FATIMA: A Firewall-Aware Transparent Internet Mobility Architecture

Stefan Mink, Frank Pählke
Institut für Telematik
Universität Karlsruhe (TH)
76128 Karlsruhe, Germany
paehlke@telematik
.informatik.uni-karlsruhe.de

Günter Schäfer
Département INFRES
Ecole Nationale Supérieure
des Télécommunications
75634 Paris, Cedex 13, France
Guenter.Schaefer@enst.fr

Jochen Schiller
Institut für Telematik
Universität Karlsruhe (TH)
76128 Karlsruhe, Germany
schiller@telematik
.informatik.uni-karlsruhe.de

Abstract

Ubiquitous communication will be one of the paradigms for the next decades. The use of the Internet in such applications demands for a highly reliable and secure system, especially when used in non-academical environments like remote offices, e-commerce, or traffic telematics. Today's Internet, even with the mobility extension Mobile IP, has not been designed with private addresses, firewalls, network address translation, quality of service etc. in mind. Several optimisations already exist—however, security is often neglected. This paper proposes the firewall-aware transparent internet mobility architecture FATIMA, which integrates security functionality but is transparent to existing Mobile IP implementations. All security critical functions are concentrated in a firewall, all control messages are authenticated, and micro-mobility is supported. Corporate networks with private addresses are supported seamlessly, and further extensions allow for the use of dynamic home addresses and quality of service support.

1. Introduction

The highest growth rate in the computer and communication business is due to mobile communications. More and more people will be connected to communication networks with mobile and wireless devices. Thus there is an ever increasing demand for Internet services as known from fixed computers also on mobile devices. The Internet community responded to this demand with Mobile IP, the extension to the Internet Protocol IP to enable mobile devices. Another trend is the use of the Internet for commercial and safety-critical applications. However, neither the standard Internet protocol suite nor the extension Mobile IP have been designed with security features in mind, but these features are basic requirements for the acceptance of the Internet for everyday business. While several enhancements related to security already exist for the fixed Internet, security support for Mobile IP and the efficient integration of mobility support into firewalls are still open topics. Up to now research has quite often neglected topics of security and assumed an open network which is not at all realistic in a non-educational environment. Thus, to be successful, Mobile IP has to be enhanced towards support for security and the integration in today's firewall architectures, dynamic addresses, and network address translators.

This paper will discuss several open topics in existing enhancements to Mobile IP related to security and then present FATIMA, the Firewall-Aware Transparent Mobility Architecture. FATIMA is not only transparent to current Mobile IP implementations, but allows for mutual authentication of all components (mobility agents, mobile nodes), efficient micro-mobility support, and the centralisation of security critical functionality. Further benefits of the architecture are the seamless support of private addresses and the possibility of adding dynamic addresses and QoS support as discussed in the context of Integrated and Differentiated Services.

2. Mobile IP and firewall/micro-mobility support

Mobile IP [9] has been developed by the IETF as an extension to the IP protocol suite in order to support mobility in the Internet. In the following sections we will briefly discuss Mobile IP and some of the extensions proposed so far to overcome its deficiencies in the areas of security and support of micro-mobility. A more detailed analysis of the security issues related to Mobile IP can be found in [7].

2.1. Mobile IP

Using Mobile IP, a communication partner, the so-called Correspondent Node (CN), sends a packet as usual to the fixed IP address of the Mobile Node (MN). The routers in

the Internet forward this packet to the standard location of the MN, called the home network. Within the home network or as router for the home network, the Home Agent (HA) intercepts the packet if the MN is currently not in the home network. As the HA knows the current location of the MN, it tunnels the packet to a Care-of-Address (COA) temporarily assigned to the MN (so-called co-located COA) or to a Foreign Agent (FA) currently responsible for the MN in the foreign network (i.e., the network currently being visited by the MN). The COA denotes the tunnel end-point where the packet is decapsulated and forwarded to the MN in case of an FA holding the COA. Typically, tunnelling is performed using IP-in-IP encapsulation, i.e., a new IP header is created by the HA with the COA as destination and the HA as source address, and the original packet is used as payload [9]. In standard Mobile IP, the return path is much simpler as the MN can send packets as usual using the FA as default gateway.

Before the MN can send and receive data it has to register its current location with the HA. Therefore, an HA and FA is installed in each physical subnet and all agents (HA and FAs) broadcast agent advertisements into their subnet. An MN entering a new network receives these broadcast messages and notices if this network is the home or foreign network. If the latter is true, the MN sends its identification and the address of its HA to the FA which forwards this registration request to the HA. The HA then checks if the MN is authorised to register and, if this is the case, acknowledges the registration. This acknowledgement is again forwarded by the FA to the MN. Both MN and HA can now trust each other, and the HA can start tunnelling data to the COA.

Several optimisations and enhancements to the standard Mobile IP have been proposed during the recent years. One enhancement [10] tries to avoid the so-called triangular routing of packets (CN-HA-FA-MN and back to the CN) by sending binding updates to the CN to inform it of the MN's current location. After receiving such an update from the HA, a CN can directly send to the MN. However, this requires the ability to update the binding cache in arbitrary CNs and raises several security issues (e.g., location tracking and malicious re-routing of packets).

Furthermore, it was soon discovered that simply sending packets from the MN to a CN via the FA does not work in real networks using firewalls. Sending a packet from a MN located within a foreign network cannot be allowed by a firewall as this looks the same as a typical spoof-attack. Such packets with topologically incorrect addresses will be filtered out immediately. [8] proposes a reverse tunnelling, i.e., the MN sends packets to the FA which tunnels them to the HA. The HA then forwards these packets as if they came from the home network. This solution also solves several problems with multicast communication and the lifetime of packets. However, this introduces an additional triangular routing making the whole approach even more inefficient.

As explained above, in Mobile IP a tunnel is set up between a home and a foreign agent, or the mobile node, respectively, in case of a co-located COA. This tunnel generally traverses both the home and the foreign networks' firewalls. Like e.g. dial-in servers, the tunnel endpoints have to be administered carefully in order not to compromise the security ensured by the firewalls, as common firewalls will not further look into the encapsulated packets. This decentralisation of security-critical functionality is undermining the main benefit of a firewall, which is the concentration of security-critical administration tasks to relatively few centrally administered systems.

Additionally, the original Mobile IP is not interoperable with private or dynamically assigned IP addresses and it does not enforce mandatory authentication of all entities. Finally, it does not provide efficient support for micromobility, i.e., efficient handling of handovers between adjacent foreign agents belonging to the same administrative domain without contacting the home agent or requiring other notification of systems outside of the currently visited administrative domain. This issue is currently being addressed by several research projects. In the following sections we will decribe the main approaches and discuss their strenghts and weaknesses.

2.2. Cellular IP

Cellular IP [2] provides local handovers without renewed registration by installing a single *Cellular IP Gateway (CIPGW)* for each domain, which acts to the outside world as a foreign agent. Inside the Cellular IP domain, all nodes collect routing information for accessing MNs based on the origin of packets sent by the MNs towards the CIPGW. Soft handovers are achieved by allowing simultaneous forwarding of packets destined for a mobile node along multiple paths. A mobile node moving between adjacent cells will thus temporarily be able to receive packets via both old and new base stations if this is supported by the lower protocol layers.

Concerning the manageability of Cellular IP, it has to be noted that the approach has a simple and elegant architecture and is mostly self-configuring. However, Mobile IP tunnels could be controlled more easily if the CIPGW was integrated into a firewall, but there are no detailed specifications in [2] regarding such an integration. It has to be mentioned that Cellular IP requires changes to the basic Mobile IP protocol and is thus not transparent to existing systems. Furthermore, the foreign network's routing tables are changed based on messages sent by mobile nodes, which should not be trusted blindly even if they have been authenticated. This could be exploited by systems in the foreign network for wiretapping packets destined for an MN

by sending packets to the CIPGW with the source address set to the MN's address. In enterprise scenarios requiring basic communications security, this may not be acceptable.

2.3. HAWAII

HAWAII [11] (Handoff-Aware Wireless Access Internet Infrastructure) tries to keep micro-mobility support as transparent as possible for both home agents and mobile nodes (which have to support route optimisation, though). Its concrete goals are performance and reliability improvements and support for quality of service mechanisms.

Upon entering an HAWAII domain, a mobile node obtains a co-located COA. Additionally, when moving to another cell inside the foreign domain, the MN sends a registration request to the new base station as to a foreign agent, thus mixing the concepts of co-located COA and foreign agent COA. The base station intercepts the registration request and sends out a handoff update message, which reconfigures all routers on the paths from the old and new base station to the so-called crossover router. When routing has been reconfigured successfully, the base station sends a registration reply to the mobile node, again as if it were a foreign agent.

The use of challenge-response extensions for authenticating a mobile node is mandatory. In contrast to Cellular IP, routing changes are always initiated by the foreign domain's infrastructure, and thus the corresponding messages could be authenticated, e.g., by means of an IPSec authentication header (AH) [4], reducing the risk of malicios rerouting of traffic initiated by bogus mobile hosts. However, this is not explicitly specified in [11]. HAWAII claims to be mostly transparent to mobile nodes, but this claim has to be regarded with some caution as the requirement to support a co-located care-of-address as well as to interact with foreign agents could cause difficulties with some mobile nodes.

2.4. Hierarchical Mobile IP

Hierarchical Mobile IP [3] provides micro-mobility support by installing a hierarchy of mobility agents where a mobile node has a "virtual" COA on each hierarchy level. When an MN moves locally, only mobility agents on hierarchy levels directly affected by the move must be notified. The home agent and, in case of route optimisation, the communication partners have to be notified only if the MN moves between the domains of different top-level mobility agents.

It might be mentioned as a security benefit that mobile nodes can be provided with some kind of limited location privacy because COAs on lower levels of the mobility hierarchy are hidden from the outside world. However, this applies only to micro-mobility, that is, as long as the mobile node rests in the same administrative domain. As additional infrastructure and changes to the MN protocol stack are required, the deployment of Hierarchical Mobile IP is not transparent to existing equipment. Additionally, in case of a handover, all hierarchy levels have to be reconfigured by the mobile node itself, which may be connected to the network by a bandwidth-limited wireless link, possibly resulting in efficiency problems.

3. The firewall-aware transparent internet mobility architecture FATIMA

Each of the architectures described in section 2 addresses some of the deficits of Mobile IP described in section 2.1. However, as has been pointed out above, none of these architectures can be considered a completely satisfying solution yet. The aim of FATIMA [6] is to define a clear, simple and flexible architecture which integrates the advantages of each of the abovementioned approaches while avoiding their disadvantages, and which provides a solid base for adding new features (e.g., support for dynamically assigned home addresses or for quality of service mechanisms) in a consistent and straightforward manner. The basic design objectives of FATIMA can be summarized as follows:

- *Transparency to mobile nodes and correspondent nodes:* Any necessary extensions of the Mobile IP standard should be hidden from mobile nodes as well as correspondent nodes.
- *Centralisation of security-critical functionality:* This property is the main security benefit of a firewall architecture and should thus be preserved.
- *Mutual authentication of all instances involved:* This is required in order to prevent attacks using forged control messages.
- *Efficient micro-mobility support:* Handovers between adjacent subnets of the same foreign network should be considerably more efficient than handovers between different foreign networks.

3.1. Network entities

In order to a convert a standard Mobile IP network into a FATIMA-enhanced network, it is at least necessary to insert a *FATIMA gateway* into the network's firewall, and to replace all home/foreign agents by so-called *home/foreign agent proxies* (figure 1). In large networks, the scalability of the architecture can be improved by inserting a hierarchy of *routing agents* (figure 2). In the following, we will motivate and explain the functionality of the different FATIMA network infrastructure entities.

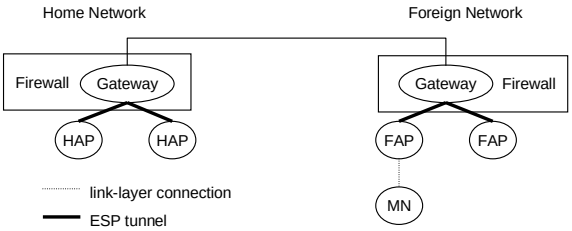

Figure 1. FATIMA entities: minimal setup

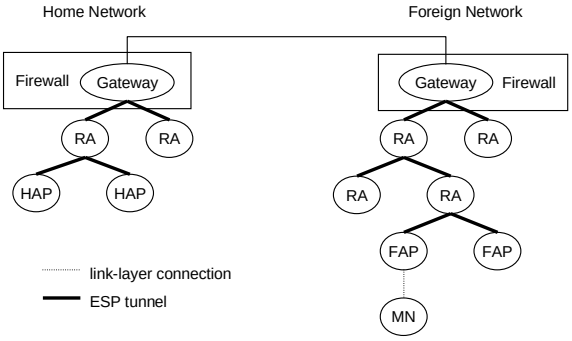

Figure 2. FATIMA entities: advanced setup with routing agents

- *FATIMA Gateway:* The FATIMA gateway is the central mobility-supporting entity inside a network. It is located on a bastion host inside the demilitarized zone of the network's firewall. Any security-critical mobility supporting functionality (e.g., registration of mobile nodes or decapsulation of tunneled data packets) is concentrated in the gateway and can thus be centrally administered. To the outside, the gateway acts as both a home and foreign agent. Actually, every host outside a FATIMA-enhanced network believes that the gateway is the only home agent and the only foreign agent in that network. Every visiting mobile node is assigned the FATIMA gateway's address as care-of address.

- *Foreign Agent Proxy (FAP):* All foreign agents are replaced by considerably simpler entities called foreign agent proxies. Towards visiting mobile nodes, an FA proxy acts as a foreign agent. However, it does not process Mobile IP messages (e.g., registration requests) itself, but forwards them to the gateway. Any replies by the gateway are in turn forwarded to the visiting mobile nodes, which cannot distinguish them from messages generated directly by a standard foreign agent.

- *Home Agent Proxy (HAP):* All home agents are replaced by considerably simpler entities called home agent proxies. An HAP is still responsible for tunnelling packets destined for absent mobile nodes, but does not process registration messages. All registration messages are processed by the FATIMA gateway, which sends control messages to the responsible HAP in order to (de)activate tunnelling of data packets.

- *Routing Agent (RA):* In order to improve scalability in large networks, a tree of routing agents can be used to connect the FATIMA gateway with each home/foreign agent proxy in the network. Each RA maintains a table of visiting mobile nodes inside its own sub-tree. Based on this table, it forwards data and control packets from its parent RA to its child RAs, and vice versa. Every connection between adjacent routing agents (i.e., each edge of the RA tree) must be secured by an encapsulating security payload (ESP) tunnel as defined in [5] in order to protect the mobility supporting infrastructure from attacks by outsiders. The ESP tunnel must be configured to provide authentication; optionally, the packets may also be encrypted. All packets related to mobility-supporting functionality are forwarded along the edges of the RA tree. In particular, no packet is sent directly from a FA proxy to the FATIMA gateway, or vice versa, if there are any intermediate routing agents.

3.2. Registration of mobile nodes in a foreign network

When a mobile node enters a new foreign subnetwork, it first determines the link-layer address of the corresponding foreign agent proxy as in standard Mobile IP. After that, it sends a Mobile IP registration request to the FAP, together with an MN-HA authentication extension. The FAP does not process the registration request itself, but forwards it (possibly via a chain of routing agents) to the FATIMA gateway. Between each pair of adjacent entities, the forwarded packet is secured by the pre-configured ESP tunnel. Every routing agent, including the gateway, inserts a temporary entry for the mobile node into its routing table.

The FATIMA gateway checks the registration request and makes a preliminary decision whether to allow the mobile node to enter the foreign network. After that, it inserts its own address as care-of adress and forwards the registration request to the mobile node's home agent as in standard Mobile IP. The forwarded request must be protected with an FA-HA authentication extension. The home agent then tries to authenticate the registration request and decides whether to accept it. If the home network is FATIMA-enhanced, the "home agent" is in fact its FATIMA gateway which accepts the registration request and tells the home agent proxy in the mobile node's home subnet (i.e., the subnet where the MN's IP address belongs to topologically) to start intercepting packets destined for the mobile node and tunnelling

them to the care-of address. Finally, a registration reply indicating acceptance or denial of the registration request is sent back to the foreign FATIMA gateway together with an HA-FA authentication extension.

The foreign gateway forwards the registration reply (possibly via a chain of routing agents) to the responsible foreign agent proxy using the temporary routing entries created before, and the FAP finally transmits the reply to the mobile node. As the registration reply is forwarded towards the FAP, each routing agent converts the MN's temporary routing entry into a normal one.

3.3. Deregistration of mobile nodes

When a mobile node returns to its FATIMA-enhanced home subnet, it sends a registration request to its home agent proxy as to the home agent in standard Mobile IP, protected by an MN-HA authentication extension. The HAP forwards the registration request to the home network's FATIMA gateway, which authenticates it and deletes the corresponding registration. After that, it sends back a reply, together with an HA-MN authentication extension. The HAP forwards the reply to the mobile node, which cannot distinguish it from a reply by a standard home agent, and stops intercepting and tunnelling data packets.

3.4. Route optimisation

No special care has to be taken when FATIMA is to be combined with route optimisation [10]. A home FATIMA Gateway behaves exactly as a standard home agent, in that it informs correspondent nodes when the mobile node has moved to another subnet. However, these binding update messages are sent much less frequently if the foreign network is FATIMA-enhanced because of its micro-mobility support: Since the mobile node is assigned the foreign gateway's address as care-of address, the care-of address does not change when the mobile node moves between subnets of the same foreign network. The home agent interprets the corresponding registration messages as renewals of a previous registration and does not inform any correspondent nodes, thus avoiding a major bottleneck of Mobile IP with route optimisation and substantially improving its scalability.

As far as described in this paper, FATIMA does not allow for completely local handovers, which would vastly improve the scalability of Mobile IP with and without route optimisation. The home agent must be contacted upon each handover in order to ensure mutual authentication of mobile nodes and foreign network infrastructure. This is not an architectural deficit, however: Mechanisms for adding local handovers to FATIMA are currently being developed. One possible solution is the *fast handoff extension* which has already been defined in [6].

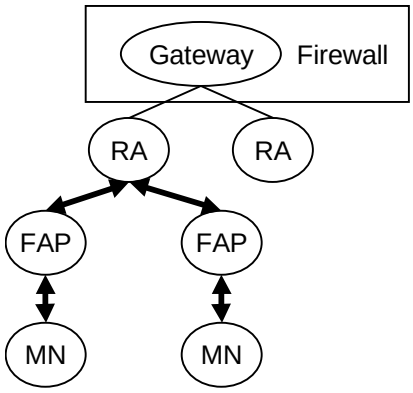

Figure 3. Routing between mobile nodes visiting the same foreign network

3.5. Routing of data packets

If the home network is FATIMA-enhanced, data packets destined for an absent mobile node are intercepted by the home agent proxy in the MN's home subnet and forwarded (possibly via a chain of routing agents) to the home FATIMA gateway. The gateway then tunnels the packets to the care-of address. If the foreign network is FATIMA-enhanced, the care-of address is the address of its FATIMA gateway. In this case, the foreign gateway decapsulates the tunneled packet, checks if it is destined for a registered mobile node and forwards it (possibly via a chain of routing agents) to the correct foreign agent proxy, which finally delivers the packet to the mobile node.

Packets sent by a mobile node are forwarded via the FAP and any intermediate routing agents to the foreign gateway, which filters out packets whose source address does not correspond to a registered mobile node and forwards the remaining packets to their destination, either directly or via a reverse tunnel. In case of direct forwarding, the FATIMA gateway is the only system inside a foreign network which must be allowed to send topologically incorrect packets whose source address belongs to a mobile node. Since the gateway is located on a bastion host inside the demilitarized zone of the network's firewall and should thus be thourougly supervised, this should not introduce any uncontrollable risks to the foreign network, which is a great improvement over standard Mobile IP.

Packets exchanged between two mobile nodes visiting the same foreign network are forwarded by the foreign agent proxy towards the FATIMA gateway. However, as in the other discussed approaches, the packets need not be

routed via the gateway, but can instead be intercepted by the first routing agent which has a routing entry for the destination mobile node. This is a considerable improvement of routing efficiency compared to standard Mobile IP without route optimisation, where all data packets must be sent via the destination node's home agent.

In order to protect the foreign network against malicious mobile nodes, it is necessary to route data packets sent by mobile nodes and destined for fixed nodes in the foreign network via the foreign network's gateway and process them as if they had originated outside. This is less efficient, but far more secure than standard Mobile IP without reverse tunnelling, and it is a considerable efficiency improvement in case of a firewall-protected foreign network requiring reverse tunnelling, because the packets need not be routed via the mobile node's home network.

If the foreign gateway was given limited control over the routing tables of the firewall's external router (i.e., the router between the demilitarized zone and the global internet), packets sent by fixed nodes in the foreign network to a mobile node visiting that network could be routed directly to the gateway and treated as if they had arrived via a tunnel from outside. In order to keep firewall semantics unchanged, the packets should be intercepted after passing the complete firewall, i.e., at the external interface of the external router. Again, the packets would not be routed via the mobile node's home network, which is a great efficiency improvement over standard Mobile IP both with and without reverse tunnelling. It is still an open question, though, whether the efficiency improvements due to shorter routing paths will be greater than the efficiency drawbacks due to substantially growing routing tables in the interior router.

3.6. Security aspects

Authentication of control messages is necessary to protect all instances against attacks using forged IP source addresses. In FATIMA, several cases of authentication can be distinguished:

- *Mutual authentication of infrastructure entities inside a network:* This is achieved by installing ESP tunnels between each pair of communicating entities (FATIMA gateway, routing agents, home/foreign agent proxies) and by requiring that all packets must be forwarded along the edges of the RA tree. It should be feasible to install the required shared secrets even when no public-key infrastructure (PKI) is available, because the complete infrastructure belongs to the same administrative domain.

- *Mutual authentication of mobile nodes and home network infrastructure:* This is achieved by requiring all registration messages to carry an MN-HA authentication extension. Again, key management should be feasible even without a PKI because the MN and its home network infrastructure belong to the same administrative domain.

- *Mutual authentication of home and foreign network infrastructure:* This is achieved by requiring all registration messages exchanged between the home and foreign network to carry an HA-FA authentication extension. It is generally difficult to install a shared secret when no PKI is available and when the home and foreign network do not belong to closely cooperating institutions. However, FATIMA considerably reduces the number of shared secrets required in this case because only one secret has to exist between any pair of home and foreign *networks*, not between any pair home and foreign *agents* inside these networks as in standard Mobile IP: If N is the number of networks, and S is the number of subnets per network, and if each subnet contains one HA/FA, then the number of shared secrets is reduced from $O(N^2S^2)$ to $O(N^2)$. Note that in standard Mobile IP, each subnetwork must contain a home/foreign agent pair because link-layer connectivity is needed in order to enable the HA to intercept packets and the FA to send packets with topologically incorrect destination addresses to the MN.

- *Mutual authentication of mobile nodes and foreign network infrastructure:* In standard Mobile IP, this is the most difficult authentication task because the involved instances are generally not known to each other before. In FATIMA, this problem is solved with help of the home network's infrastructure (home agent or gateway): The home agent/gateway authenticates the mobile node and the foreign agent/gateway upon receiving a registration request and informs both foreign agent/gateway and mobile node of the authentication results using the authenticated registration reply. There is one problem remaining, however: The foreign network's infrastructure has to trust the home network's infrastructure. This problem is common to all similar security architectures and can only be avoided in presence of a global public-key infrastructure which can be used to directly authenticate all visiting mobile nodes.

FATIMA does not contain any provisions for mutual authentication of mobile nodes and correspondent nodes and for integrity and confidentiality of transmitted data packets, because we believe that this kind of security functionality should rather be implemented end-to-end, without involving any intermediate systems. Our aim is to protect the infrastructure and to avoid creating mobility-specific security holes, not to provide end systems with more security than they would typically expect from a fixed network.

The problem of allowing uncontrollable tunnels through firewalls is solved by letting any mobility-related tunnels end in the FATIMA gateway—a concept similar to e.g. HTTP proxies. Since the gateway shares security associations with all registered mobile nodes, it is able to check the validity of all tunneled packets. The gateway can be centrally administered, and there is no decentralised replication of security-critical functionality deep inside a network, which is considered inherently dangerous.

3.7. Differences between FATIMA and related approaches

Many aspects of FATIMA are inherited from the approaches introduced in section 2. All approaches have a hierarchical topology, which is a direct consequence of the demand for efficient micro-mobility support. As an additional advantage, the root node of a hierarchical structure is a natural candidate for integration into a network's firewall.

The idea of introducing a gateway which acts to the outside world as a foreign agent and whose address is used as care-of address is inherited from Cellular IP. However, in FATIMA, as well as in HAWAII, messages causing reconfiguration of routing tables can only be sent by infrastructure entities, whereas in Cellular IP, routing tables are automatically reconfigured due to data packets sent by mobile nodes. The latter is similar to Hierarchical Mobile IP where all routing reconfigurations are explicitly triggered by the mobile node. This is not transparent at all and raises both efficiency and security concerns—in fact, we do not foresee any network provider that would allow users to reconfigure its routing infrastructure as proposed in Cellular IP and Hierarchical Mobile IP. In addition to the security precautions taken in HAWAII, FATIMA explicitly demands that all messages exchanged between infrastructure entities must be authenticated by means of ESP tunnels.

Whereas both Cellular IP and Hierarchical Mobile IP concentrate exclusively on micro-mobility and do not discuss any macro-mobility aspects other than stating that macro-mobility support should be provided by Mobile IP, both HAWAII and FATIMA provide an integrated approach which addresses both micro-mobility and macro-mobility issues.

Another common aspect of both HAWAII and FATIMA is the way how transparency to mobile nodes is maintained: Each HAWAII base station and each FATIMA foreign agent proxy masquerades as a standard foreign agent. However, in HAWAII, mobile nodes must obtain a co-located care-of address prior to contacting the "foreign agent", whereas in FATIMA it is assigned the address of the network's gateway as care-of address. We consider this the natural choice for providing micro-mobility support.

3.8. Additional benefits of FATIMA

There are additional benefits which come for free when using FATIMA to implement a mobility-supporting infrastructure:

- *Seamless support for private addresses:* Since the FATIMA gateway acts as a gateway for all mobility-specific network traffic, the gateway's address is the only network address required to be reachable from outside as well as from inside a FATIMA-enhanced network. Since the gateway is located in the demilitarized zone of the network's firewall, it does not matter at all if the network uses private addresses, which is the normal case in enterprise environments.

  Private addresses are not supported by standard Mobile IP. Support for private addresses could probably be added as an extension to Cellular IP and Hierarchical Mobile IP. In HAWAII, the demand for a co-located COA prohibits the use of private addresses.

- *Possibility of adding support for dynamic addresses:* In some cases, it might not be desirable that a mobile node possesses a permanent home address—e.g., when addresses in the home network are assigned by DHCP anyway, or when "travelling aliases" should be assigned for privacy reasons. This functionality could be implemented by means of the Network Access Identifier (NAI) extension of Mobile IP [1]: A mobile node requiring dynamical address assignment could set the address field of its registration request to all-zero and include an NAI whose realm part unambigously identifies the home network's FATIMA gateway. The gateway could then assign a home address and include it in the registration reply. It must be noted, however, that this extension would not be completely transparent to mobile nodes.

  HAWAII provides a somewhat simpler support for dynamically assigned home addresses: when a mobile node is powered on inside a HAWAII foreign network, it is simply assigned a "home address" from the foreign network's address space. Regarding Cellular IP and Hierarchical Mobile IP, both approaches do not address macro-mobility issues, and it would probably be quite difficult for a mobile node to obtain a dynamical home address without IP connectivity to its home network.

- *Possibility of adding QoS support:* If TCP connections between a mobile node and a correspondent node outside the current foreign network are to be provided with Quality of Service (QoS) guarantees, the necessary resource reservations (e.g., RSVP flows or DiffServ aggregates) should be made independently for the

two paths from the CN to the FATIMA gateway, and from the gateway to the MN, respectively. If the MN subsequently roams inside the foreign network, only reservations between the gateway and the MN have to be updated—an operation which should be relatively efficient if the foreign network is not really huge. The reservations for the IP-in-IP tunnel from the CN across the Internet to the gateway, which are much more expensive to change, need not be altered unless the MN moves into a different foreign network, which should happen much less frequently than local intra-network handovers.

HAWAII also claims to provide a base for QoS mechanisms, using a substantially different approach. Cellular IP and Hierarchical Mobile IP do not discuss this issue at all, and it is unclear whether it would be feasible to add such mechanisms.

4. Conclusion and outlook

FATIMA is completely transparent to mobile nodes as well as to all nodes outside a FATIMA-enhanced network. All security-critical functionality is concentrated in the FATIMA gateway, which is located inside the network's firewall. Furthermore, all control and data traffic between entities of the mobility supporting infrastructure is authenticated by means of ESP tunnels, and mutual authentication of mobile nodes and the foreign network's infrastructure is ensured. The architecture considerably improves the efficiency of local handovers (micro-mobility) together with route optimisation, and can be extended with mechanisms providing comprehensive micro-mobility support. Finally, FATIMA provides seamless support for private addresses, a must in today's non-academic IP networks, and can be extended to support dynamic addresses and QoS mechanisms. With FATIMA we have thus reached all design objectives listed in section 3.

Up to now, we have achieved a complete specification of FATIMA's system architecture together with functional descriptions of the required protocols. Further efforts for designing an efficient implementation architecture have already been started. As a first step, a simulation environment is developed which can be used to compare performance aspects of mobility-supporting protocols and architectures, and to evaluate the impacts of FATIMA's centralized design on efficiency and scalability. The ultimate goal is a full implementation of all infrastructure entities (FATIMA gateway, routing agents, home and foreign agent proxies).

As our research also includes issues of controlling road traffic and mobile communications with and within vehicles, further research efforts are necessary regarding privacy, anonymity, but also reliability, flexibility, and robustness. Our goal is to provide mobile Internet services in an integrated, efficient, and secure way to be used in all kinds of devices (internet appliances), in vehicles, or for people.

References

[1] P. R. Calhoun and C. E. Perkins. *Mobile IP Network Access Identifier Extension for IPv4*. IETF, Mobile IP Working Group, Jan. 2000. Internet Draft. draft-ietf-mobileip-mn-nai-07.txt (work in progress).

[2] A. T. Campbell, J. Gomez, C.-Y. Wan, S. Kim, Z. R. Turanyi, and A. G. Valko. *Cellular IP*. IETF, Mobile IP Working Group, Jan. 2000. Internet Draft, draft-ietf-mobileip-cellularip-00.txt (work in progress).

[3] C. Castelluccia. A Hierarchical Mobile IPv6 Proposal. In *Proceedings of AMOS ACTS Mobile Summit*, Sorrento, Italy, June 1999. Also published as INRIA technical report TR-0226, November 1998.

[4] S. Kent and R. Atkinson. *IP Authentication Header*. IETF, Nov. 1998. RFC 2402.

[5] S. Kent and R. Atkinson. *IP Encapsulating Security Payload (ESP)*. IETF, Nov. 1998. RFC 2406.

[6] S. Mink. *Konzeption einer Firewall-Architektur für Mobile IP (Conception of a firewall architecture for mobile IP)*, Oct. 1999. Diploma Thesis, Universität Karlsruhe (TH), Institut für Telematik (In German).

[7] S. Mink, F. Pählke, G. Schäfer, and J. Schiller. Towards Secure Mobility Support for IP Networks. In *Proceedings of the IFIP International Conference on Communication Technologies (ICCT 2000)*, Beijing, China, Aug. 2000.

[8] G. Montenegro. *Reverse Tunneling for Mobile IP*. IETF, May 1998. RFC 2344.

[9] C. Perkins. *IP Mobility Support/IP Encapsulation within IP*, Oct. 1996. RFC 2002+2003.

[10] C. Perkins and D. B. Johnson. *Route Optimisation for Mobile IP*, Feb. 2000. Internet Draft, draft-ietf-mobileip-optim-09.txt (work in progress).

[11] R. Ramjee, T. La Porta, S. Thuel, K. Varadhan, and L. Salgarelli. *IP micro-mobility support using HAWAII*. IETF, Mobile IP Working Group, June 1999. Internet Draft, draft-ietf-mobileip-hawaii-00.txt (expired).