In Proc. of IEEE Global Communications Conference (GLOBECOM'04), pp. SN06-1, Dallas, Texas, USA, November 2004.

Security Analysis and Concept for the Multicast-Based Handover Support Architecture MOMBASA

L. Westerhoff, S. Reinhardt, G. Schäfer, A. Wolisz
Telecommunication Networks Group, Technische Universität Berlin
Einsteinufer 25, 10587 Berlin, Germany
Email: [wester, schaefer, wolisz]@tkn.tu-berlin.de

***Abstract*— In order to achieve a low latency handover with minimum packet loss in mobile Internet communications, the multicast-based mobility architecture MOMBASA has proven to be an efficient and elegant approach [1]. The original MOMBASA specification, however, did not comprise any precautions against malicious attacks on its protocol operation. In this paper[1] we present the principal results of our security analysis of the MOMBASA architecture and describe our security concept in order to counter the identified threats. A main focus is put on attacks against the MOMBASA protocol operation coming into the access network from two main sources: the public Internet and the wireless link. The design of our security concept is specifically suited to ensuring a seamless handover by augmenting the predictive handover functionality of MOMBASA with an accompagnying predictive distribution of authentication keys. Furthermore, the security concept comprises a rate control mechanism for traffic destined for idle mobile nodes in order to limit the risks arising of potential Denial of Service (DoS) attacks against the paging mechanism. While our security measures effectively counter the identified threats from the wireless link and the Internet, first measurements with our prototype implementation show only neglectable degradation of handover performance compared to unsecured MOMBASA operation.**

I. Introduction

While in current mobile communication networks and even in upcoming third generation mobile networks, such as UMTS [2], IP is only used within the core network (and potentially in parts of the access network) so that mobility is supported by special purpose protocols, the fourth generation of cellular phone networks is envisaged by many to work entirely based on IP protocols. This requires support for IP-based seamless handover.

The basic approach of the Internet Engineering Task Force (IETF) *Mobile IP* [3] enables IP-based mobility. However, there is wide consensus that basic Mobile IP is not suited for the support of seamless handover. Therefore, several approaches such as Hierarchical Mobile IP [4] have been proposed to decrease the handover latency in the case of local mobility.

MOMBASA (**Mo**bility Support - A **M**ulticast-**Bas**ed **A**pproach) [1], [5], [6] is an alternative architecture for the support of IPv4-based micro mobility, which employs IP multicast for predictive distribution of data and signaling traffic to the neighborhood of the current location of a mobile host.

Hosts within the Internet face a variety of threats, such as masquerading, Denial of Service attacks and others [7]. With the integration of IP and cellular phone networks, appropriate protective measures have to be taken against these threats. In this paper, we therefore conduct a systematical security analysis and develop a security concept for MOMBASA, as the original MOMBASA Software Environment implementation was mainly developed as a proof-of-concept architecture without explicit security mechanisms.

The remainder of this paper is organized as follows: Section II gives a short overview over the original MOMBASA architecture. In Section III we systematically analyze security threats against the MOMBASA architecture and its protocol operation. A concept to secure MOMBASA against the identified threats is presented in Section IV and discussed in Section V. Section VI describes experiences with our prototypical implementation of the security concept and Section VII concludes the paper.

II. MOMBASA Architecture

The infrastructure of a MOMBASA access network (see Fig. 1) consists of access points running so-called Mobility-Enabling Proxies (MEPs) and is connected through multicast-capable routers (MR). The gateway between the public Internet and the access network runs a Gateway Proxy (GWP). The mobile hosts execute Mobile Agents (MAs).

It is assumed that mobile hosts – at least for the duration of their stay in the access network – each possess a globally unique IP unicast address lying in the address range of the access network. Thus, all packets from the public Internet destined to the mobile reach the gateway due to normal Internet routing. The block of mobile unicast addresses is associated a block of multicast groups within the access network. When a mobile registers at a MEP, the MEP joins the associated multicast group. Data packets for the mobile are translated to multicast at the gateway and back to unicast at the MEP.

The usage of multicast facilitates predictive handover. In this case, neighboring MEPs of the primary MEP the mobile

[1]This work has been supported in part by a research contract with Siemens AG, Information and Communication Networks (ICN), Enterprise Networks.

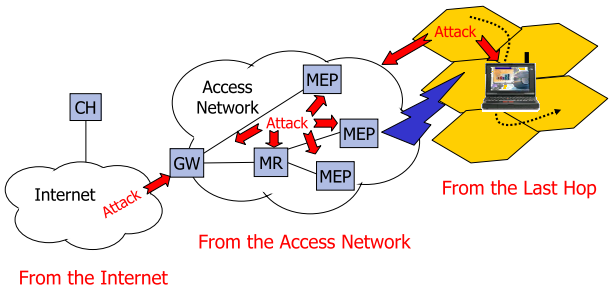

Fig. 1. Potential sources of Attacks

host is directly registered at are invited to join the multicast group. While only having an indirect registration they buffer data in a ring buffer. On handover, recently received traffic in the buffer is forwarded to the mobile to compensate for packet loss during handover.

If a mobile host does neither receive nor send data for a certain period of time, it will switch to idle mode. In this case, the multicast group is torn down and the position of the mobile is only known coarsely as a paging area represented by a permanent mobile-independent multicast group. When data for an idle mobile node arrives at the gateway, a paging request is multicasted to the last known paging area of the mobile and forwarded to the last hops of the MEPs being member of the paging area causing the mobile to wake up and register. For a more detailed description of MOMBASA protocol operation please refer to [1], [5], [6].

III. Security Analysis of MOMBASA

In this section, we analyze security threats to the MOMBASA architecture. Since MOMBASA provides its service at the network layer and is independent of the deployed access technology, we concentrate on layer 3 and on problems specific to MOMBASA in comparison to other IP mobility architectures.

A. Taxonomy of Attacks

On a first level, potential attacks can be classified according to the following four properties:

- *Source of the attack:* An attack is either coming from the public Internet (via the gateway into the access network), from within the access network itself or from the usually wireless last hop via an access point (see Fig. 1). As the access network is usually under the control of a single authority and possesses a limited inherent protection by buildings or is buried below the surface, this paper will concentrate on threats from the Internet and the last hop. Moreover, existing security protocols can easily be deployed in a network under administration of a single organization (see also Section IV-J).
- *Target of the attack:* Potential attack targets are MOMBASA protocol operation, multicast protocol operations and data traffic.
- *Attacker's objectives:* An attacker may pursue the objectives information disclosure, tracking of position, masquerading, repudiation of events, authorization violation, manipulation or sabotage (Denial of Service, DoS).
- *Attack techniques:* Basic techniques are eavesdropping, insertion, replay, modification, deletion and delaying of messages. These techniques may be combined to construct more complex attacks.

B. Threats to MOMBASA Protocol Operation

Our security analysis identified the following classes of threats:

T1) **Injecting internal messages from external links** may be used in many kind of attacks to reach all classes of objectives.

T2) **Internal access network signaling** may be used by an attacker that has access to the access network either as an insider, by direct access to the network infrastructure or by compromising a host within the access network. All classes of objectives can be reached.

T3) **Communication on the last hop with known parties** can be used by an attacker who pretends to the access network to be a legitimate user and thereby is able to eavesdrop on or manipulate data, as well as to masquerade as and use service at the expense of the impersonated mobile node.

T4) **Masquerade of access network entities** A mobile user usually does not know in advance the identity of the access point. Therefore, by producing forged MEP Advertisements on the last hop, a mobile host may be mislead to register at an attacker. The problem here is the following: MEP Advertisements are not meant for a single mobile but for a group of mobiles. Using symmetric cryptography would enable each mobile involved to produce forged advertisements itself. Using asymmetric cryptography implies using check values from several hundred up to 2048 bits. However, a false access point could potentially still be unmasked later in the registration process when mobile node and access point are communicating directly with each other.

T5) **Denial-of-Service attacks** First, even when employing countermeasures against other threats, DoS attacks may be performed from the last hop against the authentication process itself, at a time where the authenticity of the identity of the peer node can not be guaranteed.
Second, DoS attacks can be performed from the Internet, by using data packets. Sending data packets (potentially with varying sources and protocols) to multiple idle mobile nodes, causes them to be paged and to wake up simultaneously, resulting in a signaling burst to the access network and AAA server (see below).

IV. Security Architecture for MOMBASA

Based on the security analysis, we developed a security concept that consists of three parts: packet filtering at access network boundaries, deployment of an AAA infrastructure and

securing of protocol operations with this infrastructure, and rate control for Denial-of-Service prevention.

A. Packet Filtering at Access Network Boundaries

To provide protection against injection of internal messages from external links, i.e. from the Internet and the last hop, packet filters have to be installed at the gateway and the access points. These packet filters can also be used to prevent a certain class of attacks with spoofed source addresses: Mobile source addresses may only appear from the direction of the last hop, non-mobile and non-access-network source addresses may only come via the gateway.

At the gateway, MOMBASA last hop messages and Paging Requests unless originated by the gateway itself should be dropped. When coming from the world interface, any message denoting a mobile (or access network) source address, MOMBASA signaling messages and any IGMP or PIM-SM message denoting a multicast address used internally by the access network should also be dropped.

At the access points, the following packets should be dropped when coming from the last hop: any packet denoting a non-mobile source address, Inter-MEP Advertisements, Paging Requests, Paging Updates and any IGMP or PIM-SM message denoting a multicast address used internally by the access network. MOMBASA last hop messages should be dropped when arriving at the upstream interface.

The following packets should only be originated but not forwarded by an access point, i.e. they should be dropped if they are arriving at an incoming interface: MEP Advertisements, MH Registration Replies, IGMP Membership Report, and IGMP Leave Group.

In general, the described filter rules do not protect mobile hosts against attacks. They are only meant to protect internal access network signaling from external attacks.

B. Trust Model

To offer service only to legitimated users, mobile hosts must be authenticated and authorized to use the service level they request. Signaling messages must be secured against forging and manipulation, critical content also against eavesdropping. For this reason, a security architecture employing symmetric cryptography (keyed hash functions, encryption) is deployed.

Core of the MOMBASA Security Architecture is the introduction of an AAA (Authentication, Authorization and Accounting) server for the administration of security associations.

The MOMBASA SE security architecture distinguishes between permanent and temporary (session) security associations. The following permanent security associations (SAs) based on shared secrets exist (see Fig. 2):

- $\mathbf{SA_{MEP:i,AAA}}$ Permanent security association between each MEP and AAA server.
- $\mathbf{SA_{GWP,AAA}}$ Permanent security association between gateway proxy and AAA server.

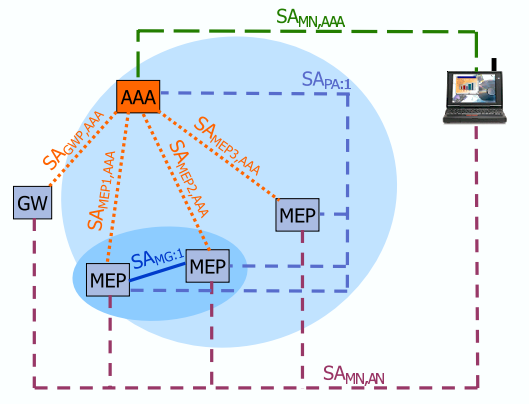

Fig. 2. Trust Model

- $\mathbf{SA_{GWP,MEP:i}}$ Permanent security associations between gateway proxy and each MEP.
- $\mathbf{SA_{MG:i}}$ Permanent security association for each MEP group, known only to the members of the group.
- $\mathbf{SA_{PA:i}}$ Permanent security association for each paging area known only to the members of the paging area.

For each mobile admitted to the access network a permanent security association $\mathbf{SA_{MN,AAA}}$ with the AAA server exists. During the initial registration process of a mobile host, the AAA server issues a temporary security association $\mathbf{SA_{MN,AN}}$ for the use between the mobile host and access network instances. For external customers, the local AAA may contact other AAA servers to establish a trust relationship. However, this is beyond the scope of this paper.

Although it is not strictly necessary to use predictive handover (involving membership of the multicast group and buffering) and predictive authentication at the same time, we will only describe the case where both are used.

C. Initial Registration

When entering the MOMBASA access network (e.g. when being turned on), a mobile host performs an initial registration. The message sequence for this operation can be seen in Fig. 3:

1) MEPs send regular MEP Advertisements containing a challenge to be repeated in a MH Registration Request to prevent replay attacks (see [8] for a similar approach). Without the challenge/response mechanism it would be possible for an attacker to snoop a valid (i.e. authenticated) MH Registration Request and replay it at another MEP or at a later time. With the mechanism an attacker could replay the request only at the same MEP as the legitimate mobile and only within a short time period effectively repeating the request in behalf of the legitimate user.
2) The mobile host sends a MH Registration Request containing the last challenge heard in a MEP Advertisement authenticated with $SA_{MN,AAA}$.
3) The MEP checks for the validity of the challenge. However, the MEP can not determine if the message was modified by an attacker. The MEP sends a Key Request

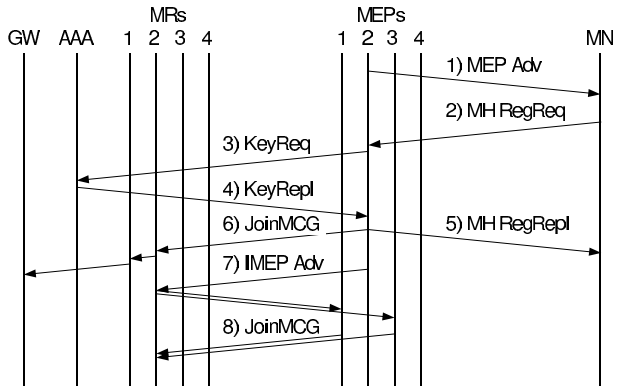

Fig. 3. MSC Initial Registration

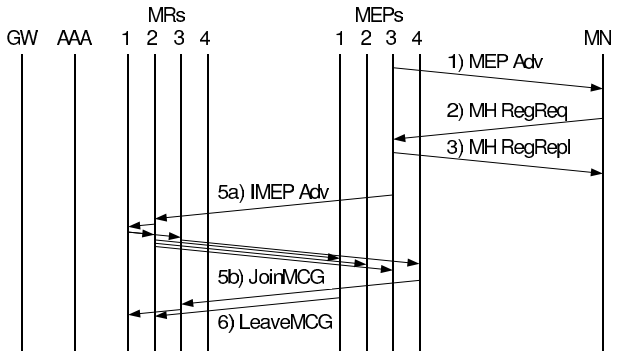

Fig. 4. MSC Handover

message to the AAA server containing the original request and additional changes to requested parameters (e.g. lifetime limited due to local policy). The message is authenticated with $SA_{MEP:i,AAA}$.

4) The AAA server checks the message authentication code (MAC) of the mobile's part of the message and the MAC created for the whole message by the MEP and verifies that the demanded services are allowed for the mobile according to its profile. It creates the session security association $SA_{MN,AN}$ encrypts the session key once with $SA_{MEP:i,AAA}$ and creates a MH Registration Response authenticated with $SA_{MN,AAA}$ and containing the session key encrypted for the mobile. The response is sent back to the requesting MEP.
5) The MEP forwards the MH Registration Reply contained in the Key Response, decrypts the session key and inserts the mobile into its database.
6) The MEP joins the mobile-associated multicast group and enables forwarding for the mobile.
7) The MEP inserts the mobile host, its service class and its session key encrypted with $SA_{MG:i}$ into the next Inter-MEP Advertisement sent to its neighboring MEPs multicast group.
8) When receiving the Inter-MEP Advertisement, neighboring MEPs will create a database entry of the mobile containing $SA_{MN,AN}$, join the mobile-associated multicast group and start buffering traffic for the mobile.

Securing messages with Message Authentication Codes (MACs), ensures that only legitimate users receive service and that messages can not be modified without detection. Encrypting sensitive information and using MACs within the access network protects against attackers that happen to be able to eavesdrop an internal access network link, unless they are able to compromise an access network node.

Rate control should be applied to initial registrations for Denial of Service prevention (see Sec. IV-I).

D. Handover

Handover to a new MEP is performed as follows (see Fig. 4):

1) The necessity for handover is detected by the mobile by receiving MEP Advertisements from a new MEP.
2) The mobile host sends a MH Registration Request containing the last challenge heard in a MEP Advertisement. As there is already an established session with the access network, the message is authenticated with $SA_{MN,AN}$.
3) Usually, the new MEP is one of the neighboring MEPs of the old MEP and thus already has the session key of the arriving mobile. Thus, it can check the MAC locally and generate a MH Registration Reply signed with $SA_{MN,AN}$. If the new MEP does not have an entry for the arriving mobile, failure will be indicated to the mobile, which has to perform an initial registration process in this case.
4) The new MEP enables forwarding to the mobile and flushes its buffer to compensate for packet loss during handover.
5) The operation continues as in the case of initial registration.
6) MEPs being neighbor of the old but not of the new MEP will leave the multicast group and delete the entry containing the security association when receiving the next Inter-MEP Advertisement of the old MEP no longer containing the mobile anymore.

E. Transition into Inactive State

The transition into inactive state (as described in Sec. II) happens as follows (see Fig. 5):

1) The mobile host sends a MH Registration Request with inactive flag set and authenticated with $SA_{MN,AN}$ to its current MEP.
2) The MEP checks the message and sends a Paging Update containing its paging area and the encrypted session key of the mobile authenticated with $SA_{GWP,MEP:i}$ to the Gateway Proxy (GWP).
3) The MEP leaves the multicast group and deletes the mobile entry.
4) The GWP checks the message and creates a paging entry for the mobile.
5) Neighboring MEPs will remove the mobile entry and leave the multicast group due to Inter-MEP signaling.

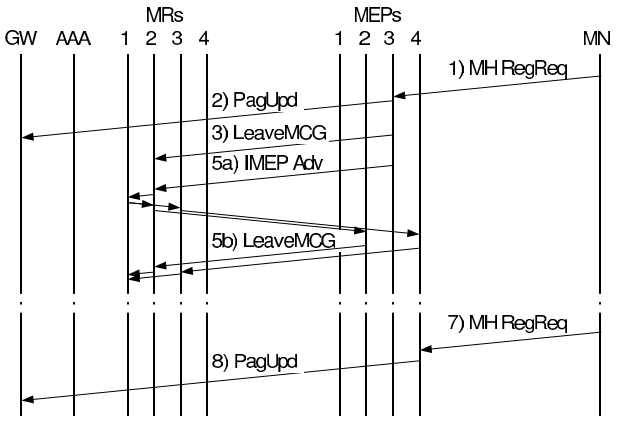

Fig. 5. MSC Transition into Inactive State and Paging Update

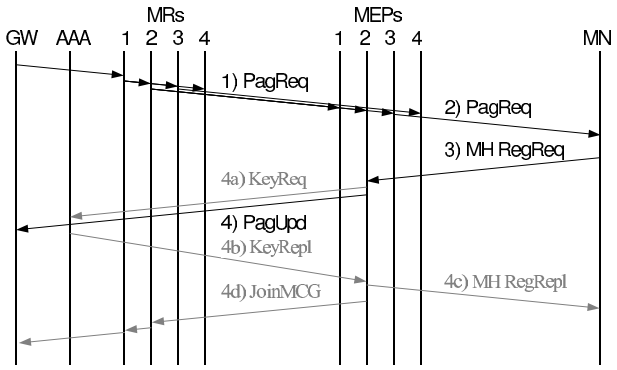

Fig. 6. MSC Paging

F. Paging Update

The idle mobile host refreshes its location regularly, although less frequently than in active state (see Fig. 5 for details):

1) The mobile sends an MH Registration Request with inactive flag authenticated with $SA_{MN,AN}$. As the MEPs are not holding any state concerning idle mobiles, the receiving MEP can not check the validity of the message. Rate control may be applied for such messages to avoid Denial-of-Service attacks against the GWP.
2) The message is forwarded as a Paging Update to the GWP and validated there. The paging entry in the GWP is updated.

G. Transition into Active State

Transition from inactive into active state may be triggered by two events: Either the mobile wants to send data, or data for the mobile arrives at the gateway. In the first case, an initial registration (see Sec. IV-C) is performed by the mobile, otherwise the mobile is paged by the gateway.

H. Paging

When data for an idle mobile arrives, paging is performed by the gateway (see Fig. 6):

1) The GWP multicasts a Paging Request authenticated with $SA_{MN,AN}$ and $SA_{PA:i}$ to the last reported paging area.
2) All MEPs in the paging area check the Paging Request strip off the $SA_{PA:i}$ authenticator, and forward it onto their last hops.
3) The mobile host verifies the Paging Request and performs an initial registration (see Sec. IV-C) with an additional wakeup flag.
4) Additionally to the operations of an initial registration, the MEP sends a $SA_{GWP,MEP:i}$-signed Paging Update with lifetime zero to the GWP.
5) The GWP verifies the Paging Update and completes paging.

I. Denial-of-Service Protection

An authentication service with its usually computationally expensive cryptographic operations may represent an attractive target for Denial-of-Service attacks.

The presented security architecture for MOMBASA has some features that prevent DoS attacks in certain cases. Since the authentication of the user in case of handover is performed decentrally at the MEPs, attacks against the central AAA server can be avoided and Denial-of-Service would have only local effects which can be caused by easier measures, such as jamming, anyway.

On the other hand, operations like the initial registration, the Paging Updates during idle periods and the wakeup sequence have to be performed via the AAA server as storing permanent shared secrets decentrally would impose a major vulnerability to the architecture.

As already described in Sec. III-B the paging of idle mobiles is vulnerable to DoS causing a burst of signaling load on the access network and especially on the AAA server. Detection of such an attack is hard, as varying spoofed source addresses, differing protocols etc. can be used.

To restore the symmetry between attacker and victim, so-called client puzzles have been proposed [9]. A client puzzle is a task for the client that needs some effort to answer for the client, but is easy to generate and verify by the server. The server refrains from processing a request until the client has solved the puzzle. One problem is, that in the case of a distributed Denial-of-Service the strength between attacker and victim may still be highly asymmetric and, what is worse, MOMBASA is designed to be transparent for the corresponding host, which is only required to be IP-capable but needs not support any mobility-specific signaling. Thus, there is no protocol that could be used to offer a client puzzle to the corresponding host without dropping this basic design constraint.

What can be done against such an attack, is rate control, e.g. by a token bucket algorithm, allowing for a certain average rate of requests and (if the bucket is full) for a burst of a certain number of requests.

Such a rate control can be achieved with the netfilter/iptables architecture present in standard Linux kernels. Table I shows

TABLE I
GATEWAY FILTER TABLES FOR DENIAL-OF-SERVICE PROTECTION

Main Table

#	Dir.	Src.	Dst.	Matches	Action
1	Inb.	Ext.	MH	`-m pool --dstpool active`	ACCEPT
2	Inb.	Ext.	MH	`-m limit --limit 10/s --limit-burst 2`	`-j idle`
3	Inb.	any	any	—	DENY

Table `idle`

#	Dir.	Src	Dst	Matches	Action
1	Inb.	any	any	—	`-j POOL --pool active --add-dst-ip`
2	Inb.	any	any	—	ACCEPT

the rules necessary to limit the number of data packets causing paging requests to 10 per second with a burst size of 20. Netfilter provides a module which allows IP addresses to be dynamically inserted into and removed from a pool of addresses within a certain range. This can be used to distinguish idle from active mobiles. Table I assumes a pool named `active` containing all mobile host addresses in the beginning with idle mobiles being removed from the pool by the GWP.

When an inbound data packet arrives at the gateway it is matched against rule no. 1 in the main table. If its destination address is contained in the pool `active` it will be accepted. Rule no. 2 is only reached by packets to idle mobiles. The rule may only match ten times per second with a burst size of twice the refresh rate, i.e. 20 packets (please note that `--limit-burst` is interpreted as a multiplier in contrast to the netfilter documentation). If the rule matches processing will continue in table `idle`. All other packets failing the activity check in rule no. 1 and the rate limit in rule no. 2 will match rule no. 3 and be denied.

Rule no. 1 in table `idle` causes the destination of the packet to be added to the pool `active` because additional packets to the same destination do not trigger another paging process but are buffered in a ring buffer by the GWP. Thus, they may be treated by the packet filter in the same way as packets to active mobiles. Rule no. 2 causes the data packet triggering the paging process to be accepted.

The operations affected by rate control are not time-critical (initial registration usually only happens when first entering the network, paging normally at the beginning of a communication session, Paging Update messages report mobile's position only coarsely anyway). Thus, a certain delay due to rate control on high load is acceptable. Of course, if a Denial-of-Service attack is ongoing, legitimate users are affected also, but only for the operation used for the attack. Therefore, the DoS attack that would otherwise affect the whole access network and all users in it is limited to only part of the users, i.e. to inactive users and users trying to perform an initial registration, respectively.

J. Securing Access Network Infrastructure

Assuming that the access network has a limited inherent protection against tampering (it is usually controlled by a single authority, the infrastructure is often wired and protected by buildings or buried below the surface), this security architecture concentrated on securing the interfaces to the external world, i.e. the last hop and the Internet. Only critical messages (e.g. the ones carrying session keys) are authenticated and encrypted. Where this is not appropriate, a standard VPN solution such as IPsec [10] could be deployed to secure the links between MEPs, Multicast Routers (see [11] on how to secure the multicast routing protocol PIM-SM) and Gateway. Since the access network infrastructure is fixed (even in the presence of radio links, the peers stay the same), this imposes no challenges related to host mobility.

V. SECURITY DISCUSSION

Summarizing, the proposed security concept prevents the threats identified in Sec. III-B as follows: T1 is prevented by packet filtering at access network borders (Sec. IV-A), provisions against T2 are discussed in Sec. IV-J, T3 is dealt with by introducing a trust model and securing messages with MACs (Sec. IV-B- IV-H) and finally T5 is discussed in Sec. IV-I. No special measures have been taken against T4, but as was already mentioned in Sec. III-B, false access points can be unmasked later-on, as they are not able to obtain a valid session key from either the AAA server or the neighboring MEPs.

To facilitate seamless handover, confidential information such as key material must be distributed to avoid a high handover latency due to signaling to a centralized AAA server. To reduce the risk induced by a decentralized architecture, temporary SAs are used. The architecture assumes trustworthy MEPs. If a MEP is compromised, all sessions of mobiles registered in its neighboring MEPs are compromised. However, permanent mobile keys are safe, since they are only stored at mobiles and AAA server and never given away to access network instances. Of course, if the AAA server is compromised, the whole architecture is compromised.

VI. EXPERIMENTAL TESTBED

We extended the existing MOMBASA Software Environment to support the challenge/response mechanism in the MEP Advertisements, initial registration via a simple (local) AAA server [12] and predictive authenticated handover via Inter-MEP Advertisements. The libgcrypt [13] was used for the cryptographic algorithms (namely AES for encryption and HMAC-SHA1 [14] for MACs).

The testbed setup can be seen in Fig. 7. We used IEEE 802.11 WLAN as access technology. The multicast router and the gateway were hosting PIM-SM routing daemons. To facilitate synchronization of sending of samples and triggering of handover, correspondent and mobile host were co-located. Address translation is used to enforce that packets indeed leave the correspondent host via the wired interface, traverse the

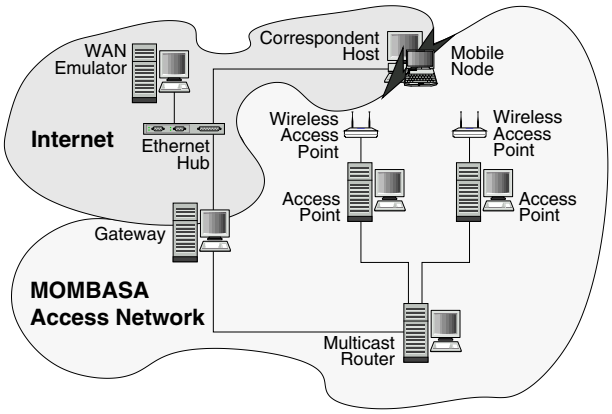

Fig. 7. Testbed setup

testbed and enter the mobile host at the wireless interface. To emulate the Internet, we used the NistNet WAN emulator [15].

To evaluate the impact of the security measures on handover performance, we sent short VOIP samples across the testbed and performed handover between two WLAN access points during the transmission. We measured handover latency, packet loss and packet duplication for MOMBASA predictive handover with and without security enhancements, when flushing the last 0 to 400ms of data to the mobile after handover. The WAN emulator was configured to emulate a route between Germany and Sweden.

The measurements resulted in no significant difference between predictive handover with and without security, so we omit figures and detailed tables of results at this place. The neglectable difference is not very astonishing as the handover latency of about 250ms is highly dominated by the link layer handover latency and the time to detect an IP-layer advertisement. The only difference between secured and unsecured handover lies in two HMAC-SHA1 calculations, which lies in the order of several microseconds.

Only initial registration, wakeup and handover to an unexpected access point require signaling to an AAA server. Otherwise, the session SA of the mobile is already present at the new MEP.

VII. Conclusion

In this paper, we analyzed threats to the IP-based mobility support architecture MOMBASA and its protocol operation. Based on the results of this analysis, we described a security architecture consisting of the following three main parts:

1) *Packet filtering at the gateway and the access points* provides protection against injection of internal messages and source spoofing attacks from the Internet and the last hop.
2) *Introduction of a local AAA server* for managing trust relationships between AAA server and access network instances/mobiles, respectively, and among access network instances. The AAA server issues temporary security associations for the use between the access network and the mobile to protect signaling operations. Session keys are sent by multicast to potential future access points in advance.
3) *Performing rate control on operations that require processing of signaling messages at central entities* provides protection against DoS attacks. This rate control can, for example, easily be implemented on a standard Linux operating system using the netfilter/iptables architecture.

Furthermore, due to the decentralized architecture the properties of seamless handover are preserved and the AAA server is disburdened, since authentication of active and registered mobile nodes can be performed locally at the access points.

References

[1] A. Festag, L. Westerhoff, and A. Wolisz, "The MOMBASA Software Environment – A Toolkit for Performance Evaluation of Multicast-Based Mobility Support," in *Proc. of Performance Tools 2002*, London, GB, Apr. 2002, pp. 212–219.
[2] P. Lescuyer and F. Bott, *UMTS: Origins, Architecture and the Standard*. Springer Verlag, 2003.
[3] C. Perkins, "IP Mobility Support for IPv4," Internet RFC 3344, August 2002.
[4] D. Forsberg, J. T. Malinen, T. Weckstroem, and M. Tiusanen, "Distributing mobility agents hierarchically under frequent location update," in *Proceedings of Sixth IEEE International Workshop on Mobile Multimedia Communications (MOMUC'99)*, San Diego, CA, USA, 1999, pp. 159–168.
[5] A. Festag and L. Westerhoff, "Protocol Specification of the MOMBASA Software Environment," Telecommunication Networks Group, Technische Universität Berlin, Tech. Rep. TKN-01-014, Oct. 2001. [Online]. Available: http://www-tkn.ee.tu-berlin.de/publications/papers/tr_01_014.pdf
[6] L. Westerhoff and A. Festag, "Implementation of the MOMBASA Software Environment," Download at http://www-tkn.ee.tu-berlin.de/research/mombasa/mse.html.
[7] G. Schäfer, *Security in Fixed and Wireless Networks*. John Wiley & Sons, 2003.
[8] C. Perkins and P. Calhoun, "Mobile IPv4 Challenge/Response," Internet RFC 3012, November 2000.
[9] C. Dwork and M. Naor, "Pricing via Processing-or- Combatting Junk Mail," pp. 139–147, 1993, Lecture Notes in Computer Science (LNCS) No. 740.
[10] S. Kent and R. Atkinson, "Security architecture for the Internet Protocol," Internet RFC 2401, November 1998.
[11] B. Fenner, M. Handley, H. Holbrook, and I. Kouvelas, "Protocol Independent Multicast - Sparse Mode (PIM-SM): Protocol Specification (Revised)," Internet Draft, February 2004, work in progress.
[12] S. Glass, T. Hiller, S. Jacobs, and C. Perkins, "Mobile IP AAA Requirements," Internet RFC 2977, October 2000.
[13] Free Software Foundation, "libgcrypt," Download at http://www.gnu.org/directory/security/libgcrypt.html.
[14] H. Krawczyk, M. Bellare, and R. Canetti, "HMAC: Keyed-hashing for message authentication," Internet RFC 2104, February 1997.
[15] National Institute of Standards and Technology, "NIST Net – A Network Emulation Package for Linux," Download at http://snad.ncsl.nist.gov/itg/nistnet.