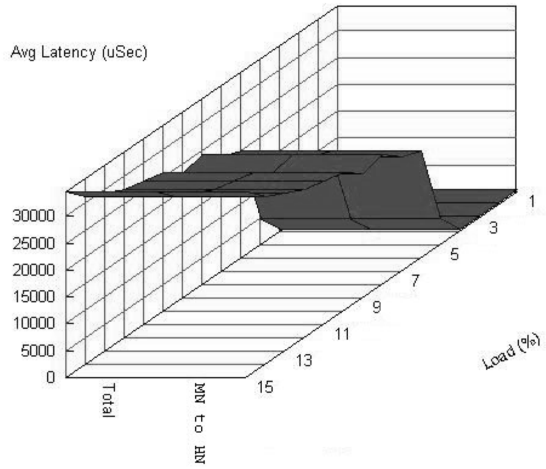


Figure 16: SecMIP performance with 64 byte packets

6. Conclusions

This presented an approach to allow Mobile IP users to access firewall protected VPNs. The solution is based on available standards and required minor modifications of the communication stack in end systems. The prototype implementation has been successfully tested with Wireless LAN, Ethernet and HSCSD network devices. Tests with GPRS and Bluetooth are in progress [12]. Further work is also required to minimize handover delays.

7. Acknowledgements

The Swiss National Science Foundation (SNSF) and Swisscom AG have funded the work presented in this paper. The work has been performed in the framework of the SNSF project no. 5003-057753 “Advanced Network and Agent Infrastructure for the Support of Federations of Workflow Trading Systems” (ANAISOFT). Swisscom AG, Bern, provided technical and infrastructure support for the implementation and evaluation of SecMIP.

8. References

[1] D. Maughan, M. Schneider, M. Schertler, J. Turner: Internet Security Association and Key Management Protocol (ISAKMP), November 1998, RFC 2408

[2] John K. Zao, Matt Condell: Use of IPSec in Mobile IP, Internet Draft, November 1997

[3] Jim Binkley, John Richardson: Security Considerations for Mobility and Firewalls, Internet Draft, November 1998

[4] Charles Perkins, David B. Johnson: Mobility Support in IPv6, Internet Draft, November 2000

[5] V. Gupta, G. Montenegro, Secure and mobile Networking, Mobile Networks and Applications 3 (381-390), Baltzer Science Publisher BV, 1998

[6] Dynamics Mobile IP documentation, http//www.cs.hut.fi

[7] Linux FreeS/Wan documentation, http://www.freeswan.org

[8] James R. Binkley, John McHugh, Portland State University: Secure Mobile Networking Final Report, June 1999

[9] A. Aziz and M. Patterson, Design and Implementation of SKIP, http://skip.incog.com/inet-95.ps.

[10] F. Pählke, G. Schäfer, J. Schiller: Paketfilter- und Tunnelkonfiguration zur Firewall-verträglichen Mobilitätsunterstützung in IP-Netzen, KiVS 2001, Hamburg, February 2001.

[11] M. Danzeisen: Secure Mobile IP Communication, Diploma Thesis, Institute of Computer Science and Applied Mathematics, University of Bern, May 2001.

[12] M. Danzeisen, T. Braun: Access of Mobile IP Users to Firewall Protected VPNs, Mobile Communication over Wireless LAN, Workshop at Informatik 2001, Vienna, September 26-29, 2001

[13] D. Harkins, D. Carrel: The Internet Key Exchange (IKE), RFC 2409, November 1998