Design and Implementation of a Secure Mobile IP Architecture

Kostas Siozios, Pavlos Efraimidis and Alexandros Karakos

Department of Electrical and Computer Engineering
Democritus University of Thrace
67100 Xanthi, Greece

Abstract. The increasing number of portable computers, combined with the requirement for non-stop connections to networks, makes the provision of Internet mobility important. Mobile IP defines protocols and procedures by which a mobile node can exchange packets, regardless of its current point-of-attachment to the Internet, and without changing its IP address. In this work we describe the design and the implementation of SMA (Secure Mobile IP Architecture), a new approach for Mobile IP services. SMA is a complete operational system that supports the functionality of main Mobile IP requirements and, at the same time, achieves significant results for several interesting aspects of transparent mobile connectivity. SMA is based on standard software components and can therefore be considered as platform-independent, since it can support the common operation systems. The architecture has been tested on heterogeneous networks built with nodes running Linux, Solaris and MS-Windows, using both wireless and non-wireless networking technology.

1 Introduction

In this work we describe the design and the implementation of SMA (Secure Mobile IP Architecture), a new approach for Mobile IP services. The primary objective of our implementation is the design of a system that admits the transparent move of nodes from a network to another. In other words, the way a Mobile Node (MN) that uses the network services must not be affected when it is moved to a new network location and this transparent connectivity has to be accomplished without the requirement for any manual changes to the network configuration. We also aim at some important practical goals, less visible to the user. The protocol should provide security, as well as it should not limit the number of active MNs. Furthermore, there will be no change in existing IP routers or non-MNs, although changes to the latter are supposed to increase the efficiency. The acronyms and terms used in this work are shown in Table 1.

2 Related Work

Recently, many universities and companies all over the world have implemented the Mobile IP protocol for educational and commercial purposes on a variety of operating systems, i.e. Linux, FreeBSD, Solaris, and Microsoft Windows.

Term	Explanation
MN	The Mobile Node
HN	The Home Network of the Mobile Node
HA	The corresponding Home Agent of the Home Network
HN_IP	The static IP address of the Mobile Node at the Home Network
FN	The Foreign Network that visits the Mobile Node
FA	The corresponding Foreign Agent of the Foreign Network
COA	The IP address of the Mobile Node at the Foreign Network
CN	The Correspond Node that exchanges packets with the Mobile Node
VND	Visitors Network Database
HND	Home Network Database
CSD	Central Server Database

Table 1. Terms used in this paper and their explanation.

The various implementations substantially differ in at least three areas. First of all in the way the Home Agent (HA) determines where the MN is attached. Also, in the way an ordinary host sends data directly to the MNs current point of attachment, avoiding the wasteful trip through the HA. And finally, in the way the two previous mechanisms interact when the MN is moving to a new network. Apart from these differences, all these implementations are very interesting and have useful features.

The implementation of the Mobile IP protocol designed at Helsinki University of Technology [12] is one of the most interesting implementations the authors are aware of. This implementation is a dynamical and hierarchical Mobile IPv4 software for Linux operation systems. Also the implementation from the Stanford University [13] allows the MN to dynamically choose the level of mobility, which is desired for the different traffic flows. The implementation of Lancaster University [14] is able to work without any problem with IPv4 and IPv6. Furthermore, it includes the appropriate software for demonstrating real-time Mobile applications with IPv6. The product of Sun Microsystems [15] is also very interesting, as it can work both in Solaris (running either on SPARC workstation or an Intel processors) and Linux systems. Last but not least, Ecutel [16] has designed a system that provides dynamic IP routing, dynamic registration, IP forwarding, IP encapsulation, encryption, authentication, firewall and access control.

3 How Classic Mobile IP Works

A classical IP router realizes connections among networks by forwarding packets from a source to a destination endpoint according to the routing table. Such a table usually maintains the next-hop information for each destination IP address. For this reason it is obvious that the need of developing new techniques for computer connectivity is crucial, especially the ability of a MN to connect to different networks without the need of making any manual changes to the network settings [1].

In order to maintain transparent-layer connections when the MN changes its physical location, it has to keep the same IP address (Home IP address). This address can be

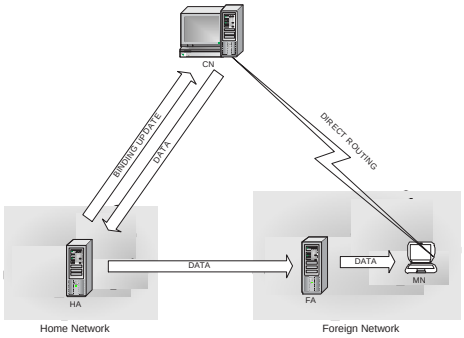

Fig. 1. How a MN communicates when it is away from its HN.

a private or a registered IP and makes the MN appear, as if it is constantly connected on its HN.

Every time the MN is attached to a FN, a new, additional IP address (COA) is assigned to it [2]. Usually the COA is a private IP address and changes whenever the MN moves to a new network, in order to save registered IPs. In such a case, the MN every time has two distinct IP addresses, a registered and a private one.

Figure 1 illustrates the basic architecture of the Mobile IP protocol. In this case, the HA and FA belong to different networks and they are responsible for providing mobility extensions to the MN. The MN is a Node that has a registered IP address at the HN, where the HA is also located, but now it is connected to Internet through the FA [3].

When the Correspond Node (CN) sends for the first time a packet to the MN, it does not know if the destination Node is stationary or not. Hence it uses simple IP routing to forward the packet to the MNs HN, where it is received by the HA. Then the HA in turn, checks the packet to find out if the Node with this destination IP address is currently attached to this network on not. If the destination Node is attached to the local network, the packet is delivered to it through classic IP routing. Otherwise, the HA uses IP in IP encapsulation [4, 5] in order to tunnel the packet at the network to which the MN is currently attached. There, the packet is received from the FA and after its decapsulation, is delivered to the MN. On the other hand, when the MN sends a packet, in most cases it uses normal IP routing to forward it directly to its destination. The indirect routing through the HA causes unnecessary overhead to the network resources.

3.1 Routing Optimization

To overcome the problem of indirect routing, networks that support the Mobile IP must be able to perform Routing Optimization [6]. With this technique, when the CN sends for the first time a packet addressed to the MN, the packet is delivered in the way that is described above. Then the HA sends a binding update message to the CN to

inform it about the MN's current IP address. Future packets will be forwarded directly to the network that the MN is connected, without first bypass the HA.

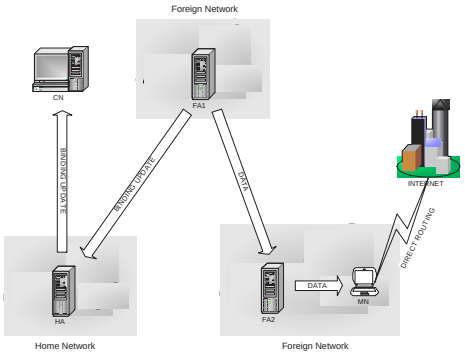

Fig. 2. What happens when the MN changes its point of attachment.

Figure 2 illustrates what happens when the MN moves from one Foreign Network (FN1) with corresponding agent FA1 to another Foreign Network (FN2) with corresponding agent FA2. In this case, in order to keep the connections alive, the FA1 has to forward the incoming packets from CN to FA2, where the MN is currently attached. At the same time the FA1 informs the HA about the MNs movement to the new network [7]. Next, the HA send a Binding Update message to the CN, that informs it about the change that happened, so that the last one will be able to send future packets addressed to the MN directly to its new point of attachment. After this transition state, the network returns to a stable state again.

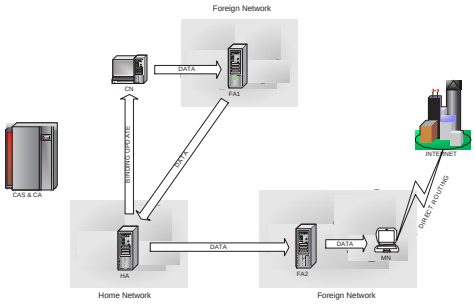

Fig. 3. What happens when FA1 is not able to directly communicate with FA2.

This forwarding technique is working properly when all the networks belong to the same administrative domain, since in this case the connections can be trusted. However,

in many cases Mobile IP has to work in an environment of independent networks, protected by firewalls. This means that some packets may not be delivered [8], even among agents (i.e. between HA and FA) due to the firewall policy, which discards the connections. In this case, a possible solution is shown in Figure 3. When the MN moves to a new network, the FA1 either does not know where the MN is now attached, or it can not forward the packet to that network. So, in order not to discard the connection, it sends the packet to the HN, where the HA after retrieves from the HVD database the current location of the MN, forwards the packet directly to this location address. In addition HA informs and the CN about the new point of attachment of the MN, in order future packets to delivered directly there.

4 Secure Mobile IP Architecture (SMA) Overview

Most of the problems described above can be prevented by using the Secure Mobile IP Architecture (SMA) that is described at this paper. This architecture requires a Central Administrative Server (CAS) [9] which is responsible for the whole system. CAS uses a database (CSD Central Server Database) where it tracks some critical information about the Nodes that are involved in the Mobile IP protocol (HA, FA, MN and CN). Scalability problems can be prevented by using additional CAS mirrors. problems, there is an option in order to use more than one CAS, where mirroring each another.

4.1 Improving Dynamic Registration

Every time a MN moves to a new network, it first has to determine if the network supports the Mobile IP protocol. The most common way to find this out is to broadcast an encrypted "hello" message. Unfortunately, this action may not be permitted to anyone, as if any Node is able to send broadcast messages to the whole network without any control, then it would put the system into a security risk.

To overcome this problem, when the MN is connected to a new network a temporary "special IP" address is assigned to it, for a very small time span. The mechanism which provides this IP is the DHCP protocol. With this IP, the MN sends the encrypted "hello" message and tries to find out if it is connected to HN or FN. By finding this out, the MN sends the encrypted registration request directly to the corresponding agent (HA/FA) with which it is connected to the network.

At the time the corresponding agent receives the registration request, it checks its local database to find out if the MN has permissions to get access at the local network. Finishing this search, and if the result is positive, the agent contacts to the CAS and informs it about the MN request. The CAS, in turn, makes a new search at its database, in order to find out if the MN has access to that network. After the corresponding agent receives the acknowledge from the CAS about the MN, it grant access to the MN. Then it updates the local database with the new coming MNs, as well informs the CAS in order to update its main database. Finally the CAS informs the HA about the MNs current point of attachment in order to update the HND. Of course, each network can have its own security policy. This means that even though the MN could be granted

access to a network that supports this implementation of Mobile IP, it is possible that this connection is refused by the local firewall. In this case, the agent informs the CAS about this refusal, so that if this MN tries to connect again to the same FN, the access to be blocked directly from the CAS. In case this security policy changes, the agent sends an administrative message to the CAS in order to stop blocking these connections any more.

4.2 Handoff Mechanism

Every agent of the system (HA and FA) periodically sends a digitally signed "heartbeat" message, which is received from all the Nodes that are successfully connected to the same administrative domain. This message is used to determine if all the MNs are still connected to the network. When a MN receives such a message, it replies immediately with a new encrypted message that includes its identity and a timestamp. By the time this reply arrives to the agent during a specific time span, the last one (agent) recognizes that the MN is still connected to the network. Otherwise, it assumes that the MN may be still connected to the same network [10]. This assumption is based on the fact that the agent has not received any sign that the MN attempts to register to a new network. Thus, agent expects another "heartbeat" message to clarify the situation. If the agent does not receive and the second reply from the same MN, then it assumes that the MN has already left from the network. In this case, agent after reserving the MNs IP address and updating its database, in order to block packets destined to the MN and to reduce the network load, it contacts the CAS and informs it. Finally, the CAS sends an administrative message to the HA of the MN, in order to stop forwarding any more packets to the previous FN that the MN was attached.

At the time the MN visits a new network, and after the authentication step has passed without problems, an administrative message is send from the corresponding agent to the CAS. This message includes all the necessary data for the current corresponding agent to be able to describe the MN to the CAS. This step involves two distinct phases. The first one is the mechanism that takes place in order to give a static IP address to the MN, as it has already been described. The second step involves the informing of the previous corresponding agent of the MN through the CAS about the current point of attachment. The second step helps the previous agent to improve its routing, as it is described briefly in the specific paragraph.

5 How SMA Improves Classic Routing Optimization

In this section we examine what happens when the CN wants to send packets to the MN. The CN probably does not know if the target host is mobile or not. It only knows the MNs IP at the HN, so it sends the packet there. When the HA receives the packet, it contacts with the CAS to find out if the CN is responsible for attacks to known networks. If the answer is affirmative, the CAS warms the HA either to discard the connection or to monitor it. Otherwise, the packet is tunnelled to the MNs current FN. Afterwards, the HA informs the CN about the MNs current point of attachment

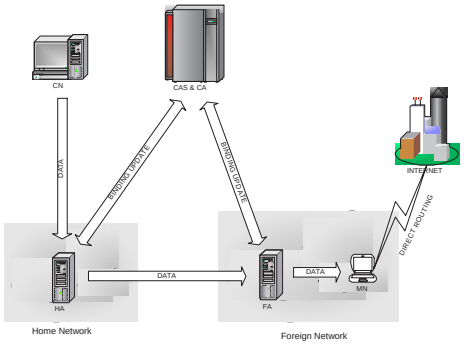

Fig. 4. The Secure Mobile IP Architecture (SMA) - What happens when the MN moves to a new network.

in order future packets to delivered directly to MNs FN bypassing the HA. Figure 4 shows what happens when the MN moves to a new network.

Sometimes it is desirable for the MN not to advertise its current point of attachment. For instance, the MN may not want to receive packets that comes from a certain CN. In this case, it sends a special encrypted message to the FA informing it about this. The agent with its row, first notifies the CAS to update its database (CSD) about this decision and then informs the HA, not to forward any more packets send from the specific CN to this MN. Moreover, the HA should not inform any more the CN about the MNs current point of attachment.

Finally, when the MN is located at the HN, it is important that its performance should be approximately the same as if it was an immovable node. This ensures that the extensions of the Mobile IP protocol do not reduce the HN performance. In this case, the MN no longer needs to periodically re-register with its HA and the MNs routing table should be set for normal IP routing.

5.1 Packet Forwarding Techniques

This section describes the available techniques that are supported by the SMA to forward packets from the CN to the current point of attachment of the MN. Those are the DNS Update, the Tunnelling, and the Transfer IP.

Tunnelling The tunnelling is a well know technique for connecting Nodes with end-to-end encryption. This is the default method that used by the Mobile IP protocol to route packets from the HN to the MN.

DNS Update The target of this mechanism is to permit the MN movements among networks and the preservation of the same host name. To manage this, a technique similar to the Dynamic DNS protocol should be used. Due to this, every time the MN

registers to a new network and gets an IP, the corresponding agent send an administrative message to the CAS to update the DNS record which targets to the specific MN. The disadvantage of this method is that all the Nodes (mobile or non-mobile) as well as the agents that wants to exchange packets with the MN, have to use the CAS as the main DNS server.

Transfer IP The method that called Transfer IP used to permit the MN to move across networks without changing the IP address or its hostname. This technique requires every agent to have access to the router / firewall rules of the correspond network in order to release and bind IP addresses. So, when the MN leaves its network and registers successfully to a new one, the previous correspond agent removes the rule from the routing table that target to this MN in order to stop routing locally any more packets for this Node and then informs the CAS. Next, the new corresponding agent contacts to the CAS requesting the IP address that should bind for the MN. By receiving the reply from the CAS, the agent binds the new IP address and modifies its routing and firewall rules in order to permit the MN to exchange packets as if it is connected to the HN.

5.2 Bandwidth Management

The Secure Mobile IP Architecture can be used to help combined networks to handle situations of network congestion with the minimum cost for them. To achieve in this, the agents should be able to make a decision about when the network that are responsible for, is going to be in congestion. When something like this is going to happen, the corresponding agent informs the CAS to find out a "backup network". This network should have good network speed with the FN, where the MN is attached, and must support the SMA. When the CAS finds this network, informs the CN not to send packets to the congested network, but instead to redirect them to the "backup network". When the congestion is passed by, the packets moved from the backup network to MN.

6 Security in SMA

Security is one of the most important issues in the design and implementation of Mobile IP solutions. There are several security threats like eavesdropping, denial of service and replay attacks inherent in the provision of mobility services. The common way to encounter the above threats is the use of cryptography. In SMA, public key and symmetric key cryptographic techniques [17] are used for this purpose. More precisely, public key cryptography techniques and one way hash functions are used for authentication, non-repudiation, integrity, and safe key exchange. Secret or symmetric key cryptographic algorithms are used for encrypting the data that is transferred. In this way, unsecured data links are made confidential, i.e. only authorized entities can read the transmitted data.

The security features of SMA are built on standard software components like the OpenSSL library. In this way SMA inherits the reliability and the platform independency of these proven and wide-spread software libraries.

The center of SMA's security architecture is the Certification Authority (CA). Hence the security of the whole SMA architecture largely depends on the security of the CA. The CA possesses a public cryptography key pair that is very important. The secret part of the key is used to certify-sign any other public key of any node (agents, mobile node, etc) of the network. The public key is used to check the certified public keys. All nodes of the network are assumed to know and trust the public key of the CA. Any other public key is considered valid only if it signed by the CA. The CAS, the agents and the mobile nodes must each first generate its own key pair and then get it certified by the CA. This certification process is completed of-line. After each node has a unique certified key pair it can participate in the network.

The backbone of the SMA network consists of the CAS and the agents. These nodes have permanent secure network connections established by using SSL. Each mobile node has also its own key-pair and can be attached at any point of the SMA network.

Each FA sends periodically a heartbeat packet to the subnet that it serves. The packet is signed with the private key of the FA and contains its certified public key, info about the FA and a timestamp.

When a mobile node is attached to the network it waits until it receives a heartbeat packet from the corresponding FA. The node uses CA public key to check the packet and sends a signed and encrypted request to the FA. The FA checks if the MN has the right to connect and queries the CAS to verify that the MN has the right to use the SMA services. Then the mobile node is granted the right to use the SMA services.

7 Low Power Techniques

The implementation of SMA has been optimized with programming techniques for low energy consumption. Most of the transformations [11] that are applied to the source code are general and can be applied to any algorithm family languages. The improvements that are made to the code are legal. A transformation can be characterized as legal if the original and the transformed programs produce exactly the same output for all identical executions. Two executions of a program are identical executions if they are supplied with the same input data and if every corresponding pair of non-deterministic operations in the two executions produces the same result.

The final code of the implementation is structured in a way that maximizes the use of computational resources (processors), minimizes the number of operations performed, minimizes the use of memory bandwidth (register, cache, network), and minimizes the size of total memory required.

8 Implementation

We have implemented and tested the SMA system on a heterogeneous network of Linux, Solaris and MS Windows nodes connected with wireless and non-wireless network technology. The flowchart with the HA, FA and MN operations during the execution of our implementation is shown in Table 2.

HA / FA Flowchart		MN Flowchart	
1. Start 2. Read configuration file 3. Initialize network 4. Wait MN request 5. Authenticate MN		1. Start 2. Read configuration file 3. Reset network 4. Request access to network	
YES	NO	ACCEPT	REJECT
a. Add MN at HN b. Check HN_IP c. Update VND, HND and CSD d. Give IP to MN e. Go to step 4	a. Update VND, HND and CSD b. Go to step 4	a. Modify network b. Store statistics c. Wait d. If connection remains go to step b, else go to step 4	a. Wait b. Go to step 4

Table 2. Comparison table.

9 Conclusion

The design and the implementation of the Secure Mobile IP Architecture (SMA) have clearly some advantages over the classic one. The most important of them is the systems capability to reduce the system administrators load, without reducing the security standard. In other words, the scripts which run on the CAS and the agents act as a super administrator who is authorized to protect all the combined networks. Moreover, the log-files from the whole system are available to the whole network administrator, so that the protection is even better. On the other hand, in the classic Mobile IP protocol, any network has to protect itself alone, ignoring the experience of previous attacks to other networks. Figure 5 summarizes the features of SMA compared to the related projects.

Categories	SMA	Related Projects
Cryptography algorithms	■ ■ ■ ■ ■	■ ■ ■ ■ ■
Secure Administrative Messages	■ ■ ■ ■ ■	■ ■ ■ □ □
Protection from attacks	■ ■ ■ □ □	■ ■ ■ ■ ■
Secure registration	■ ■ ■ ■ □	■ ■ ■ ■ □
Central administration	■ ■ ■ ■ ■	■ ■ ■ □ □
Bandwidth control	■ ■ ■ ■ ■	■ ■ □ □ □
Packet filtering	■ ■ ■ ■ □	■ ■ ■ ■ □
Routing optimization	■ ■ ■ □ □	■ ■ ■ ■ ■
Statistics	■ ■ ■ ■ □	■ ■ ■ □ □
Portability	■ ■ ■ ■ ■	■ ■ ■ □ □
Without kernel modifications	■ ■ ■ ■ □	■ ■ ■ □ □
Low-power techniques	■ ■ ■ ■ □	■ □ □ □ □

Fig. 5. Comparison table.

References

1. C. Perkins: IP Mobility Support. RFC 2002 (available from `http://www.faqs.org/rfcs/rfc2002.html`) (1996)
2. R. Droms: Dynamic Host Configuration Protocol. RFC 1541. Available from `http://www.faqs.org/rfcs/rfc1541.html`), (2000)
3. S. Cheshire, M. Baker: Internet Mobility 4x4. SIGCOMM'96. Available from `http://mosquitonet.stanford.edu/publications`, (1996)
4. G. Montenegro: Bi-directional Tunnelling for Mobile IP. Available from `http://www.watersprings.org/pub/id/draft-montenegro-tunneling-00.txt`), (1996)
5. C. Perkins: IP Encapsulation within IP. RFC 2003. Available from `http://www.faqs.org/rfcs/rfc2003.html`, (1996)
6. D.B. Johnson, D.A. Maltz: Protocols for Adaptive Wireless and Mobile Networking. Available from `http://citeseer.nj.nec.com/johnson96protocols.html`, (1996)
7. E.M. Royer, C.K Toh: A Review of Current Routing Protocols for Ad Hoc Mobile Wireless Networks. *IEEE Personal Communications*, 45-55, Apr (1999)
8. S. Glass, T. Hiller, S. Jacobs, C. Perkins: Mobile IP Authentication, Authorization and Accounting Requirements. RFC 2977. Available from `http://www.faqs.org/rfcs/rfc2977`, (2000)
9. A. Karakos, K. Siozios: Secure Networking Using Mobile IP. *Proceedings 8th Panhellenic Conference in Informatics*, Vol.I, (2001) 284-293
10. D.G. Leeper: A Long-term View of Short Range Wireless. *IEEE Computer*, 39-44, June (2001)
11. D.F. Bacon, S.L. Graham, O.J. Sharp: Compiler Transformations for High-Performance Computing. Computer Science Division, Univ. of California, Berkley, California 94720
12. The HUT Mobile IP system developed at Helsinki Univ. of Technology. Available from `http://www.cs.hut.fi/Research/Dynamics`
13. The MosquitoNet MoIP Implementation. Available from `http://gunpowder.stanford.edu/mip`
14. The Lancaster MoIPv6 Implementation. Available from `http://www.cs-IPv6.lancs.ac.uk/MobileIP`
15. The SUN's MoIP Implementation. Available from `http://playground.sun.com/mobile-ip`
16. The ECUTEL commercial MoIP Implementation. Available from `http://www.ecutel.com/`
17. J. Viega, M. Messier, P. Chandra: *Network Security with OpenSSL*. O.Reilly, (2002)