Technical University Berlin

Telecommunication Networks Group

Rationale, Design and Functionality for Secure, QoS-enabled Mobility Support in All-IP Networks – the SeQoMo Approach

Tianwei Chen, Andreas Festag, Axel Neumann, Sven Hermann,
Holger Karl, Günter Schäfer
[chen,festag,neumann,hermann,karl,schaefer]@tkn.tu-berlin.de

Berlin, 03/2003

TKN Technical Report TKN-04-012

TKN Technical Reports Series

Editor: Prof. Dr.-Ing. Adam Wolisz

Abstract

This document describes the Secure, Quality of Service (QoS)-enabled Mobility (SeQoMo) approach addressing the issues of optimization of handover operations, low-latency QoS re-establishment for IP-level handover, authentication, QoS-aware authorization and Denial of Service (DoS) attack protection. This work [1] presents the rationale, design and functionality of this approach in a coordinated framework.

[1]This work has been supported by Siemens AG, ICM N PG SP RC in the context of the project “Mobility in Multi-Domain, Multi-Technology, IP-based Network”.

Contents

List of Figures

List of Tables

Chapter 1

Introduction

The combined effects of plummeting equipment costs, liberalization of the telecommunications sectors, and the expanding array of technologies able to exploit new areas of the radio frequency spectrum have produced a dynamic but relatively immature field where clear answers are often not yet available. The rapidity of developments has resulted in many differing schools of thought who have not yet reached agreement on the most appropriate way to make use of these new communications systems.

The developed technologies such as Wireless Local Area Network (WLAN), Bluetooth, Hiperlan or even IrDA provide ways to liberate the tethered devices and let them go wireless. The devices can set up a connection with an access point and move around freely without losing connectivity.

To ensure normadic wireless access, the movement over distances exceeding coverage of a single access point should not interrupt the consecutive sessions. The sessions should be handovered from one access point to another. Many solutions have been proposed aiming at challenges posed by wireless communications.

Mobile IP (MIP) [11] is one of them to enable IP-based Internet services to a mobile node. Since the wireless link may have a substantially lower bandwidth and higher error rate than traditional wired networks, as well as mobile nodes are likely to be battery powered, and minimizing power consumption is important, the number of administrative messages sent over the link by which a mobile node is directly attached to the Internet should be minimized, and the size of these messages should be kept as small as is reasonably possible.

1.1 Background

While Mobile IPv4 (MIPv4) [11] and Mobile IPv6 (MIPv6) [31] are designed for mobility management in IP networks, they result in high latency and signaling overhead during handover. Therefore, advanced mobility mechanisms improving Mobile IP are desirable to perform efficient handovers. Also, appropriate QoS support is needed for mobility-enhanced Internet Protocol (IP) in order to meet end users' expectations. QoS support should be in an end-to-end way, i.e., both wireless and wired parts that serve a mobile communication should support and maintain the required QoS for communicating peers, in particular, during and immediately after handover. However, this is not sup-

ported by current MIP. In this context, the Internet Engineering Task Force (IETF) is developing the requirements for a QoS solution for MIP [7]. Furthermore, security measures are required to protect network infrastructure. The provision of the Authentication, Authorization, Accounting (AAA) service in a mobile environment [4] [14] will require inter-domain exchange of AAA information, which is essential to provide access services and resource usages within the visited domain. However, the Diameter processes do not address the low-latency feature in either inter-domain handovers or intra-domain handovers.

1.2 Project Goals

This project focuses on the Secure, QoS-enabled Mobility (SeQoMo) architecture addressing the above issues concerning IP mobility. Figure 1.1 shows the goals of the SeQoMo project.

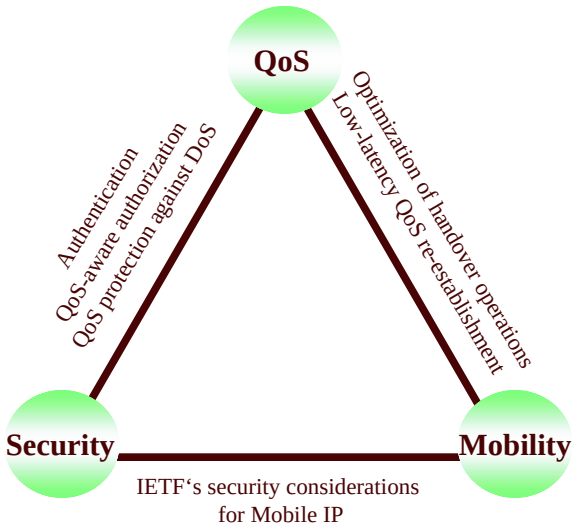

Figure 1.1: Goals of the SeQoMo project

- *Optimization of handover operations and low-latency QoS re-establishment for IP-level handover.* In addition to basic mobility support (location management and handover), support of horizontal (intra-technology) as well as vertical (inter-technology) handover is desired. Furthermore, signaling overhead caused by mobility support as well as service interruption and packet losses caused by handover should be minimized.
  Traffic flows should obtain QoS treatment as soon as the packet flow as such has been (re-) established after a handover, while additional signaling traffic overhead should be kept low. In addition, a handover to a particular Access Router (AR) should not be performed if minimal QoS requirements can not be met along such a new path that the user receives a service quality lower than e.g., that he is willing to pay for. It is also desirable for higher layers to know if a path is unable to provide required QoS.

- *Security considerations.* The security considerations lie in the following aspects:

- *Authentication.* The visited network should verify the MN's identity in both inter-domain handover (including power-up) and intra-domain handover cases.
- *Authorization.* The visited network should control the resource consumption by the MN according to the total amount of resources which the MN is entitled to use.
- *QoS protection against Denial of Service attacks.* In an access network, a mobile user sends a request to an access point for a QoS. If there is no security check on QoS requests, attackers can also send requests to reserve resources. Extensive bogus requests from attackers could reserve all resources along a path so that this path has no available resource for any legitimate users. This threat is a kind of DoS attacks.

  Therefore, when an access point receives a QoS request, it must perform an security check. If the access point communicates with an local security entity (e.g. a local AAA server) for authentication and authorization checks, it is obvious that the propagation delay for this signaling is unfavorable for a fast handover. Furthermore, the same checks have to be done to the requests from attackers. Thus, intensive and extensive bogus requests may degrade substantially the signaling capacity of the access network including a path and the local AAA server. This is another kind of DoS attacks.

The goal from the security considerations is to avoid these threats and support the optimization of handover operations and low-latency QoS re-establishment for IP-level handover.

1.3 Steps To Achieve The Project Goals

The steps to realize the projects goals are the following:

- Start with a "state of the art" analysis
- Identify requirements and open issues
- Collect required building blocks: chose existing approaches and concepts to meet requirements; and develop concepts to resolve open issues
- Integrate the chosen and developed concepts into one unified architecture
- Evaluate developed approach by simulation and measurement on a prototype testbed
- The above process is not a linear but an iterative one and it has to take into account current developments (new ideas, standardization, etc.)

Chapter 2

Architecture

This chapter presents the requirements for the project goal, the assumption and the architecture of the project.

2.1 Requirements

The requirements of the three components (Mobility, QoS and Security) are explained separately in the following sections.

2.1.1 Mobility

In addition to basic mobility support (location management and handover), the following requirements have been identified:

- Support of heterogeneous end systems (palm-tops, notebooks, etc.) and heterogeneous access networks (The Institute of Electrical and Electronics Engineers (IEEE) 802.11, General Packet Radio Service (GPRS), etc.);
- Support of horizontal and vertical (inter-technology) handover;
- Minimal signaling overhead caused by mobility support;
- Minimal service interruption and packet losses caused by handover.

2.1.2 QoS

The requirements for QoS support for handover are as follows:

- Support for traffic flows to obtain QoS treatment as soon as the packet flow as such has been (re-) established after a handover;

- Minimal additional overhead (e.g., signaling traffic);
- Ability to inform higher layers in case of inability of QoS support in a path;
- Ability to choose an access point that is best suited from the QoS perspective.

2.1.3 Security

The security requirements in this context are:

- When an MN enters an access network or it powers up, the network needs to authenticate it before granting rources or providing services : “who is the mobile node is trying to register?”
- The access network also needs to authorize QoS requests from the MN: “what resources or services is the MN allowed to use”.
- The access network should prevent adversaries from reserving resources for malicious purposes with bogus QoS requests.
- The whole security operations should not take long time to contribute non-trivial latency to the (re-)registration procedures.

2.2 Assumptions

This section lists some general assumptions about the network architecture for the project:

- We assume a cellular network in which different radio cells will generally be addressed in different IP subnetworks, each one under the control of one foreign agent (or another mobility supporting device). This implies, for example, that a handover from one Base Station Controller (BSC) to another one will result in a handover-operation in the IP layer and the Mobile Node (MN) will change its temporary IP address (Care-of Address (CoA)).
- However, if a specific technology allows to address multiple radio cells within a single IP address space (e.g. a GPRS-like architecture), this might interoperate with our approach with the mobility within this subnetwork being “invisible” to the protocol functions developed in the context of this project.
- An eventually existing hierarchy of cells (macro- / micro- / pico-cells), e.g. motivated by the underlying link-layer technology, will quite probably not be reflected in the IP addressing scheme in order to avoid fragmentation of IP address space.
- We assume the IP networks are composed of multiple domains, each of which can provide some QoS mechanism, e.g, Differentiated Services (DiffServ) [1] or Multi-Protocol Label Switching (MPLS).

- We assume that the visited network authenticates an MN when it receives a (re-)registration request from an MN. Normally, the network needs to perform an authorization check to ensure that the MN has right to access the requested resources before the network grants access to the MN. In brief, authentication and authorization are prerequisities for a successful reservation and guarantee.

2.3 Architecture Overview

To reach the goals, SeQoMo exploits the following capabilities:

- Hierarchical Mobile IPv6 (HMIPv6) [41] with enhanced mobility management by using layer-2 trigger;
- QoS signaling for mobile hosts through the QoS-conditionalized handover scheme;
- protection for mobile communications by extending the Diameter MIPv6 extension with QoS-enabled mobility support in HMIPv6.

As shown in Figure 2.1, the SeQoMo architecture framework is a joint architecture of HMIPv6 and AAA components.

In Hierarchical Mobile IP, the Mobile Anchor Point (MAP) will receive all packets on behalf of MNs it is serving and will encapsulate and forward them directly to the MN's current address (Local Care-of Address (LCoA)). In the QoS-conditionalized binding updates approach, each QoS request is to be checked and forwarded hop-by-hop from AR to the switching MAP. The hierarchy includes AR and the MAP.

In the basic model of AAA servers, the local AAA server (AAAL) is the local AAA server which is the local authority to perform AAA functions in the visited access network while home AAA server (AAAH) standing for the home AAA server is MN's home authority which knows the MN's specific authorization data in a user profile. AAAB is the broker authority which is used for managing trust relationships among AAA servers and relaying authorization messages between AAAL and AAAH. It is possible, but not mandatory for the network with Corresponding Node (CN) to have an AAAL.

In the HMIPv6 and AAA joint architecture, SeQoMo consists of three functional components:

- an IP-level handover assistant (IHA), which improves the handover performance by a layer-2 trigger and initiates a secure, QoS-aware handover process upon detection of an MN movement;
- a QoCoo controller (QHC), which performs an efficient QoS signaling by way of piggybacked QoS object(s) in the binding messages and QoS-conditionalized the handover process; and
- a QoS-aware security entity (QSE), which provides authentication and QoS-aware authorization services when an MN sends QoS requests to the visited network.

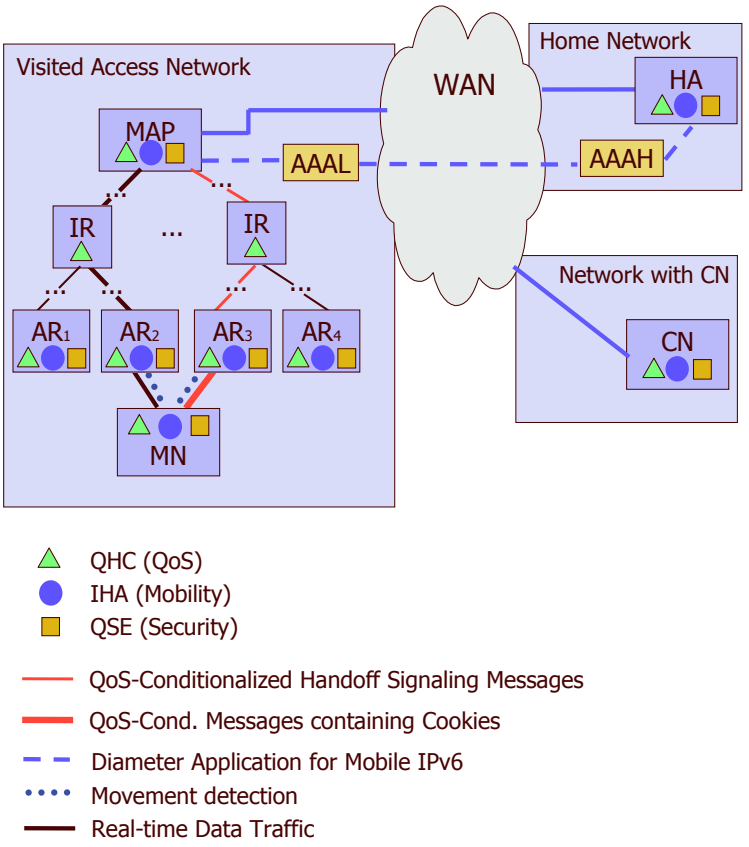

Figure 2.1: The SeQoMo architecture

2.3.1 IHA

In general, we differentiate between global and local mobility support. Local refers to mobility support between access points belonging to the same access network, whereas global means mobility support between different access networks. Hierarchical Mobile IPv6 is a scalable and efficient solution to improve local mobility for Mobile IPv6, however, it does not explicitly provide mechanisms for fast detection of MN movement.

The IHA in the SeQoMo architecture extends the HMIPv6 with fast detection of MN movements based on layer-2 (L2) information to assist the IP-level handovers. The discussion on Fast Handovers for Mobile IPv6 and L2 triggers is covered in [35].

After the IHA obtains the knowledge of layer-3 (L3) information (the IPv6 address of the new AR as well as of the MAP) assisted by the L2 trigger, it initiates the QHC and the QSE processes (as described below) and will finalize a handover upon positive results from the QHC and the QSE processes.

2.3.2 QHC

When several access points are available to an MN, it would be desirable for the MN to maintain an existing QoS assurance during handover but at the same time to conditionalize its handover upon the availability of sufficient QoS resources along a new network path through another access point. Thus, QoS-conditionalized a handover upon the ability of providing required QoS in a new potential path (detected by the IHA) would be desirable. On the other hand, to overcome the long latency of QoS-re-establishment introduced by RSVP-based approach, a mobility-piggybacked QoS signaling scheme would be beneficial.

This is done by the QHC. Triggered by the IHA, the QHC transfers QoS information required by mobile nodes along the new potential path, and ensures that QoS requirements can be met after a handover (if this is at all possible, depending on the network situation the mobile is faced with after moving around). Note that the design for the QHC is to provide a generic means for signaling a mobile node's QoS requirements to the QoS-aware routers during handovers, the actual resource reservation process is out of scope and relies on underlying QoS provisioning models such as Integrated Services (IntServ), DiffServ or MPLS.

In order to do so, the QHC checks the resource availability in the QoS controllers (entities responsible for interpreting the user QoS parameters, optionally inserting/modifying the parameters according to local network QoS management policy, and invoking local QoS provisioning mechanisms [3]) along the path, influences handover decisions and security policies. A detailed description of QoS-conditionalized handover scheme can be found in [25].

The QoS components in the intermediate QCs interpret the QoS information combined in the QoS-conditionalized binding update/acknowledgement messages to the internal resource reservation mechanisms and finds or makes appropriate changes when necessary. Particularly, the QoS components in the AR will inquire the security component for whether to reserve resources in the rest of path.

The QHC in the MAP (in case of local movement) or the HA/CN (in case of global movement) performs a handover provided that the following conditions are met: QoS requirements in the route that the QoS-conditionalized binding update message travels are met and the QSE agrees to use requested QoS. If this succeeds, the QHC in the MAP will initiate a tear-down process (regarding QoS reservations) in the old path (optionally after some small delay, in order to allow the MN to smoothly switch to the new path).

2.3.3 QSE

The QSE provides authentication and authorization services when mobile nodes demand services with different QoS requirements in a visited network.

The QSE in the MN incorporates necessary security information in the registration message to initiate the (re-)authentication and (re-)authorization process, which is integrated with the binding update processes.

In the global movement (i.e., inter-domain) or power-up case, after processing the BU at MAP, the QSE sends an AA-Mobile-Node-Request (AMR) message which includes necessary Attribute Value Pairs (AVP)s to AAAL. The AAAL gets to know which is the MN's home domain from the MN's

network access identifier (NAI) and forwards the AMR to the MN's AAAH. The AAAH authenticates the MN and authorizes the MN's QoS request based the MN's authorization data in its service level agreement. Optionally after locating the HA and performing a handover at the HA or the CN, the AAAH responses an AA-Mobile-Node-Answer (AMA) message to the AAAL. Then the AAAL forwards the AMA to the QSE.

After the first registration procedure is successfully complete, the associated AR grants the MN a cookie for the purpose of preliminary authentication check in its next local movement.

In the local movement case, since the authentication and authorization data is already cached in the AAAL after its first registration in the visited domain, the re-authentication and re-authorization can be done locally at the AAAL without involving the AAAH to reduce the latency caused by traversing backbone networks.

In order to achieve the seamless local movement and prevent DoS attacks, an AR verifies the cookie after receiving a re-registration request. If the verification passes, the AR starts the QoS-Conditionalized Binding Update (QCB) process and re-authentication and re-authorization process.

2.4 Component Interactions

The integration of the mobility, QoS and security components in the SeQoMo framework involves the protocol interactions in related network elements. The following section describes the interactions of three components of SeQoMo architecture in different network elements.

2.4.1 Mobile Node

In the MN, QoS component obtains the security information (including cookie when exists) from the security component and composes QoS option. When detecting a movement or power-up, mobility component notifies the QoS component to initiate the joint process of authorization and QoS-conditionalized BU.

When a registration acknowledgement message arrives, the QoS component gets to know how its QoS request is satisfied; if so, it triggers the mobility component. A cookie and the (re-)authentication and (re-)authorization results are sent to the security component.

2.4.2 Access Router

In the AR, the QoS component checks whether there is a cookie in the registration message. If no, it disables reservation function (i.e., only remain the finding function in the rest of path) of the QoS option. If yes, the cookie is delivered to security component and a computation result (based on cookie-related information) - success or fail - will be returned. In case of fail, the registration request message will be marked as security check failure (and possibly directly sent back to the MN). If the security check is passed, the QoS component continues the binding update process.

2.4.3 Mobility Anchor Point

In the MAP, if a binding request received is destined to the MAP, the security component checks whether the security policy (through AAAL even perhaps AAAH - in case of inter-domain movement) can accommodate the QoS request. In case the QoS can be fulfilled (or the unfulfilled QoS can be tolerated) and security policy allows, the mobility component does the handover, then replies to the MN with a registration acknowledge message (along with a cookie generated by the security component), with the type of QoS option is marked as reservation; meanwhile the security component should also send a cookie to the security entity in the MN. A cookie key should be periodically distributed by the MAP to all the security component in ARs to verify the cookie(s).

2.4.4 Home Agent / Correspondent Node

In the HA/CN, upon receipt of a registration request, the security component checks whether the security policy (through AAAH) can accommodate the requested QoS. In case the QoS request can be fulfilled (or the unfulfilled QoS can be tolerated) and security policy allows, the mobility component does the handover, then replies to the MN with a registration acknowledgement message.

Chapter 3

Mobility

At the initial stage of the project, the current development and trends in handover design for All-IP wireless networks were studied [21]. The issues and requirements of QoS and security support result from the mobility study. Therefore, we first discuss the mobility components of the SeQoMo in this chapter, then we will discuss QoS and security in the following chapters.

3.1 Problems

Handover describes a mechanism in cellular networks that transfers the association of a mobile end system from one access point - which is presently active - to a new access point. In general handover is applied when a user moves through the coverage area of a cellular network and crosses cell boundaries. The handover between wireless cells of the same type (in terms of coverage, data rate and mobility) is often referred to as horizontal handover, whereas the handover between wireless cells of different type is characterized as vertical handover. Traditional IP-based mobility approaches, such as IETF Mobile IP, were designed with respect to horizontal handover. Thus, the vertical handover and other new services and network architectures pose new requirements on handover design. Nevertheless the fundamental mobility problem in IP based networks still remains: IP protocols were designed for stationary end systems. The IP address of an end system identifies a host uniquely and also the IP subnet to which the host is attached.

Therefore the meaning of the IP address is twofold: end point identification and location identification. When a host changes its point of attachment the IP address must be modified in order to route packets to the mobile's new subnetwork. Unfortunately, ongoing TCP connections break since the IP address is part of the Transmission Control Protocol (TCP) connection identifier and used at TCP connection setup. Also, UDP sessions are interrupted since the IP addresses are used for communication establishment in the mobile host as well as the correspondent host.

Handover has received considerable attention in recent years. Foremost a number of system-specific solutions have been developed for Global System for Mobile Communication (GSM), GPRS and Universal Mobile Telecommuniation System (UMTS) networks, for mobile extensions of Asynchronous Transfer Mode (ATM) networks, as well as for wireless LANs, such as IEEE 802.11 networks. From

the Internet point of view these solutions can be regarded as layer 2 solutions for wireless access networks working transparently to the IP layer.

3.2 State of the Art Analysis

In this section recent research-oriented handover approaches are described:

- IETF Mobile IPv4
- Extensions of IETF Mobile IPv4
- IETF Mobile IPv6
- Reverse Address Translation (RAT)
- Multicast-Based Handover
- Handoff Aware Wireless Access Internet Infrastructure (HAWAII)
- Cellular IP
- Mobile People Architecture
- Internet Core Beyond the Third Generation (ICEBERG)
- Extended Session Invitation Protocol (SIP) Mobility.

In order to work out the basic assumptions behind the schemes, the description is organized according to the following structure: Motivation to develop a new approach; Addressing concept; Required mobility infrastructure; Routing of packets; Handover, in particular vertical handover; Advantages and drawbacks of the approach. Details refer to [20, 21].

Table 3.1 gives a summary of these approaches.

3.3 Design Rationale, Approach and Steps on Mobility

Resulting from the state of the art analysis, we realize the design rationale, goals, approach and steps for the mobility research.

In addition to basic mobility support (location management and handover), the following requirements have been identified:

- Support of heterogeneous end systems (palmtops, notebooks, etc.) and heterogeneous access networks (IEEE 802.11, GPRS, etc.)
- Support of horizontal and vertical (inter-technology) handover;
- Minimal signaling overhead caused by mobility support;

General functions	Basic Mobile IPv4 *(v6)*	Mobile IP with Hierarchical FA	MosquitoNet's Extended Mobile IP	Multicast-based handover	RAT	Cellular IP	HAWAII	Mobile People Architecture	ICEBERG	Extended SIP Mobility
Detection of new link availability	FA advertisement / soliciation *(router)*	Similar to basic Mobile IP	Similar to basic Mobile IP	IGMP advertisement by multicast router	Access network specific	Access network specific	Access network specific	Dependent on policy	Dependent on policy	Access network specific
Registration	At FA and HA *(At HA)*	At FA(s) and HA	At HA (Co-located FA)	Multicast join operation	At registration server in home network	Once at HA, route update for active hosts	Once at HA, path setup for active hosts	At MPA's personal proxy	At preference registry	At SIP Server
Registration update	Registration and binding update at HA *(and CHs from BU list)*	Regional registration at FA(s)	Similar to basic Mobile IP	Multicast join-/leave-operation	At registration server in home network	Route update towards the gateway router	Path setup update for active hosts towards Domain Root Router	At MPA's personal proxy	At preference registry	At SIP Server
Database for location information	Registration table in Home Agent *(and binding cache in CHs)*	Registration table in HA and tables in FAs	Similar to basic Mobile IP	Distributed in multicast routers	Registration server	Routing and paging caches	Host-based routing table entries and paging caches	Personal Proxy	Preference registry, naming server	SIP server
Address translation	Encapsulation	Encapsulation	Similar to Mobile IP or direct communication	None	NAT	None	None	Directory service	Directory service	Via SIP server
Rerouting node	HA in home network *(or CH directly)*	Switching FA in visited domain	Similar to basic Mobile IP	Multicast router close the base station	Registration server in home network	*Inter domain:* Home Agent *Intra domain:* Node close to mobile	*Inter domain:* Home Agent *Intra domain:* Router close to mobile	MPA's personal proxy	ICEBERG Access Point (IAP)	CH / Mobile
Support of user mobility	NAI extensions	Similar to basic Mobile IP	Similar to basic Mobile IP	No	No	No	No	Yes	Yes	Yes
Support of multiple interfaces in mobile	Yes, with multiple IP addresses	Similar to basic Mobile IP	Yes, with multiple IP addresses	Yes, with same IP multicast addresses	No	NA	NA	Yes	Yes	Yes
Simulcasting to multiple base stations	Yes, with Simultaneous Binding Option	Similar to basic Mobile IP	Yes, simultaneous binding and flow-to-interface-binding in additional to basic Mobile IP	Yes	No	Yes	No	No	No	No
Differentiation of active and idle hosts	No	No	No	No	No	Yes, paging for idle hosts	Yes, paging for idle hosts	No	No	No
Differentiation between state-full and state-free sessions	No	No	No	No	No	No	No	No	No	No
Location privacy	Yes	Yes	Selectable	Yes	Mobile initiated sessions: No CH initiated sessions: Yes	Yes	Yes	Yes	No	Yes

Table 3.1: Comparison of handover approaches with respect to general functions

- Minimal service interruption and packet losses caused by handover.

For mobility support three basic assumptions have been made: First, the components of the system (router, gateway, access points and mobile) are IP capable. Second, host mobility is supported at network level. Third, different solutions are used for global and local mobility support: mobility between access networks is referred to as global mobility, whereas local characterizes mobility within an access network. This differentiation offers the opportunity to utilize mobility mechanism and protocols which are more suitable for certain requirements.

In the SeQoMo architecture, two approaches for local mobility support will be utilized: Address translation and tunneling (IETF Mobile IP) and Multicast addressing and routing (Mobility Support - A Multicast Based Approach (MOMBASA)) [23]. Both options use and augment IETF Mobile IP for global mobility support.

3.4 Hierarchical Mobile IP

Originally, the TCP/IP based Internet technologies were designed for wired networks with mostly fixed hosts. The Internet Protocol (IP) routes packets to their destinations according to the network prefix part of their IP addresses. And these IP addresses identify the network to which a host is attached. Additionally, a host is uniquely identified by the IP address. This identification is used to establish communication between hosts by means of a socket interface. When a host becomes mobile and changes its point of attachment, the network prefix of the IP address can change. This in turn requires the re-establishment of ongoing communication relations between hosts and affects adversely the communication service. Particularly, the TCP connection will be disrupted and must be re-established.

To solve this problem, MIP [11] extends IP by allowing the mobile host to effectively utilize two IP addresses, one for host identification and the other for routing. When a mobile host moves to a new location, it registers its current care-of-address (e.g. in Mobile IPv4 the address of the foreign agent it connects to) with its home agent, which is attached to its home network. A host in the Internet sends packets to the mobile host s home address. The home agent intercepts the packet, translates the address(es) by means of IP encapsulation and tunnels the packet to the mobile host via the foreign agent. Mobile IPv4 [12] and Mobile IPv6 [32] are based on same principles. For Mobile IPv6 the basic scheme is extended by mechanisms for address configuration and route optimization. In this study the focus is on Mobile IPv4, nevertheless many statements can be generalized to Mobile IPv6, also.

However, Mobile IP faces several performance problems. Foreign agents providing small cells and fast moving mobile hosts result in frequent handovers between the access points and require the attached foreign agent to register with a home agent for each of such local handovers. Even when the foreign agent is distant from the home agent, frequent handover cause high overhead and further aggravates packet loss. While handover messages are transported to or from the home agent, the mobile host is not connected to the Internet.

Mobile IP with hierarchical foreign agents [24] [26] is an extension of standard Mobile IP to meet the requirements of high mobility. The solution distributes the functionality of the Mobile IP foreign

agents to multiple instances arranged in a hierarchy. This enables localized location updates in order to reduce frequent location updates to the home agent.

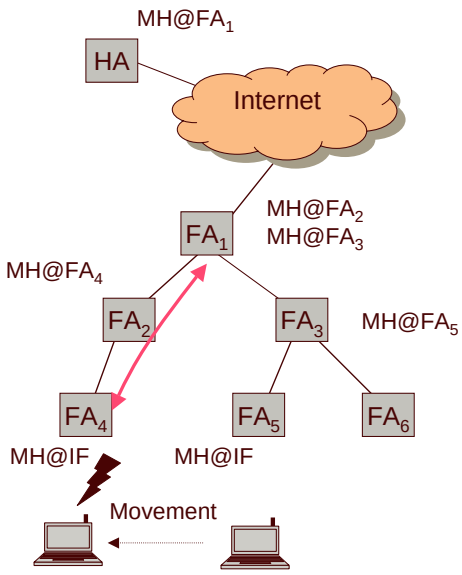

Figure 3.1: Hierarchy of Foreign Agents

Figure 3.1 shows a picture of hierarchy of foreign agents. The Lowest Foreign Agents send announcements which include the own address and the address of the next higher level (and possibly all other levels including the Highest Foreign Agent). When a mobile first arrives at a visited domain, it sends a registration request to the Lowest Foreign Agent which creates an unacknowledged binding update and forwards the registration request upwards to the next higher Foreign Agent.

When a handover occurs the mobile generates a registration request which is forwarded by the Lowest Foreign Agent. At some point the Switching Foreign Agent receives the request and detects that a binding update already exists but is coming from a different Lower Foreign Agent. This is interpreted as a handover. The Switching Foreign Agent replies to the mobile with a registration reply message.

The main advantages of this approach are:

- The rerouting node is close to the mobile. This results in a shorter service disruption and less packet loss.
- The amount of signaling is reduced since less signaling data is sent to the Home Agent (HA). This assumes that the lifetime of the binding is relatively long in order to avoid frequent binding refreshes sent from the mobile to the Home Agent.

Figure 3.2 shows the testbed for Hierarchical MIP (HMIP). The result will be shown in a later section.

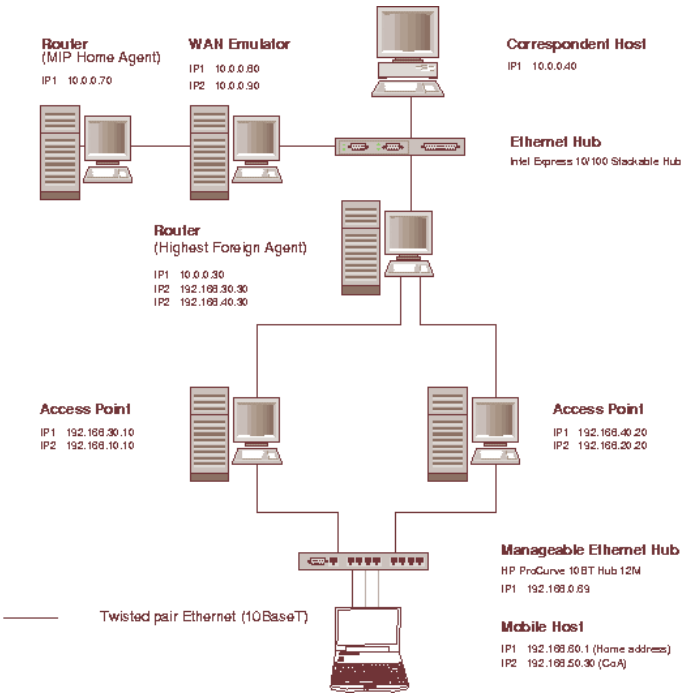

Figure 3.2: Testbed for HMIP

3.5 Multicast-Based Mobility Support

In general IP multicast supports location-independent addressing and routing in IP networks. This ability is similar to the requirement of mobility support though in a different context. Thus the motivation of multicast-based handover is to reuse multicast mechanisms.

Principally, in the multicast-based handover approach a mobile gets assigned a temporary address, which is a unique IP multicast address. This address does not change for the lifetime of the session even when the mobile moves to a new IP subnet.

In multicast-based handover approach is at least one multicast router located in every IP subnet, where multicast services are offered. Multicast routers can be regarded as the mobility infrastructure, but the originally usage is efficient data distribution to a group of receivers.

The establishment of a session is based on multicast mechanisms and different from the unicast case: The mobile acquires a multicast address and joins the multicast group via registration at the temporary multicast router. The multicast router in turn joins the multicast distribution tree which is constructed between the multicast routers with members of the particular multicast address with a multicast routing protocol (e.g. Distance Vector Multicast Routing Protocol (DVMRP), Protocol Independent Multicast - Sparse Mode (PIM-SM), etc.). The correspondent host sends packets with the mobile s temporary IP multicast address and the packets are distributed via the multicast distribution tree. In the reverse direction the mobile uses the (unicast) IP address of the correspondent host.

When a handover occurs, the mobile registers at the new multicast router with the same IP multi-cast address and the new multicast router joins the multicast distribution tree. The old multicast router leaves the multicast distribution tree (e.g. due to a time out or an explicit leave operation).

There are different sub-approaches to utilize multicast-based handover. In [37], it is intended to use today's IP multicast as it is available today in order to support handover. In [42] the IETF Mobile IP approach is extended by multicast: The Mobile IP Foreign Agents carry IP multicast addresses. When an handover event occurs packets are delivered efficiently from the Home Agent to at least two Foreign Agents and the handover latency can be decreased. In [22] an IP-style multicast is applied which realizes multipoint-to-multipoint communication in a switched access network. In this approach packets are distributed over a direct multipoint distribution tree of virtual circuits.

In the multicast-based mobility approach followed in the SeQoMo approach the endpoint of the multicast is located in the access point. The mobile host carries a unicast address, whereas this unicast address is mapped to a multicast address. The multicast-based mobility support is applied in an access network, only. Hence, multicast is utilized for local mobility and supplement an approach for global mobility support, such as basic Mobile IP. The approach employs standard IP multicast according to the Any Source Multicast (ASM) service model of IP and uses IGMP and PIM-SM [13, 15] as multicast protocols. Different handover policies are defined that utilize the underlying multicast scheme in a different way: With soft handover, the mobile host registers with the new access point immediately when an advertisement from the new access point is received (eager cell switching). The access point joins the mobile host's multicast group, and hence the old and the new access point belong to the multicast distribution tree for a certain duration of time. The soft handover scheme aims at a short service interruption caused by handover. With predictive handover, neighboring access points belong to the mobile host's multicast group in advance of handover and buffer the packets. When the mobile host registers with one of these access points during a handover, the data are already available and are immediately forwarded. Unlike the soft handover scheme, the predictive handover aims at reducing the packet loss at the cost of packet duplication, and hence an handover is initiated when the advertisement lifetime of the old access point expires (lazy cell switching).

In general, the advantages of the multicast-based approach are:

- The network node for the rerouting operation is located in this node, where the old and the new route diverge (and not e.g. in the home network distant from the mobile's temporary location).
- A dedicated mobile infrastructure in the network is not required, since the multicast infrastructure is re-used.
- It is not required that the mobile acquires a new multicast address when it has moved to a new subnet, whereas an IP multicast address is acquired only once for a session.
- For vertical handover a simultaneous distribution of packets to access points at different hierarchical level decreases the handover latency. In that case the usage of multicast reduces the overhead for traffic distribution in the backbone network.

Figure 3.3 shows the testbed for MOMBASA. The result will be shown in a later section.

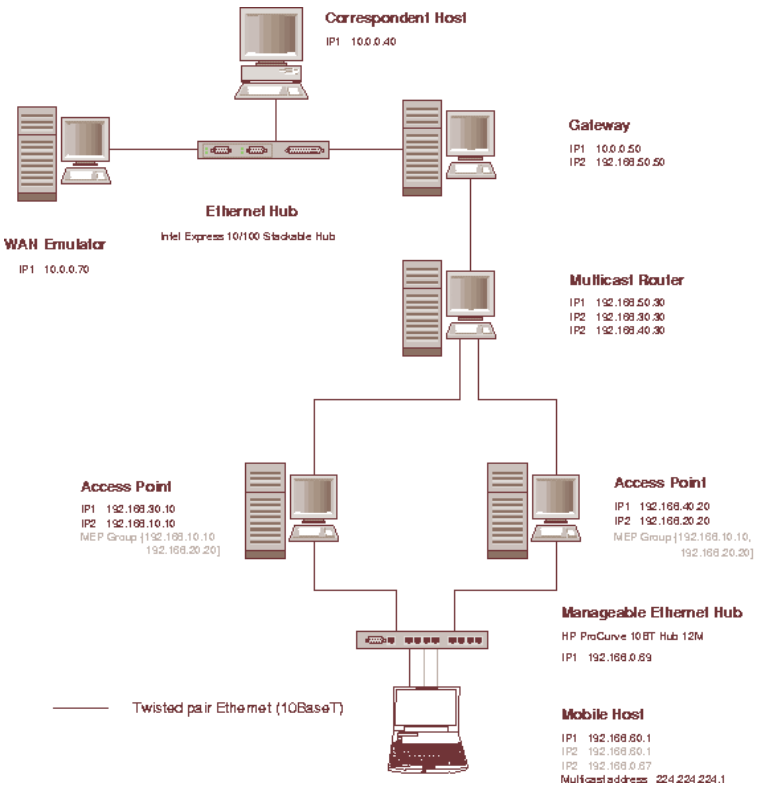

Figure 3.3: Testbed for MOMBASA

3.6 Comparison of the Two Approaches

We compare the two approaches conceptually as well as by means of their performance.

The conceptually comparison of the two approaches is shown is Figure 3.4.

The metrics for the experimental evaluation of the two approaches are:

- Handover latency: service interruption caused by handover;
- Packetloss and duplication for UDP traffic;
- TCP goodput;
- Overhead for signaling and buffering.

Exemplary, the handover latency metric is explained. The handover latency is defined as the service interruption caused by handover and is measured in the mobile host at the IP layer. A continuous packet stream is sent downlink from the correspondent host to the mobile host. During the receive

Addressing	*Unicast (home+CoA)*	*Multicast*
Routing	*Indirect: w/ address translation in HA*	*Direct: via multicast tree*
Registration	@FAs and HA	@MEP and MC router
Location management	With HA	With IGMP & routing protocol
Handover	Location update to FA of higher level or HA	Multicast join- and leave-operation
Rerouting node	Close to base station	Close to base station
Soft handover	*With replicated unicast*	*With inherent multicast*

Figure 3.4: Conceptual comparison of HMIP and multicast

process, the mobile host executes periodic handovers between both access points. The duration between two subsequent handovers (cell dwell time of a mobile host in a particular cell) is exponentially distributed with a mean duration of 10s plus an offset of 5s. Each run took 1 hour with about 230 handovers. Figure 3.5 shows the meaning of this metric.

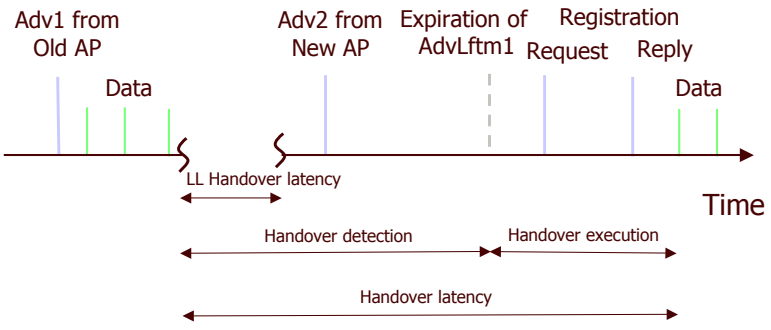

Figure 3.5: Illustration of the handover latency

In Figure 3.6, the mean handover latency for MOMBASA (soft and predictive handover), hierarchical Mobile IP and basic Mobile IP is plotted. In the scenario, advertisements were sent at 100 ms intervals with a lifetime of 300 ms. Each point in the graph is obtained by averaging the handover latency over about 230 handovers. The handover latency for MOMBASA soft and predictive handover as well as hierarchical Mobile IP are independent of the round-trip time between the correspondent host and the mobile host. More precisely, with hierarchical Mobile IP the handover latency is independent of the round trip time between mobile host and home agent. For basic Mobile IP the handover latency is constantly growing with the round trip time (RTT).

The mean handover latency for MOMBASA soft handover is less than 200 ms, for MOMBASA predictive handover about 260 ms and for hierarchical Mobile IP about 350ms.

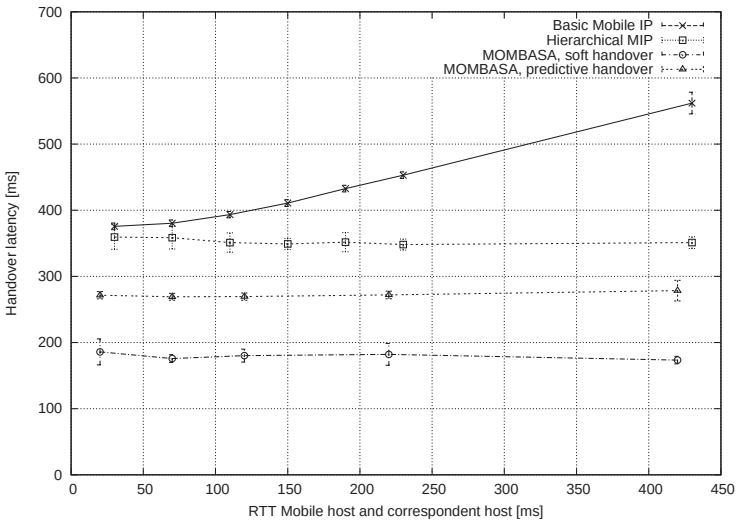

Figure 3.6: Handover latency comparison among different mobility schemes

Hence, with soft handover the subscribe operation contributes to the handover latency, whereas with predictive handover it does not. In comparison with hierarchical Mobile IP, the latency for MOMBASA soft handover is twice of the latency of hierarchical Mobile IP. With predictive handover, the handover latency amounts to 70 percent of the latency for hierarchical Mobile IP.

More performance results, also investigating other metrics (such as UDP packet loss and TCP throughput), are available in [16, 17, 19].

3.7 Conclusions

The experimental study shows that hierarchical Mobile IP as well as MOMBASA predictive handover provide fast handover with small service interruption whereas the MOMBASA predictive scheme reduces the handover latency to a minimum. The remaining handover latency with the MOMBASA predictive scheme can not be considerably reduced further by means of network layer mechanisms since it is caused by the duration for handover detection. Under our experimental conditions, the handover latency with the MOMBASA soft handover scheme is about 50% of the hierarchical Mobile IP scheme. In comparison to Mobile IP, the handover latency of all schemes is independent from the delay between mobile and correspondent host.

Hierarchical Mobile IP as well as MOMBASA predictive handover are superior to basic Mobile IP. The MOMBASA predictive scheme provides smooth handover, avoids any UDP packet loss at the expense of overhead and significantly improves the TCP throughput in cases with high service interruptions and frequent handover. With MOMBASA the mobile host may dynamically select between handover policies, such as predictive and soft handover, and hence, the optimal policy that meets the need of the application can be selected.

Handover detection based on advertisements significantly contributes to handover latency. The study

of link layer trigger issue refers to [18].

Based on the fact that Mobile IP is widely accepted as a mobility management protocol and HMIP gets more support in the IETF community, the choice of HMIP with enhancement has been favored In SeQoMo architecture.

Chapter 4

QoS

4.1 State of the Art Analysis

With the advent of various radio access technologies and increasing deployment of sophisticated applications in mobile end systems, IPv6- based networks will increasingly have to support Quality of Service (QoS) in mobile environments. Mobile IPv6 ensures correct routing of packets to a mobile node when the mobile node changes its point of attachment with the IPv6 network. However, it is also required to provide proper QoS forwarding treatment to the mobile node's packet streams at the changed route in the network due to node mobility in a fast, flexible, and scalable way, so that QoS-sensitive IP services can be supported over Mobile IPv6 [32]. A QoS scheme for Mobile IPv6 should (i) be able to localize the QoS (re-) establishment to the affected parts of the packet path in the network, and (ii) in cases where more than one access technology or Access Router (AR) is available, it may be desirable for the MN to choose an appropriate AR that can satisfy its QoS requirements among several potential new ARs when the MN moves into such a region (especially since in vertical handover scenarios, choosing a "good" access router might be more important than the mere speed of reestablishing a QoS path). In these cases, a handover should not be performed if the MN's QoS requirement is not met; yet if the QoS can be met, handover should be performed as quickly as possible.

In reference [7] a new IPv6 option called "QoS option" is introduced. One or more QoS objects are included as a hop-by-hop option in IPv6 packets carrying Binding Update (BU) and Binding Acknowledgement (BA) messages. When one packet for this purpose traverses different network domains in the end-to-end path, the QoS option is examined at these intermediate network domains to trigger QoS support for the MN's data packets.

4.2 Overview of QoS-Conditionalized BU Process

The requirements of a QoS solution for mobile IP are discribed in [6].

The mechanism described in reference [7] outperforms RSVP [43] [2] in which its signaling overhead is decreased. However, it does not allow to check whether the QoS requirements are satisfied along

the new route before performing the handover. We therefore introduce a QoS- conditionalized binding update. The node at which old and new paths diverge ("switching router") makes the final decision whether or not to update the binding, depending on the result of QoS checks. A binding update will only take place (in the sense of modifying the route) if all nodes along the route between the AR and the switching router are capable of complying with the QoS request, otherwise, the old route will still be used and a negative acknowledgement will be returned to the MN.

The proposed scheme is based on the architecture of Hierarchical Mobile IPv6 (HMIPv6) [41] to localize the QoS-conditionalized bindings. In HMIPv6, a new entity, the Mobility Anchor Point (MAP), is introduced and a MN only needs to perform one local BU through MAP when changing its layer 3 access point within the MAP domain. HMIPv6 is not able to express QoS requirements, let alone to provide feedback regarding the success of such request. We built on the work described in reference [7] to overcome these limitations.

In the proposed scheme, a QoS hop-by-hop option is carried in the message containing the BU option to the MAP - this message is called BU+QoS message. Each node concerned with QoS management between the MN and the MAP (including the MAP) will pass the QoS requirement represented by the QoS option to internal QoS mechanisms and check its resource availability. If resources are available locally, they are reserved and the message will be forwarded along its route. If specified in the BU+QoS message, reservations covering less than the desired amount of resources are also be possible; the request in the BU+QoS message is then updated accordingly. If resources are not available, negative feedback will be provided to the MN. Upon receiving the BU+QoS message, the MAP also checks resource availability and, if successful, will update the binding status and respond with a positive BA+QoS message, including the actual amount of reserved resources, if different from the requested amount. Otherwise, no binding update is performed and a negative BA+QoS message is returned to the MN.

By way of this scheme, QoS (re-)establishment due to local handovers is managed locally and transparently to the CNs, while in the worst case (global mobility) it is managed with Mobile IPv6 and [7]. Only if all routers along the new path find that sufficient resources are available will a handover (switching from old to new path) take place. In this sense, the handover process is conditional on the availability of QoS resources and our scheme can take advantage of HMIPv6. The additional advantage, however, is that mobile terminals will only perform a handover to an AR that can fulfill the QoS requirement (if there are multiple ARs to choose from; in case there is only a single AR able to serve the mobile terminal, even best-effort service would likely be acceptable, however, this is an application-level concern).

4.3 Description of the Approach

Figure 4.1 and 4.2 show the QoS-conditionalized BU process in cases of reservation success and failure.

The MN in our scheme behaves different to the one in the HMIPv6 basic mode when responding to a few events: detecting connectivity to a new AR, loosing connectivity to an existing router, and the arrival of BA+QoS. As a simplification, the processing here assumes that whenever a new AR becomes available, a binding update to this AR should be attempted. In reality, more sophisticated

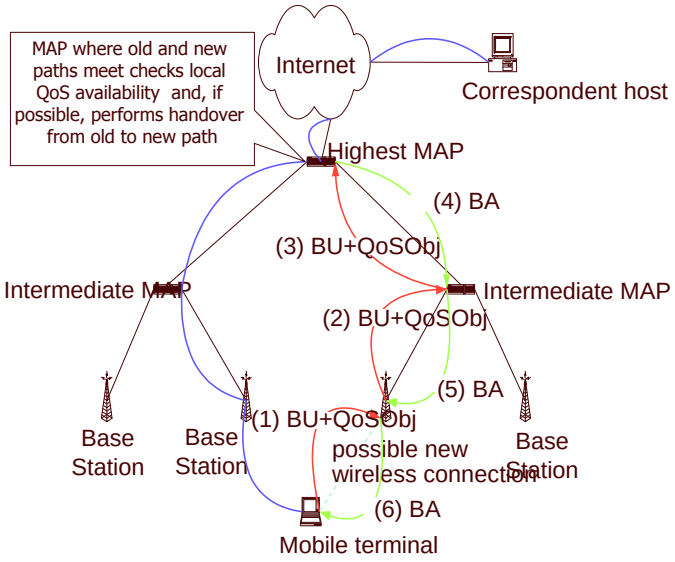

Figure 4.1: QoS-Conditionalized BU: Reservation succeeds

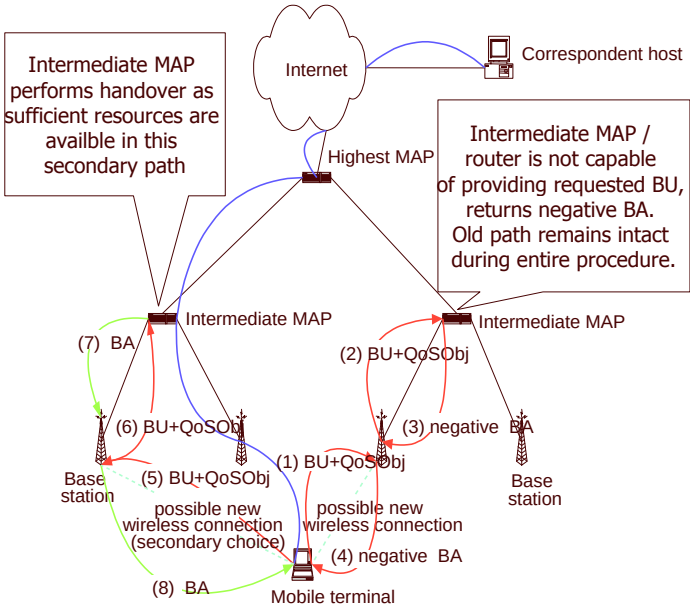

Figure 4.2: QoS-Conditionalized BU: Reservation fails

schemes may be implemented (e.g., only sending BU+QoS messages when the link quality to the old AR is deteriorating, keeping track of a list of prospective ARs, etc.); also, immediately obtaining an IP address from any new AR might not be cost-efficient, these are out of the scope of this draft. Note that the treatment of acceptabled or desirable QoS is also not discussed here; the necessary modifications are reasonably straightforward.

The MN detects the connectivity to a new AR either by listening to Router Advertisements or performing Router Solicitation as specified in [32]. After MN acquires new local IP address (LCoA), it should compose a BU+QoS message and send it towards MAP (via new AR).

If the MN receives a BA+QoS message, it should check whether the "F" bit is set in the QoS Option. If not set, the AR which this BA+QoS message passing through should be set as the default route for future data transmission. Otherwise no action is required: either still use old AR, or go with no QoS guarantees.

To optimize the QoS-conditionalized binding update procedure, the MN may maintain at least two lists of LCoA-AR-QoS pairs for which are available in connectivity and for which the MN has received positive BA+QoS messages. Once a BU+QoS message is responded with a negative BA+QoS, the QoS requirements embedded in the next BU+QoS message may differ from the previous one, e.g., the desired level of QoS could be reduced. There are several possibilities of how the number of available access routers could influence the setting of lowest acceptable QoS. E.g., acceptable QoS could be a function of the number of available ARs and/or the MN's speed.

Upon receiving a BU+QoS message, a router should check whether the "F" bit is set. If not set, it should ask QoS entity for resources. If sufficient resources are not available, this router should set "F" bit in QoS packet. If this router is the switching MAP, the MAP should compose a BA+QoS packet from the BU+QoS packet, with "F" bit set as in the BU+QoS packet and return the BA+QoS message to the MN.

If "F" bit is not set, the switching MAP should update the MN's binding to the new LCoA. It may compose a negative BA+QoS message and send it along the old path to release reservations. A MAP with MAP functionalities, but is not the switching MAP, behaves like a normal router.

Upon receiving a BA+QoS message, a router should check whether the "F" bit is set. If set, it should ask QoS entity for releasing any possibly reserved resources. Note that a router MUST NOT interpret the QoS option inside a BA+QoS as request for new resources, even when the "F" bit is not set. Rather, this QoS option is interpreted as providing more up-to-date information about a flow for which reservations have already been made.

Note that in order to correctly process the BA+QoS message, all routers concerned with QoS management, such as MAPs, ARs, and possibly DiffServ and MPLS edge routers (ER), as well as IntServ nodes need to maintain state for each flow. However, this is not an additional burden to these entities as they need to maintain this same state anyway: MAPs must maintain the binding cache, and also the AR has to keep information, including QoS information, for each MN. ERs typically act as aggregation routers, i.e. they (as opposed to interior routers) still know individual flows, just as IntServ nodes do. Nevertheless, this constitutes an argument in favor of restricting QoS control to AR and MAP.

There are two ways to release the resources that have been reserved. One is to release them explicitly via a message carrying a QoS option with "F" bit set. Another is to use soft-state for the QoS reservations and to rely on time-out of the reservation along an unused path. The timer of QoS option may differ from that for the BU option.

4.4 Prototypical Implementation of the Approach

This section introduces the implementation of the SeQoMo architecture. We first give an introduction about the testbed, then we discuss several representative functional tests.

The experimental testbed of SeQoMo has been set up. Details refer to [38].

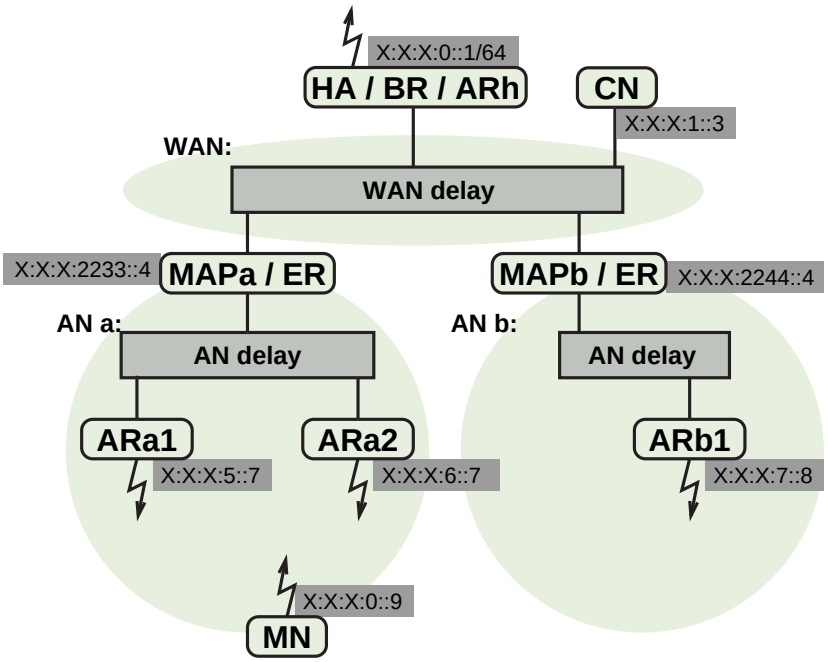

Figure 4.3: Testbed setup from IPv6 point of view

Figure 4.3 shows a simplified testbed setup from a IPv6 point of view is illustrated. The relevant IPv6 address of the different entities are given in the dark grey boxes. For the HA, ARa1, ARa2, and ARb this is the address which is advertised by their RtAdvs. MN and CN are depicted with their HoA. The address depicted next to the MAPs is the address which is carried by means of MAP discovery to the MNs. An artificial but controlled WAN-delay is enforced for all IPv6 packets traveling between a MAP and the HA or CN. Another controlled transmission delay is introduced in the two AN of the model and is referred in the following text as the AN-delay. This affects all packets traveling between any AR and the responsible MAP of each AN. Since no IPv6 enabled WAN emulator which is capable to enforce some controllable delay to traversing packets could be found, the Nist Net Delay tool [5] for IPv4 was used. To accomplish the delay of IPv6 packets, they are routed through an IPv4 tunnel via an additional PC serving as IPv4- WAN- and AN-emulator.

A detailed description of the testbed setup is given in Figure 4.4.

The Figure shows 6 physical Linux PCs where some of these machines virtually serve for multiple purposes. These machines are named as HA, MAP, CN/WAN, ARa, ARb, and MN. The smaller, black-bordered boxes represent network interfaces, where those attached from the outside represent real physical interfaces and those in the inside virtual, tunnel or dummy interfaces. All interfaces are illustrated with an abbreviation for its type. If the interface is IPv6-enabled, its most relevant IPv6

address is depicted in the dark grey box. If the interface is IPv4-enabled, its IPv4 address is given in the light grey box.

All computers are Intel Pentium II machines with a CPU speed between 300 and 500 MHz. All NICs are 100BaseT 3Com cards. Because link b and f employ only a 10Mbps hub, the bandwidth of these links is reduced to 10 Mbps.

The WAN-delay is enforced to all IPv4 packets, which are sent or received from interface eth2 of the HA or eth0 of the MAP and which are routed via interface eth0 of the machine WAN. From IPv6 point of view, the tunnel route provided by the sit2 interfaces on the HA and MAP is the only possible packet exchange route between HA and CN on one side and the MAP on the other side of the modeled wide area network. In this setup the HA also serves as ER for the CN which is physically located in the same machine as WAN and AN emulator. However, since only the CN's interface eth0 is IPv6 enabled and the HA is the only known IPv6 default router, all IPv6 packets leaving the CN are routed via the HA. The IPv6 layer of the CN does not know about the IPv6-in-IPv4 tunneled packets.

The machine MAP serves as MAP with two different address spaces and tunnel interfaces virtually like two MAPs for AN a and b. Therefore the SeQoMo-modified router advertisement daemon (radvd) is configured to advertise the availability of MAP (1) with the RCoA-address space X:X:X:2233::/64 via interface sit3 and the availability of MAP (2) with the RCoA address space X:X:X:2244::/64 for Access Network (AN) b via interface sit4.

The AN-delay between the MAP and the AR a and b is achieved in the same way as the WAN-delay described above. None of the physical interfaces connected to link f is enabled for IPv6. For AN a, all packets traveling between the ARa and the MAP are IPv6-in-IPv4 tunneled and routed via the interface eth1 of machine WAN. The machine WAN then delays the packets for a certain amount of time (AR-delay). Finally the ARa serves as AR for its two interfaces eth1 and eth2.

The connection of the MN to the access links of HA, AR a, or AR b is controlled via an SNMP manageable hub. All ports of the hub can be disabled and enabled through certain SNMP commands. When, for example, an overlapping movement from AR a eth1 to AR a eth2 is desired the corresponding ports are turned on and off respectively. In the following the MN's link-connection state will be given as a vector where the terms h, a1, a2, and b1 stand for the home, ARa1, ARa2 and ARb1 link. These terms are followed by a ":0/1" indicating whether the connection to this link is disabled or enabled by the controlling hub. One disadvantage of the manageable hub used in this testbed is the indeterministic duration (between 2 and 6 seconds) it takes from sending the Small Network Management Protocol (SNMP) command until the desired action is finally executed by the hub.

An alternative approach to emulate movements is provided by the Netfilter module. The basic idea is to let the MN physically always be connected to all potential AR interfaces, but drop packets from certain interfaces based on their MAC address. If the packets are dropped before they are further processed by the IPv6 layer, the MN has no means to deduce the connection to this particular link of the AR. By way of this, tools utilized for performance evaluation can immediately trigger a handover and have the possibility to consider for example the time when a handover was executed with a much better accuracy. Also it becomes possible to increase the maximal handover rate from only one HO in 6 seconds (possible with the SNMP manageable hub) to more than one HO per second. This concept of a "virtual manageable hub" is employed as a software module in the MN.

Simple connectivity test between the MN and the HA or CN were performed with the diagnostic tool

ping6. For evaluation of application packet loss a simple tool called udp6traffic was developed for sending and receiving User Datagram Protocol (UDP) messages between MN and CN. The transmitted messages and their content were monitored via selected interfaces with the tool tcpdump. If monitoring of certain processing parameters of a node was desired this was achieved by inserting appropriate debug messages in the kernel code. The amount of debug message provisioning could be accessed via an entry in the proc-file system, ranging from an error level where only serious problems are reported to an informal level where all interesting function calls and variables are logged.

4.5 Conclusions

QoS support in all-IP mobile networks brings about great challenges and requirements. The QoS-conditionalized BU approach presents a hierarchical, edible, and scalable solution that makes use of an IPv6 hop-by-hop option. Our scheme reduces the signaling bandwidth on the backbone by hiding local mobility while still providing ability to do QoS signaling. Our work extends the work in [7] by: 1)enabling mobile users to choose a good access point when several (or overlapping) ones are available (e.g.,WLAN and UMTS in hot spots); 2)having handovers QoS-conditionalized handovers could be performed only when QoS requirements are met or most satisfied. The latency for QoS re-establishment is reduced compared to RSVP-based approaches during a handover.

In the work of the prototypical implementation and experimental testbed setup, a QoS-enabled mobility concept based on HMIPv6 [41] and the QoS-conditionalized BU approach [25] has been accomplished. To achieve this, the following intermediate steps have been conducted. The leveraged architectures such as IPv6 and MIPv6 have been reviewed and relevant procedures for this work have been summarized.

The underlying concepts – described specifications of HMIPv6 and QoS-conditionalized BU approach – have been analyzed. Their behavior has been re-examined in a more formal way to provide a basis for the implementation design. Open issues and possible solutions according to the protocols' specifications have been identified. Especially the composition of a QoS option needed to be reorganized and the possibilities to release reserved resources on a stale data path has been neglected in the specification and required additional investigation.

The implementation design has been adapted to the selected operating system and existing MIPv6 implementation environment. Thereby, it was discovered that especially the proper management of movement detection, selection of a suitable new default router, and the execution of related registration operations proved to be a difficult task.

A new method, based on a so-called "context field" (essentially summarizing the overall context of a path, represented by an AR, in a single value), has been designed to overcome this challenge. This selection method can easily be extended to consider new information and different movement policies.

Based on the implementation design, a prototype implementation called QoCoo has been realized to provide support for HMIPv6 and the QoS-conditionalized BU approach. QoCoo has been setup in an experimental testbed. Various representative scenarios have been successfully tested, with the objective to demonstrate the key capabilities of the underlying protocols. Performance experiments

showed that the packet loss per handover for micro movements can be reduced by more than 80 percent (depending on the transmission delay between access network and CN) when using HMIPv6 or the QoS-conditionalized BU approach instead of MIPv6. However, it was also shown that an enhanced movement detection mechanism is necessary to let the application layer benefit from the reduced signaling latency introduced by the use of HMIPv6.

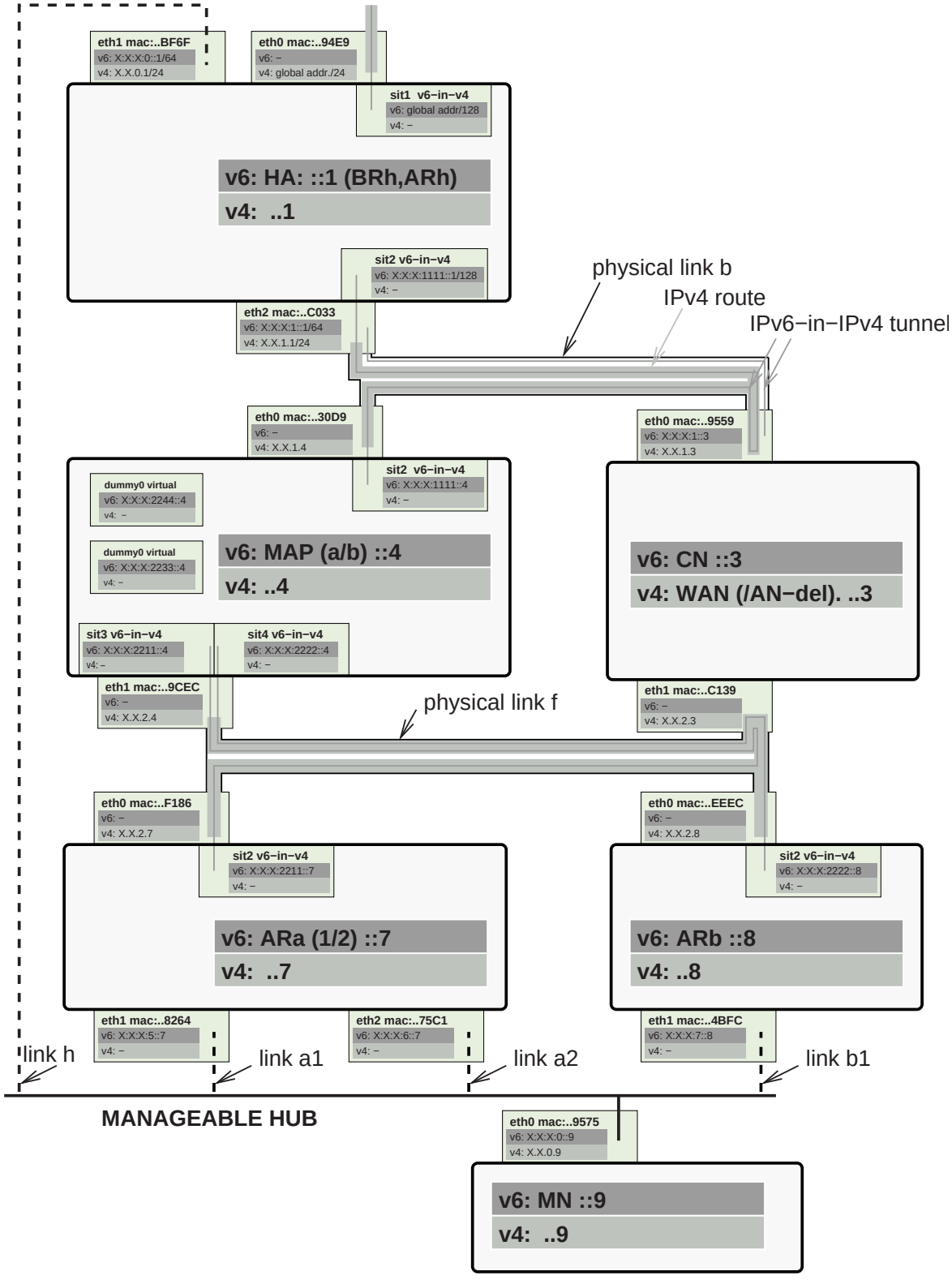

Figure 4.4: Concrete testbed setup

Chapter 5

Security

The security aspect of the project lies in authentication, QoS-aware authorization for mobile users and Denial of Service (DoS) protection of handover process. The visited network should verify the MN has the identity it claims to have. Also, the visited network needs to learn what kinds of services or how many QoS resources the MN is allowed to use and verify the resource usage of the MN to ensure that the total resource consumption does not exceed what the MN is entitled to.

To support efficient handovers, it is also necessary to minimize the registration latency introduced by authentication and authorization (AA) procedures in handovers taking place both within an administrative domain and between such domains.

Furthermore, all AA messages should be stored and transmitted securely to prevent both passive and active attacks.

5.1 Issues and Steps

Briefly, the issues are the following:

- Authentication performance during handovers: how to realize efficient identity check during a handover should be addressed;
- Authorization of mobile devices in access networks: how to check what resources a mobile node is allowed to use is another issue;
- Protection QoS against DoS attacks: how to ensure that QoS-reservation can not be abused to reduce the availability of an access network is a challenge.

To address the identified issues, we first evaluate the integrated AAA and Mobile IP authentication with a simulation, then we design the QoS-aware authorization processes and the appropriate DoS protection mechanism, finally we evaluate the developed QoS protection scheme with a simulation and implement it on the testbed.

5.2 AAA and Mobile IP Authentication

The principal approach of the IETF to authenticate a mobile node during handover operations is to integrate authentication during Mobile IP registration with a general AAA infrastructure based on the so-called Diameter protocol [4] [14].

The main focus of authentication in this respect is the problem of securely identifying entities for IP access in a mobile network with roaming capabilities. Strongly related to this problem is the task of managing the cryptographic keys that are needed for secure entity authentication and data origin authentication for signalling messages, respectively. A special requirement to the authentication infrastructure arises out of the fact that mobile devices require frequent handovers from one access point to another. These handovers can either occur within an administrative domain (intra-domain handover) or between two administrative domains (inter-domain handover). An important issue is the performance of the (re-)authentication during a handover operation. In order to assess the performance impact of the authentication procedure on handover events we developed a simulation model which takes into account three different types of handover events and analyzed this model with two different traffic models [29].

Figure 5.1 shows the trust relationships in the AAA and Mobile IP joint architecture. It is noted that static trust relationships between AAA attendants (e.g. FAs) and AAA servers, between AAA servers and brokers, between mobile node and its home AAA server already exist. The dynamic trust relationships between an AR and HA, between MN and AR, between MN and HA are created by the AAA server in the home network (AAAH).

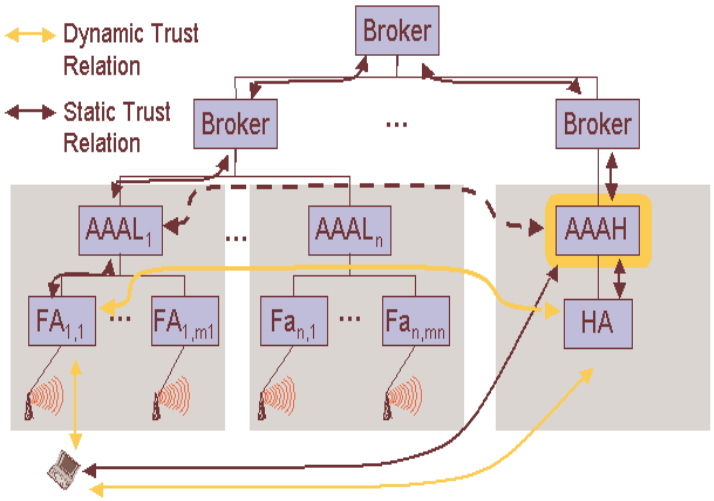

Figure 5.1: Trust relationships in AAA and Mobile IP infrastructure

The results of our simulation study show, that:

- The delay experienced by a mobile node in case of a full authentication dialogue involving entities of the mobile node s home network is largely determined by the end-to-end delay between the foreign and the home network.

- The workload of AAA servers remains moderate in case of a load- and mobility model inspired by established values of GSM networks as well as in case of a more progressive mobility model.

- The workload of AAA servers grows infinitely under both mobility models if cryptgraphic algorithms are used that require about 100 (30) times the processing capabilities of algorithms currently envisaged by the IETF (cryptographic hash functions and symmetric encryption).

An important consequence of the third finding is that the use of asymmetric cryptography would possibly lead to overload situations under the investigated conditions, as those operations often require processing capabilities in this range.

Figure 5.2 shows that the system is only under light load if operated with the symmetric cryptographic algorithm and hash functions as intended by the IETF.

Figure 5.3 shows that if computationally intensive cryptographic operations (factor in the range 80 to 100) are used, the system gets to overloaded because asymmetric cryptography is too "expensive" in this context.

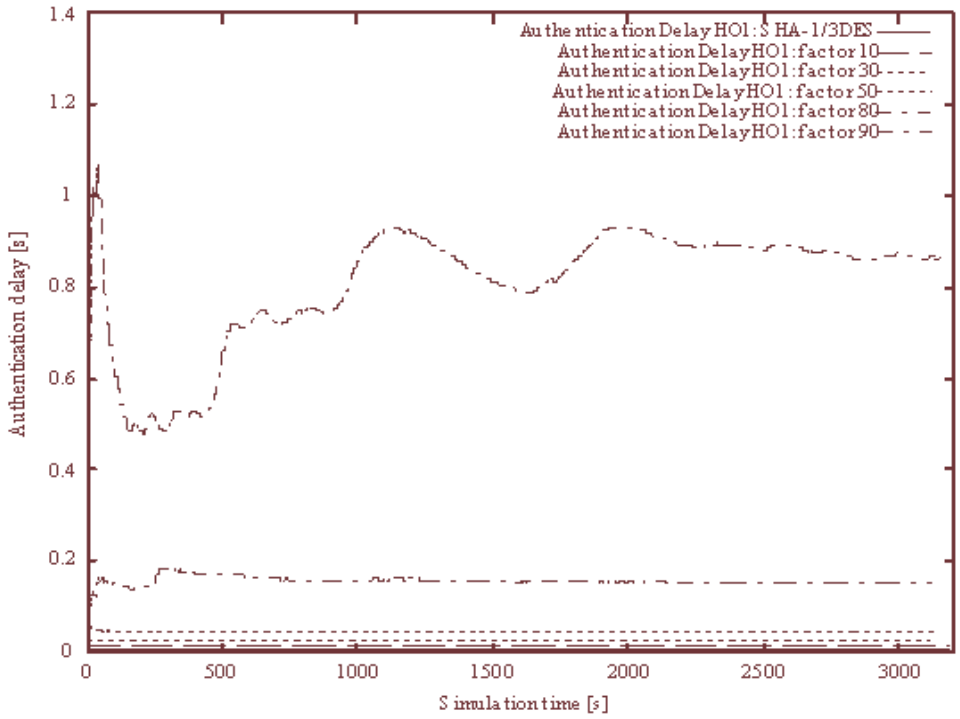

Figure 5.2: Authentication delay with symmetric cryptographic algorithm

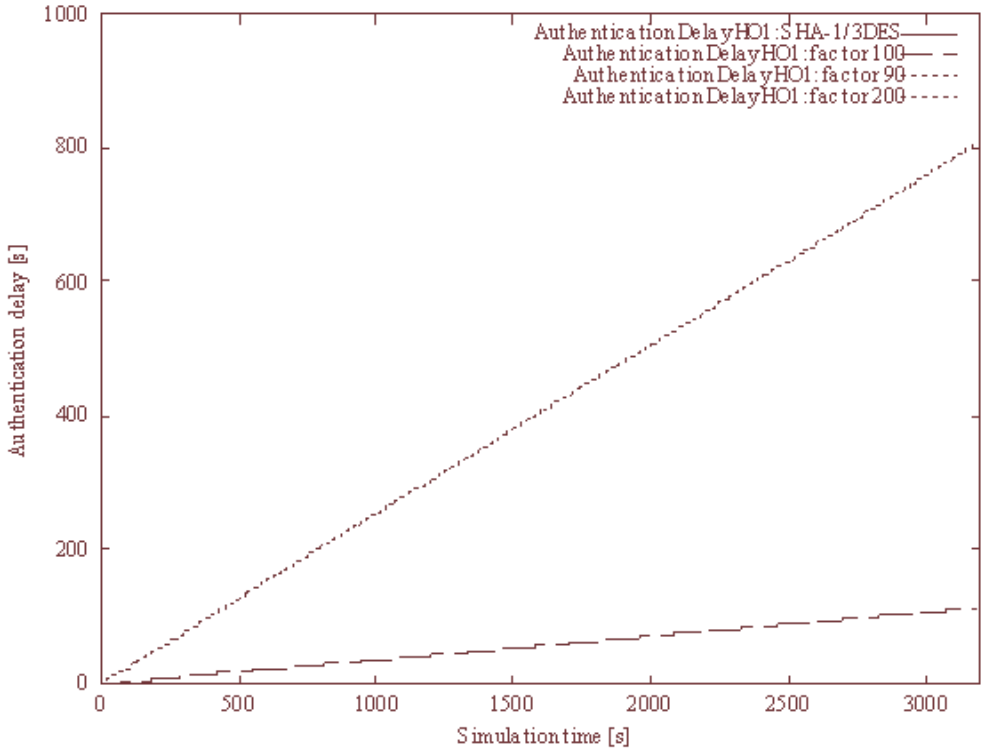

Figure 5.3: Authentication delay with asymmetric cryptographic algorithm

5.3 QoS-aware Authorization

With the development of all-IP communications in mobile computing, a large amount of research efforts have been focusing on provisioning Quality of Service (QoS) to mobile users who are expecting similar services in a visited network as in their home network. From the service or resource provider's point of view, however, before allocating or reserving its available resources according to the mobile user's QoS requests, the visited network should authorize the request to make sure that the user has permission to use the requested resources.

5.3.1 Goals and Requirements

The goal of the authorization work [8, 9, 10] is to design an authorization scheme for HMIP and AAA joint networks aiming at QoS-capable and low-latency micro-mobility handovers.

The identified requirements are:

- Authorization information availability: When a MN registers in a visited network and requests for a service for the first time during an inter-domain handover, the network can authorize the

QoS requests whether the MN has permission to use the requested resources with the help of e.g. the MN's home network.

- Mapping of authorization data expression to QoS: The authorization data expression should ensure an unambiguous mapping to the QoS requests in order to make the QoS requests understandable and verifiable at an authorization entity. Efficient handover support: It is necessary that the authorization process adds minimal latency to the registration and handover procedures.
- Capability to handle an MN's various activities: MN can upgrade its QoS requests dynamically based on the conditions of the network. The authorization scheme must be capable to handle QoS request upgrading cases without losing other optimizing features.
- Security considerations: Security measures are needed for both hop-by-hop QoS signaling protection and end-to-end authorization protection against the attacks that a malicious node forges or modifies legitimate MN's QoS requests. Another security concern is MN's misbehavior, which means that an MN could possibly attach to multiple access routers (ARs) at the same time and try to use more resources than it is entitled to. Even if the requested QoS over each link meets the MN's authorization limits, it could eventually happen that the total amount of QoS requested in the visited network exceeds the limit. If the network can not efficiently check the ”credibility” of a QoS-request, malicious entities could flood the network with bogus QoS-requests in order to cause exhaustion of the available resources by temporal reservations.

5.3.2 Use Cases of the Authorization Processes

In this section, we describe the integrated processes of the three components in the SeQoMo architecture.

When an MN enters the visited access network or just powers up, it can detect its movement and distinguish whether the movement is the inter-domain or intra-domain handover based on L2/L3 information. We will describe the (re-)registration process in inter-domain and intra-domain handover cases separately.

Inter-domain Handover

Figure 5.4 illustrates the registration process in the inter-domain handover cases.

1. MN receives an advertisement from an AR (e.g. AR2), and its IHA indicates that it is in an inter-domain handover process;
2. MN composes a registration request message, including a range of QoS parameters, for example a Desired Bandwidth (DBW) and an Acceptable Bandwidth (ABW) in a Hop-By-Hop option, assigning the address of MAP as the destination address;
3. AR2 receives the message. Since it notices that there is no cookie being presented, it indicates that the request will go through an inter-domain handover process. Then it starts the uplink QoS-Conditionalized Binding Update (QCB) procedure. During this procedure, every node

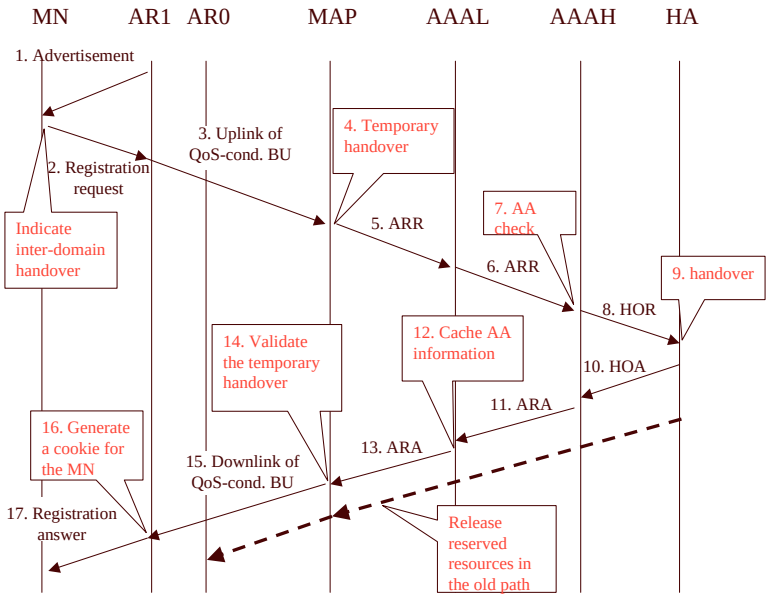

Figure 5.4: The registration process in case of inter-domain handover

along the path, including AR2, intermediate routers and MAP, checks whether it can satisfy the DBW. If yes, it reserves the resource for the flow; if not but it can satisfy the ABW, it reserves what it can provide, modifies the range of requested QoS parameter according to satisfied value, and passes the message to the next node; if it can not satisfy even the ABW, it indicates a negative check result in the message;

4. MAP checks whether the path can satisfy the requested QoS. If not, it sends a ICMP message to MN acknowledging registration fails; if yes, it creates an entry for the binding of LCoA and RCoA;

5. and it composes an AA-Registration Request (ARR) message with the destination address of AAAH. The BU message destined to HA is embedded in ARR;

6. AAAL receives the ARR. When it realizes that it is under an inter-domain process, it forwards the message to AAAH;

7. AAAH checks the authentication and authorization of the QoS request from MN;

8. If the check succeeds, it composes a HOme-agent-Request (HOR) including the BU to HA;

9. HA caches the binding of MN's RCoA and its home address;

10. HA sends a HOme-agent-Answer (HOA) to AAAH. Meanwhile, it initiates the process to release the reserved resource on the old path;

11. AAAH generates a session key and inserts it in the AA-Registration Answer (ARA) message;

12. AAAL caches the session key, the bandwidth value as MN's Maximum Bandwidth (MBW) in order to authorize the MN's further QoS requests locally;
13. AAAL forwards the ARA to MAP;
14. MAP caches the session key, validates the handover and starts the downlink procedure of QoS-cond. BU;
15. During this procedure, each node along the path adjusts or confirms the reserved bandwidth;
16. AR2 caches the session key, generates a cookie, encrypts the cookie with the session key, and sends a registration answer to MN;
17. MN receives the registration answer message, decrypts the cookie with the session key. MN gets the session key due to its long term security association with AAAH.

Strictly, the QoS-Conditionalized Binding Update (QCB) procedure, which starts from MN and ends at MN, includes the steps of registration request and registration answer. It is noted that the illustrated procedure is identical with the procedure of Diameter Mobile IPv6 application [14].

Intra-domain Handover

Figure 5.5 and Figure 5.7 illustrates the re-registration process in case of intra-domain handover which does not involve the AAAH for the re-authorization. We propose two schemes how to integrate the QoS-cond. BU procedure and re-authorization procedure. We first describe the two schemes and then a comparison of them.

- BU and re-authorization in series

  As shown in Figure 5.5 and 5.6, the re-registration process is the following:

  1. MN receives an advertisement from an AR (e.g. AR2), and its IHA indicates that it is in an intra-domain handover process;
  2. MN composes a registration request message, including a range of QoS parameters, for example a desired bandwidth (DBW) and an acceptable bandwidth (ABW) in a Hop-By-Hop option, assigning the address of MAP as the destination address, inserting the cookie;
  3. AR2 receives the message. Since it notices that there is a cookie being presented, it indicates that the request will go through an intra-domain handover process. It first verifies the cookie. Details about the cookie mechanism refer to the patent application document. If the cookie verification fails, the request is dropped silently; if it passes, AR2 notifies the use of the presented cookie while starting the uplink QoS-Conditionalized Binding Update (QCB) BU procedure;
  4. This procedure goes as in the inter-domain handover case;

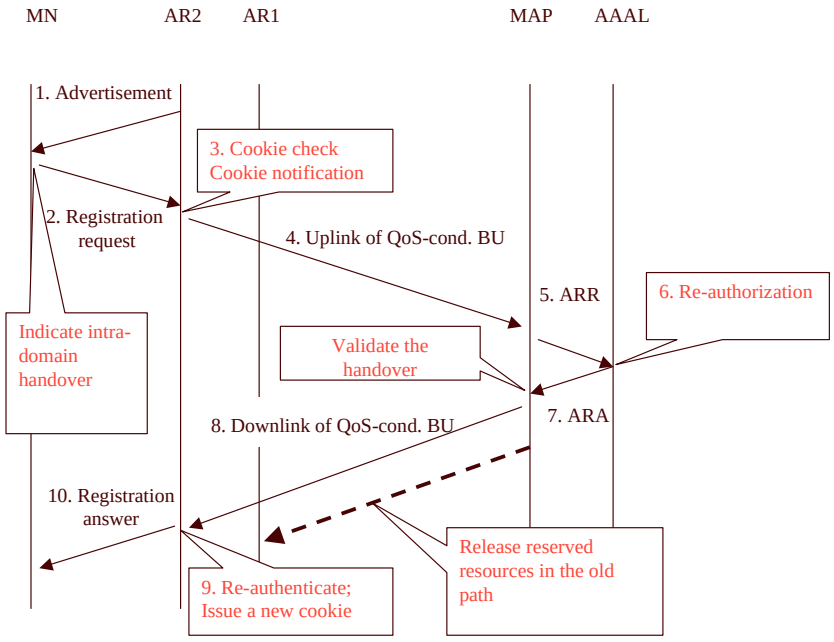

Figure 5.5: BU and re-authorization in series

5. MAP checks whether the path can satisfy the requested QoS. If the path can satisfy the QoS request, it creates an entry for the binding of LCoA and Regional Care-of Address (RCoA). MAP also composes ARR and sends it to AAAL;
6. AAAL re-authorizes the request based on the cached MN's authorization information (e.g. MBW);
7. If the re-authorization succeeds, AAAL composes a ARA message;
8. MAP validates the handover, includes the session key in the downlink Acknowledgement (ACK) message of QoS-Conditionalized Binding Update (QCB) process. Meanwhile, it initiates to release reserved resource in the old path;
9. AR2 re-authenticates the MN with the session key. If it is successful, it generates a new cookie, encrypts it and sends it to MN;
10. MN receives re-registration answer message and gets the new cookie.

- BU and re-authorization in parallel

As shown in Figure 5.7 and 5.8, the re-registration process is the following:

1. MN receives an advertisement from an AR (e.g. AR2), and its IHA indicates that it is in an intra-domain handover process;
2. MN composes a registration request message, including a range of QoS parameters, for example a desired bandwidth (DBW) and an acceptable bandwidth (ABW) in a Hop-

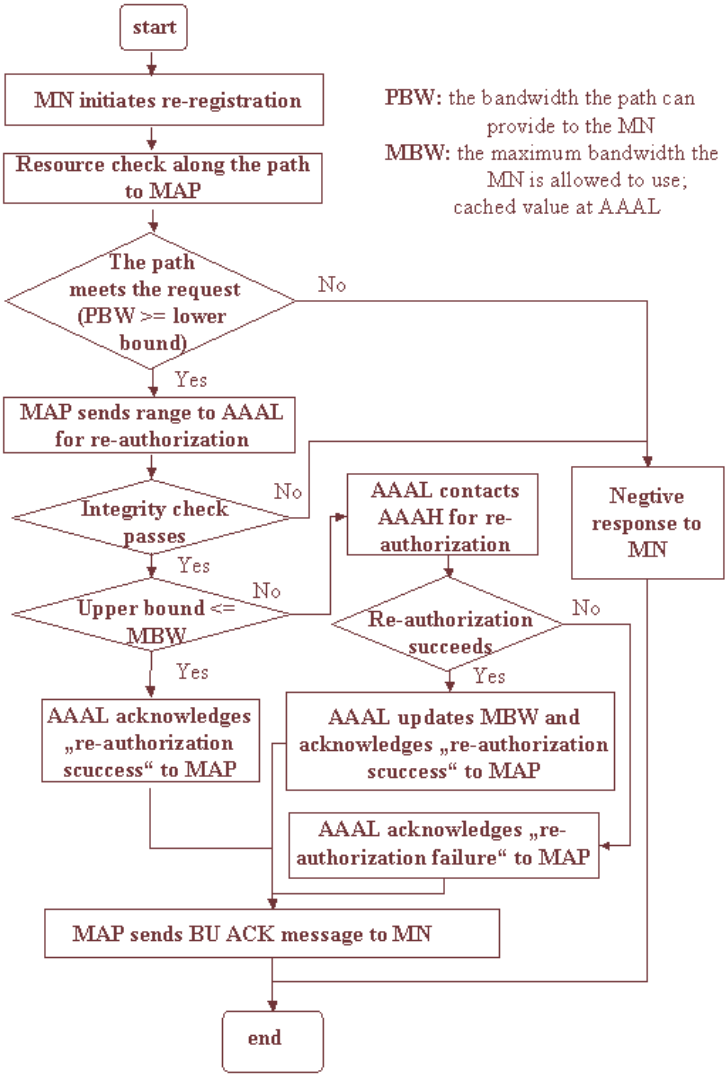

Figure 5.6: Process flowchart of BU and re-authorization in series

By-Hop option, assigning the address of MAP as the destination address, inserting the cookie;

3. AR2 receives the message. Since it notices that there is a cookie being presented, it indicates that the request will go through an intra-domain handover process. It first verifies the cookie. Details about the cookie mechanism refer to the patent application document. If the cookie verification fails, the request is dropped silently; if it passes, AR2 notifies the use of the presented cookie while starting both the uplink QoS-conditionalized (QoS-cond.) BU procedure and the re-authorization procedure;
4. The uplink procedure is the same as in the previous subsection; Meanwhile, AR2 com-

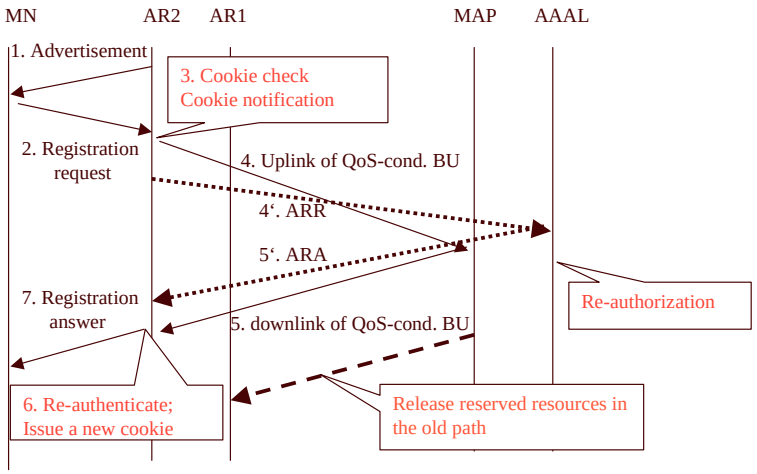

Figure 5.7: BU and re-authorization in parallel

poses the ARR message and sends it to AAAL for re-authorization;

5. ARA is sent back to AR2. It is assumed that the re-authorization result arrives earlier than the downlink of BU procedure;
6. If the two procedures result in positive acknowledgements, AR2 re-authenticates the MN with the session key. If it is successful, it generates a new cookie, encrypts it and sends it to MN;
7. MN receives re-registration answer message and gets the new cookie.

- Comparison

  The second scheme is more optimized in terms of low-latency re-registration. However, if re-authorization takes longer time especially when AAAL involves AAAH for the re-authorization, the downlink message of QoS-Conditionalized Binding Update (QCB) arrives at AR2 before the re-authorization result does. This is a tough situation for AR2 to deal with. If AR2 holds the downlink procedure and waits for the re-authorization result, the QoS-cond. procedure is interrupted; if AR2 continues the downlink procedure without the re-authorization result, when a negative re-authorization result arrives later, it has to take some actions to adjust reserved resources or even tear down the path.

  The first scheme avoids the potential trouble. But the QoS-cond. BU procedure is definitely interrupted by the re-authorization procedure.

5.3.3 Discussion on the Authorization Process

The authorization process in SeQoMo is the first QoS-aware authorization scheme in HMIPv6 architecture.

In order to meet the requirement of low-latency (re-)registration process, a couple of measures are taken:

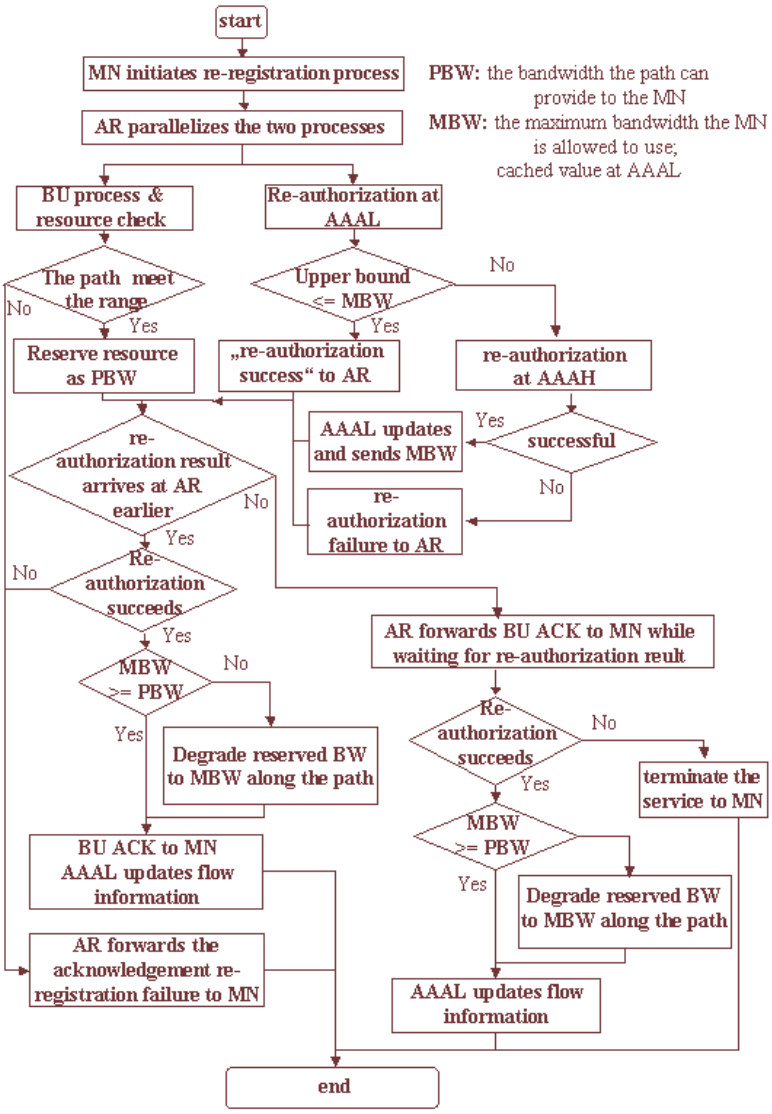

Figure 5.8: Process Flowchart of BU and re-authorization in parallel

- the (re-)authorization process takes place in a hierarchy-based AAA architecture;
- the (re-)authorization process is integrated with the BU process, or happens in parallel with the BU process;
- (re-)registration request enables a range of QoS parameters rather than a specific value as to simplify the authorization negotiation process;

- Authorization data is cached at AAAL to authorize MN's QoS request without involving AAAH if possible.

Additionally, in order to avoid expose the subscribed value of QoS parameters which is cached by MN's AAAH, only the desired value or the resource the visited access network can provide is cached at AAAL as the maximum value MN is entitled to use. When MN upgrades its QoS request or generates a new flow so that AAAL is not capable to authorize it, AAAL should communicate with AAAH for authorization. If the authorization succeeds, AAAL updates the cached "the maximum value". Therefore, the authorization is a continuous process.

Comparison With Authorization Token

Authorization token is a Cryptographic Message Syntax (CMS) protected (digitally and encrypted) collection of objects [27, 28]. The "token" is generated by a policy server and transparently replayed through the host to the edge router where it is used as part of the policy-controlled flow admission process. It can be used to allow Cross Application Signaling Protocol (CASP) nodes along the path to execute policy based admission control or authorization check without triggering the communication of Policy Execution Point (PEP) and Policy Decision Point (PDP) [39][40].

The use of authorization token raises some security concerns. For example, as mentioned in [44], the authorization token might be eavesdropped by an adversary so that the adversary might replay it and gain access to resources with the successful verification.

In contrast, the cookie mechanism aims to prevent replay attacks and DoS attacks. If a cookie extends to contain some authorization information (that means cookies with different colors represent different amount of resources being authorized to an MN.), it can be used to:

- provide authentication at the edge router;
- provide admission control at CASP nodes;
- authorize requested QoS to reserve resource;
- provide protection against replay attacks, message modification and DoS attacks.

Additionally, it can be useful to achieve optimized handovers.

Comparison With Context Transfer Protocol

The primary motivation of Context Transfer (CT) Protocol [34, 36] is the need to quickly re-establish context transfer-candidate services without requiring the mobile host to explicitly perform all protocol flows for those services from scratch. An additional motivation is to provide an inter-operable solution that works for any Layer 2 radio access technology.

Access Routers typically establish state in order to effect certain forwarding treatments to packet streams belonging to nodes sharing the access router. For instance, an access router may establish

an AAA session state and a QoS state for a node's packet streams. When the link connecting a mobile node and the access router is bandwidth- constrained, the access router may maintain header compression state on behalf of the mobile node.

As described in [33], one of the more compelling applications of context transfer is facilitating the re-authentication of the mobile host and re-establishment of the mobile host's authorization for network access in a new subnet by transferring the AAA context from the mobile host's previous AAA server to another. This would allow the mobile host to continue access in the new subnet without having to redo an AAA exchange with the new subnet's AAA server. Naturally, a security association between the AAA servers is necessary so that the mobile host's sensitive authentication information can be securely transferred.

Therefore, the differences between CT and the authorization process in SeQoMo in terms of authentication and authorization are:

- In CT, AAA data are transferred from previous visited network to the current visited network; In SeQoMo, AAA is performed with AAAH. However, in the case that MN upgrades its requested QoS so that the authorization can not be done based on the authorization information from the previous network, is the authorization solution in SeQoMo is more flexible and generic;
- In CT, when MN's movement is unpredictable, AAA information is transferred in a one-to-many manner in order to quickly re-establish the AA service; In SeQoMo, when MN sets up association with an AR which does not know it, a cookie can help AR to authenticate MN as a preliminary check. The further AA can be integrated with other processes e.g. BU process.

5.3.4 Summary

Our authorization scheme takes the following measures to support the efficient (i.e. low-latency) handover feature:

- the AAA protocol is integrated with the hierarchical Mobile IP. More precisely, the authorization process takes place in series with the BU process in inter-domain handover cases and in parallel with the BU process in intra-domain handover cases;
- QoS requests include a range of QoS parameter rather than a specific value so as to simplify the authorization negotiation process;
- Authorization data is cached locally (i.e. at AAAL);
- A preliminary check is performed to protect QoS against DoS; (find details here).

5.4 DoS Protection

Quality of Service (QoS) mechanisms in networks supporting mobile Internet communications give rises to new threats that these mechanisms could be abused by malicious entities to launch so-called Denial of Service (DoS) attacks, which aim to reduce the availability of services to legitimate users.

5.4.1 Motivations, Goals and Approach

In an access network, a mobile user sends a request to an access point for a QoS. If there is no security check on QoS requests, attackers can also send requests to reserve resources. Intensive bogus requests from attackers could reserve all resources along a path so that this path has no available resource for any legitimate users. This threat is a kind of DoS attacks as shown in Figure 5.9.

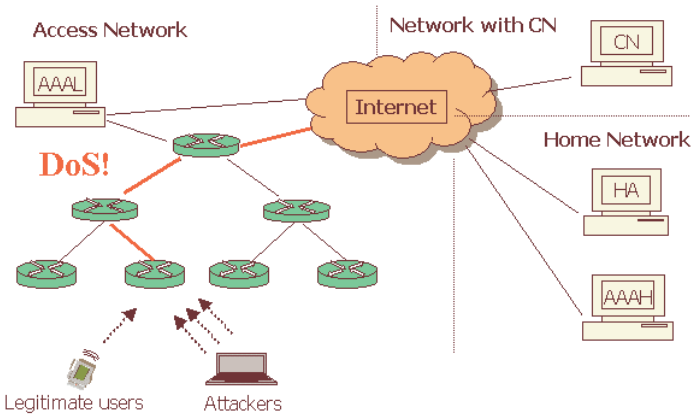

Figure 5.9: Resource exhaustion as a kind of DoS attack

Therefore, when an access point receives a QoS request, it must perform an security check. If the access point communicates with an local security entity (e.g. a local AAA server) for authentication and authorization checks. Obviously, the propagation delay for this signaling is unfavorable for a fast handover. Furthermore, the same checks have to be done to the requests from attackers. Thus, intensive and extensive bogus requests may degrade substantially the signaling capacity of the access network including a path and the local AAA server. This is another kind of DoS attacks as shown in Figure 5.10.

Therefore, we need to protect QoS-aware communications from DoS attacks and achieve an optimized handover by reducing the registration latency caused by the security checks. For these purposes, we propose that before the resource reservation and authentication and authorization process, the access point performs a preliminary check with a "cookie". The cookie mechanism is in a process of patent application. The detailed solution will be published soon.

5.4.2 Description of the Cookie Mechanism

A cookie contains the cookie information and a hash code.

The cookie information includes:

- Identity of the MN: the MN's unique identifier in the access network. This can be a local unique identifier the MN gets after its first registration.

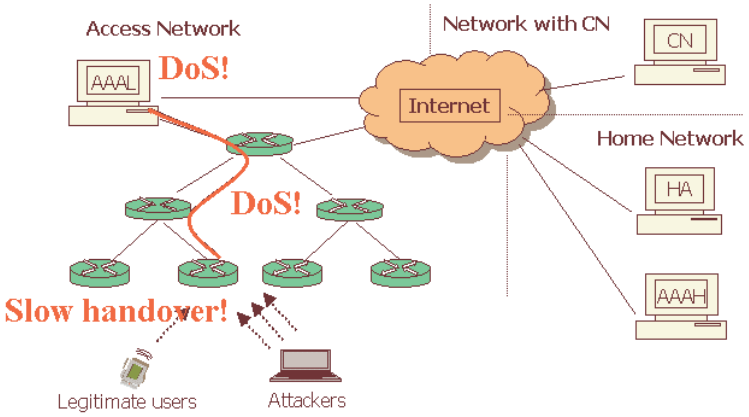

Figure 5.10: Signaling capacity depletion as a kind of DoS attack

- Identity of the AR who generates the cookie: the AR's unique identifier. It can be the AR's IP address or another unique identifier acceptable in the access network.
- Creation time: A timestamp when the cookie is generated. It is used to limit the cookie's period of validity.
- Random number: It is used to distinguish two cookies which are generated at the same time.
- Hash code: The hash code is a message digest of the cookie information and a cookie key. The hash function can be of either Keyed-Hashing for Message Authentication using MD5(Message-Digest 5 (HMAC-MD5) or Keyed-Hashing for Message Authentication using SHA1(Secure Hash Algorithm 1 (HMAC-SHA1). The cookie key is distributed from the MAP to each AR and updated by the MAP periodically, for example a new cookie key is distributed by the MAP once per hour or day.

In summary, a cookie is defined according to the following formula:

$$\begin{aligned} CookieInfo &:= \big(Identity_{MN}, Identity_{ARi}, Timestamp_{ARi}, \\ &\quad RandomNumber_{ARi}\big) \\ CookieHash &:= HMAC\big(CookieKey, CookieInfo\big) \\ Cookie &:= \big(CookieInfo, CookieHash\big) \end{aligned}$$

Cookies are always generated by an AR. The first cookie the MN gets is generated by the AR to which the MN attaches when it powers up or when it performs an inter-domain handover. That means, after its successful registration, this cookie is encrypted with the session key established between the MN and all ARs in the access network and transmitted from the AR to the MN along with the BU acknowledgement message. Figure 5.11 shows how MN gets the first cookie.

Each AR maintains two lists: *a trusted list* and *a trusting list*. The AR only accepts the cookies generated by the ARs on the trusted list. On the trusting list are ARs who accept the cookies generated

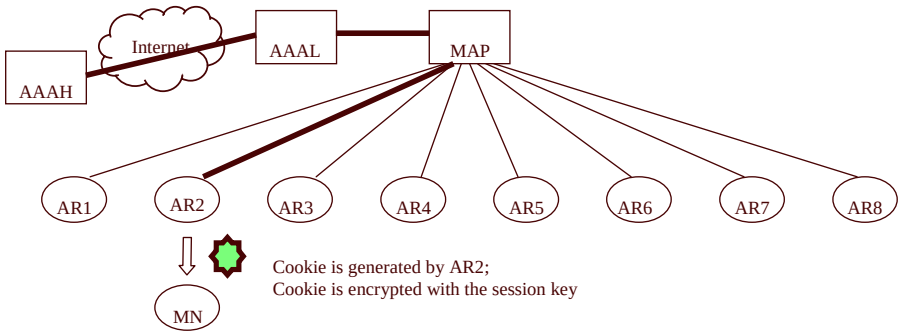

Figure 5.11: First cookie generation

by this AR. Of course, it is necessary to contain corresponding entities in the trusting list and the trusted list of the various ARs in the access network. An AR puts its neighboring ARs (at least the adjacent ARs) on its trusted and trusting list. The AR is on its own two lists since AR accepts the cookies generated by itself.

When the MN performs an intra-domain handover, it submits the cookie to the new AR in plaintext. The new AR then takes three actions as the verification:

- check the timestamp to see whether the cookie is expired;
- check the identity of the cookie generator to see whether the cookie is created by an AR on its trusted list;
- If the above two checks pass, re-compute a key-hashed digest of the cookie information by using the cookie key, and compare it to the hash digest contained in the cookie. If the two hash digests match, the cookie check verification has been completed successfully.

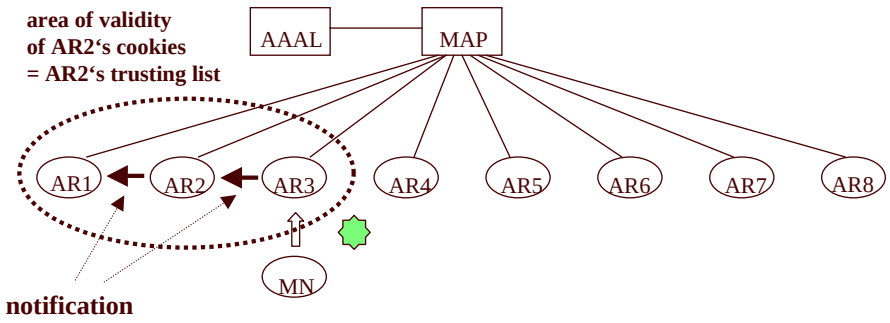

Figure 5.12: Cookie verification

Figure 5.12 shows how AR verifies a cookie. If the verification succeeds, the QoS-conditionalized BU process and re-authorization process begin. The new AR will re-authenticate the re-registration request when it gets the session key embedded in the BU ACK message from the MAP.

If the verification fails, the AR will drop the re-registration request silently in order not to devote further resources to this possibly bogus request. If after a certain amount of time the MN has not received any re-registration answer from the AR, it has to initiate an authentication and authorization process involving AAAL and AAAH as in an inter-domain handover or power-up case since the old cookie has been transmitted in plaintext and can not be used anymore. Thus the MN can not get the benefit of the optimized handover processing. Even though the verification failure could happen due to packet loss over wireless interfaces, cookie key updating or interfere by an attacker, the cookie-based preliminary check can prevent DoS attacks to the access network. However, it is assumed that an MN does not experience this case very often during its normal operation (i.e. continuous moving without interrupting the service use).

After verifying a cookie, the new AR informs the old AR who generated the cookie about the cookie usage. The old AR then notifies all ARs on its trusting list except the new AR to invalidate the cookie preventing the second cookie usage attempt at these ARs since an attacker could eavesdrop the cookie from the open wireless interface and replay it to cheat these ARs for access.

After the expiration of a cookie's lifetime, all ARs can delete their knowledge about its usage.

A new cookie encrypted with the session key is granted to the MN for its next intra-domain handover unless the re-authentication check fails. The old cookie can not be used in the access network anymore. Figure 5.13 shows MN is granted a new cookie.

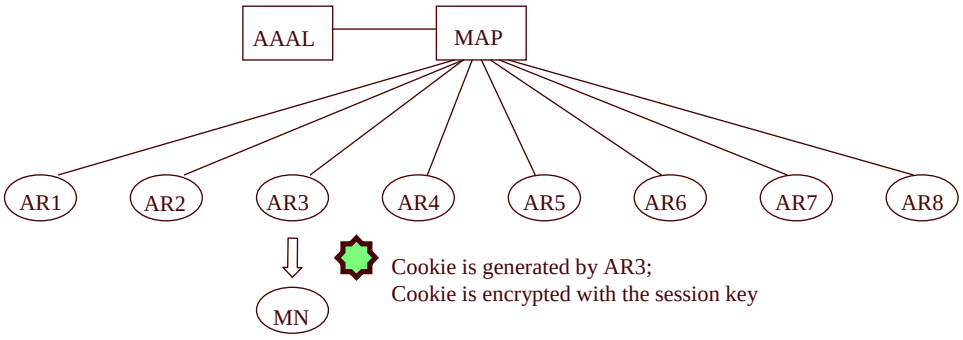

Figure 5.13: New cookie granting

5.4.3 Simulation Results

A performance evaluation is performed by simulating three cases in the re-registration processes in HMIPv6 intra-domain handovers with OMNET++(Objective Modular Network Testbed in C++), an object-oriented modular discrete event simulator.

- Case 0: there is no cookie protection.

  In the case that there is no cookie check at an AR, AR should contact AAAL for the purpose of re-authentication and re-authorization (re-AA) after receiving a re-registration request. When it receives a positive re-AA ACK message for a request from AAAL, the AR starts a QoS-conditionalized BU process for the request. If the re-AA fails, AAAL drops the packets silently without notifying the AR.

- Case 1: AR verifies the presented cookie and if the check passes, it starts two processes (QoS-conditionalized BU process and re-authorization) in series.

  In this case, an AR performs a preliminary check with cookie, which is included in the Hop-by-Hop option in the IPv6 header, after receiving a re-registration request destined to the MAP. If the check passes, the AR continues the uplink of the BU process, as well as it does the notification. When the message arrives at MAP and the path can satisfy at least the minimal QoS, MAP initiates an re-authorization process to AAAL. If the authorization succeeds, MAP sends a downlink message of the BU process towards MN. When the AR receives the message, it performs the re-authentication with the knowledge of the session key. If the check is successful, it generates a new cookie, encrypts it with the session key, and inserts it in the Hop-by-Hop option in the BU ACK message.

- Case 2: AR verifies the presented cookie and if the check passes, it starts two processes (QoS-conditionalized BU process and re-authorization) in parallel.

  In this case, an AR performs a preliminary check with cookie, which is included in the Hop-by-Hop option in the IPv6 header, after receiving a re-registration request destined to the MAP. If the check passes, the AR start the two processes in parallel, as well as it does the notification. It is assumed that the result of the re-authorization process arrives earlier than that of the QoS-conditionalized BU process so that the time spent on the former process has no contribution to the contribution to the re-registration delay.

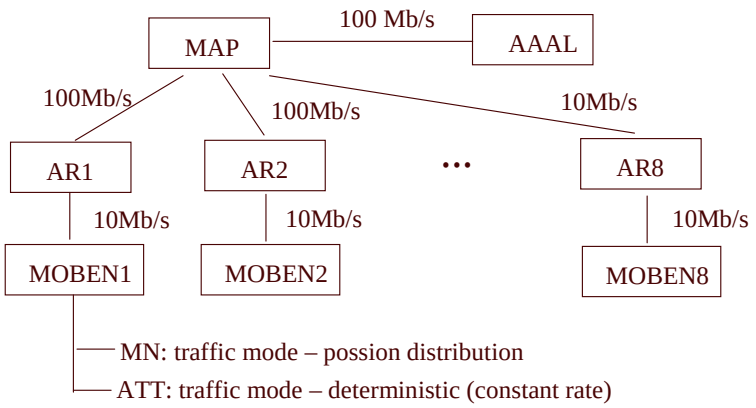

Figure 5.14: Topology assumed in the simulation

Figure 5.14 shows the topology used in the simulation.

The simulation model consists of one AAAL, one MAP, eight ARs and eight mobile environment (MOBEN). The AAAL connects the MAP with a 100 Mbps Ethernet link; the MAP connects every ARs with 100 Mbps Ethernet links; Each AR is responsible for one MOBEN, which represents 4000 MNs and one attacker. Each MN or the attacker sends requests to the corresponding AR as re-registration requests via a wireless link of 10 Mbps data rate.

At each AR, the inter-arrival traffic from legitimate MNs is modeled with a Poisson process with the mean inter-arrival time of 0.5s [30]; Each of the 4000 MNs in one MOBEN performs 1.8 intra-domain handovers per hour.

The traffic of an attacker is modeled with deterministic process. That means an attacker always sends bogus requests with a constant rate.

To evaluate how efficient the cookie mechanism works in the re-registration processes, we focus on how the attacking rate influences the following three parameters in three different cases:

- Mean re-registration delay: the duration between the transmission of the first bit of a re-registration request of a legitimate MN and the arrival of the last bit of the corresponding re-registration response. This parameter can reflect the signaling capacity of a path the efficiency of an intra-domain handover.
- Number of tasks in AAAL per second: how many re-AA tasks in Case 0 and how many re-authorization tasks in Case 1. When AAAL has too high throughput of re-AA, the computing capacity is threaten by DoS attacks.
- The Queue length at AAAL: how many messages waiting in the incoming queue for being processed. When AAAL has too many messages waiting in its queue, its storage capacity is being exhausted.

Figure 5.15 is given for illustrative purposes and shows how the attacking rates increases over time during the simulation. The starting point of the attacking rate is set to 100, and the attacking rate increases by 10 every six minutes. During each six-minute period, the attacking rate is constant.

Figure 5.16 shows how the increasing attacking rate influences the average re-registration delay. Before the attacking rate reaches 200 per second, the average re-registration delay stays relatively constant. That means attackers does not give the access network any trouble with the attacking rate less than 200 per second.

Afterwards, with the increasing of the attacking rate, the average re-registration delay in no-cookie case (Case 0) goes up gradually while the parameter in cookie cases (Case 1 and Case 2) still keeps stable. This proves that the cookie mechanism is efficient in preventing depletion of signaling capacity and beneficial of optimized intra-domain handovers.

Figure 5.17 shows that the cookie verification at ARs can prevent AAAL from heavily loaded by re-authentication and re-authorization works, and prevent AAAL's queue from being filled up shown in Figure 5.18.

Therefore, this performance evaluation shows that the cookie-based mechanism is efficient to deal with DoS attacks as identified in Section 5.4.1, and therefore improves the optimized and QoS-aware handovers.

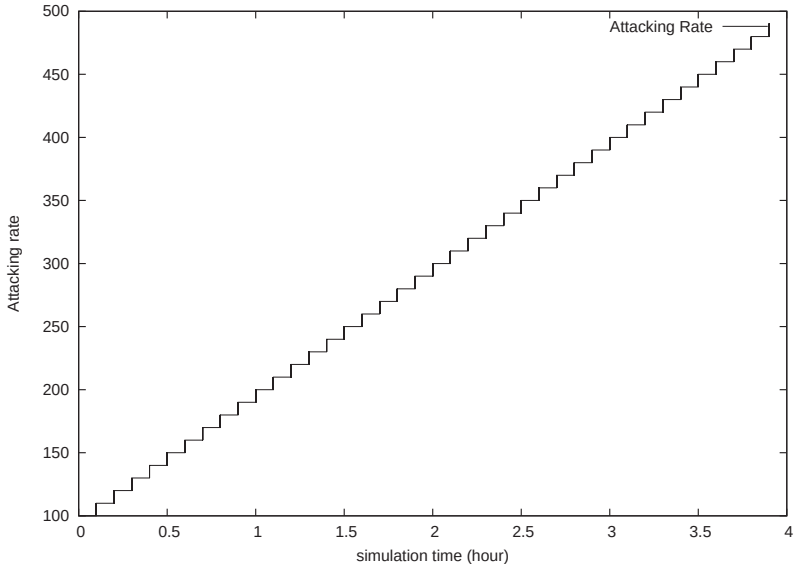

Figure 5.15: Increase of attacking rate over time

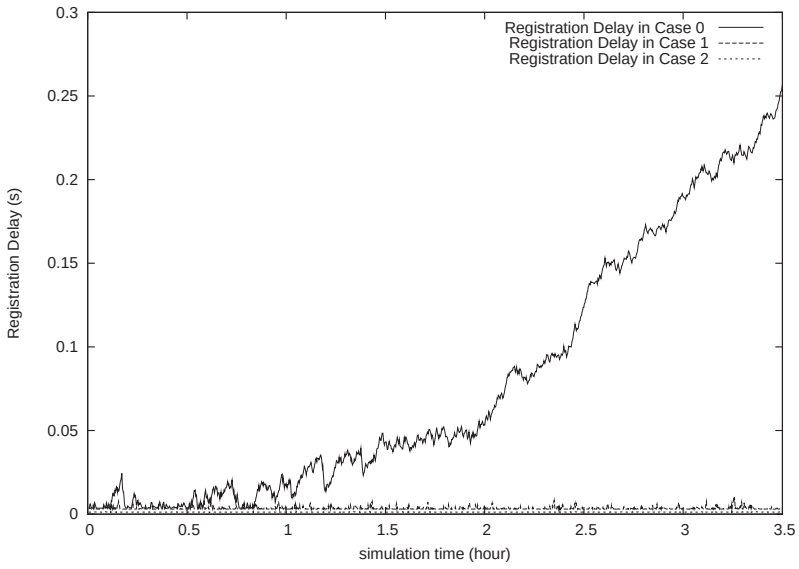

Figure 5.16: Impact of increasing attacking rate on mean re-registration delay

5.4.4 Discussion on the Cookie Mechanism

A couple of concerns of the cookie mechanism might deserve further discussion:

- *Discussion on session keys:*
  Originally a session key is used to secure end-to-end communications between MN and MAP or MN and CN. In our cookie mechanism, the session key is used for authenticating the MN

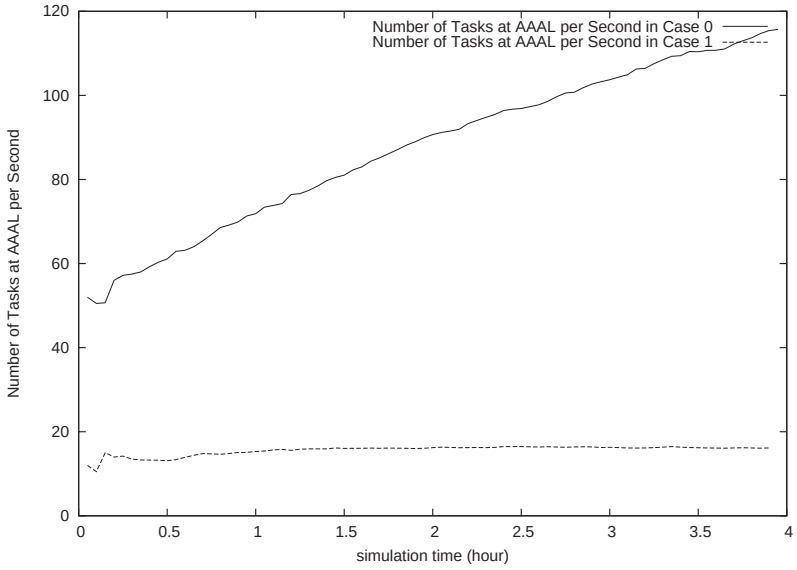

Figure 5.17: Impact of increasing attacking rate on number of tasks in AAAL

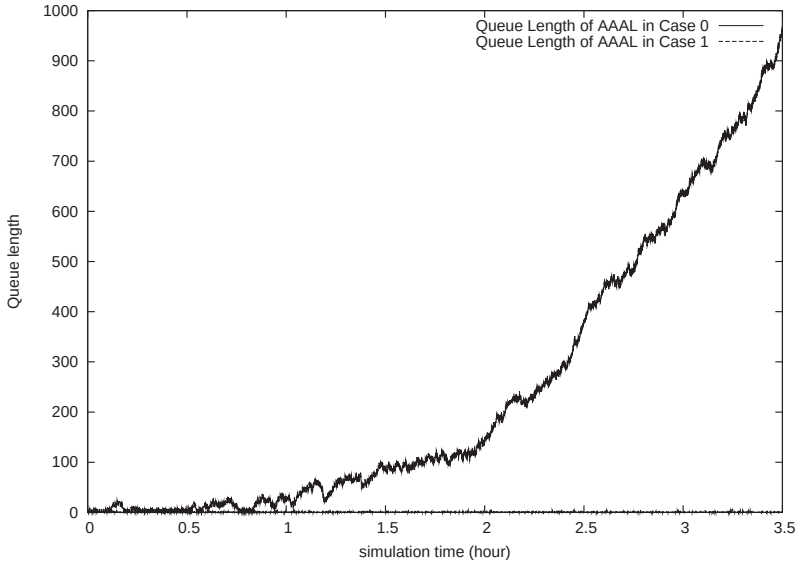

Figure 5.18: Impact of increasing attacking rate on queue length of AAAL

when the new AR gets the session key from MAP and encrypting a new cookie granted to the MN by the new AR.

It might be useful as the authentication key to protect message integrity of hop-by-hop BU packet at each node along a QoS path.

Since the session key can be used for multiple purpose and is known by many entities such as ARs, MAP and AAAL, it easily becomes compromised. The threat of a compromised session

key should be evaluated.

- *Discussion on cookies:*
  It theoretically proves that DoS attack to a path can be completely prevented with the assumption that notifications will arrive at destinations ahead of replayed cookies. However, when the cookie itself or the cookie key is compromised, the risk of DoS attacks can not completely removed.

  If the cookie is compromised at MN before being sent out, an attacker can present the cookie to gain access at the ARs who are on the cookie generator's trusting list masquerading the victim MN. After the attacker gains access, it makes the ARs start the QoS-conditinalized BU process - reserving resources along the path for the malicious requests. The ARs can not realize the attack until the BU ACK arrives and ARs re-authenticate the requests with the session key. If the session key for the victim MN is not compromised, the re-authentications surely fail. But the attacker has already make the attacked path reserving resources for nothing and make the ARs computing the expensive cryptographic re-authentication check. Also the victim MN's request with the cookie will be rejected due to the used cookie; If the session key for the victim MN is also compromised, the re-authentications at the ARs can also pass! Hence, the attacker can get new cookies to continue its DoS attack on the ARs and the paths they lead. As a result, the paths are blocked to any legitimate users and the reserved resources are charged to the victim MN (potentially non-repudiation threat). This attack is strict within the area of the validity of the compromised cookie. Results will be: in the first case, the victim MN has to be authenticated and authorized as a new user; in the second case, auditing should be useful to limit the loss of the victim MN. This attack is not very serious.

  If the cookie key is compromised, an attacker can forge as many cookies as it wants since it can generate randomly user ID, random number if it knows the rule to create them and fill in the target AR's ID and a timestamp. All paths in the access network may suffer the DoS attack by the so much amount of cookie-enabled malicious QoS requests. If the user ID doesn't exist, MAP cannot find a session key accordingly, and AAAL cannot find an authorization record. Thus MAP starts the downlink process to release the reserved resources. Attacker thus deliberately keep the attacked paths busy with reserving and releasing; If the user ID does exist, the reserved resources will be charged to the victim user. This attack spreads in the whole access network. Solution: if the MAP notices so many non-existing user ID, it will update the cookie key invalidate the legitimate users' cookies.

5.4.5 Conclusions

Conceptually, the cookie mechanism can be regarded as a method to classify the special users who has cookies from the ordinary users who do not have cookies. We can imagine that two queues are formed at ARs: MNs with valid cookies are under a fast registration process while MNs without valid cookies have to proceed the normal registration process as described in inter-domain handover cases. Figure 5.19 shows the concept.

Conclusively, the cookie mechanism is claimed to be:

- a method to speed up re-registration in the intra-domain handover case by parallelizing QoS

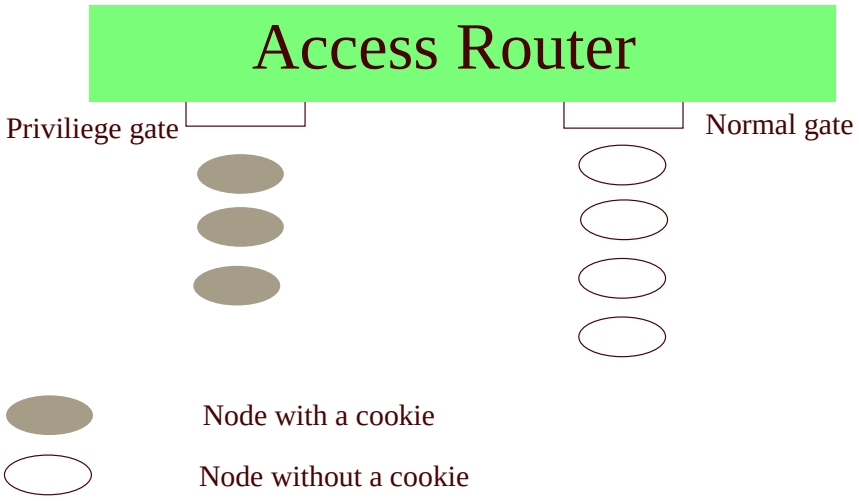

Figure 5.19: An Analogy of the Cookie Concept

reservation process and re-AA process;

- a method to protect against DoS attacks in QoS reservation process in a distributed scenario;
- a method to reduce the risk of replayed cookies by implementing an *"area of validity"* in which a cookie is acceptable, and by communicating cookies that have been used once at a particular AR to other ARs in the same area of validity.

The mechanisms of this solution furthermore can protect against the following depletion threats (which exist when re-authentication and resource reservation are performed in parallel or sequentially:

- against depletion of the memory of access routers that would have to maintain state while the authentication of the MN is fetched from the AAAL;
- against depletion of signaling capacity in the access network (by preventing signaling traffic for bogus requests which have not been verified before as being "credible"), and
- against depletion of the resources of the AAAL (by shielding the AAAL form re-authentication requests which result from bogus QoS requests).

However, it is not a scheme to deal with:

- DoS attacks when malicious nodes send bogus registration requests which cause the normal authentication processes in the access network;
- the attacks played by credible nodes;

- the threat that an attacker eavesdropped a cookie in plaintext and replays it to ARs faster than the notification messages propagate.

Chapter 6

Implementation and Demonstration

In the SeQoMo project, all the three components (Mobility, QoS and Security) have been integrated on a prototypical testbed as shown in Figure 4.3 and 4.4.

6.1 Implementation

The prototypical implementation of the QoS-Conditionalized Handover (QoCoo) testbed has been described in 4.4. To integrate the cookie mechanism in the testbed, the following cookie-related steps are implemented [9]:

- When MN sends a re-registration request packet to an AR, a cookie is appended to the Hop-by-Hop QoS option in IPv6 header.
- When the AR receives the packet with the QoS monitoring module, the verification is performed immediately before the QoS information is cached. Also the AR needs to remove the cookie before it forwards the packet.
- When MAP generates a BU ACK packet, it reserves a place for a cookie so that the AR can insert a new cookie.
- When the AR receives the BU ACK packet, it generates a new cookie, encrypts it and appends the encrypted one to the Hop-by-Hop QoS option in IPv6 header.
- When MN receives the BU ACK packet, it extracts the cookie by decrypting it with the session key.

6.2 Demonstration

A demonstration is shown based on Figure 5.5 in Section 5.3.2.

- Demo 1: An intra-domain handover to ARa1 (see Figure 4.3) with AVailable Bandwidth (AVBW)(10) > DBW(8) > ABW(2)
  - Observation 1: BU at MAP: 3ffe:b80:44c:2233:5aff:fec4:9575(HoA) 3ffe:b80:44c:5:210:5aff:fec4:9575(CoA)
    - in the binding cache at MAP, Home Address is the RCoA of the MN; Care-of Address is the LCoA of the MN;
  - Observation 2: BU at HA: 3ffe:b80:44c::9(HoA) 3ffe:b80:44c:2233:5aff:fec4:9575(CoA)
    - in the binding cache at HA, Home Address is the Home Address of the MN; Care-of Address is the RCoA of the MN;
  - Observation 3: Reservation information at MAP and AR: Reserved Bandwidth (RBW):8 ABW:2
    - the total bandwidth is set to be 10. When 8 is requested, 8 is reserved and 2 is available.
  - Observation 4: Reservation information at MN: DBW:8 ABW:2 RBW: 8
  - Observation 5: Cookie information at AR: a cookie is presented and cookie verification is OK.
  - Observation 6: Cookie information at MN: a new cookie generated by ARa1 is received.
- Demo 2: An intra-domain handover from AR2 to ARa1 with the same QoS parameters
  - Observation 1: BU at MAP: the home address is unchanged; the CoA is changed to 3ffe:b80:44c:6:210:5aff:fec4:9575
    - when MN receives advertisement from ARa2, it generates a new LCoA. When the link to ARa1 is disconnected to simulate a handover, it performs the BU process via ARa2.
  - Observation 2: BU at HA: unchanged
    - in intra-domain handovers, only local BU with MAP needs to be done. There is no BU packet to HA.
  - Observation 3: Reservation information at MAP, AR and MN is unchanged.
  - Observation 4: Cookie information at AR: a cookie generated by ARa1 is presented and the cookie verification is OK.
  - Observation 5: Cookie information at MN: a new cookie generated by ARa2 is received.
- Demo 3: An intra-domain handover from AR1 to ARa2 with DBW(12)>AVBW(10)>ABW(2)
  - Observation 1: BU at MAP: the home address is unchanged; the CoA is changed back to 3ffe:b80:44c:5:210:5aff:fec4:9575
  - Observation 2: BU at HA: unchanged
  - Observation 3: Reservation information at MAP, AR and MN is 10

    - Since the maximum bandwidth the path can provide is 10, only 10 is reserved even though the desired bandwidth is 12.
  - Observation 4: Cookie information at AR: a cookie generated by ARa2 is presented and the cookie verification is OK.
  - Observation 5: Cookie information at MN: a new cookie generated by ARa1 is received.

- Demo 4: increase ABW to 12. i.e. DBW(12)=ABW(12)>AVBW(10)
  - Observation 1: BU at MAP: The BU is gone.
    - Since the path can not provide the minimum bandwidth MN requests, the BU at MAP fails and there is no micro-mobility support to this MN.
  - Observation 2: BU at HA: 3ffe:b80:44c::9(HoA) 3ffe:b80:44c:5:210:5aff:fec4:9575(CoA)
    - Since there is no micro-mobility support in the foreign domain, MN performs a BU with its HA with only MIP support.
  - Observation 3: Reservation information at MN, AR, MAP is 0
    - Since there is no HMIP and QoS support, no resource is reserved in the foreign domain.

- Demo 5: an attacker sends a QoS request (AVBW(10)>DBW(8)>ABW(2)) with a wrong cookie
  - Observation : AR displays cookie verification fails. There is no BU entry at HA and MAP for the attacker. Also there is no resource reservation at MAP and AR for the attacker.
    - Since the cookie verification fails at AR, the AR just drops the request silently.

- Demo 6: MN sends normal QoS requests while the attacker sends QoS requests with wrong cookies at a constant rate.
  - Observation 1: all the requests with wrong cookie fail.
    - Since the cookie verification fails at AR, the AR just drops the request silently.
  - Observation 2: The QoS-Conditionalized Binding Update (QCB) operations for MN's quests is not interrupted.

Chapter 7

Conclusions and Future Work

The SeQoMo architecture supports advanced mobility mechanisms, security and QoS support based upon IP protocol in a unified framework.

In this report, we described the rationale, design and functionality of the architectural components and their interactions. As a unified framework, SeQoMo architecture is implemented on a prototypical testbed and some typical functional tests and performance measurements are finished.

To address the difficult problem of efficient (low latency and low overhead with QoS-enabled security protection) handovers for mobile IP traffic, a couple of measures are taken:

- HMIPv6 is employed as the micro-mobility management protocol.
- In intra-domain handover cases, QoS signaling information is piggybacked in a BU packet.
- A range of a QoS parameter (e.g. upper and low bounds of bandwidth) rather than a specific value is used in a QoS request.
- Mobile node's authorization information is cached locally at AAAL after its successful inter-domain handover in the foreign domain.
- A cookie is used for a preliminary authentication check to save time on performing a re-authenticate at AAAL before the QoS-Conditionalized Binding Update (QCB) process begins.

Additionally, the developed concepts and results also include that:

- a dynamically updated authorization process prevents disclosure of a mobile node's subscribed QoS parameters;
- the cookie mechanism counters potential DoS attacks to the access network in the foreign domain.

Future work includes investigations on using CASP as the signaling protocol in the SeQoMo architecture, cooperating with other fast handover mechanisms regarding re-establishment of QoS and security states.

Furthermore, enhanced advertisements of access routers which include additional information such as currently available bandwidth and price can help a mobile node to select the most suitable access router as the target of its next QoS-conditionalized handover.

Chapter 8

Acronyms

AA Authentication and Authorization

AAA Authentication, Authorization, Accounting

AAAL local AAA server

AAAH home AAA server

ABW Acceptable Bandwidth

ACK Acknowledgement

AMA AA-Mobile-Node-Answer

AMR AA-Mobile-Node-Request

AN Access Network

AP Access Point

API Application Program Interface

AR Access Router

ARR AA-Registration Request

ARA AA-Registration Answer

ARP Address Resolution Protocol

ASM Any Source Multicast

ATM Asynchronous Transfer Mode

AVBW AVailable Bandwidth

AVP Attribute Value Pairs

BA Binding Acknowledgement

BC Binding Cache

BdR Border Router

BR Binding Request

BSC Base Station Controller

BU Binding Update

BUL Binding Update List

CASP Cross Application Signaling Protocol

CIDR Classless Inter Domain Routing

CMS Cryptographic Message Syntax

CN Corresponding Node

CoA Care-of Address

CT Context Transfer

DAD Duplicate Address Detection

DBW Desired Bandwidth

DHCP Dynamic Host Configuration Protocol

DiffServ Differentiated Services

DLL Data Link Layer

DoS Denial of Service

DSCP DiffServ Code Point

DVMRP Distance Vector Multicast Routing Protocol

ER Edge Router

FTP File Transfer Protocol

GPRS General Packet Radio Service

GSM Global System for Mobile Communication

HA Home Agent

HAO Home Address Option

HAWAII Handoff Aware Wireless Access Internet Infrastructure

HMIP Hierarchical MIP

HMIPv6 Hierarchical Mobile IPv6

HO Handover

HoA Home Address

HOA HOme-agent-Answer

HOf handover frequency

HOR HOme-agent-Request

HMAC-MD5 Keyed-Hashing for Message Authentication using MD5(Message-Digest 5

HMAC-SHA1 Keyed-Hashing for Message Authentication using SHA1(Secure Hash Algorithm 1

ICEBERG Internet Core Beyond the Third Generation

ICI Interface Control Information

ICMP Internet Control Message Protocol

ICMPv6 Internet Control Message Protocol version 6

ID identification

IDU Interface Data Unit

IEEE The Institute of Electrical and Electronics Engineers

IETF Internet Engineering Task Force

IHA IP-level handover assistant

IntServ Integrated Services

IP Internet Protocol

IPng IP Next Generation

IPv4 Internet Protocol version 4

IPv6 Internet Protocol version 6

IR Intermediate Router

L2 layer-2

L3 layer-3

LAN Local Area Network

LCoA Local Care-of Address

LXR Linux Cross Reference

MAC Medium Access Control

MAP Mobile Anchor Point

MAO Mobile Anchor Point Option

MBW Maximum Bandwidth

MD Movement Detection

MHC Manageable Hub Configuration

MIP Mobile IP

MIPL Mobile IP for Linux

MIPv6 Mobile IPv6

MIPv4 Mobile IPv4

MN Mobile Node

MOBEN mobile environment

MOMBASA Mobility Support - A Multicast Based Approach

MPLS Multi-Protocol Label Switching

NAI network access identifier

NbAdv Neighbor Advertisement

ND Neighbor Discovery

NbSol Neighbor Solicitation

NIC Network Interface Card

NSIS Next Steps in Signaling

OS Operating System

PDP Policy Decision Point

PDU Protocol Data Unit

PEP Policy Execution Point

PIM-SM Protocol Independent Multicast - Sparse Mode

PIM-SSM Protocol Independent Multicast - Single Source Mode

QCB QoS-Conditionalized Binding Update

QHC QoCoo controller

QoS Quality of Service

QoCoo QoS-Conditionalized Handover

QSE QoS-aware security entity

RA Router Advertisement

radvd router advertisement daemon

RAT Reverse Address Translation

RBW Reserved Bandwidth

RCoA Regional Care-of Address

RD Redirect

RFC Request For Comment

RH Routing Header

RS Router Solicitation

RtAdv Router Advertisement

RtSol Router Solicitation

RSVP Resource Reservation Protocol

RTT round trip time

SAP Service Access Point

SDL Specification and Description Language

SIP Session Invitation Protocol

SNMP Small Network Management Protocol

SP Service Primitive

TBA To Be Added

TCP Transmission Control Protocol

TLV Type-Length-Value

UDP User Datagram Protocol

UMTS Universal Mobile Telecommuniation System

VoIP Voice over IP

WAN Wide Area Network

WLAN Wireless Local Area Network

Bibliography

[1] S. Blake, D. Black, M. Carlson, E. Davies, Z. Wang, and W. Weiss. An Architecture for Differentiated Services. RFC 2475, December 1998.

[2] B. Braden, D. Clark, and S. Shenker. Integrated Services in the Internet Architecture: An Overview. RFC 1663, June 1994.

[3] M. Brunner. Requirements of QoS Signaling Protocols, April 2002.

[4] P. R. Calhoun and C. E. Perkins. Diameter Mobile IPv4 Application, October 2002.

[5] M. Carson. Application and Protocol Testing through Network Emulation, September 1997.

[6] H. Chaskar. Requirements of a QoS Solution for Mobile IP. Internet Draft draft-ietf-mobileip-qos-requirement-03.txt, July 2003.

[7] H. Chaskar and R. Koodli. A Framework for QoS Support in Mobile IPv6. Internet Draft draft-chaskar-mobileip-qos-01.txt, March 2001.

[8] T. Chen and G. Schäfer. Design of QoS-aware Authorization For Mobile Devices. SeQoMo project deliverable D-Security-2, May 2002.

[9] T. Chen and G. Schäfer. Intermediate Implementation Report: Security measures in the SeQoMo project. SeQoMo project deliverable D-Security-3, September 2002.

[10] T. Chen and G. Schäfer. QoS-aware Authorization for Mobile Devices. SeQoMo project deliverable D-Security-1, March 2002.

[11] C. Perkins (ed.). IP Mobility Support. RFC 2002, October 1996.

[12] C. Perkins (ed.). IP Mobility Support for IPv4. RFC 3344, August 2002.

[13] D. Estrin, D. Farinacci, A. Helmy, D. Thaler, S. Deering, M. Handley, V. Jacobson, C. Liu, P. Sharma, and L. Wei. Protocol Independent Multicast-Sparse Mode (PIM-SM): Protocol Specification. Internet RFC 2362, June 1998.

[14] S. Faccin, B. Patil, and C. Perkins. Diameter Mobile IPv6 Application, March 2002.

[15] W. Fenner. Internet Group Management Protocol, Version 2. Internet RFC 2236, November 1997.

[16] A. Festag. Performance Evaluation of MIP w and w/o Hierarchical FAs: Goal, Metrics, Parameters and Testbed Setup SeQoMo project deliverable D-MM-3, February 2001.

[17] A. Festag. Performance Evaluation of Multicast-based Handover: Goal, Metrics, Parameters and Testbed Setup. SeQoMo project deliverable D-MM-8, October 2001.

[18] A. Festag. Optimization of Handover Performance by Link Layer Triggers in IP-Based Networks; Parameters, Protocol Extensions, and APIs for Implementation. Technical Report TKN-02-014, Telecommunication Networks Group, Technische Universität Berlin, July 2002.

[19] A. Festag. Performance Comparison of HMIPv4 and MOMBASA SeQoMo project deliverable D-MM-10, March 2002.

[20] A. Festag. Update on Current Development and Trends in Handover Design for All-IP Wireless Networks SeQoMo project deliverable D-MM-1, March 2002.

[21] A. Festag, H. Karl, and G. Schaefer. Current Developments and Trends in Handover Design for ALL-IP Wireless Networks. Technical Report TKN-00-007, Telecommunication Networks Group, Technische Universität Berlin, August 2000.

[22] A. Festag, L. Westerhoff, A. Assimakopoulos, and A. Wolisz. Rerouting for Handover in Mobile Networks with Connection-Oriented Backbones - An Experimental Testbed. In *Proc. of ICATM 2000*, pages 491–499, June 2000.

[23] A. Festag and A. Wolisz. MOMBASA: Mobility Support - A Multicast-based Approach. In *Proc. of European Wireless 2000 together with ECRR 2000 (EW'2000)*, pages 491–499, Dresden, Germany, September 2000.

[24] D. Forsberg, J.T. Malinen, J.K. Malinen, and H.H. Kari. Increasing Communication Availability with Signal-based Mobile Controlled Handoffs. In *Proc. of IP based Cellular Net-works (IPCN2000)*, May 2000.

[25] X. Fu, H. Karl, and C. Kappler. QoS-Conditionalized Handoff for Mobile IPv6. In *Proc. of the Second IFIP-TC6 Networking Conf. - Networking2002*, pages 721–730, Pisa, Italy, May 2002. Springer-Verlag.

[26] E. Gustavsson, A. Jonsson, and C. Perkins. Mobile IP Regional Registration. Internet-Draft: draft-ietf-mobileip-reg-tunnel-03.txt, July 2002.

[27] L-N. Hamer, B. Gage, M. Broda, B. Kosinski, and Hugh Shieh. Session Authorization for RSVP, June 2002.

[28] L-N. Hamer, B. Gage, M. Broda, and Hugh Shieh. Framework for Session Set-up with Media Authorization, June 2002.

[29] A. Hess and G. Schaefer. Performance Evaluation of AAA / Mobile IP Authentication. Technical Report TKN-01-012, Telecommunication Networks Group, Technische Universität Berlin, August 2001.

[30] A. Hess and G. Schäfer. Performance Evaluation of AAA / Mobile IP Authentication. In *Proc. of 2nd Polish-German Teletraffic Symposium (PGTS'02)*, Gdansk, Poland, September 2002.

[31] D. Johnson and C. Perkins. Mobility Support in IPv6. Internet Draft draft-ietf-mobileip-ipv6-19.txt (work in progress), October 2002.

[32] D. Johnson, C. Perkins, and J. Arkko. IP Mobility Support for IPv6. Internet-Draft: draft-ietf-mobileip-ipv6-21.txt, February 2003.

[33] J. Kempf. Problem Description: Reasons For Performing Context Transfers Between Nodes in an IP Access Network, September 2002.

[34] G. Kenward. General Requirements for Context Transfer, October 2002.

[35] R. Koodli(ed.). Fast Handovers for Mobile IPv6. INTERNET DRAFT draft-ietf-mobileip-fast-mipv6-06.txt, March 2003.

[36] J. Loughney, M. Nakhjiri, and C. Perkins. Context Transfer Protocol, October 2002.

[37] J. Mysore and V. Bharghavan. A New Multicast-based Architecture for Internet Mobility. In *ACM MOBICOM 97*, October 1997.

[38] A. Neumann. Prototypical Implementation and Experimental Testbed Setup of a QoS-Enabled Mobility Concept Based on HMIPv6, October 2002.

[39] H. Schulzrinne, H. Tschofenig, X. Fu, and J. Eisl. A Quality-of-Service Resource Allocation Client for CASP, March 2003.

[40] H. Schulzrinne, H. Tschofenig, X. Fu, and A. McDonald. Cross-Application Signaling Protocol, March 2003.

[41] H. Soliman, C. Castelluccia, K. El-Malki, and L. Bellier. Hierarchical Mobile IPv6 mobility management (HMIPv6). Internet-Draft: draft-ietf-mobileip-hmipv6-07.txt, October 2002.

[42] M. Stemm and R. Katz. Vertical Handoffs in Wireless Overlay Networks. In *ACM Mobile Networking (MONET), Special Issue on Mobile Networking in the Internet*, December 1998.

[43] M. Thomas. Analysis of Mobile IP and RSVP Interactions, February 2001.

[44] H. Tschofenig. NSIS Threats, July 2002.