Technical University Berlin

Telecommunication Networks Group

Secure, QoS-enabled Mobility Support in All-IP Networks

Tianwei Chen, Sven Hermann, Günter Schäfer
[chen,hermann,schaefer]@tkn.tu-berlin.de

Berlin, 06/2003

TKN Technical Report TKN-04-013

TKN Technical Reports Series

Editor: Prof. Dr.-Ing. Adam Wolisz

Abstract

In the last several years mobile communication services have evolved from sparse coverage and constrained mobile devices to an almost ubiquitous coverage with very small-size and multifunctional devices that enable both classical telephony and data oriented applications. Furthermore, the growing trend towards network convergence predicts that upcoming ubiquitous mobile Internet access will be realized by an All-IP-based infrastructure that supports a diverse set of wireless technologies and that realizes seamless interoperability based on protocols of the IP protocol suite. However, IP networks have been originally designed under the assumption that hosts are stationary, such that significant extensions are required in order to make this vision a reality.

This work [1] addressed this challenge and investigated the suitability of IP-based networks for support of mobility under the perspective of advanced mobility mechanisms, security and Quality of Service provisioning. In the course of the project, a series of well balanced mechanisms has been developed, integrated into one unified architecture, and conceptually tested with a prototypical implementation.

Aiming at secure and QoS-aware mobility support in Mobile IP based networks, we mainly focused on an optimized (re-)registration procedure with respect to low latency and small overhead. Additionally, we also developed solutions for securely maintaining or establishing QoS paths in case of session refreshment or initial power up.

With respect to mobility support, we differentiate between global and local mobility scenarios in order to optimize local movements that are expected to happen much more frequently than global movements. The re-routing node is placed close to mobile nodes by employing the Hierarchical Mobile IP architecture (HMIP). Extending the existing HMIP-concepts, the (re-)registration procedure is integrated with QoS signaling and security measures.

As far as QoS is concerned, the handover depends on QoS availability so that a mobile node can choose the AR which is able to provide the most suited QoS. In order to introduce minimum latency to the (re-)registration procedure, QoS and mobility signaling are combined with security mechanisms into one integrated signaling procedure.

Regarding security, we introduce a concept of a two-step authentication in order to protect resources in the access network against Denial of Service (DoS) attacks. Furthermore, efficient authentication and QoS-aware authorization are also addressed in the project. Moreover, in order to allow for fast setup of a secure communication channel upon handover, a scheme has been developed to protect signaling and user data with temporary session keys before a fresh security association between the mobile node and the new access router can be set up.

The developed concepts have been implemented in a prototype testbed and and some selected aspects have further been evaluated by simulation studies.

[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 recent years have seen a rapid development of mobile computing and communication. The technological progress was driven by advances in wireless and wireline transmission technology, cellular technology, communication protocols, micro-electronics and standardization efforts. Mobile service has evolved from a sparse coverage and heavy mobile devices to an almost ubiquitous coverage with very small-size devices affordable to users.

While today's mobile systems are still being optimized for voice communication, they support an increasing variety of mobile data services at low data-rates. In recent years, the demand of data services at high data-rates has been increasing substantially. Meanwhile, the future of mobile communication is considered in the context of ubiquitous computing.

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.

1.1 Background

A vision like this makes great demands on mobile networks, and in this context, problems need to be solved before ubiquitous computing becomes a reality. Certainly, the next generation of mobile network will cope with some of these problems. For example, technologies such as GPRS and UMTS will offer a connection-less service in the near future and, therefore, introduce a paradigm shift from connection-oriented to connection-less communication in mobile networks. In order to shape future networks, it is crucial to identify trends in the development of present-day mobile networks [23].

A variety of new wireless technologies, such as IEEE WLAN [36], UTRAN based on WB-CDMA [15], or Bluetooth [30] is destined to substitute or complement the existing radio technology, such as GSM and IS-95 radio technology. Each of the new these technologies offers a different service in terms of bandwidth and (partly overlapping) spatial coverage. There is no wireless technology that provides all requirements all the time, and there is a tradeoff between coverage, data rates and costs.

Hence, future mobile networks will not base on a single standardized wireless interface, instead, on a set of different technologies and standards.

In the aspect of IP-based network nodes and protocols, future mobile networks will use the Internet model where Internet Protocol (IP) packets are used for both transport and signaling. IP-aware network nodes and devices can give better support to IP applications. They will reduce the cost of deployment, and in addition IP-style engineering is faster and cheaper, as the Internet development has proven. IP-based protocols facilitate a natural convergence of fixed and mobile networks. Finally, considering the wireless interface, an IP-based protocol enables the movement between access points and networks that use different wireless interfaces.

While Mobile IPv4 (MIPv4) [17] and Mobile IPv6 (MIPv6) [37] 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 Quality of Service (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 supported by current Mobile IP (MIP). In this context, the Internet Engineering Task Force (IETF) is developing the requirements for a QoS solution for MIP [9]. Furthermore, security measures are required to protect network infrastructure. The provision of the Authentication, Authorization, Accounting (AAA) service in a mobile environment [7, 20] 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.

Consequently, new wireless technologies which make use of the Internet Protocol as the network protocol press the demand of applicable solutions in the aspects of QoS, mobility and security. As discussed above, the original design of IP mobility schemes lacks of intrinsic architectural flexibility in supporting QoS and security needed in 4G networks. To fill this gap, in the SeQoMo project, we investigate the suitability of existing solutions of QoS, security and mobility in 4G architecture, and we aim to design appropriate protocol functionality to need the requirements.

1.2 Project Goals

This project contributes to the investigation of the suitability of IP-based networks for support of mobility under the perspective of advanced mobility mechanisms, security, and Quality of Service (QoS).

We aim to design appropriate protocol functionality to realize efficient handover operations (mobility support) taking Quality of Service (QoS) and security into account. The three components is targeted to be integrated into an overall Secure, QoS-capable Mobility architecture (the SeQoMo architecture) based upon IP protocols.

The specific objective of this project is to integrate the solutions developed in the SeQoMo project into one joined architecture that uses the Cross-Application Signaling Protocol(CASP) as the principal

signaling protocol. While the goal of the CASP protocol is to provide a simple, flexible and efficient means of signaling a large number of different applications requirements, modularized so that many different application needs can be fulfilled, this project will design and prototypically implement a mobility client protocol for CASP that is specifically suited to the signaling needs of mobile networks with frequent handovers.

1.3 Overview of the Report

The reminder of the report is organized as follows:

Chapter 2 discusses the background and motivation of the SeQoMo architecture;

Chapter 3 gives an overview of architecture;

All involved protocols and mechanism are discussed in Chapter 4;

Chapter 5 illustrates the interactions between the SeQoMo components;

In Chapter 6 details the CASP Mobility Client protocol, which is the main signaling protocol in our context;

In Chapter 7, we draw a conclusion.

Chapter 2

Background and Motivations for the SeQoMo Architecture

This chapter presents the background and motivations for the SeQoMo architecture.

2.1 General Problems of IP Based Mobile Networks

The general problems of current solutions for IP-based mobile networks lie in three aspects: mobility, QoS and security.

2.1.1 Mobility

Originally, IP networks have been designed under the assumption that hosts are stationary. This assumption implies that the IP address does not change and a host is reachable from other hosts by an IP address that does not change. Data are carried by means of IP packets which contain source and destination addresses. Internet routers inspect the destination address contained in an IP packet. They make a forwarding decision based on the network part of the IP destination address and forward packets to the determined next hop. Consequently, this addressing scheme puts restrictions on the address usage. In particular, an IP address can only be used within the network of its definition.

As shown in Figure 2.1, if a mobile host moves to a new network, the old IP address becomes topologically incorrect. Therefore, a new topologically correct IP address must be assigned to a mobile host. In the TCP/IP protocol suite applications access communication services through a socket layer - a protocol independent interface to the protocol-dependent below. When an application establishes a session between two hosts, the IP address of the application‘s source node is used as the source address for the session. Meanwhile, the IP address is interpreted as a host identifier.

When a mobile host moves to a new network then the network part of the mobile host’s IP address does no longer match the IP network address of the new point of attachment. The same problem occurs if the network is divided into subnetworks: When a mobile host moves to a new subnetwork the subnet-id becomes incorrect. The assignment of a new IP address, which is topologically correct,

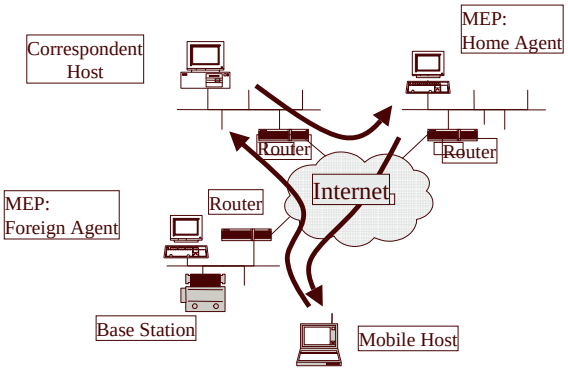


Figure 2.1: The general IP mobility problem

enforces the closure and re-opening of existing communication sockets. In fact, sockets are bound to source and destination addresses. Hence, the re-establishment pertains to the mobile as well as to a correspondent host communicating with the mobile host and disrupts communication service. This dichotomy - an IP address represents both host identification and location - is the fundamental mobility problem in IP-based networks. This problem needs to be solved by mobility concepts.

In summary, the identified problems are as follows:

- current IP-based protocols assume to be stationary hosts;
- IP address reflects both identity and location;
- when hosts become mobile, the ongoing network sessions are disrupted;
- No "user mobility" -concept in Internet as is is common in e.g. GSM.

2.1.2 QoS

With the advent of various radio access technologies and increasing deployment of sophisticated applications in mobile end systems, QoS mechanisms, including resource reservation, admission control and other traffic control functionalities which allow multimedia applications to get certain guarantee on bandwidth and delay of its packets delivery, should be supported in IP based networks. However, the current solutions for mobile IP networks is short of QoS consideration.

As a mobile node moves to a new domain or powers up, it needs to (re-)establish a QoS path. When a mobile node has established QoS flows, it would be preferable to perform a handover only when QoS of these flows can be guaranteed. It may be desirable for the MN to choose an appropriate Access Router (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. Therefore, a handover should be QoS-aware and local QoS signaling is required for handover decisions.

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 [37].

In reference [10] 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.

The traditional QoS signaling protocols (e.g. RSVP [71]) has problems in the IP-based mobile scenarios in the aspects of scalability and signaling overhand.

The requirements for QoS support for handover are as follows:

- Support for traffic flows to obtain QoS treatments 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

Mobility introduces more security holes especially in QoS support, including authentication, confidentiality, integrity and authorization issues; in order to enable seamless IP mobility, security capabilities (especially authentication) are of particular importance to be part of the integrated framework that allows incremental development and deployment of 4G technologies.

The security issues in Mobile IPv6 networks have been identified in [37]. The security features include the protection of Binding Updates both to home agents and correspondent nodes, the protection of mobile prefix discovery, and the protection of the mechanisms that Mobile IPv6 uses for transporting data packets. Binding Updates are protected by the use of IPsec extension headers, or by the use of the Binding Authorization Data option. This option employs a binding management key, Kbm, which can be established through the return routability procedure. Mobile prefix discovery is protected through the use of IPsec extension headers. Mechanisms related to transporting payload packets - such as the Home Address destination option- have been specified in a manner which restricts their use in attacks. However, a simple, efficient and flexible security scheme is needed to suit the demand of 4G networks. It is one of the goals of the SeQoMo project.

The security aspect of the project lies in

- authentication performance over handover - The visited network should verify the MN has the identity it claims to have;
- authorization of QoS requests - 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;
- Denial of Service (DoS) protection of QoS-aware handover process - how to ensure that QoS-reservation can not be abused to reduce the availability of an access network;
- secure the signalings and data traffic over the wireless channel.

2.2 Related Work

2.2.1 Mobility

Mobility support in IP networks has been the subject of intensive research efforts beyond Mobile IP for several years. Therefore, it is worth reviewing the following approaches: hierarchical Mobile IP, Mobile IP extensions by MosquitoNet, Reverse Address Translation (RAT), HAWAII, Cellular IP, IAPP, Mobile People Architecture, ICEBERG, and Extended SIP Mobility. These approaches attempt to supplement or to replace the classical solution for mobility support Mobile IP.

In order to work out the basic assumptions behind the schemes, the motivation to develop a new approach, the required mobility infrastructure as well as the addressing and routing concept are emphasized.

Hierarchical Mobile IPv6

The Mobile IP extension of hierarchical foreign agents [26, 27, 59] addresses a drawback of Mobile IP: If the distance between the foreign agent and the home agent is large, the signaling delay for the registration may be long, which then results in long service disruption and packet losses.

The aim of HMIPv6 is to minimize the latency due to handover operations by reducing the amount of mobility signaling.

In MIPv6 mobility management is done by the Home Agent (HA) (no hierarchy). In HMIPv6 at least one level of hierarchy is introduced, a new function called Mobility Anchor Point (MAP) is done in a router at the visited domain. The MAP is not constrained to be in the same subnet as the Mobile Node (MN), in fact any physical location for the MAP is possible within the visited domain, although better performance is achieved by connecting the MAP to the border router of the network is serving. Thus, a MAP is not needed in each subnet, although there can be more than one MAP in a domain, allowing the use of more than one level of hierarchy in mobility management of MN's. A MAP provides an address or a prefix to form addresses that can be used as a global CoA by MN's visiting the domain. The HA or CN's (after route optimization) use this address to send packets to the MN. The MAP will tunnel these packets to the MN within the MAP domain using a Local CoA (LCoA). The LCoA is an on-link IPv6 address in the subnet where the MN is. If the MN moves to another subnet within the

MAP domain, the global CoA does not change, only the MAP must be informed of the new LCoA of the MN. Compare this with MIPv6, in the case of a handover, the HA and all the CN's must be informed of the new MN CoA. Now we can see the advantages of HMIPv6 for micro-mobility. The handover latency is reduced because mobility is managed locally.

mobility signalling load is reduced. No mobility signalling is sent out of the MAP domain in case of an intra-domain handover, and only the MAP (perhaps more than one if the MN is using a multi level hierarchy) must be informed of the change (in MIPv6 the HA and all the CN's must be informed).

HMIPv6 is an extension to MIPv6, a MN that is HMIPv6-aware can use the MAP or can use the standard MIPv6 implementation (ignoring the MAP and registering the LCoA in the HA). Moreover, the MN can use the LCoA with certain MN's (for example, those in its same subnet to avoid going through the MAP) and the global CoA with the rest. There are two MAP modes in HMIPv6. In Basic Mode, the MN forms an IPv6 address in the MAP subnet (Regional CoA or RCoA) using the MAP announced prefix. The MN uses the RCoA as the global CoA. In Extended Mode, the MN uses the MAP IPv6 address as an alternate-CoA. The decision of which mode to use is a network administration one. Each MAP can support only one mode at a time. To use HMIPv6, a MN must discover the MAP's serving the domain it is visiting. To do this, a new MAP option for Router Advertisement messages is proposed. This option includes the distance to the MAP in number of hops, a level of preference in using this particular MAP, the MAP global IPv6 address, and an indication about the mode of operation (basic or extended) of the MAP. If the MAP is operating in basic mode, the MAP option includes also the MAP's subnet prefix. To propagate the MAP option from the MAP to the MN there are different possibilities. For example, the routers in the domain, including the MAP and the Access Routers (AR's) can be manually configured to propagate the MAP option on certain interfaces. The result is that the MN receives router advertisements from its AR including a MAP option for each MAP that it is serving the subnet where the MN is. It is up to the MN to choose one or more (more than one level of hierarchy) MAP's to use. A MAP domain is defined as the subnets where the MAP option of a particular MAP is received. The domains of different MAP's can overlap. After discovering the MAP, the MN must register in it. This is done using a extended Binding Update (BU) option that allows to indicate a MAP registration, differentiating it from a HA registration or a BU sent to CN's. Summarizing the advantages of HMIPv6, it allows reducing the signalling load in intra-domain handovers (no signalling is sent outside the domain), and intra-domain handovers delay is reduced because the handovers are managed locally.

Hierarchical proposals seem to be useful also in the integration of AAA infrastructure and QoS provision in MIPv6, mainly due to the idea of using the MAP as a point to provide context transfer to the MN in handovers, but how this can be exactly done is not clearly defined yet. Last, a paging framework can be easier to create in a HMIP environment. HMIPv6 also has disadvantages, it implies some modifications to the basic MIPv6, it means more complexity in the network, end-to-end delay can be longer because the intermediate processing, and potentially inter-domain handovers delay can be increased.

MosquitoNet Extensions of Mobile IP

Other extensions have been proposed by the MosquitoNet group in [72]. The goal of these extensions are to use Mobile IP most efficiently and flexibly on mobile hosts. Mobile IP is extended by the

following functionalities:

- The regular IP routing table is extended by a Mobile IP specific routing table.
- The Mobile IP home agent can manage multiple CoAs for a single mobile host simultaneously and bind a flow to a certain interface.
- The protocol supporting registration between the mobile hosts and the home agent is extended.

First of all, these extensions allow to decide whether to use transparent mobility support or not. It is argued that Mobile IP implies some remarkable overhead which should be avoided when transparent mobility support by indirect routing is not necessary. Second, the mobile host can decide whether to use triangular routing or bi-directional routing. Mobile IP route optimization (triangular routing) fails when router ingress filtering is used: Packets are dropped when they do not carry a topologically correct IP source address. Therefore, a mobile may use the more robust bi-directional tunneling although it implies an additional overhead. The information whether to use transparent mobility or indirect routing, as well as triangular or bidirectional tunneling, is contained in the Mobile IP specific routing table on a per socket basis.

In the context of this approach the support of multiple interfaces in a mobile host is essential. Each interface carries a temporary IP address. A flow can be bound to a specific interface. This is done with the help of a socket option. For transmission, the route lookup has been modified, so that only routes with that specific interface are considered. For reception of data, a flow-to-interface binding (flow is recognized by IP addresses and port number) is sent to the Mobile IP home agent which forwards datagrams to the appropriate CoA. The handover is similar to Mobile IP, but extends the protocol by an update of the flow-to-interface binding in the Mobile IP home agent. The extension is mainly intended for vertical handover of mobile hosts with multiple network interfaces.

Reverse Address Translation (RAT)

The RAT approach [58] is motivated by the limited deployment of Mobile IP. It is intended to simplify mobility support in order to break the chicken and egg-trap between the lack of applications which require mobility support and the poor deployment of Mobile IP. The RAT approach can be considered as a tradeoff: On the one hand it dispenses with the requirement to maintain TCP connections. On the other hand overhead is decreased and most of the traffic can be routed directly. Moreover, the inventors of RAT argue that implementation of Mobile IP functionality is operating system dependent (e.g. registration, tunneling, etc.), whereas RAT aims at a solution that is independent of the operating system.

In the RAT approach the mobile host owns an IP home address and acquires a temporary IP address in the foreign network. The RAT approach adds new entities to the home network: a registration server and a RAT device. The network infrastructure remains unchanged. In particular, there are no mobility-specific entities required in the foreign network. The RAT approach applies Network Address Translation (NAT) [60]. NAT is an Internet paradigm that has been widely applied recently, for extending the IP address space in IP version 4, but also supports the security when used in firewalls.

The RAT approach works as follows: Suppose a correspondent host wishes to send a packet to the mobile host and directs it to the mobile host's home address. In the home network, the RAT device intercepts the packet and performs a network address translation. Therefore, it replaces the destination address with the mobile host's temporary address and the source address with the address of the RAT device. Then, the packet is sent directly to the mobile host without tunneling. In the reverse direction, the mobile host sends a packet to the RAT device, which in turn performs the address translation and sends it to the correspondent host. This scheme is referred to as reverse address translation. One of the main advantages of this approach is that the indirect routing is deployed for correspondent host initiated sessions only. When the mobile host initiates the session, it will use its temporary address (which is topologically correct) and communicate with the correspondent host directly5, and thus no indirect routing via the home network is required. This results in shorter routes and does not increase the packet length by encapsulation.

Handover Aware Wireless Access Internet Infrastructure (HAWAII)

HAWAII [53, 54] was proposed since Mobile IP results in high control overhead and high latency for local mobility. Also, HAWAII eases the usage of resource reservation protocols (such as RSVP) in a mobile environment, where a mobile host acquiring a new CoA on each handover would trigger the establishment of a new resource reservation. The HAWAII approach extends Mobile IP and addresses its limitations.

HAWAII defines a domain. This is a division of the wireless access network under the administrative control of a single authority. The domain consists of routers and access points. All of them are mobility-enabled by supporting HAWAII-specific signaling in order to optimize routing and forwarding. The router interconnecting the HAWAII domain and the Internet core network is called foreign domain root router. Each access point has Mobile IP foreign agent functionality. In the HAWAII approach mobility is separated between intra-domain handover and inter-domain handover. For both cases different mechanisms are defined. The first case is supported by HAWAII and the second case by Mobile IP. Both cases will be explained below.

In the HAWAII approach a mobile host has a home domain (similar as the home network in Mobile IP) and a temporary unicast IP address. The home domain may support the HAWAII protocol. When the mobile host is in a foreign HAWAII domain the temporary IP address is assigned once to the mobile host and does not change as long as the mobile host stays in the domain. No address translation mechanism is required, and the Mobile IP home agent is not notified of the mobile host's movement. Instead, connectivity is maintained by using dynamically established paths in the foreign HAWAII domain based on host entries in the routing table of selected routers. Thus, a HAWAII enabled access network does not rely on IP routing in the sense of routing based on the network's portion of the IP address. Instead, the IP address is interpreted as a unique identifier and not as a location identifier.

As mentioned above, for global mobility support HAWAII reverts to traditional Mobile IP mechanisms. At first, the case is considered where the mobile host is within the HAWAII home domain. In this case the mobile host carries a unicast IP address. When the mobile host powers up, it sends a Mobile IP registration message to the present access point. The access point then propagates a HAWAII path setup message to the domain root router using a configured default route. Each router in the path between the mobile host and the domain root router adds a forwarding entry for the mobile host.

Finally, the domain root router acknowledges to the access point. The access point in turn replies the Mobile IP registration to the mobile host. Packets for the mobile host are sent to the domain root router based on the subnet's portion of the mobile host's IP address. The packets are routed within the domain using the host-based forwarding entries. It is important to note that the entries are soft-state being kept alive by periodic hop-by-hop messages.

When the mobile host moves within the HAWAII domain the mobile host registers with the new access point by sending a Mobile IP registration request. The new access point then sends a HAWAII path setup update message to the old access point. The old access point performs a routing table lookup for the new access point and adds a forwarding entry for the mobile host's IP address. Then the message is sent to the upstream router. This router performs similar operations. If the router receiving this message is the crossover router, then this router adds a forwarding entry to the new access point and packets for the mobile host are sent to the new access point. The path via the old access point will time out. This scheme is called forwarding path setup scheme since the HAWAII path setup update message is sent from the new to the old access point, and the old access point forwards packets to the new access point only for a limited time. This scheme is optimized for networks where the mobile host listens/transmits to only one access point simultaneously. An alternative scheme is the Non-Forwarding scheme, which is optimized for networks where the mobile host is able to listen/transmit to two or more access points simultaneously. In this path setup scheme the path setup update message travels from the new access point to the old access point via the crossover router. Thus, packets are not forwarded from the old access point.

In order to interact with Mobile IP the mobile host is assigned a co-located CoA from its HAWAII foreign domain. A correspondent host directs the packets to the mobile host's home address. The Mobile IP home agent intercepts the packets and tunnels them to the HAWAII foreign domain root router with the network portion of the outer IP address. This foreign domain root router and the following routers forward the packets according to its host-based routing entries.

The HAWAII approach differentiates between active and idle users as well as appropriate states for the mobile host. For an active user the network knows the mobile host's current access point, and for an idle user the network only knows the access point approximately, such as a set of access points. When packets for an idle mobile host arrive, the network pages the mobile to determine the mobile's current access point.

Cellular IP

The Cellular IP approach [66] envisions a networking environment with ubiquitous computers where highly mobile hosts often migrate during active data transfers and the users expect minimal disturbance to ongoing sessions. The authors argue that Mobile IP is not an optimal solution, because it is optimized for macro-level mobility and relatively slowly moving hosts. Moreover, it is stressed that Mobile IP does not scale for a large number of mobile hosts, since every handover between Mobile IP foreign agents generates a binding update irrespective of the fact whether the mobile host is idle or active.

The Cellular IP approach proposes a hierarchical mobility management which separates global from local mobility. For global mobility, Mobile IP is applied to support handover across the Internet backbone. To support local mobility within the Cellular IP access network, regular IP routing is

replaced with routing of packets hop-by-hop via lookup in specific tables. The tables apply soft-state principles which are referred to as caches.

In a Cellular IP network a mobile host is assigned a unique identifier which is used to route packets. It is not required that a mobile host has an IP CoA. For simplicity reasons, the unique identifier is an IP address (e.g. home address) that makes inter-working with Mobile IP more easy. However, this is not really required, since within the Cellular IP access network no IP routing is performed.

For mobility support Cellular IP adds a gateway router and Cellular IP nodes to the network infrastructure. A gateway router interconnects the Internet backbone and the Cellular IP access network. The Cellular IP nodes are located in the Cellular IP access network and can be considered as access points working at network level. They execute the Cellular IP protocol. It is not required that they are equipped with a wireless interface (if not, they act as a regular network node). The global mobility support in Cellular IP is provided straightforward by Mobile IP. The Gateway router is co-located with a Mobile IP foreign agent. The mobile host registers the gateway's IP address with its Mobile IP home agent. Packets from a correspondent host are first routed to the Mobile IP home agent and then tunneled to the gateway. The gateway de-tunnels packets and forwards them towards the access points. As long as the host is interconnected to the same access network, local mobility is hidden from the agent in the gateway router.

The local mobility support works as follows: Inside the Cellular IP access network, nodes are provided with a Paging Cache (PC) and a Routing Cache (RC). Both contain mappings between mobile host IDs and node ports (Output port similar to a router port) on a soft-state basis. Paging caches are available in a few nodes. A paging cache is updated by data originating from the mobile host (data packets or specific signaling packets). The paging cache is used to locate a mobile host when there is no routing cache entry. In that case, the Gateway Router caches the IP data packets in order to send a paging packet to the mobile host across the Cellular IP nodes. The mobile host replies to that paging packet and creates routing cache entries in every node along the route. Now, the cached IP packets can be sent along this route without address translation and tunneling. paging cache and routing cache entries are cleared by timers, with different timeout values: The routing cache timeout is on the order of several IP packets, whereas the paging cache timeout is set according to the handover frequency. Thus, an idle and active mobile host can be managed separately with different data bases.

When a handover occurs two cases have to be considered. In the first case the mobile host generates a route update packet when it enters the new cell in order to update the route caches in those nodes where the old and new route diverge. After the route caches are updated, data packets are sent to the new location of the mobile host via the new route. For a limited time the old and the new routing cache entry can exist in the routing cache and data packets are sent via the old and the new route. This is used for semi-soft handover. In the second case, the routing cache entry in the Gateway was cleared, triggered by a timer. Then a new paging packet is generated to locate the mobile host. This explicit search causes a small delay in sending packets, but it allows longer timeouts decreasing the amount of signaling packets.

Inter Access Point Protocol (IAPP)

The IAPP [46] defines, how access points of an IEEE 802.11 network communicate with each other to support handover of mobile hosts. The protocol facilitates the support of handover within the

boundaries of an IEEE 802.11 network which can be regarded as local handover working below the network layer. For global handover an other mobility solution is required (e.g. Mobile IP).

An IEEE 802.11 system achieves a spatial coverage common to local area networks by connecting wireless cells by a wired backbone, termed distribution system. The internals of the distribution system are not defined in the IEEE 802.11 standard. The IAPP provides a mechanism by which access points can exchange information, even for access points from different vendors.

The IAPP consists of two modules - the announce protocol and the handover protocol. The announce protocol is for informing other access points that a new access point has become active and other management tasks. The handover protocol is used to inform the old access point that a mobile host is taken over by another access point, update the old access point's registration table to forward frames destined for the mobile host appropriately. The handover procedure is directly tied into the IEEE 802.11 re-association procedure at link layer. The IAPP protocol is mainly developed to provide inter-operable interaction between access points from different vendors for mobility support within a IP network/subnetwork.

Mobile People Architecture (MPA)

The main goal of the Mobile People Architecture [43] is to maintain a person-to-person reachability while preserving the mobile user's person privacy. In the Mobile People Architecture a user is identified by a Personal Online ID. Additionally, a user is addressed by Application Specific Addresses. Mobility is supported by mapping the Personal Online ID to Application Specific Addresses (ASAs).

In the Mobile People Architecture a new entity is added to the network. This entity is called a personal proxy and acts as a person level router (The person level is added to the communication layer model on top of the application level.) The personal proxy tracks the user's current reachability, converts media, and forwards data to a specific end system. It is located in the mobile host's home network (if any), or is offered by a trusted third party server.

When a user wishes to communicate with the mobile person a call (call is regarded as a kind of session) is directed to the Personal Proxy, and then to the mobile person's preferred end system. When the reachability of the mobile person changes, the proxy state is updated by the tracking agent. The update can be done in a scheduled manner, manually or automatically.

It is assumed that local mobility is handled within the access network and hidden from the Personal Proxy. The case that a user changes the end system can be regarded as vertical handover. Then the user updates the Personal Proxy (manually or automatically) and new calls will be directed to the user's new ASA. The case that a user changes the ASA while receiving service is not being considered.

Internet Core Beyond the Third Generation (ICEBERG)

The motivation of the ICEBERG project [68] is the current diversity of access networks, end systems, and services; in particular, traditional telephony services and data services. Therefore, the ICEBERG project aims at supporting personal mobility in the sense of seamless access to services independent of the access network and end system. It is intended to give the control of the communication to the callee, and not to the caller.

In ICEBERG, a user can be uniquely identified (by means of a unique-id). Additionally, the user is associated with one or several service-ids (e.g. phone number, email address, IP address). To achieve mobility the unique-id is mapped to the service-id.

In general, the ICEBERG network architecture consists of the Internet Core and several different access networks (e.g. GSM, PSTN, WLAN). At the interface between the core network and an access network an Iceberg Access Point (IAP) transforms services (media converter). Additionally, ICEBERG adds service agents to the core network: preference registries, Personal Activity Tracker (PAT), and extended naming services. The preference registry stores user preference that can be modified by user interaction or by the PAT which gives inputs about location information.

Suppose a correspondent user wishes to call the mobile user. The call is routed to the IAP. In the access point a name service lookup is performed, the preference registry of the called user is located and the preferred end system is determined. After that the call is established via the correspondent interface. A service conversion (e.g. fax to jpeg) is executed in the IAP.

The ICEBERG approach focuses on user mobility between several access networks. It is implicitly assumed that host mobility is transparently supported in the access networks by technology specific handover schemes (e.g. for GSM, IEEE 802.11, etc.).

Extended SIP Mobility

Extended SIP Mobility [69] is an mobility approach that utilizes the application level signaling capabilities of the Session Invitation Protocol (SIP) protocol. The motivation of the extended SIP mobility can be found in drawbacks of the Mobile IPv4 approach. The authors argue that for real-time traffic over IP, which is mostly RTP over UDP traffic, there is a need for fast handover, low latency, and high bandwidth utilization. Mobile IPv4 suffers from indirect communication which increases the delay and causes an overhead due to tunneling, which on its part decreases bandwidth utilization.

The extended SIP mobility approach introduces mobility awareness at a higher layer than the network layer. SIP already supports user mobility, and the approach is meant to extend SIP as an application-layer signaling protocol in order to support end system mobility.

The main assumption behind the extended SIP mobility approach is that a mobile user is identified by a unique address (e.g. user@realm). This unique address is mapped to the current IP address of the mobile user's end system. No explicit home IP address is required. SIP introduces a SIP agent on the user's side and a SIP server (SIP redirect server or SIP proxy server) and location server to the network infrastructure.

User mobility is supported by means of the original SIP protocol: When a user wishes to initiate a session, an invitation is directed to the SIP server which in turn queries the location server for the current IP address of the mobile user's end system. The SIP server sends the invitation to the called user. The invitation contains the IP address of the callee. If the mobile user moves, the location server is updated, and new sessions will be set up to that new IP address.

End system mobility with this scheme is mainly understood as an increased roaming frequency and as a change of an IP address during an ongoing session. Assuming that a session is already established, then the mobile registers the new temporary address with the location server and the mobile re-invites

the correspondent host with the same session identifier and the new temporary address (in the contact field of the SIP message). The session can be continued, although the IP address has changed.

It is important to note that SIP does not support TCP. Therefore, extended SIP mobility supports UDP traffic only. For TCP traffic it is proposed to use Mobile IP. It is argued that both approaches can coexist: For TCP traffic Mobile IP is applied and for UDP traffic the extended SIP mobility approach. For the simultaneous usage of network interfaces the MosquitoNet approach of a mobile routing table is adopted.

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 [48], it is intended to use today's IP multicast as it is available today in order to support handover. In [61] 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 [24] 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.

Summary

In summary, the approaches to mobility support in IP networks based on IP unicast can be divided into three main categories as shown in the diagram in Figure 2.2, and a comparison is shown in Table 2.1.

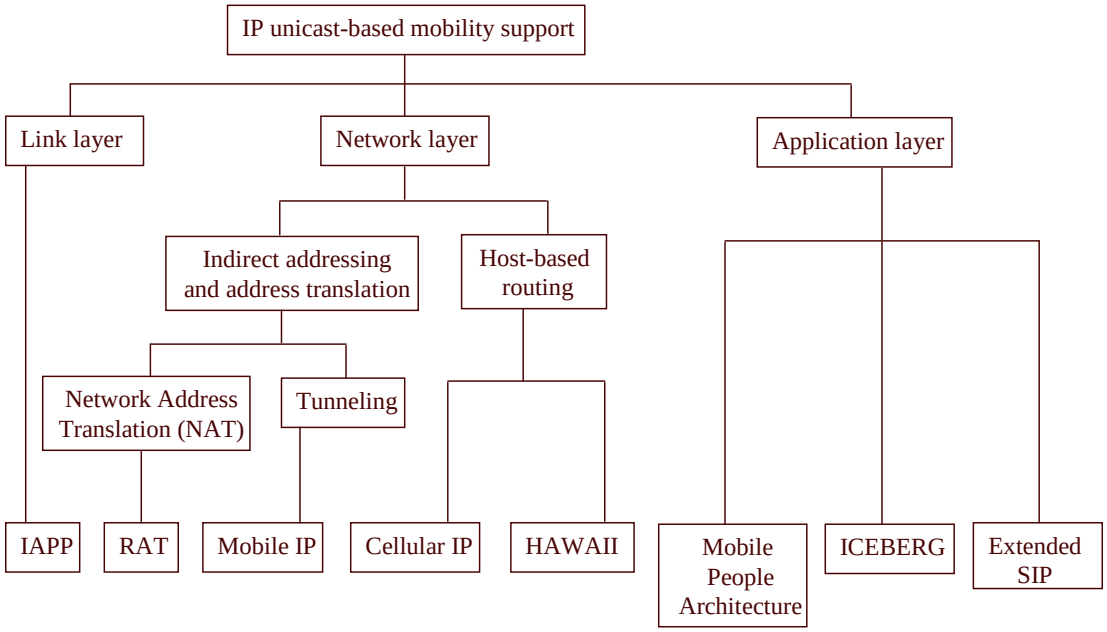


Figure 2.2: Classification of IP unicast-based mobility approaches

The classical solution for mobility support is Mobile IP. Mobile IP overcomes the general mobility problem by using additional agents in the network to map the mobile host's identity to its current location ensuring that arbitrary hosts can communicate with a mobile host in an uninterrupted way even while the host moves around. Despite this achievement, Mobile IP has been widely criticized for its performance problems and for not matching all possible requirements for a mobility concept. Some of these requirements are technology-driven: The need for higher bandwidths results in the use of ever higher frequency bands with high attenuation and low wall penetration making very small cells a necessity. In highly mobile environments very frequent handovers occur resulting in performance degradation and frequent disturbances of communication. Using different types of cells with different technologies and communication radii, organized into a hierarchical system, could overcome some of these problems but would also result in new problems. Other requirements are user-driven: Examples include different types of access needs (e.g. WB-CDMA offering soft handover capability) or service requirements (low loss versus low jitter). As Mobile IP has been criticized on the grounds of such diverse requirements, other concepts have been proposed that also solve the fundamental mobility problem in a different manner. Approaches applying host-based routing (such as Cellular IP and HAWAII) aim at micro-mobility support and require a complementing solution for macro-mobility. Application-layer mobility approaches provide a scalable solution in combination with network-layer

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 2.1: Comparison of handover approaches with respect to general functions

micro-mobility approaches. But they do not provide a general solution for all applications, instead they are specific to particular applications. However, they offer a short-term solution for network-layer micro-mobility approaches.

2.2.2 QoS

The Next Steps in Signaling Working Group (NSIS) is responsible for standardizing an IP signaling protocol with QoS signaling as the first use case. This working group will concentrate on a two-layer signaling paradigm. The requirements of QoS signaling protocols is documented in [6]. The existing QoS signaling protocols is analyzed in [1].

A comparison of signaling protocols in the aspect of mobility support is discussed as follows.

Mobility Support of RSVP

The RSVP was designed without the issue to support scenarios with high mobility. The addresses of the hosts were assumed to be fixed and route changes were considered as an exception.

The reservations are initiated by the receiver of a data flow. It sends a Path message to the sender of the flow. The message traverses the routers and establishes states for the subsequent reservation of the path. The sender replies with a Resv message, which establishes the reservation based on the former states in the routers. Every reservation needs therefore a two-way message exchange. A simultaneous reservation setup in uplink and downlink direction with only one message exchange is not possible.

The protocol was originally designed to support multicast applications. A RSVP router can merge different data flows based on the information in the Path message.

RSVP is often considered as being to complex and therefore fault-prone. It supports many different features like flow merging, reservation styles and scopes and is not light-weight implementable.

Some issues raise concern when RSVP is used by a mobile node (MN), e.g. the identifier of the session (i.e. data flow) and the reservation refresh [1].

When an MN changes locations, the handover may force a change of its assigned IP addresses. RSVP uses the destination address of a message flow as identifier. As a consequence the filters associated with a reservation are not able to identify the flow anymore and the resource reservation is ineffective, until a refresh with a new set of filters is initialized.

When the route between the communicating end hosts changes, a Path message has to be sent to set the state of the reservation on the new route and a subsequent Resv message (re-) establishes the resource reservation. By sending only a Resv message a host is not able to update the reservation, and to perform a local repair. In order to provide fast adaptation to routing changes without waiting for the end of refresh periods, the RSVP process should use the handover information to trigger a quick refresh of state for the paths immediately. However, not all local mobility protocols, or even Mobile IP, affect routing directly in routers, and thus mobility may not be noticed at RSVP routers. Thus, it may take a relatively long time before a reservation is refreshed after a handover.

There have been several designs for extensions to RSVP to allow for more seamless mobility. One

solution is presented as localize RSVP [44], distinguishing local network reservations from the end-to-end reservations. The end host does not need to know the access network topology or the nodes that will reserve the local resources. The reservation message itself identifies the intention and the access network will find the correct network node(s) to respond to the reservation. Note that the scheme is not tied to only mobile networks but can be used in any access network that needs flexible local resource allocations.

Mobility support of MRSVP

The Mobile RSVP (MRSVP) [62] is another protocol which extends the RSVP in order to support mobility. It is based on the mechanism to reserve resources for a mobile node in advance before it performs a handover.

For making advance reservations, it is necessary to specify the set of access routers a mobile node will eventually visit. Each access router has the function of a proxy which reserves the resources for the mobile node with the proper parameters. The currently unused reservations are called passive reservations.

When the mobile node arrives at a particular access router, the path becomes active and the path to the previous one passive, so the data can still be delivered effectively. The active and passive reservations can be merged by calculating an effective Flowspec. This avoids multiple reservations over long distances through the Internet.

Due to the fact that the reservations have been established before a mobile node arrives at an access router, the protocol can provide the re-establishment of existing reservations after a nearly optimal short time. But the drawbacks of the protocol are the necessarily reserved resources at other access routers and paths. See section 2.2.2 for more details.

There is no security analysis in this work. The protocol relies on the security mechanisms of the RSVP. Additional security mechanisms are recommended because of the enlarged risk of DoS attacks.

An overview of the various "advance reservation" schemes is given in [47]. One example is shown in [14] which proposed a Mobile IPv6 and RSVP integration model. When the MN performs a handoff, it gets a new CoA and subsequently sends a binding update to the CN. The CN then sends a Path message associated with the new flow from CN to MN. Upon receiving this Path message, the MN replies with a Resv message immediately to reserve resources for the new flow. For each handoff, the MN as receiver has to wait for a new Path message from the CN, it can only issue a new Resv message to the CN after getting the Path message. However, all these RSVP re-negotiations are conducted end-to-end even though the path change may only affect a few intermediate routers. Hence, the long handoff resource reservation delays and large signaling overheads caused by this end-to-end RSVP renegotiation process could lead to notable service degradation in providing real-time services.

Mobility support of the QoS client for CASP

To treat a CASP message flow according to particular rules, a Flow ID is defined as an object class. It allows policy-based forwarding and NAT devices to inspect this object easily. It typically contains the IP addresses of the data sender and data receiver, and possibly some additional demultiplexing

information. Sessions are identified by a special session ID. This ID is independent from the IP addresses of the sender and receiver and therefore suited to be used even after a handover and subsequent address change.

In contrast to RSVP the CASP was designed to be able to react on route changes in a more comfortable way. It only requires the creation of a reservation along the new path until the merge point (crossover router) with the old path is reached. The scope of a reservation can be restricted to the new part of the path by generating and deleting the appropriate signaling messages at the affected nodes. The separation of the Session ID and the Traffic Selector enables the merge point to associate an existing reservation with the ID provided by the incoming signaling message.

A CASP signaling message is either triggered by the refresh timer or a mobility management component, as soon as the MN detects a route change. The signaling message is forwarded until it reaches the cross over router, which is the first node along the path which can identify the provided Session ID. An interaction of the signaling and mobility messages can enable a performance improvement.

A micro-mobility scheme which is able to trigger CASP messages would further limit double reservations and accelerate the reservation setup time.

To avoid time consuming exchanges of messages after an unsuccessful reservation request, the QoS client for CASP offers the opportunity to define a reservation range. The range is defined by a lower and an upper bandwidth value. If the reservation of the requested upper bandwidth fails, the CASP node can reserve another value, as long as it is greater or equal the specified lower value.

Figure 2.3 shows a comparison of the signaling protocols RSVP, MRSVP and QoS Client for CASP under the aspects of mobility support and security.

Summary

RSVP was designed specially and optimally for multicast while it needs to be adapted for unicast reservations. However, many signaling scenarios do not need the full-fledged set of features of multicast support. Instead, it is necessary to keep the mandatory components of the signaling protocol as simple as possible. CASP, which was designed initially as a light-weighted signaling protocol, has a two-layer structure. The separation of the client layer and messaging layer provides flexibility to deal with different signaling scenarios.

Non end-to-end QoS signaling demands a more flexible and applicable protocol than RSVP. CASP is a suitable signaling protocol which can provide the end-to-end QoS signaling function.

Finally, in CASP, the interaction with a mobility protocol can speed up the QoS re-establishment time. After comparing the technical details of the three investigated protocols, we got the following result of the duration for a reservation re-establishment after a handover:

Long duration for reservation re-establishment with RSVP, medium for the QoS client for CASP and short for MRSVP.

The result is based on some assumptions:

- RSVP: The reservation is reestablished with a Path and a Resv message after a handover. The

re-establishment may be triggered by the mobility protocol before the expire of the reservation refresh interval.

- MRSVP: The mobile node could already reserve the require bandwidth before the handover with a proxy. It performs a handover to the expected access router and only needs to activate the existing passive reservation.

- QoS client for CASP: After a handover, the mobile node discovers the next suited CASP node with a Scout message. The usage of a Scout message adds one additional message exchange to the procedure. It reestablishes the reservation on the new path only at the part of the path which differs from the old one. However, if the new access router has not enough bandwidth available for the request of the mobile node, the node must perform a handover again to find a suitable access router.

The MRSVP seems to be the best solutions to combine QoS provisioning with mobility. But it has some shortcomings, which make it inapplicable in the considered scenario:

- It is not economical to reserve the multiple bandwidth for a mobile node that it is going to use.

- If the access networks serves many mobile nodes and can not provide more bandwidth than that amount which will be usually requested by the nodes, it can not accept reservations in advance.

- The network or the mobile node is not able to predict the next access router and will therefore reserve the bandwidth in all neighbor cells.

- The duration for a RSVP reservation is not reduced by the mechanism. If the mobile node traverses an access network very fast, it may not be able to setup a passive reservation before it performs the handover.

After having gained this result and based on the knowledge of the SeQoMo project, we collected the following requirements and conclusions for QoS provisioning in mobile access networks:

- The available resources in the access network should be used economically. The existing networks may have over-provision, but only regarding voice applications.

- The mobile node should avoid a handover to an access router which is not able to provide the desired bandwidth. An additional handover after an unsuccessful reservation attempt can cause a long service interruption.

- Seamless QoS provisioning can only achieved by combining mobility with QoS signaling. Additional message exchanges increase the delay for the re-establishment of reservations after a handover.

- Signaling protocols which reserve bandwidth for nodes are very vulnerable to DoS attacks. The protocols need a good protection mechanism against those attacks.

The result from the first point is that general reservation in advance is not possible. The only exception would be to predict the next access router with a high probability and to reserve the resources in it. This would imply a higher interaction of the network which has other negative drawbacks.

The second point comprises two things. The first one is that a mobile node should be able to select the next suited access router by its own. The second one is that it needs some information about the access routers to determine which is the most suited one. The solution for this problem is to advertise the information about the bandwidth directly to the mobile node. Combined with the other information about the access router this solution satisfies even point three.

2.2.3 Security

Security is a very important concern for NSIS. The working group has studied and analyzed the threats and security requirements for signaling [64, 65]. The new signaling protocols aims to be Compatible with authentication and authorization mechanisms such as those of Diameter, COPS for RSVP [5] and RSVP Session Authorization [31].

In the aspects of mobility and AAA, signaling protocols in NSIS work with existing IETF mobility and AAA protocols, including Mobile IP, SeaMoby Context Transfer, etc. However, the mobility issue in NSIS is being discussed as one of NSIS activities [29, 57].

2.2.4 A Case Study: the Moby Dick project

Moby Dick - Mobility and Differentiated Services in a Future IP Network [18] has the following main objectives regarding QoS mobility and security:

- To facilitate the development of seamless access to existing and emerging IP-based applications.
- To propose an architecture for wireless Internet access by developing new mechanisms for seamless hand-over, QoS support after and during hand-over, AAA, and charging.

AAAC design in Moby Dick project

Authentication, authorization, accounting and charging design in the Moby Dick project (AAAC) [70] mainly aims at three things: essential AAAC functionalities for any commercial applications which will be supported in the future Internet; deployment of IPv6 infrastructure and mobility of users, devices and applications as well as services in a large distributed environment across the world. The AAAC targets as an evolutionary AAAC architecture based on the generic AAA protocol from the IRTF.

Figure 2.4 presents the registration message exchanges among AAAC mobility entities in the following steps:

1. MN detects movement by either receiving a router advertisement or a router solicitation after receiving a layer-2 indication e.g. from a network card driver.

2. MN configures the IPv6 stateless address based on the router prefixes delivered in the router advertisement.

3. MN sends a registration request message to the router containing a binding update request, the MN's NAI, data for replay protection and authentication information.

4. The router also acting as AAAC attendant copies the above message content and forwards it to AAACL.

5. AAACF authenticates the message from the router and routes the message to AAACH.

6. AAACH checks if the MN-AAACH authentication is correct and checks if the message is replayed. If there is no problem with the above two checks, AAACH generates a session key for future MN-HA binding updates and sends the binding update request along with the key to HA. The message is authenticated by the HA and the session key is encrypted with either AAACF-HA shared key or HA public key.

7. HA processes the message which is either in AAAC format or a normal binding update formate with some extension or option. HA sends a binding update acknowledgment back to AAACH and keeps the session key for the later communication with MN.

8. AAAH then assigns a session lifetime to the AAA authentication and sends it to AAACL with MN's NAI, binding acknowledgment, encrypted session key and the authentication AAACH-MN.

9. AAACL decides whether to grant access to the MN based on the AAACH and AAACF authentication information and some other non-mobile-IP specific AVPs that the AAACH could have appended. If it decides to grant access, it informs the router the MN's NAI, binding acknowledgment, encrypted session key, session lifetime, authentication AAACH-MN, AAACL-router OK AVP and AAACL-router authentication.

10. The router adds a rule enabling traffic forwarding for the MN and sends the binding acknowledgment, session key, lifetime and authentication AAACH-MN to the MN.

After the above steps, the MN gets the session key which will be used for any subsequent communication for the session lifetime. When lifetime of the binding update expires, a new binding update request procedure starts among MIPv6 entities without the involvement of AAAC entities. The session lifetime is running out, a new AAAC-involved process will occur as the above steps. The binding lifetime should be much shorter than the session lifetime in order to detect disconnected MNs.

When the binding lifetime expires, the HA will inform the AAACH that the MN is no longer registered.

AAACH will forward this information to AAACL which will inform the router to stop forwarding the traffic from or to the old MN address.

When the MN moves to a new network, it will use the same procedure. The HA will inform AAACH that the MN moved and the old session will be deleted.

AAACL is responsible for accounting and charging the MN's resource utilizations.

With respect to authorization, some assumptions on AAAC interactions has been pointed out as follows:

- Two entities play a major role in authorizing a service request with QoS requirements: QoS entity should make decisions upon QoS request based on current network conditions while AAAC entity should make decisions based on other conditions.
- An authorization request should contain CoA of MN, service name or service identifier and QoS requirements if needed.
- QoS requirements should contain upper and lower bound of the QoS classes rather than a specific QoS class in order to make QoS negotiation more flexible.
- Authorization information can be derived from the user profile or applied policy.
- Authorization should be a continuous process as long as the session is going on because the conditions on which authorization decisions are based might change during the session.

Comparison between Moby Dick and SeQoMo

The Moby Dick project proposes an IP-based QoS architecture for 4G operator scenarios. The architecture is based on IPv6 which is running on top of different access technologies.

It supports end-to-end DiffServ per service and per user. To achieve seamless L3 handovers, it deploys Fast MIPv6 [40] and Context Transfer [42] protocols. It does not distinguish local and global movements and performs a unique operation for handover.

In the aspect of security, it uses AAA protocols for authentication, authorization, accounting and charging. It does not address Denial of Service specially.

A comparison between the Moby Dick project and this project is shown in Table 2.2.

2.3 Motivations

The different operations for global and local movements are preferable since special treatments can optimize (re-)registration procedures in local movements which occur much more frequently. Therefore, it is beneficial to implement hierarchical mobile IP architecture for mobility support.

Furthermore, handover should be QoS aware, and a two-layer signaling protocol for QoS state (re-)establishment in mobility scenarios. Global QoS signaling for local handovers is inappropriate. Local QoS signaling is required for handover decisions.

Security checks, authentication performance during handover and authorization of QoS requests in access networks, should introduce minimum latency to a registration procedure. Moreover, measures to protect signaling and data traffic over the wireless channel and protect against DoS attacks should also be considered.

The requirements of the SeQoMo project are summarized in Table 2.5.

	Moby Dick	SeQoMo
Goal	An architecture of integrating of QoS, IPv6 mobility and AAA for 4G	A secure, QoS-aware mobility management approach for 4G
Network Architecture	IPv6 on top of different access technologies entities:MH, AR, QoS broker, AAA server	Hierarchical Mobile IPv6 on top of different access technologies entities: MH, AR, MAP, AAA server
QoS	DiffServ:QoS broker, DSCP per service, per user end-to-end: three situations - registration, authorization and handover	DiffServ:DSCP; IntServ:CASP Mobility/QoS Client protocol per flow end-to-end: four cases - power up, session refreshment, inter-domain and intra-domain handovers
Mobility	MIPv6 + FMIPv6 + CT AAA server $<->$ QoS broker: SLA seamless: bicasting, serval QoS broker	MIPv6 + HMIPv6 AR $<->$ MAP $<->$ AAA server: combined signaling seamless: local management, low latency
Security	authentication: AAA protocol authorization: DSCP marked to request QoS broker protection against DoS: no signaling data protection: not addressed	authentication: AAA protocol authorization: requested QoS is mapped directly to authorization data protection against DoS: cookie-based mechanism signaling data protection: preliminary session keys and temporary SA
Management Protocols	COPS, Diameter, Mobile IPv6	Diameter, HMIPv6, CASP Mobility/QoS Client protocol
Advertisement authentication	no	TESLA-alike

Table 2.2: Comparison between Moby Dick and SeQoMo

Protocol / Features/ Requirements	RSVP	MRSVP	QoS client for CASP
Reservation setup/ required message exchanges	Receiver oriented; Reservation is established after receipt of PATH message; Two-path exchange	Mobile host initiates reservation based on MSPEC in both directions	Direction neutral
Repair and reestablishment of reservations	PATH message followed by RESV message; Usually end-to-end	PATH message followed by RESV message; Usually end-to-end	Partial repair of path
Reservation Scope	End-to-end	End-to-end	Scope can be restricted; Information can be generated and deleted anywhere
Bidirectional reservations	Not supported	Not supported	Yes
Support of multiple reservations per session	No	Support of active and passive reservations	One session identifier can use different flow identifiers
Reservation range	No	No	Lower and upper bandwidth range to reduce required message exchanges
Partial reservation	Domains without RSVP are transparently traversed	Domains without RSVP are transparently traversed	Reservations in only some routers are possible
Dependency on IP routing	RSVP messages are routed by the standard IP routing (routing table)	Standard IP routing	Reservations are established along the path which is discovered by scout messages
Support for multicast	Originally designed for multicast, support for flow merging	Yes; Proxy agents can join multicast groups	No
Complexity	High; various reservation features (flow merging, states, scopes etc.)	High	High complexity but modular design
Reservations over tunnels	No	Yes	No
Mobility supporting functions	Not a design issue	Advance (passive) reservations	Mobility is treated as local route change
Filtering of the message flow	Session identifier based on the IP address	Session identifier based on the IP address	Session identifier
Identification of the Endpoint	Based on the IP address	Based on the IP address	IP address in flow identifier
Support for Soft Hand-over (usage of simultaneous reservations)	No	No; Change between active and passive connection	Yes with different flow identifiers
Seamless QoS handovers	Not supported	Yes	No provision
QoS Information before Handover	Not supported	Not required due to design	Not supported
Price information before the handover	Not supported	Not supported	Not supported
Security model	Hop-by-hop	See RSVP, no additional protection mechanism	M-layer: Hop-by-hop; C-layer: End-to-end
Protection against bogus reservation requests	User authentication	See RSVP, no additional protection mechanism	Authentication of hosts before accepting a reservation

Figure 2.3: Comparison of the signaling protocols RSVP, MRSVP and QoS Client for CASP

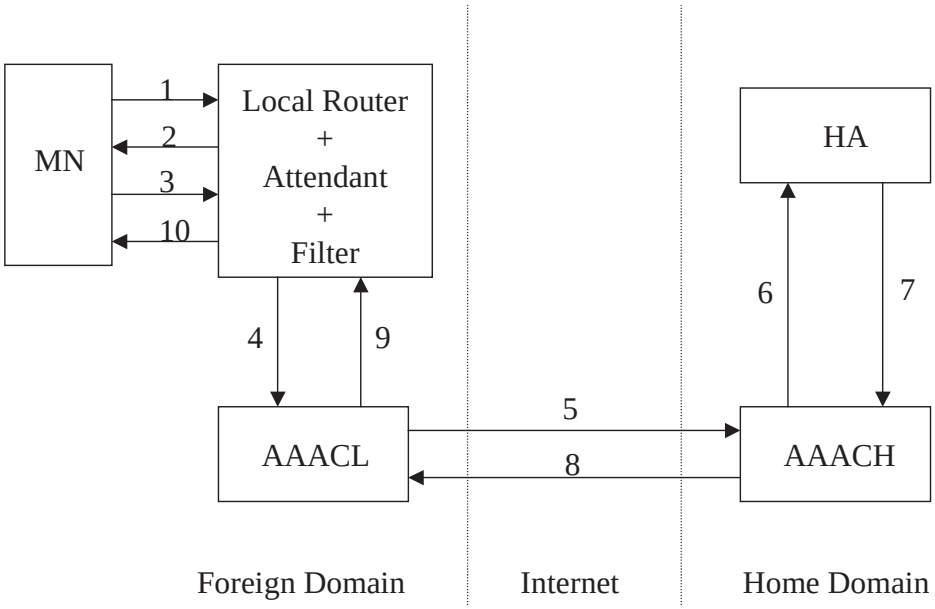


Figure 2.4: Registration message exchange in the Moby Dick Project

Component	Requirements
All components	- Low latency for every signaling process - Only small additional overhead
Mobility support	- Differentiation between global and local mobility - Support for mobility of idle hosts - Placement of re-routing node close to mobile nodes - Fast local handover support - Integrated registration / handover procedure with QoS signaling and security measures
QoS provisioning	- Handover has to be QoS-aware - Local QoS signaling required for handover decisions - Local handover should only need local QoS signaling - Handovers are dependent on if QoS can be ensured - Ability to choose the best suited access router for the next handover - Ability to inform higher layers, if QoS can not be ensured - Support of traffic flows for fast (re-) establishment of reservations - Handover & QoS re-establishment in one operation
Security	- Authentication of MNs with optimized re-Authentication - Authorization of mobile devices in access networks - Authorization check on what MNs are allowed to request - Denial of Service (DoS) protection of handover process - Protection of the infrastructure against DoS attacks

Figure 2.5: The Requirements of the SeQoMo project

Chapter 3

SeQoMo Architecture Overview

In this chapter the complete architecture of the network and the topological overview of the involved protocols are discussed.

3.1 Architecture of the Network

As shown in Figure 3.1, the SeQoMo architecture framework is a joint architecture of HMIPv6 and AAA components.

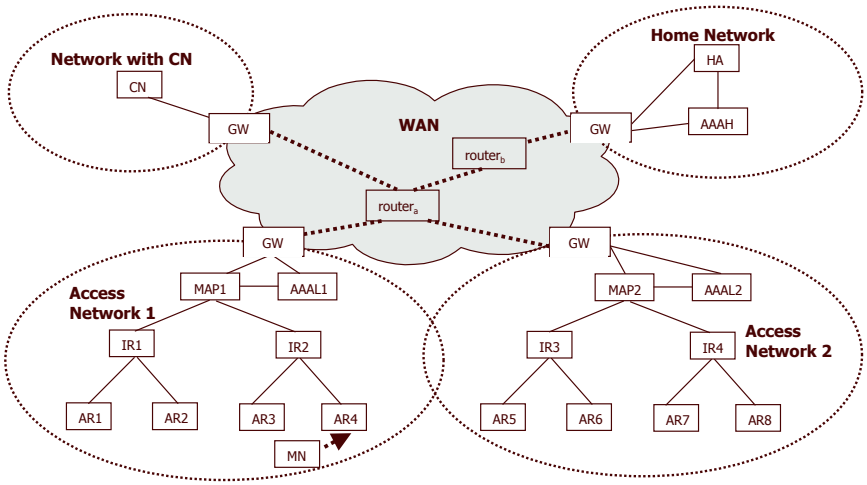


Figure 3.1: The SeQoMo architecture overview

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. Each access domain has a gateway to connect the core network.

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. Optionally, 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.

The overall architecture is HMIPv6-based, supporting seamless mobility between different access technologies, including Ethernet(IEEE802.3) for wired access, 802.11a/b for wireless LAN access, W-CDMA (the physical layer of UMTS) for cellular access.

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 access router (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 also assume the IP networks are composed of multiple domains, each of which can provide some QoS mechanism, e.g, Differentiated Services (DiffServ) [4] or Multi-Protocol Label Switching (MPLS).

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 prerequisites for a successful reservation and guarantee.

3.2 Topological Overview of the Involved Protocols

Figure 3.2 shows the topological overview of the involved protocols.

3.2.1 Mobility - Choice between HMIP and MOMBASA

In the first phase of the project, we examined the multicast-based mobility approach, namely MOMBASA (Mobility Support - A Multicast-based Approach) [25].

In the MOMBASA scheme, the endpoint of the multicast is located in the access point. The mobile

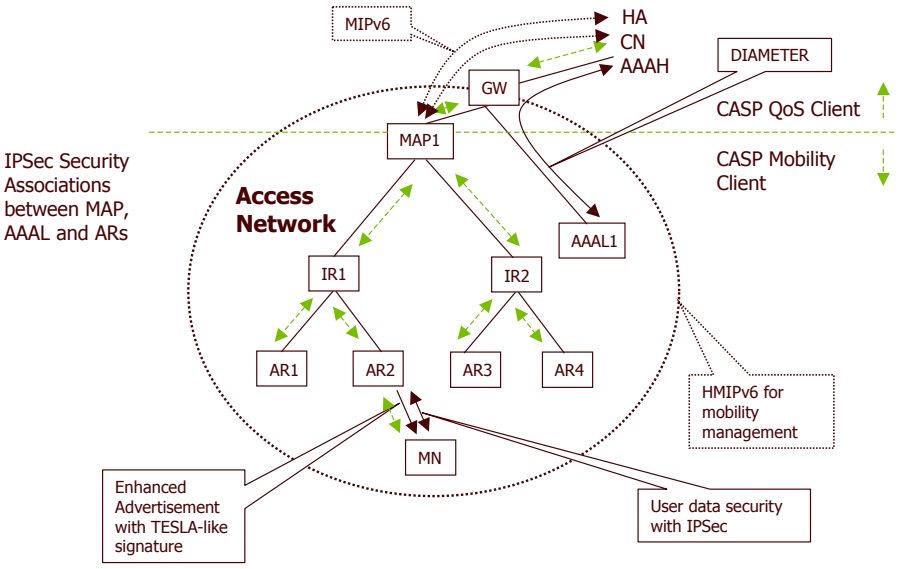


Figure 3.2: A topological overview of the involved protocols

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 [19, 21] 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).

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 [22].

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.

Use of HMIPv6 As the Mobility Management Protocol

In one access network, HMIPv6 is used as the micro-mobility management protocol. Details about HMIPv6 has been discussed in 2.2.1.

In the global movement and power-up cases, MIPv6 [37] serves as the mobility management protocol.

A mobile node is always expected to be addressable at its home address, whether it is currently attached to its home link or is away from home. The "home address" is an IP address assigned to the mobile node within its home subnet prefix on its home link. While a mobile node is at home, packets addressed to its home address are routed to the mobile node’s home link, using conventional Internet routing mechanisms.

While a mobile node is attached to some foreign link away from home, it is also addressable at one or more care-of addresses. A care-of address is an IP address associated with a mobile node that has the subnet prefix of a particular foreign link. The mobile node can acquire its care-of address through conventional IPv6 mechanisms, such as stateless or stateful auto-configuration. As long as the mobile node stays in this location, packets addressed to this care-of address will be routed to the mobile node. The mobile node may also accept packets from several care-of addresses, such as when it is moving but still reachable at the previous link.

The association between a mobile node’s home address and care-of address is known as a "binding" for the mobile node. While away from home, a mobile node registers its primary care-of address with a router on its home link, requesting this router to function as the "home agent" for the mobile node. The mobile node performs this binding registration by sending a "Binding Update" message to the home agent. The home agent replies to the mobile node by returning a "Binding Acknowledgement" message.

Any node communicating with a mobile node is referred to in this document as a "correspondent node" of the mobile node, and may itself be either a stationary node or a mobile node. Mobile nodes can provide information about their current location to correspondent nodes. This happens through the correspondent registration. As a part of this procedure, a return routability test is performed in order to authorize the establishment of the binding.

There are two possible modes for communications between the mobile node and a correspondent

node. The first mode, bidirectional tunneling, does not require Mobile IPv6 support from the correspondent node and is available even if the mobile node has not registered its current binding with the correspondent node. Packets from the correspondent node are routed to the home agent and then tunneled to the mobile node. Packets to the correspondent node are tunneled from the mobile node to the home agent ("reverse tunneled") and then routed normally from the home network to the correspondent node. In this mode, the home agent uses proxy Neighbor Discovery to intercept any IPv6 packets addressed to the mobile node's home address (or home addresses) on the home link. Each intercepted packet is tunneled to the mobile node's primary care-of address.

The second mode, "route optimization", requires the mobile node to register its current binding at the correspondent node. Packets from the correspondent node can be routed directly to the care-of address of the mobile node. When sending a packet to any IPv6 destination, the correspondent node checks its cached bindings for an entry for the packet's destination address. If a cached binding for this destination address is found, the node uses a new type of IPv6 routing header to route the packet to the mobile node by way of the care-of address indicated in this binding.

Routing packets directly to the mobile node's care-of address allows the shortest communications path to be used. It also eliminates congestion at the mobile node's home agent and home link. In addition, the impact of any possible failure of the home agent or networks on the path to or from it is reduced.

When routing packets directly to the mobile node, the correspondent node sets the Destination Address in the IPv6 header to the care-of address of the mobile node. A new type of IPv6 routing header is also added to the packet to carry the desired home address. Similarly, the mobile node sets the Source Address in the packet's IPv6 header to its current care-of addresses. The mobile node adds a new IPv6 "Home Address" destination option to carry its home address. The inclusion of home addresses in these packets makes the use of the care-of address transparent above the network layer (e.g., at the transport layer).

Mobile IPv6 also provides support for multiple home agents, and a limited support for the reconfiguration of the home network. In these cases, the mobile node may not know the IP address of its own home agent, and even the home subnet prefixes may change over time. A mechanism, known as "dynamic home agent address discovery" allows a mobile node to dynamically discover the IP address of a home agent on its home link, even when the mobile node is away from home. Mobile nodes can also learn new information about home subnet prefixes through the "mobile prefix discovery" mechanism.

3.2.2 QoS - From QoSBU to CASP Mobility Client Protocol

In the first phase of the project, the QoS-conditionalized binding update (QoSBU) approaches [28] was invented and deployed [51]. QoSBU is designed to optimize the QoS-aware re-registration procedure of an intra-domain handover in HMIPv6-based networks. The main point is to piggyback QoS signaling on local binding update message being sent from MN to MAP. The detailed description of QoSBU refers to 4.2.1.

Due to the following drawbacks of the QoSBU approach,

- it can not used for end-to-end QoS path establishment;

- it is short of scalability;
- it is not a generic QoS signaling protocol.

in the second phase of the project, we invent CASP Mobility Client protocol and and employ CASP QoS Client protocol as the QoS signaling protocol in the SeQoMo project.

The CASP protocol is used as the QoS signaling protocol. During a local movement in an access network, MN uses CASP Mobility protocol for the QoS state re-establishment; During a global movement or power-up procedure, MN uses CASP QoS client protocol for the QoS state establishment.

CASP Mobility protocol and CASP QoS protocol will be introduced in details in 4.1.4 and 4.1.5 respectively.

3.2.3 Security

The Diameter protocol, an AAA protocol is communicated between AAAL and AAAH for the purposes of authentication and authorization. The detail of Diameter protocol refers to 4.1.2.

IPSec is deployed to secure the signaling and data traffic over the wireless channels. The scheme (see 5.1.5) is based on preliminary session keys and temporary security associations. It is assumed that IPSec security associations (SAs) between MAP, AAAL and ARs are pre-existing. IPSec will be detailed in 4.1.3.

To protect against DoS attacks and meet the requirement of low-latency handover procedure, a cookie-based mechanism has been proposed in 4.2.2.

The enhanced advertisement, which contains QoS information (e.g. the aggregate available bandwidth), price information and address of the first CASP node, is secured by means of TESLA-like signature approach (see 4.2.3).

3.3 SeQoMo Principal Features and Approaches

The principal features and approaches lie in three aspects: mobility, QoS and Security:

- *Mobility:*
  - Placement of re-routing node close to mobile nodes;
  - Fast local handover support;
  - Integrated registration and handover procedure with QoS signaling and security measures.
- *QoS:*
  - Handover and QoS (re-)establishment in one operation;
  - Local handover only needs local QoS signaling;
  - Handovers are dependent on if QoS can be ensured.

- *Security:*
  - Authentication of MNs with optimized re-authentication;
  - Authorization check on what MNs are allowed to request;
  - Protection of the infrastructure against DoS attacks;
  - Protection of signaling and data traffic over wireless channels.

3.4 Scope of Applicability

The SeQoMo approach applies in any IP based homogeneous and heterogeneous networks. This approach can be used for (re-)establishment of mobility, QoS and security in cases of power-up, global movement, local movement and session refreshment (see Chapter 5 for details).

Chapter 4

Protocols and Mechanisms

In this chapter, We describe the involved protocols and mechanisms.

4.1 Protocols

The involved protocols include HMIPv6, Diameter protocol, IPSec, CASP QoS client protocol, and CASP mobility client protocol.

4.1.1 Hierarchical Mobile IPv6 (HMIPv6)

HMIPv6 has been discussed in 2.2.1. This section gives a summary of this protocol.

HMIPv6 is motivated that MIP performs poorly with fast moving mobile nodes because frequent registrations with a distant home agent (HA) cause high latency and packet loss.

Figure 4.1 shows a application scenario of HMIPv6. The key points of the registration operations in HMIPv6 is described briefly as follows:

- A mobility anchor point (MAP) is introduced for regional registration.
- Initial registration is performed with MAP and HA.
- re-registration in local movement is done with MAP only.

This approach provides prerequisite in order to save QoS re-establishment after local handover s MN's address towards the Internet does not change.

4.1.2 Diameter Protocol

The Diameter is a follow-on AAA protocol to the RADIUS and it is intended to provide an AAA framework for Mobile-IP, Network Access Server Requirements (NASREQ) and the Roaming Oper-

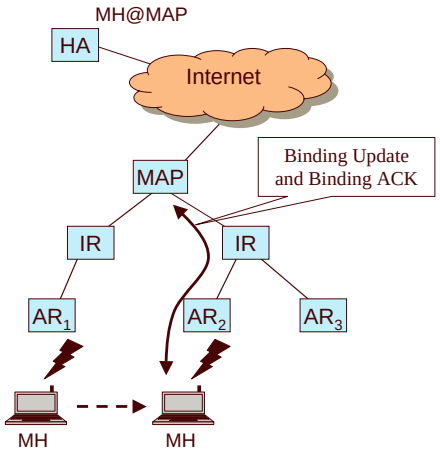


Figure 4.1: Application scenario of HMIPv6

ations Working Group (ROAMOPS). The Diameter mobile IP applications [7], which is based on [8], enables a Diameter server to provide authentication, authorization and accounting services to an MN. Diameter Mobile IPv4 application has been described in detail in [34]. In this section, we introduce first the integration of Mobile IP and AAA in general, then we describe a solution of Diameter Mobile IPv6 application.

Mobile IP / AAA

We introduce a multi-domain model of Mobile IP and AAA joint architecture.

Figure 4.2 depicts the trust model in AAA infrastructure.

In this model each network contains mobile nodes (MNs) and an AAA server (AAA). Each mobility device shares a security association (SA) with the AAA server within its own home network. As an example, MN always shares a trust relationship with its AAAH even when it moves to a foreign domain. Each of the administrative domains' AAA servers have an SA with an intermediate broker.

Based on a trust model like the one mentioned above, the registration actions after MN appears within the a foreign network is described as follows:

- MN issues a registration to access router (AR).
- AR sends an AAA request to AAAL including authentication information and the registration request.
- AAAL determines whether the request can be satisfied locally through the use of the Network Access Identifier (NAI) which has the format of user@realm. AAAL can use the realm portion of the NAI to identify the Mobile Node's home AAA Server. If AAAL does not share any security association with the MN's AAAH, it may forward the request to its broker.

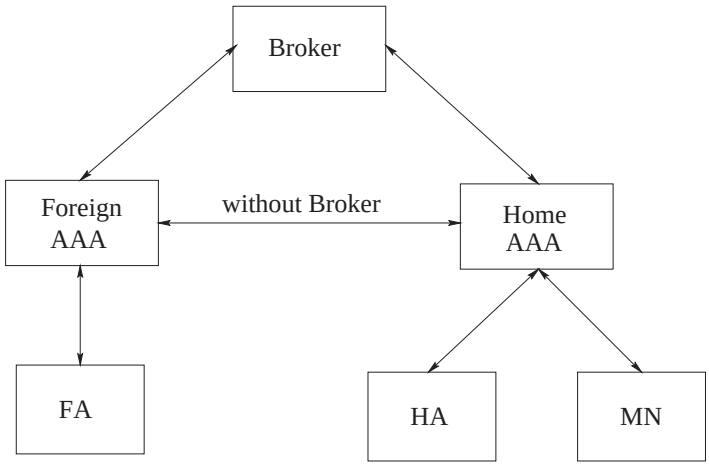


Figure 4.2: Trust Model in AAA Infrastructure

- The broker which shares an SA with AAAH will forward the request.
- AAAH receives the AAA request and authenticates the MN since it has a security relationship with it. Afterwards, it begins to authorize the request.
- The authorization includes the generation of dynamic session keys to be distributed among all mobility agents, optional dynamic assignment of a home agent, optional dynamic assignment of a home address (HA) (this could be done by home agent also) and optional assignment of QoS parameters for the MN [35].
- Once authorization is complete, the AAAH issues an unsolicited AAA request to the home agent including the information in the original AAA request as well as the authorization information generated by the AAAH.
- The home agent generates a registration reply that is sent back to the AAAH in an AAA response. The message is forwarded to AAAL via the broker and finally arrives at the AR which provides services to MN.

Concerning minimized latency involved in getting wireless (cellular) access to the network, only one single traversal is needed to authenticate the user, perform authorization and process the registration request. AAAL maintains session state information based on the authorization information. If the MN moves to another FA within the foreign domain, a request to the AAAL can immediately be done in order to immediately return the keys that were issued to the previous FA. This minimizes an additional round trip through the Internet when micro mobility is involved, and enables smooth handover.

The key distribution issue is one of our interests. After the MN is authenticated, the stage of authorizing the AAA requests includes the generation of three session keys which to be shared between MN and HA, MN and FA and FA and HA respectively. Each key is propagated to its related mobility entity through either the AAA protocol or MIP. Once the session keys have been established, the

mobility entities can communicate without the AAA infrastructure. However the session keys have lifetimes after which the session keys need to be updated.

A Solution of Diameter Mobile IPv6 application

According to [20], a model for the involved entities is shown as Figure 4.3. Figure 4.4 illustrates a typical registration procedure which is detailed as follows:

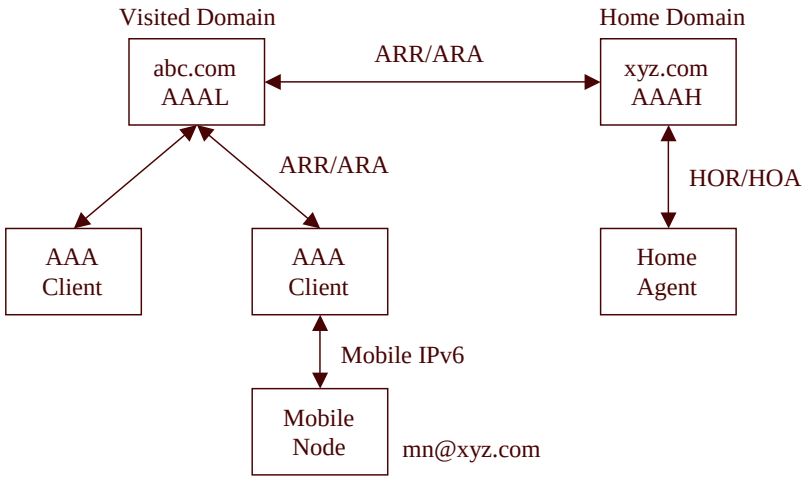


Figure 4.3: A model of Involved entities in a solution of Diameter MIPv6 application

1. When entering a new network or at power up, the MN listens to the router advertisements and retrieves the local challenge, the visited network identifier The information to derive the CoA.

2. MN computes the CoA based on the information of NAI, the long-term security key shared with its AAAH, * the Home Address (it is assumed that MN has a pre-configured Home IP address with a pre-existing Home Agent. It composes a registration request message destined to the AR which also acts as an AAA client.

3. The AAA Client first verifies the freshness of the request thanks to the local challenge contained in it. If successful, it performs Duplicate Address Detection and creates a Diameter ARR (AA-Registration-Request) message. It then sends the message to AAAL.

4. When AAAL receives an ARR message, first it verifies the message is coming from a valid AAA Client and then, checks the MIPv6 Feature Vector AVP, and then sends it to the MN's home AAA server.

5. When receiving an ARR message from an AAAL, AAAH first verifies the message is coming from a valid AAAL. Security associations between AAA server are assumed to be pre-existing. AAAH then authenticates the user using the NAI provided by the MN as MN identity. If the

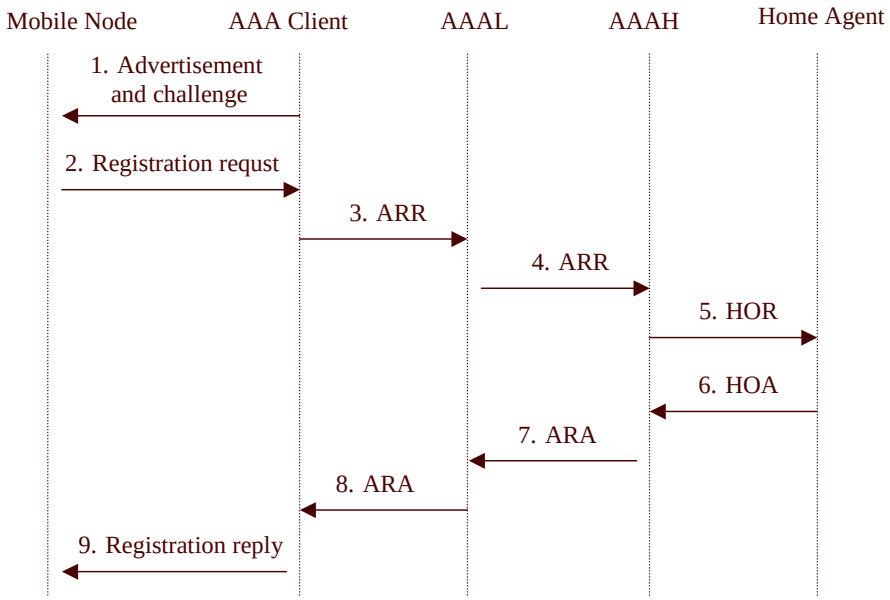


Figure 4.4: Message flow of a registration procedure in a solution of Diameter MIPv6 application

mobile Node is successfully authenticated, AAAH also computes some network authentication data based on the Host Challenge and eventually other information depending on the authentication algorithm adopted. AAAH sends a HOR (Home-Agent-MIPv6-Request) message to the HA including a newly created binding update. It also sends some security keying material to allow the Home Agent to compute the key(s) for the security association between the MN and the Home Agent to authenticate future Binding Updates.

6. Home Agent creates the Binding Cache and computes the key(s) for the security association with the MN from the data received. It also generates a Binding Acknowledgement message to be sent encapsulated to the MN. HA sends a HOA (Home-Agent-MIPv6-Answer) message to AAAH including the Binding Ack.

7. AAAH may also compute other keying material according to the keys requested by the MN and send it to the MN passing through the AAAL. AAAH then send an ARA (AA-Registration-Answer) message to AAAL including the MIP- Binding-acknowledgement AVP if the MN sent an embedded BU or request for a HA.

8. When receiving a ARA message from AAAH, the AAAv may optionally, according to the behavior specific for specific EAPs or other mechanisms defined elsewhere, store locally information contained in the AVPs of the message received from AAAH (e.g. authorization information, session keys, etc.) and then forwards the message to the AAA Client.

9. When receiving an ARA message from AAAL, the AAA Client converts the message to the appropriate protocol to the MN; this message carries the authentication data, Binding Acknowl-

edgement, Keying material to set up the different session keys. It sends the corresponding registration reply message to the MN.

4.1.3 IPSec

IP Security (IPsec), which is an open, standard security technology, is developed by the Internet Engineering Task Force (IETF). IPsec provides cryptography-based protection of all data at the IP layer of the communications stack. No changes are needed for existing applications. IPsec is the industry-standard network-security framework chosen by the IETF for both the IPv4 and IPv6.

IPsec protects signaling and data traffic using the following cryptographic techniques:

- *Authentication:* Process by which the identity of a host or end point is verified.
- *Integrity Checking:* Process of ensuring that no modifications were made to the data while in transit across the network.
- *Encryption:* Process of ensuring privacy by "hiding" data and private IP addresses while in transit across the network.

Authentication algorithms prove the identity of the sender and data integrity by using a cryptographic hash function to process a packet of data (with the fixed IP header fields included) using a secret key to produce a unique digest. On the receiver side, the data is processed using the same function and key. If either the data has been altered or the sender key is not valid, the datagram is discarded.

Encryption uses a cryptographic algorithm to modify and randomize the data using a certain algorithm and key to produce encrypted data known as cyphertext. Encryption makes the data unreadable while in transit. After it is received, the data is recovered using the same algorithm and key (with symmetric encryption algorithms). Encryption must occur with authentication to verify the data integrity of the encrypted data.

These basic services are implemented in IPsec by the use of the Encapsulating Security Payload (ESP) [39] and the Authentication Header (AH) [38]. ESP provides confidentiality by encrypting the original IP packet, building an ESP header, and putting the cyphertext in the ESP payload.

The AH can be used alone for authentication and integrity-checking if confidentiality is not an issue. With AH, the static fields of the IP header and the data have a hash algorithm applied to compute a keyed digest. The receiver uses its key to compute and compare the digest to make sure the packet is unaltered and the sender’s identity is authenticated.

IPSec Modes

both AH an ESP support two modes of use: transport and tunnel mode.

Transport mode provides protection primarily for upper-layer protocols. The protection extends to the payload of an IP packet. Typically, transport mode is used for end-to-end communication between two hosts. As shown in Figure 4.5, ESP in transport mode encrypts and optionally authenticates the

IP payload but not the IP header. As shown 4.6, AH in transport mode authenticates the IP payload and selected portions of the IP header.

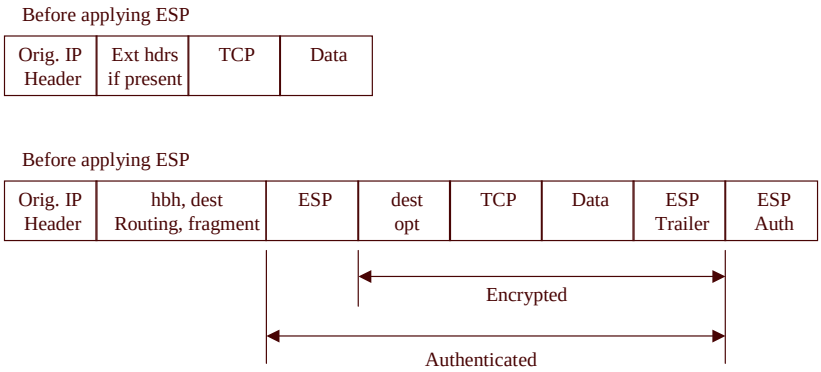


Figure 4.5: ESP Transport mode of IPv6

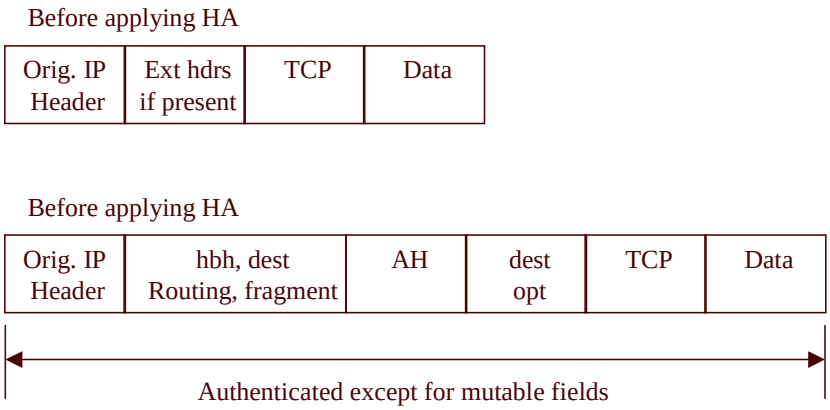


Figure 4.6: HA Transport mode of IPv6

As shown is Figures 4.7 and 4.8, Tunnel mode provides protection to the entire IP packet. After the AH or ESP fields are added to the IP packet, the entire packet plus security fields is treated as the payload of new "outer" IP packet, with a new outer IP header. The entire original, or inner, packet travels through a "tunnel" from one point of an IP network to another; no routers along the way are able to examine the inner IP header. Tunnel mode is used when one or both ends of an SA is a security gateway. In our scenarios, IPSec tunnel mode is used to protect signaling and data traffic over the wireless channel.

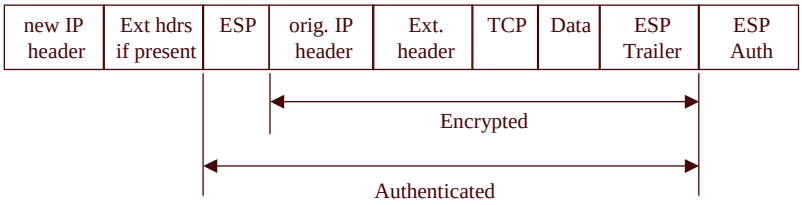


Figure 4.7: ESP Tunnel mode of IPv6

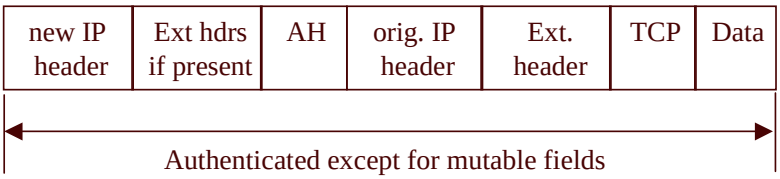


Figure 4.8: HA Tunnel mode of IPv6

Security Associations

The building block on which secure communications is built is a concept known as a security association. Security associations relate a specific set of security parameters to a type of traffic. With data protected by IP Security, a separate security association exists for each direction and for each header type, AH or ESP. The information contained in the security association includes the IP addresses of the communicating parties, a unique identifier known as the Security Parameters Index (SPI), the algorithms selected for authentication or encryption, the authentication and encryption keys, and the key lifetimes. Figure 4.9 shows the security associations between Host A and Host B. This illustration shows a virtual tunnel running between Host A and Host B. Security association A is an arrow directed from Host A to Host B. Security association B is an arrow directed from Host B to Host A. A Security association consists of the Destination Address, SPI, Key, Crypto Algorithm and Format, Authentication Algorithm, and Key Lifetime.

A SA normally includes the following parameters:

- *[required]:*
  - Authentication algorithm and algorithm mode being used with the IP AH.
  - Key(s) used with the authentication algorithm in use with the AH.
  - Encryption algorithm, algorithm mode, and transform being used with the IP ESP.
  - Key(s) used with encryption algorithm in use with the ESP.

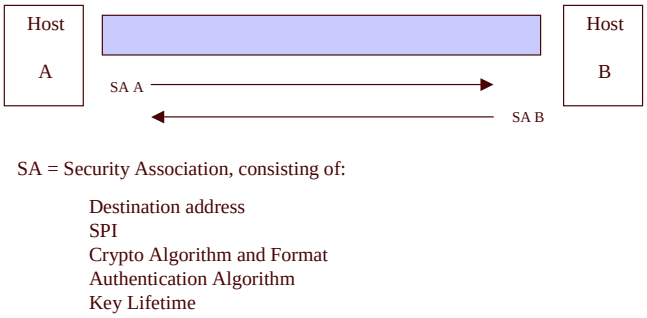


Figure 4.9: The Establishment of a secure tunnel between Hosts A and B

  - Presence/absence and size of a cryptographic synchronization or initialization vector field for the encryption algorithm.

- *[recommended]:*

  - Authentication algorithm and mode used with the ESP transform (if any in use).
  - Authentication key(s) used with the authentication algorithm that is part of the ESP transform (if any).
  - Lifetime of the key or time when key change should occur.
  - Source address(es) of the SA, might be a wild-card address if more than one sending system shares the same SA with the destination.
  - Sensitivity level (for example: Secret or Unclassified) of the protected data [required for all system claiming to provide multi-level security, recommended for all other systems].

A SA is normally one-way. An authenticated communications sessions between two hosts will normally have two SPIs in use (one in each direction).

The encryption and authentication algorithms used for IPSEC are the heart of the system. They are directly responsible for the strength the security the system can provide. There are however major drawbacks in this area. As the Internet is an global network, the IP should provide uniform security everywhere. Many countries, however, either restrict or forbid the use, or export of encryption algorithms. This means that the IPSEC must be able to balance between the legal restrictions in use of strong encryption and authentication, and the one that is available everywhere.

All hosts claiming to provide IPSEC services must implement the AH with at least the MD5 algorithm using a 128-bit key as specified in the AH RFC. An implementation may support other authentication algorithms in addition to keyed MD5. All ESP implementations must support the use of the Data Encryption Standard (DES) in Cipher-Block Chaining (CBC) mode as detailed in the ESP specification. Other cryptographic algorithms and modes may also be implemented in addition to this mandatory algorithm and mode. MD5 and DES-CBC should be set as default algorithms.

Key Management

The key management portion of IPSec involves the determination and distribution of secret keys. A typical requirement is four keys for communication between two applications: transmit and receive pairs for both AH and ESP.

Manual and automated are two types of key management. The default automated key management protocol for IPSec is referred to as ISAKMP/Oakley. Oakley [52] is a refinement of the Diffie-Hellman key exchange algorithm; ISAKMP [45] does not dictate a specific key exchange algorithm. It defines procedures and packet formats to establish, negotiate, modify, and delete security associations.

The Internet Key Exchange (IKE) [32] describes a hybrid protocol using part of Oakley and part of SKEME [41] in conjunction with ISAKMP to obtain authenticated keying material for use with ISAKMP, and for other security associations such as AH and ESP for the IETF IPsec DOI. The purpose is to negotiate, and provide authenticated keying material for, security associations in a protected manner.

4.1.4 CASP QoS Client Protocol

Signaling resource reservations is one of the possible applications of the Cross-Application Signaling Protocol (CASP). This section describes a client protocol that supports per-flow resource reservation in both sender- and receiver-directed modes operation.

Introduction

CASP-QOS [55] is a client protocol for the Cross-Application Signaling Protocol (CASP) [56]. It is one of a family of CASP signaling client protocols (NSLPs) and offers per-flow resource allocation and reservation.

CASP-QOS has the following properties:

- *Direction-neutral:* The protocol supports both receiver-oriented and sender-oriented reservations. In each mode, the non-reserving side can suggest QoS parameters. For example, the data receiver can send the first CASP message to indicate the range of bandwidths and QoS parameters it is willing to tolerate, but the data sender makes the actual reservation within that range.
- *Bidirectional reservation:* Bidirectional reservation refers to three different modes of operation.
- *Reservation range:* To reduce the number of reservation message exchanges, the bandwidth object contains a lower and upper bandwidth range. Nodes attempt to reserve the highest amount of resources below the maximum and update the amount accordingly.
- *Partial reservation:* CASP-QOS messages can indicate whether they are satisfied to obtain partial reservations, i.e., reservations that only succeed on some routers.
- *Query/reserve/commit mechanism:* If desired, an end system can query for available resources, reserve them and commit them. Only committed resources can be used.

An Example of a Resource Reservation Process

Figure 4.10 shows an example for the utilization in a resource reservation process.

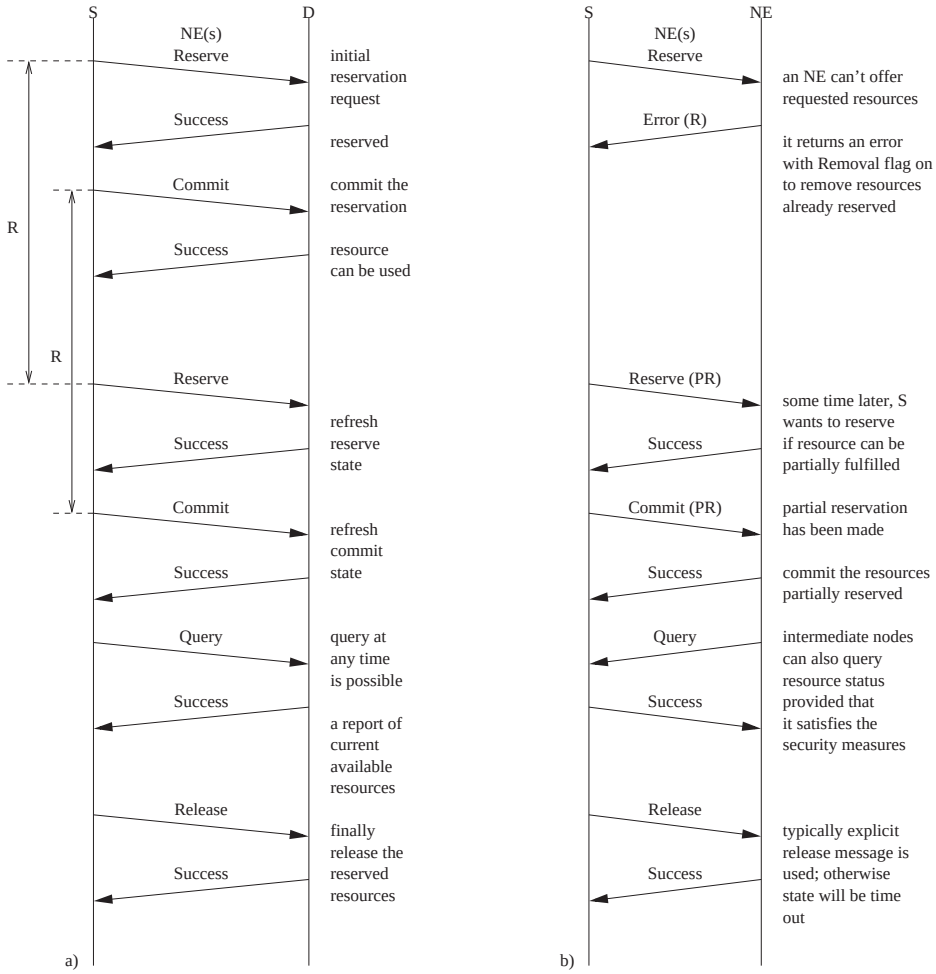


Figure 4.10: An Example of a Resource Reservation Process of CASP QoS Client Protocol

The process contains 5 message types for the reservation mechanism, Query, Reserve, Commit, Release and success. To indicate an error during the reservation process an appropriate message can be emitted.

The resources in the network are requested by a set of objects. It is possible to include several objects in one request. If one of the requests matches, the response to the reservation contains the appropriate confirmation.

Additional objects may be defined in the future. At the current state 4 objects exist:

- Bandwidth. The object contains 2 values, an upper and an lower value. Each node should try to reserve a bandwidth according to the upper value. At least it should reserve the lower bandwidth if available.

- Per hop behavior (PHB). A special treatment in each hop can be assigned to data traffic which is matching a certain traffic selector defined by the PHB object.
- IntServ Flowspec. It describes reserved resources for Integrated services.
- L2 Properties. Abstract description of the L2 connection properties, regarding the delay and packet losses.

The distribution of the QoS related information in the network can be limited to an area (e. g. an AS) or a section of the path in the network. The CASP QoS information can be added and deleted anywhere in the network. A reservation with local scoping is referred to as a localized path.

Route Change and Mobility Considerations

The separation between M-layer state and C-layer state in CASP is logically (and not physically). Hence a route change also requires to create a new reservation along the new path until the merge point (cross-over router) is reached. The separation between the Session ID and the Traffic Selector enables the merge point to associate an existing reservation with the Session ID provided by the incoming signaling message. As a difference between a standard route change and a mobility scenario the possibility of a Traffic Selector change should be mentioned. Typically the former does not require signaling messages to be forwarded beyond the merge point. The situation might be different in case of mobility and the used Traffic Selector. Thus there is an interaction with a micro/macro-mobility scheme. Using a micro-mobility scheme which is able to trigger CASP would therefore further limit double reservations and would speed the reservation setup time.

A signaling message initiator can request the deletion of the old reservation (along the old path). deleting a reservation along an old path might not always be desired. The initiator is thereby a CASP node which detects the route change first. There are some reasons why such a behavior might not be necessary or desired (for example bi-casting of data traffic to both access routers).

Particularly of interest for Candidate Access Router (CAR) discovery is the QUERY message which allows to discover the resource availability information (and possibly reservations costs) along new candidate paths.

Subsequently a few basic mobility signaling message exchanges are described. The first exchange covers a QoS reservation for upstream traffic. Subsequently the implication for downstream traffic is explained. Thereby the interworking with micro-mobility schemes is briefly described based on Context Transfer and Hierarchical Mobile IP.

4.1.5 CASP Mobility Client Protocol

In high mobility scenarios, frequent handovers may result in a significant degradation of QoS provisioning if the access network is unable to provide enhanced solutions for prompt QoS re- establishments and efficient security checks.

Several requirements have been identified for optimization of local handovers in micro-mobility scenarios:

- *Bidirectional reservation:* If the route is symmetric, it should be feasible to set up reservation in both directions with a single reservation message; if the route is asymmetric, a reservation message from the originator should trigger an independent signaling message from the responder.

- *Path repair and re-establishment of reservations:* The paths in a mobility supporting access network usually change only partially after a handover. Therefore, the protocol should support partial repairs of the paths to avoid long distance end-to-end signaling message exchanges between corresponding nodes.

- *Reservation Range:* The reservation range consists of a lower and an upper bounds of QoS parameters e.g. bandwidth. The upper bandwidth value represents the desired bandwidth while the lower value is the acceptable bandwidth. If the network is not able to satisfy the desired value, it can reserve as much as it can which is greater than the acceptable value. Thus, the mobile node is unnecessary to negotiate further with the network on the requested QoS as happens when only one value in a QoS request.

- *Modularity:* The protocol should provide a modular architecture to enable different functionalities flexibly.

- *Endpoint identifier:* The endpoint identifier must be independent from identifiers which may change due to mobility, e.g. the IP address.

- *Security model:* The Security model must provide an efficient and secure solution.

To address the issue, we describe our design of CASP Mobility Client protocol [33], which enables secure, and seamless QoS provisioning support for mobile nodes.

The mechanisms of QoSBU (see 4.2.1), QoS protection against DoS based on localized cookie (see 4.2.2), enhanced advertisements (see 4.2.3, QoS-aware authorization (see 4.2.4 and securing user and signal data in intra-domain handovers (see 5.1.5) are now all integrated into the operation of the CASP Mobility Protocol. The interaction refers to Chapter 5; and the details of the CASP Mobility Protocol are described in Chapter 6.

4.2 Mechanisms

4.2.1 QoS-conditionalized Handover

This section presents a scheme for QoS support in Mobile IPv6. A QoS hop-by-hop option piggybacked in the binding messages is used for QoS signaling. A handoff takes place only upon the availability of sufficient resources along the new transmission path. This QoS-conditionalized scheme [28] builds upon the hierarchical mobile IPv6 protocol and is especially fit for local mobility, where the signaling overhead is reduced. It also enables the mobile node to flexibly choose among a set of available access points so that the mobile node can transmit packets through a route which offers satisfying QoS.

Background and motivations

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. 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 handoff scenarios, choosing a "good" access router might be more important than the mere speed of reestablishing a QoS path).

In [10] 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.

The mechanism described in [10] outperforms RSVP [71] in that 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 handoff. 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.

Our scheme is based on the architecture of Hierarchical Mobile IPv6 (HMIPv6) 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. Hence the MAP is a reasonable place for the switching router. However 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 [10] to overcome these limitations.

Mechanism Description

As shown in Figure 4.11, the operation of QoS-conditionalized binding update is as follows. 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 QoS entity 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 resources are not available, negative feedback will be provided to the MN by means of an extended Binding Acknowledgement (BA+QoS) message. If a BU+QoS message has reached the switching MAP and passed the local QoS test as well, the binding update will take

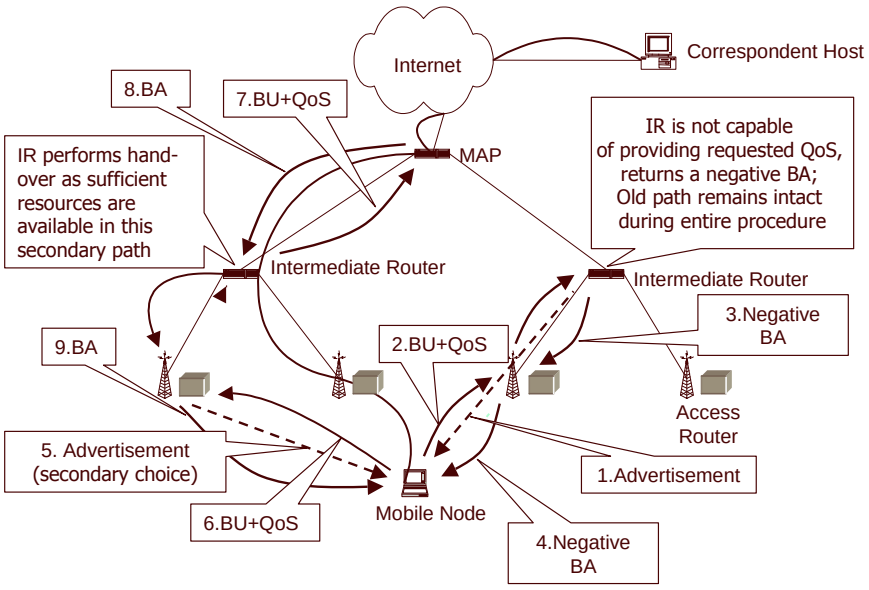


Figure 4.11: Operations of QoS checking and establishment

place (the binding cache in the MAP is updated to reflect the new LCoA) and a positive BA+QoS message is returned to the MN. Otherwise, no handoff is performed and a negative BA+QoS message is returned to the MN. When observing a negative BA+QoS message, intermediate QoS entities can release reservations that could not be granted further upstream.

- *MN considerations:*
  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 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 acceptable/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. 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 QoSOpt. 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.

- *Router Considerations:*
  when 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 re- served. 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.

Summary

The QoSBU approach is an optimization of QoS re-establishment during the local movements in an HMIPv6-based access network, by piggybacking the QoS signaling in the BU and BA messages. This mechanism has been implemented on a testbed and the data format is shown in A.11 and A.12. Details of the implmentation refer to [50].

However, due to the identified problem as shown in 3.2.2, the CASP Mobility Protocol (see Chapter 6) substitutes the QoSBU approach and is deployed in the second phrase of the SeQoMo project.

4.2.2 Cookie

Quality of Service (QoS) mechanisms in networks supporting mobile Internet communications give rise to new threats: these mechanisms could be abused by malicious entities launching so-called Denial of Service (DoS) attacks.

If the network can not efficiently check the credibility of a QoS-request during a handover process, malicious entities could flood the network with bogus QoS-requests; if the authentication check is performed by means of an AAA protocol before the access network commits its resources to the request, the authentication process may not only introduce a notable latency to the handover process, but also generate an extensive traffic which degrades the signaling capacity in the network when there are a considerable amount of malicious requests. In order to defend against these kinds of attacks and meet the low-latency micro-mobility handover requirement, we propose to have a preliminary check with a cookie-based mechanism to verify that the QoS-request sender is a registered user before processing the requests and performing authentication and authorization [11]. The performance evaluation shows that the cookie-based mechanism is efficient in dealing with the identified issues.

Background and motivations

The introduction of advanced QoS mechanisms, which aim to guarantee certain service characteristics in networks supporting mobile Internet communications give rise to new threats that these mechanisms could be abused by malicious entities to launch so-called *Denial of Service (DoS)* attacks, which aim at reducing the availability of services to legitimate users. These threats arise specifically from the fact that QoS-signaling mechanisms enable mobile nodes to make requests to a network, resulting in resource reservations.

In an IP-based access network, a MN sends a request to an AR for a certain resource. If the network can not check the credibility of a QoS request (i.e. whether the request originates from a MN that is actually authorized to use the services it is requesting), malicious entities can flood the network with bogus QoS requests in order to cause the exhaustion of the available resources through temporal reservations. This represents one specific DoS threat.

A possible solution consists in the following procedure: when an AR receives a QoS request, before starting the resource reservation process, the AR communicates with a local security authority, e.g. a AAAL, to authenticate the MN and authorize the QoS request. Only when the check passes, the path reserves resources according to the request. Obviously, the latency introduced by proceeding to security checks at the AAAL, which includes the contribution of the propagation delay and processing time at AAAL, is not desirable when low latency of the registration process is a major concern. Moreover, the same checks at an AAA server have to be performed on all the bogus requests from attackers. Thus all the security check signalings may degrade the performance of the access network substantially by depleting the signaling capacity of the path between the AR and the AAAL and exhausting the computing resource of the AAAL. This represents another specific DoS threat.

To defend against the identified DoS threats in intra-domain handovers, we propose a two-step procedure comprising of one preliminary credibility check, after which processing of the signaling request is either aborted or continued, and the second definitive authentication check as described above. This allows us to avoid the identified DoS threats. The credibility check should have the following

properties:

- performing the first check must be a quick operation;
- The AR must not keep per-session or per-user state until the verification is complete.

The "client puzzle" idea [2] might serve as the first check. A client is asked to solve a cryptographic puzzle when initiating a connection with a server. The server stores the protocol state and executes expensive operations only after it has verified the client's solution. In this way, the puzzle can prevent intensive connection initiations from attackers, thus enhancing the DoS-resistance of a server. However, solving cryptographic puzzles imposes a computational burden to all legitimate clients and the server, as well as requiring additional messages to be exchanged. It would add a non-negligible latency to the establishment of a connection between client and server.

In order to meet the low-latency requirement and protect QoS reservation against identified DoS attacks, we propose to use a cookie-based mechanism as the first credibility check. A cookie is verified by an AR to ensure that the QoS-request sender is a credible registered user before processing the requests and performing authentication and authorization. This preliminary check enables us to prevent DoS attacks, both in the form of resource reservations along a path or keeping the AR busy through the processing of malicious QoS requests, with the help of a AAAL or possibly the home AAA server (AAAH).

The Data Structure of a cookie

Figure 4.12 shows the data fields of a cookie. The purpose of each field may be listed as follows:

Figure 4.12: Cookie data fields

- *MN_ID*: is the MN's unique identifier. This can be a local unique identifier the MN gets after its first registration.
- *Gen_ID*: identifies the cookie generator which is always an AR. It can be the AR's IP address or another unique identifier acceptable in the access network.
- *Creation_T*: is the timestamp marking when the cookie was generated. It is used to limit the cookie's period of validity.
- *Random_Nr*: is used to distinguish two cookies which are generated at the same time.
- *CookieHash*: The hash code is a message digest of the cookie information and a cookie key. The hash function can be of either HMAC-MD5 or HMAC-SHA1. The cookie key could be distributed from the MAP to each AR and updated by the MAP periodically. For example a new cookie key is distributed by the MAP every hour or day.

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

$$\begin{aligned} CookieInfo &:= \big(MN\_ID, Gen\_ID, Creation\_T \\ &\quad\; Random\_Nr\big) \\ CookieHash &:= HMAC\big(CookieKey, CookieInfo\big) \\ Cookie &:= \big(CookieInfo, CookieHash\big) \end{aligned}$$

Mechanism Description

The cookie-based mechanism is described in an access network which is based on a HMIPv6 and AAA joint architecture. The architecture includes an AAAL, a mobility anchor point (MAP) and ARs positioned linearly as shown in Figure 4.13.

- *First cookie generation:*

  When a mobile user enters an access network (e.g. it performs a global movement or powers up), the authentication on its first QoS request must involve a trusted network (e.g. the mobile user's home network) because the user is unknown to the access network at the moment.

  After the authentication at AAAH, the access network knows that the user is credible, AAAL caches the MN's authorization information and MAP, AR2 (taken to be the associated AR in our example, see Figure 4.13) and MN get to know the session key which is generated by the MN's home domain.

  AR2 generates a cookie, encrypts the cookie with the session key, inserts the encrypted cookie in the BU acknowledgement (BU ACK) message which is generated by MAP and destined to MN. The MN can get its first cookie in the access network since the MN can derive the session key due to its long term trust relationship with its home domain. Thus, MN gets its first cookie in the access network.

- *Cookie verification:*

  In a local movement, as shown in Figure 4.13, MN presents the cookie to a neighboring AR server (say AR3). Because there is no security association between MN and AR3 so far, the cookie is transmitted in plaintext.

  When receiving the cookie, AR3 first verifies that the cookie is valid with the following checks:

  – check the timestamp in the cookie to verify the cookie is not expired;
  – check the identity of the cookie generator to verify the cookie is created by an AR on its trusted list;
  – verify that the cookie is not on the notified cookie list;
  – if the above checks pass, AR3 computes a key-hashed digest of the cookie information by using a cookie key, and compares the computation result with the hash digest contained in the cookie.

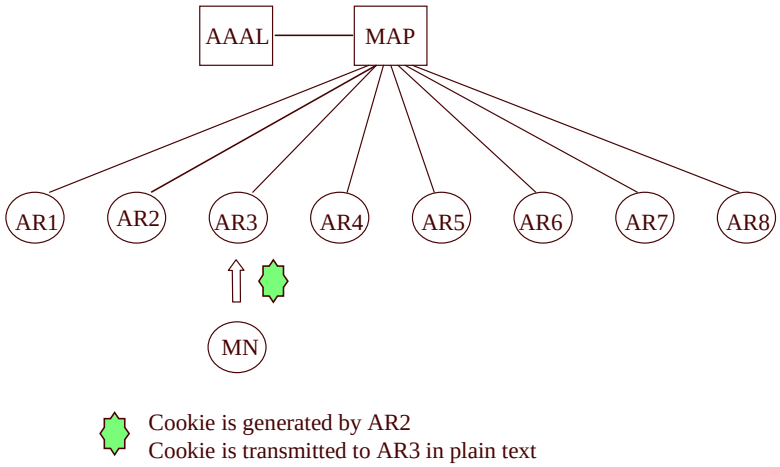


Figure 4.13: AR3 verifies the cookie presented in plain text from the MN

If the two hash digests match, the cookie check verification is completed successfully.

After verifying a cookie successfully, AR3 informs AR2 who originally generated the cookie that it has been presented to it. AR2 then notifies all other ARs on its trusting list to invalidate the cookie, preventing these ARs to accept it again; indeed, an attacker could intercept 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 it from the notified cookie list.

In case the cookie verification fails, AR3 will drop the 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 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, because the old cookie has been transmitted in plaintext and can not be used any longer. Thus the MN can not get the benefit of the optimized handover processes.

Even though a verification failure could occur, e.g. due to cookie key updating or interferences from an attacker, the cookie-based preliminary check allows to prevent DoS attacks to the access network without having a major impact on MN's normal operations (i.e. continuous moving without interrupting the service use), as it is reasonable to assume that an MN does not experience these cases very often during its normal operations.

- *New cookie granting:*

When the cookie verification is completed successfully, the QoS-conditionalized BU [28] and authorization processes start. The two processes can proceed in series or in parallel. If the two processes are successful, the AR3 can do authentication of the registration request when it gets the session key embedded in the BU ACK message from the MAP. When this check passes, the AR3 generates a new cookie, encrypts it with the session key and inserts it in the BU ACK message. The new cookie is used for its next registration and the old cookie is no longer valid in the access network.

Discussion

There are three main points in the design of this cookie mechanism: the "area of validity", the notification of a used cookie, and the presentation of a cookie in plain text.

- *Area of Validity:*

  The "area of validity" is a group of ARs at which a cookie is valid. In other words, the "area of validity" corresponds to the trusting list of the cookie generator.

  When a cookie is presented in plain text to AR3 (see Figure 4.13), if AR3 were not to notify other ARs about the use of the cookie, the cookie could be intercepted by an attacker on air and replayed to other ARs. Consequently, the attacker could gain access at these ARs so as to play DoS attacks on the corresponding paths. On the other hand, if each AR were to notify the rest of the access network when receiving a cookie, the propagation of notification messages would generate substantial traffic in the access network.

  Therefore, we introduce a limited "area of validity" for each cookie, the nodes in this area being the only ones that can accept the cookie. For example, each AR could have its adjacent ARs only on its trusting list and trusted list. AR2 would put AR1, AR3 and itself on its trusting list to form the "area of validity", this meaning that the cookies generated by AR2 are only accepted by AR1, AR2 and AR3, while being rejected by other ARs. Necessarily, both AR1 and AR3 have AR2 on their own "trusted list" and they can accept cookies generated by AR2.

- *Notification of used cookies:*

  After verifying the cookie, AR3 notifies immediately AR2 about the cookie use and then AR2 notifies AR1, who is the remaining AR on AR2's trusting list, not to accept the cookie. All ARs are then free from replay attacks, provided that the notification messages propagate faster than the time needed for an attacker to intercept a cookie and replay it.

- *Presenting a cookie in plain text:*

  Mobile nodes always send cookies in plain text to access routers, as in the case of a handover, since the MN does not yet share a session key with the new access router at the time it sends the cookie. Although the cookie might be intercepted by an attacker when being presented in plain text, the risk of DoS attacks is reduced sufficiently with the mechanisms described above. The reason for this is, that the cookie mechanism reduces the overall number of "credible looking" handover requests, as every cookie can only be presented once.

Summary

In summary, the cookie-based mechanism has the following design considerations:

- Cookies are always generated by an AR. A cookie can be verified by either its generator or other ARs which are destined to accept it.

- A cookie is transmitted encrypted from its generator to the MN and in plain text from the MN to an AR.
- A cookie is used only once since the cookie may be intercepted by an attacker during its transmission on air in plain text.
- The cookie key, which is used for generating and verifying a cookie at ARs, is updated periodically by MAP.
- 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. The cookies generated by an AR can only be accepted by those on the AR's trusting list.
- After accepting the cookie, an AR makes other ARs which can accept the cookie (ARs on the cookie generator's trusting list) know about the use of the cookie by propagating notification messages, in order to prevent further attempts to use the cookie.
- Expired cookies are removed from the notified cookies lists.
- A MN can request the cookie generator to grant a new cookie when its cookie is going to expire.

4.2.3 Enhanced Advertisements

Presently, the advertisement only includes the topology information of the access network. In MIPv6 case, mobile node can construct a new Care-of-Address (CoA) based on the advertised prefix information. Before performing a handover, a mobile node may receive more than one advertisement from different access routers before the old advertisement expires.

We introduce aggregate QoS information about a path and price tariff information regarding accounting. The mobile node may select a path which can provide more desirable QoS with cheaper price.

In order to distribute the price information and available bandwidth to the mobile nodes, the foreign agent (FA) of a network, e.g. MAP in a HMIPv6 architecture, provides the access routers and intermediate routers with information about the current state of the network.

Advertisement Propagation

The FA of a network is responsible for being discovered by mobile nodes. Therefore, it advertises its presence downstream in the access network.

Every foreign mobility agent or intermediate router (IR) must be able to receive and propagate advertisement messages from its upstream nodes in the access network.

Figure 4.14 shows how advertisement messages propagate in a hierarchical architecture. The router in level 2 sends its advertisement to the routers in level 1, including e.g. its prefix information, the bandwidth value it can provide and the price information. The routers in level 1 extracts the useful information from the advertisement message sent by the upper router and composes its own advertisement which contains 1) the prefix information of the upper router and itself; 2) QoS parameters

e.g. available bandwidth of the path; and 3) the applicable price information if any. Then it sends out its advertisement. The advertisements from routers in level 1 are sent more frequently than those from routers in level 2.

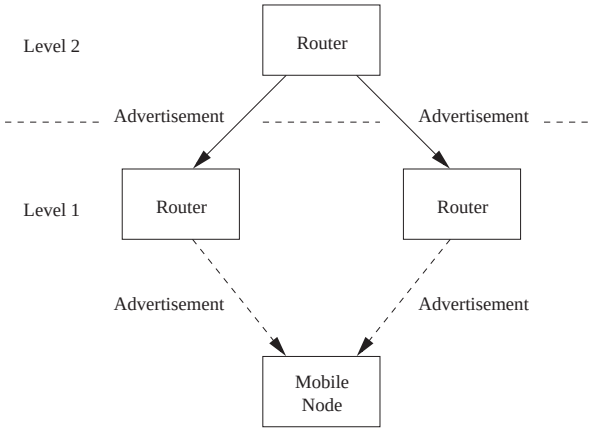


Figure 4.14: Advertisements propagate

Considerations of the Routers in the Access Network

This section describes the required operations of the routers in an access network regarding the propagation of QoS and price information [13]. Usually the information about available resources in a network varies more often than the price information.

To reduce the signaling traffic in the network it is advantageous not to advertise the resources each time after a minimal change occurred. Therefore, the routers in the network can maintain threshold values. Apart from that all the values are soft states which are continuously sent by each router. Figure 4.15 illustrates the notion of "threshold of bandwidth width".

The threshold values determine, under which condition a new advertisement must be sent out immediately. Each router (including intermediate router) maintains an upper and a lower threshold value.

When the remaining total bandwidth at a router reaches the lower threshold value, the router will not insert the normal bandwidth value which it is providing to a session in its regular advertisements any longer. It sends immediately a new advertisement with a smaller bandwidth value in it, announcing that it will provide the new bandwidth for further sessions. It will use the new bandwidth value in its regular advertisement until the remaining total bandwidth reaches the upper threshold value. This strategy aims to serve more sessions with a degraded quality instead of providing the whole bandwidth to only some mobile nodes and rejecting the requests of others.

When the remaining total bandwidth reaches the upper threshold value due to the bandwidth release from terminated sessions, the router advertises immediately the normal bandwidth since it has enough resources again to provide the normal bandwidth to each session.

When the remaining total bandwidth fall in the range of the upper and lower threshold, no irregular advertisement is necessary to be sent out. Otherwise, there would be too many unnecessary advertise-

ments being sent out when the remaining total bandwidth is oscillating around one threshold value due to the continuing process of resource releasing and reserving.

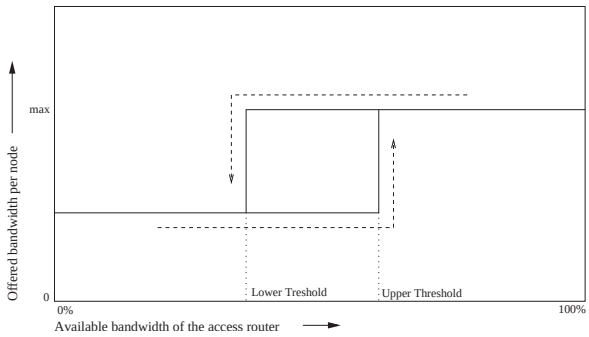


Figure 4.15: Advertised bandwidth to each mobile node depending on the total amount

In general, an advertisement must be sent if one of the following events occurs:

- The router receives a new advertisement from another router. The router must add its own information and forward the advertisement downstream.
- The available resources or the costs for the resources change if there is no threshold values; or the change makes the available resources fall below threshold values.
- The validity of advertised information expires. All advertised information are soft state and must be regularly refreshed. If a router does not receive a refresh from another router for a certain period of time, the information expires.
- The router receives a solicitation message. Nodes in an access network can request information from routers via solicitation messages. The solicitation are a fixed part of every advertising mechanism.
- Registration or de-registration of a mobile node at a foreign agent (FA). If the FA receives a registration update from a mobile node which leaves an access network, the FA can release the reserved resources and it can (depending on the application of thresholds) send an advertisement to the routers in the network.

The described process considers only the available bandwidth in the access network. It is not able to provide the QoS information outside the access network.

Advertisement Message Format

An enhanced ICMPv6 Router Advertisement message is shown in figure A.13.

The details of IPv6 header and ICMPv6 router advertisement are described in [16] and [49].

We describe only the fields of the enhanced features, which are the IPv6 address of the next CASP node, available bandwidth information, a price reference label.

Next CASP node Option:

Type	TBD
Length	8-bit unsigned integer. The length of the option (including the type and length fields) in units of 8 octets. The value is 3.
Reserved	This field is unused.
Valid lifetime	This value indicates the validity duration of the announced CASP node.
CASP node address	The IPv6 address of "the next CASP node". This address is used as the destination address for the CASP messages which are sent by the mobile node to reserve bandwidth in the access network.

Bandwidth and Price Information Option:

Type	TBD
Length	8-bit unsigned integer. The length of the option (including the type and length fields) in units of 8 octets. The value is 1.
Flg	A 2-bit flag to indicate the presence of the available bandwidth and the price reference label. 11 means the advertisement contains available bandwidth and price reference label information; 10 means only available bandwidth and no price reference label; 01 means only price reference label and no available bandwidth information.
Available Bandwidth	16-bit unsigned integer represents the available bandwidth for each mobile node at the router.
Price Reference Label	16-bit unsigned integer represents the price information in the administrative domain.

The Next CASP node option is only demanded, if the access router itself can not handle the CASP messages from the mobile nodes. In this case, it advertises the address of another CASP node in the access network, which is suited to process the reservation requests from the mobile nodes. Another application area is the usage of brokers in the access networks.

The Bandwidth and Price Information Option should be included in every advertisement. According to the available bandwidth information, mobile nodes can make decisions on 1) whether to perform a handover; and/or 2) which access router it should handoff to.

This value may be replaced by another value when a router at the lower level can provide only a smaller bandwidth. Hence a mobile node can determine the aggregate bandwidth provided by the path when it receives an enhanced advertisement. A mobile node should be able to obtain the available bandwidth information by means of e.g. sending a solicitation message.

To reduce the required number of bits in the price information field, a label is used in this field rather than the detailed price information. Each label specifies a charging model (e.g. 0.25 Euro per minute for the first 3 mins and 0.10 Euro per min for every additional min or 0.20 Euro per 100 kByte for

the first 3 MByte and 0.15 Euro afterwards). A mobile node can determine the price with the label based on the knowledge of the label defined in a price reference table. If a mobile node does not have the knowledge of the label or the price reference table, it can request the information from the access network by means of e.g. sending a solicitation message. The access network should answer each individual solicitation request with the meaning of the label by either unicast or anycast depending on a local policy unless it considers that it is under an attack with an excessive amount of such requests.

Furthermore, mobile nodes should be able to authenticate and check the integrity of the price information presented in an advertisement. More details are discussed in the section of security considerations. Other issues of price information distribution are discussed in [63].

It may be necessary that the domain administrator refreshes the price reference table periodically. The refresh interval should be much larger than that of advertisements.

When the service provider changes the charging model by replacing the old price reference label with a new one from the same price reference table, or it assigns a new charging model to a label, it must publicize the new charging model in the access network while taking into account the following considerations:

- The access network should not spend a lot of bandwidth on distributing the detailed information.
- A mobile node in the access network should be able to obtain the charging model information if he does not receive the distributed information.

Therefore, when the access network needs to publicize the new charging model, it repeats the meaning of a price reference label in advertisements for e.g. five times. It includes the information in one advertisement e.g. every three advertisements. During the charging model publication period, the access network may or may not answer solicitation requesting the information. After the period, it should answer the solicitation with the information unless it considers that it is under an attack with an excessive amount of such requests.

Security of the Enhanced Advertisements

The receiver of an enhanced advertisement has to be sure that it was send by a legitimated access router and that it was not modified during the transmission by an attacker, which tries to influence the communication between the two entities. A bogus node could try to steal or interrupt the service for mobile nodes by generating well directed information and propagate it in own advertisements or by changing existing ones. Also, DoS attacks with unspecific data are conceivable.

During the first registration with the access network the MN and the network perform a mutual authentication. The requirements for an inter-domain handover are more severe than those for the initial case, e.g. the MN can not check the Identity of an access router by contacting a third party (i.e. AAA entity).

The SeQoMo uses a mechanism, which is based on a timely restricted validity of the intervals. In a certain period of time, advertisements can be send and received by the mobile node. The integrity

of those advertisements is ensured by a message authentication code (MAC) at the beginning of the message. It is calculated with a key Ki. This key is send in an own message by the sender of the advertisement a short duration after the advertisement was send.

A mobile node, which receives the advertisement and which potentially will perform a handover stores them until it receives the key. Each entry in the list of received advertisements has a very small timeout in case that the message with the key will get lost and therefore the memory consumption for this mechanism is marginal.

If the message with the key is received, the MN calculates the MAC over the received message and compares it to the one which was included in the original message. If both match, the integrity of the message is verified.

The duration of the interval between the advertisement and the message with the key depends on the propagation delay of the messages in the access network and the clock difference between the involved entities. It must be ensured that all MNs recognize the end of an interval, before the key is emitted by the access routers (see Figure 4.16. A trade-off between the precision of the synchronization and the duration after which an advertisement should be verifiable must be found.

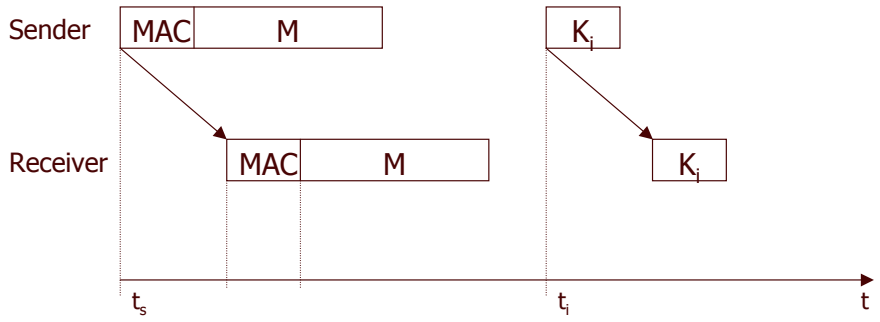


Figure 4.16: Key Distribution and Synchronization in Securing the Enhanced Advertisements

The previous chapters describe the mechanism for the integrity check of a message, but it must also provide the opportunity for an authentication check of the message. Else, an attacker could send its own advertisement and the correct key for it afterwards, and the MN would have no opportunity to check the identity respectively the affiliation to the access network of the access router.

Figure 4.17: The Hash Chain of the Key Deployment

Therefore, the deployed keys are based on an inverted hash chain (see Figure 4.17). Those chains

are a widely-used primitive in cryptography. A one-way hash function F is repeatedly applied to the last element Kl of a chain. The keys which are used to verify the advertisements are used in the order K0, K1, ... , Kl-1, Kl. At the initial registration, the MN receives the seed K0 respectively the value which is used in the current time interval. When the MN afterwards receives the key for an advertisement check, it can easily calculate the hash of the key and compare it to the seed or the previous one it received. The mechanism is also robust to packet lost, because in this case the MN only has to calculate the hash several times to verify the key, because of Fi(Ki) is equal to K0.

4.2.4 QoS-aware Authorization

In all-IP communications, mobile users may expect 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. Current authorization schemes do not fully meet the requirements in Mobile IP networks, especially regarding low-latency handover. Also they do not consider some issues such as non-disclosure of full content of an service contract which an MN subscribes in its home network, prevention of MN's misbehavior of using more resources than it is entitled to. This section presents an QoS-aware authorization scheme aiming at low-latency handover while taking the identified issues and requirements into account.

Background and Motivation

Authorizing a mobile user's QoS requests should introduce minimum latency to the registration processes because one requirement of QoS provisioning to a mobile user is to keep a mobile communication with as little interruption as possible.

While considering the low-latency handover issue, an authorization scheme should take some special concerns into account. For example, the subscribed value of bandwidth in a mobile user's service contract would be transmitted from its home network to the visited network even when the user only requested a low bandwidth for e.g. a directory service. Thus the visited network could be completely capable to authorize all of the user's QoS requests (e.g. when the user requested a much higher bandwidth for video-conferencing) without involving the user's home network again. However, it is not desirable to disclose the user's subscribed values of QoS parameters in the visited network since these values might be regarded as confidential information.

Moreover, some mobile user's activities should also be considered when an authorization protocol is designed:

- A mobile user may submit a range (i.e. a desired value as the upper bound and an acceptable value as the lower bound) of QoS parameters in its request rather than a specific value in order to simplify the negotiation process of authorization.
- A mobile user may update dynamically its QoS request when the network can provide more resources in either its current link or the new link it is handovering to.

- A mobile user may keep several data flows at one time, and terminate one of the flows or request a new service at any time.
- A mobile user may request resources for several flows in one registration packet.

The above mentioned issues are not fully covered in the existing proposals or solutions [7, 20, 67].

Mechanism Description

To meet the requirements in the above section, we propose a Hierarchical Mobile IPv6 (HMIPv6)-based AAA architecture.

This section presents the proposed authorization scheme in inter-domain handover, intra-domain handover cases and in case of QoS (re-)negotiation within the visited network by using bandwidth as a single QoS parameter of one flow request. The power-up and power-off cases are classified in inter-domain handover cases. We suppose that an MN submits a range of bandwidth as its QoS request. The upper bound is defined by a desired bandwidth (DBW) and the low bound is defined as an acceptable bandwidth (ABW). In intra-domain and QoS (re-)negotiation cases, registration attempt is termed as re-registration and authorization is termed as re-authorization.

- *Inter-domain handover:*
  The inter-domain handover case includes the situations that MN enters a visited network, leaves the network, power-up or power-down. When MN enters the visited network during a handover or it powers up, it submits a QoS request with a range of bandwidth for authorization while it should perform a BU process. Generally, there are two ways to proceed the authorization process and BU process:

  – proceeding the two processes separately: first authorizing the QoS request with the help of AAAH, then performing the BU process;
  – integrating the two processes: if the path can satisfy the QoS request in uplink procedure of QoS-conditionalized BU process [28], the MAP acting as an attendant in the AAA infrastructure initiates the authorization process. After receiving a positive authorization acknowledgement (ACK) and a positive BU ACK at the home agent (HA) from AAAH, MAP starts the downlink procedure of the QoS-conditionalized BU process.

  To meet the requirement of low-latency handover, we propose the second approach since it saves one inter-domain round-trip than the first one.

  The integrated procedure is shown in Figure 4.18. MN includes the bandwidth range as one QoS object in the QoS option of MIPv6 BU packet. When MAP determines a bandwidth value it can provide to the request, it starts the authorization process using e.g. Diameter protocol including the original range of bandwidth.

  After the successful authorization procedure, the authorized bandwidth value (i.e. the upper bound of the bandwidth range) is cached at AAAL as the maximum bandwidth the MN is allowed to use. The flow state information such as session key, session ID and reserved bandwidth

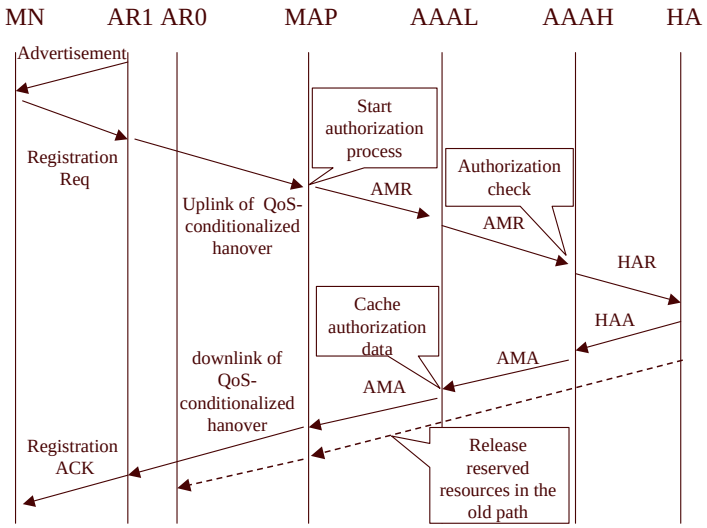


Figure 4.18: Integrated procedures of BU process and authorization process

for the flow is also cached at AAAL. Caching the information can benefit the intra-domain handover in terms of low-latency since AAAL can authorize a QoS request without involving AAAH if the MN does not start new flows or it does not upgrade requested QoS for the ongoing flow. It is noted that the subscribed bandwidth value is not disclosed to the visited network unless the upper bound of requested range is greater than the subscribed value.

When MN leaves the visited network without notification or it powers down, AAAL updates the flow state information based on the missing responses of the MN to the regular router advertisements.

- *Intra-domain handover:*
  In the intra-domain handover cases which happen more frequently, the feature of low-latency is more crucial. To meet this requirement, the bandwidth value the MN is consuming would be transferred directly from the previously associated AR (i.e. AR1) to the new AR (i.e. AR2) for re-authorization. However, when MN requests for more resource than it is currently using, the bandwidth information from AR1 could not help AR2 to re-authorize the request. Therefore, it is mandatory for AAAL to re-authorize the QoS request.

  With respect to security considerations, AAAL which is responsible for the authorization should check the integrity of the bandwidth request to prevent forgery and modification of the range; AAAL also manages the utilization of resources consumed by MN based on the flow state information.

  When MN sends a registration to AR2 for intra-domain handover, it is a new user to AR2. So AR2 needs to ask AAAL to authenticate the MN and authorize the QoS request either via MAP.

  The authorization process is identical to that in inter-domain cases, except that:

  – only when the requested bandwidth in the new path is greater than the cached value should AAAL contact AAAH for re-authorization;

– AAAL updates the cached value when AAAH re-authorizes the QoS requests successfully;
– BU process is only performed at MAP.

Figure 4.19 shows the integrated re-registration process.

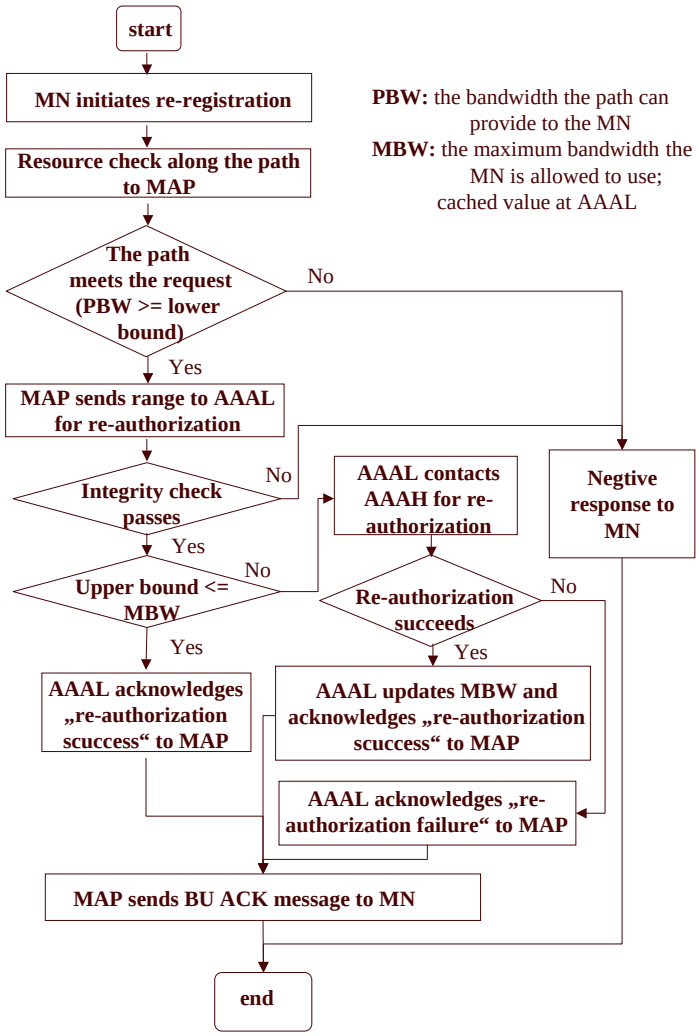


Figure 4.19: Integrated procedures of BU process and re-authorization process

Even though it loses the benefit of the efficient intra-domain handover feature when AAAL contacts AAAH for re-authorization, AAAL becomes more capable for next re-authorizations by updating the cached bandwidth value. By this means we can achieve a good balance between low-latency handover and non-disclosure of subscribed bandwidth value.

Summary

To support efficient (i.e. low-latency) handover, we proposed the following measures:

- deploying hierarchical architecture;
- integrating authorization process in BU process for inter-domain cases and parallelizing re-authorization process and BU process for intra-domain cases;
- enabling a range of QoS parameter rather than a specific value so as to simplify the authorization negotiation process;
- caching authorization data at AAAL;

However, in order to prevent the subscribed values of QoS parameters from being disclosed unnecessarily in the visited network, we caches the learned values of QoS parameters at AAAL rather than the subscribed value for re-authorization.

Consequently, the re-authorization is a continuing process: AAAL contacts AAAH for re-authorization if it is unable to re-authorize the MN's upgrading requests or new requests, and it updates the cached values of QoS parameters when AAAH re-authorization succeeds; AAAL also updates an MN's flow state information when the MN upgrades or degrades QoS of a flow, terminates or starts a flow.

AAAL must get involved in re-authorization because it has the knowledge of both the cached values of QoS parameters and the MN's flow state information of all ongoing flows. Furthermore, since the AAAL monitors the overall resource utilization of an MN, it can prevent MN's misbehavior to use more resources than it is entitled to.

Chapter 5

Interactions between the SeQoMo Components

This chapter describes the interactions between the SeQoMo components. The SeQoMo approach meets four principal signaling necessities:

- Registration upon power-up of an MN;
- Inter-domain handover:
  - it occurs when MN changes the access network operator (administrative domain);
  - it is similar with the power-up case with additional QoS signaling in order to update existing QoS reservation.
- Intra-domain handover:
  - this case happens most frequently which MN moves inside an access network;
  - the re-registration procedure is realized with optimized CASP Mobility Client protocol.
- Session refresh: the corresponding operations are triggered by the following events:
  - MN refreshes Mobile IP re-registration and QoS flow state periodically. The refreshment are realized with standard Mobile IP and CASP QoS Client procedures;
  - Security states need to be refreshed periodically. This is done with the CASP Mobility Client protocol.

Figure 5.1 shows a general SeQoMo signaling procedure.

The results of the procedure include:

- Connectivity is (re-)established;
- QoS path is set up;

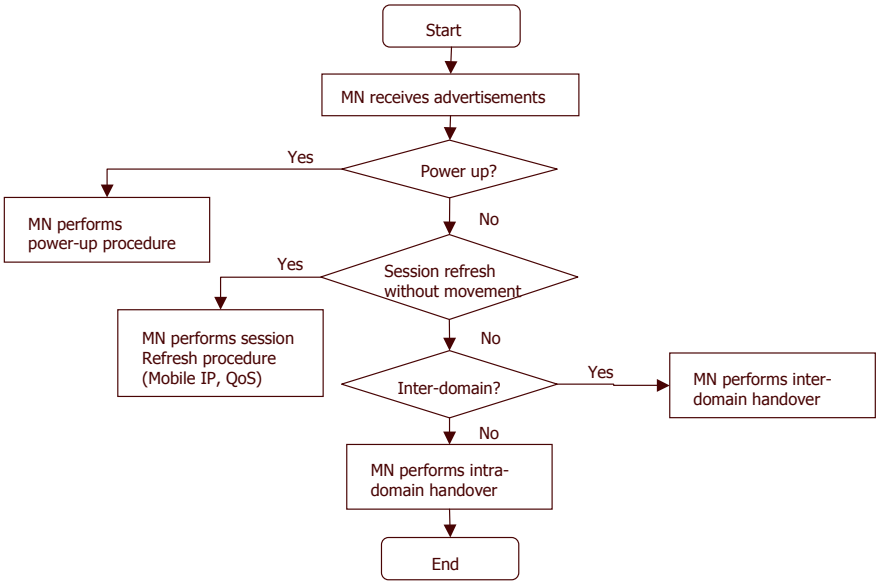


Figure 5.1: A general SeQoMo signaling procedure

- Security association are set up.

In the following sections, we describe the detailed procedures in the four cases.

5.1 Signaling Procedures

5.1.1 Signaling Procedures: Power Up Case

As shown in Figure 5.2, the procedure is detailed in Table 5.1.

5.1.2 Signaling Procedures: Inter-Domain HO

As shown in Figure 5.3, the procedure is detailed in Table 5.2.

5.1.3 Signaling Procedures: Intra-Domain HO

As shown in Figure 5.4, the procedure is detailed in Table 5.3.

5.1.4 Signaling Procedures: Session Refreshment

The session refreshment results from the following events:

Steps	Function	Remarks	Data Format
1	Enhanced advertisement	prefix information, aggregate available bw, price information and the address of the first CASP node	Figure A.13
1’	Handover decision	handover decision based on aabw and current state (lazy and eager); generate CoAs; fetch the address of the first CASP node; make decision to proceed a inter-/intra domain HO.	Not applicable
2	CASP Request	end-to-end communication	A.1
3	CASP Request	AR generates a CASP Request message and sends it to MAP1	A.1
4	Binding update	register MN’s LCoA and its home address	Not applicable
5	ARR	MAP1 acts as AAA client in Diameter protocol	Figure 4.4
6	ARR	AAAL forwards the ARR message to AAAH	Figure 4.4
7	HOR	AAAH generates a HOR message and sends it to HA	Figure 4.4
8	Binding update	register MN’s RCoA and its home address	Figure 4.4
9	HOA	HA generates a HOA and sends it to AAAH	Figure 4.4
10	ARA	AAAH generates a session key and includes it in a ARA message. It sends the message to AAAL.	Figure 4.4
11	ARA	AAAL caches the authentication and authorization information. It forwards ARA to MAP1.	Figure 4.4
12	CASP Answer	MAP caches the session key. It generates a CASP Answer message and sends it to AR.	A.1
13	Cookie generation	AR caches the session key. It generates a cookie, encrypts it with the session key.	Figure 4.12
14	CASP Answer	AR generates a new CASP Answer message including the encrypted cookie, and sends it to MN.	A.1
15	CASP Query	MN obtains the cookie thanks to the long term trust relationship with its home domain. From now on, it communicates with the access network with the protection of IPSec with the session key. It generates a CASP Query message including a QoS request.	A.1
16	CASP Query	AR generates a new CASP Query message and sends it to MAP1 assumed that there is no CASP node between AR and MAP1.	A.1
17	CASP Query	the CASP Query propagates until it reaches CN.	A.1
18	Binding update	register MN’s RCoA and its home address	Not applicable
19	CASP Reserve	CN generates a CASP Reserve message and sends it to its next CASP node in order to reserve resource for the session. The operations repeat until the CASP Reserve message reaches MAP1.	A.1
20	CASP Reserve	MAP1 generates the CASP Reserve message and sends it to AR.	A.1
21	CASP Reserve	AR generates the CASP Reserve message and sends it to MN.	A.1

Table 5.1: The signaling procedure in the power-up case

Steps	Function	Remarks	Data Format
1	Enhanced advertisement	prefix information, aggregate available bw, price information and the address of the first CASP node	Figure A.13
1’	Handover decision	handover decision based on aabw and current state (lazy and eager); generate CoAs; fetch the address of the first CASP node; make decision to proceed a inter-/intra domain HO.	Not applicable
2	CASP Request	end-to-end communication	A.1
3	CASP Request	AR generates a CASP Request message and sends it to MAP2	A.1
4	Binding update	register MN’s LCoA and its home address	Not applicable
5	ARR	MAP2 acts as AAA client in Diameter protocol	Figure 4.4
6	ARR	AAAL forwards the ARR message to AAAH	Figure 4.4
7	HOR	AAAH generates a HOR message and sends it to HA	Figure 4.4
8	Binding update	register MN’s RCoA and its home address	Figure 4.4
9	HOA	HA generates a HOA and sends it to AAAH	Figure 4.4
10	ARA	AAAH generates a session key and includes it in a ARA message. It sends the message to AAAL.	Figure 4.4
11	ARA	AAAL caches the authentication and authorization information. It forwards ARA to MAP2.	Figure 4.4
12	CASP Answer	MAP caches the session key. It generates a CASP Answer message and sends it to AR.	A.1
13	Cookie generation	AR caches the session key. It generates a cookie, encrypts it with the session key.	Figure 4.12
14	CASP Answer	AR generates a new CASP Answer message including the encrypted cookie, and sends it to MN.	A.1
15	CASP Query	same operations as Step 15 in Table 5.1	A.1
16	CASP Query	same operations as Step 15 in Table 5.1	A.1
17	CASP Query	the CASP Query propagates until it reaches the crossover router(CR) which is the joint point of the new and old paths.	A.1
18	CASP QoS signaling	CR generates a "CASP QoS signaling" message including the binding update information to CN. Any solution proposed by the CASP design group is applicable here.	Not applicable
19	Binding update	register MN’s RCoA and its home address	Not applicable
20	CASP QoS signaling	CN sends a BA to the CR. The solution proposed by CASP design team is applicable here.	A.1
21	CASP Reserve	CR generates a CASP Reserve message and sends it to its next CASP node in order to reserve resource for the session. The operations repeat until the CASP Reserve message reaches MAP2. Meanwhile, CR sends a CASP TEARDOWN message to release the old path via MAP1 to AR.	A.1
22	CASP Reserve	MAP2 generates the CASP Reserve message and sends it to AR.	A.1
23	CASP Reserve	AR generates the CASP Reserve message and sends it to MN.	A.1

Table 5.2: The signaling procedure in the inter-domain case

Steps	Function	Remarks	Data Format
1	Enhanced advertisement	prefix information, aggregate available bw, price information and the address of the first CASP node	Figure A.13
1’	Handover decision	handover decision based on aabw and current state (lazy and eager); generate CoAs; fetch the address of the first CASP node; make decision to proceed a inter-/intra domain HO.	Not applicable
2	CASP Query	message includes QoS, cookie, BU and authentication objects.	A.1
3	cookie verification and notification	AR verifies the cookie and notifies the use of the cookie. (see Section 4.2.2)	Not applicable
4	CASP Query	AR generates a CASP Query and sends it to MAP.	A.1
5	Binding update	register MN’s new LCoA and its home address	Not applicable
6	CASP Reserve	MAP sends a CASP Reserve to AR to reserve the resource. Meanwhile, it sends a CASP TEARDOWN to release the old path.	Figure 4.4
7	Temporary SA set up	AR sets up a temporary SA with MN by using the interim session key. (see Section 5.1.5)	Not applicable
8	CASP Reserve	AR sends a CASP Reserve to MN.	A.1
9	Data traffic	MN continue the communication with the access network with a SA by using the interim key. This SA is valid until a new session key comes into effect.	Not applicable
4’	ARR	In parallel with the QoS reservation process, AR perform the authorization process. (see Section 4.2.4)	Figure 4.4
5’	Re-authorization	AAAL performs the re-authorization check, probably with the help of AAAH. It updates the authorization data if necessary. (see Section 4.2.4)	Not applicable
6’	ARA	AAAL sends a ARA message to AR.	Figure 4.4
7’	authorization result arrives	authenticate the request; update the session key; generate a new cookie.	Not applicable
8’	REFRESH REQ	If both the re-authorization and re-authentication checks pass, AR sends a REFRESH REQ message, updating the session key and granting the new cookie which is encrypted with the new session key; otherwise, the network can not grant any resource to the MN. In such a case, AR sends a REFRESH REQ message carrying a negative Registration answer and the new cookie which is encrypted with the interim session key.	A.1
9’	REFRESH REPLY	when receiving the REFRESH REQ message with a positive answer, MN acknowledges to use the new session key for a new SA by sending a REFRESH REPLY message. When AR receives the message, the new session key comes into effect; When the REFRESH REQ contains a negative answer, it does not send the REFRESH REPLY message.	A.1

Table 5.3: The signaling procedure in the intra-domain case

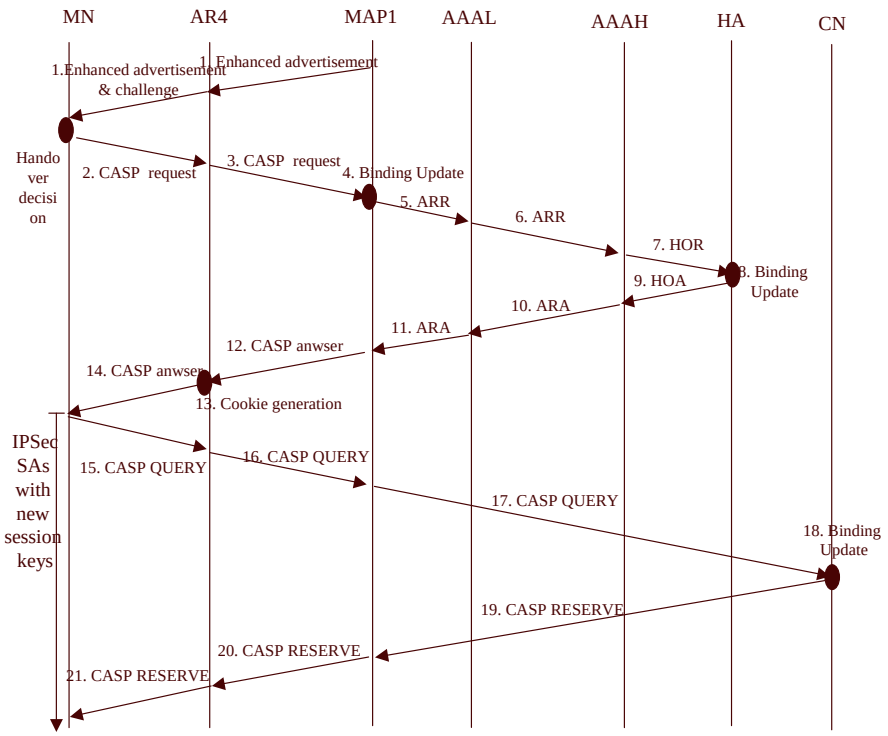


Figure 5.2: The signaling procedure in the power-up case

- Mobile IP registration times out;
- QoS state needs to be refreshed. It occurs when QoS state times out or MN updates its QoS request according to the dynamic network status;
- Session key times out;
- Cookie times out;
- IPSec sequence number turns around, In this case, a new SA needs to be set up.

The Mobile IP and QoS refreshment is signaled with BU + CASP Query message. The security refreshment is network initiated since the network has to hand out new keys, cookies so on as forth. It needs a reply to acknowledge that all these parameters have been correctly received. All the necessary information is contained in mobile client objects (see details in Chapter 6).

The message exchanges in intra-domain handover with respect of cryptography will be discussed in the subsection 5.1.5.

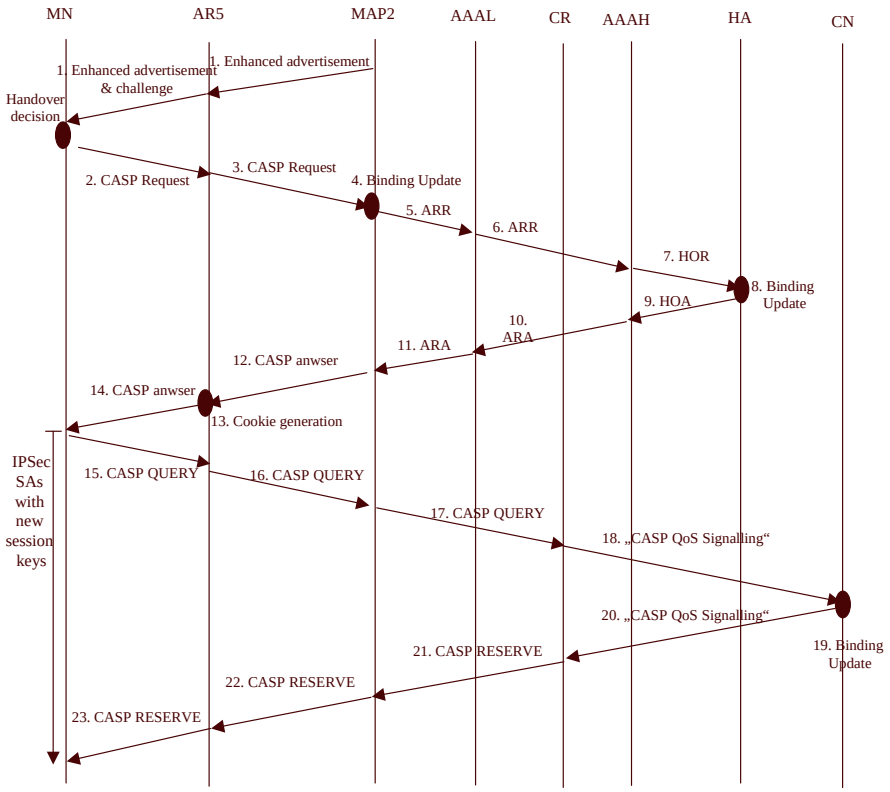


Figure 5.3: The signaling procedure in the inter-domain handover case

5.1.5 Crypto Aspects of Intra-Domain HO

The communication between mobile nodes and access routers in an IP based mobility supporting network can be protected by IPSec security associations. During a handover the exchange of user and signaling data over the wireless connection is insecure. This is due to the fact that the old security associations can not be reused at the new access router and that the setup of a new one requires some data exchanges between the mobile node, new access router and an Authentication, Authorization and Accounting (AAA) entity. Only afterwards a new association can be established. The interruption of the secure connection offers malicious entities the opportunity to launch various attacks. An attacker can e.g. start Denial of Service (DoS) attacks, eavesdrop information or gain illegitimate service from the access network. In order to defend against this kind of attacks, this section provides a mechanism to establish a temporary security association between the mobile node and the new access router which allows the protected exchange of user data immediately after a handover and simultaneously protects other signaling information without involving the time consuming information exchanges with the AAA entities. The communication with the AAA entity happens in parallel and after finishing the communication the temporary security association is replaced. In our previous work on mobility support with IP protocols, a cookie based mechanism was proposed to protect the access network against DoS attacks by performing a preliminary check of the data [1]. A cookie is also used to

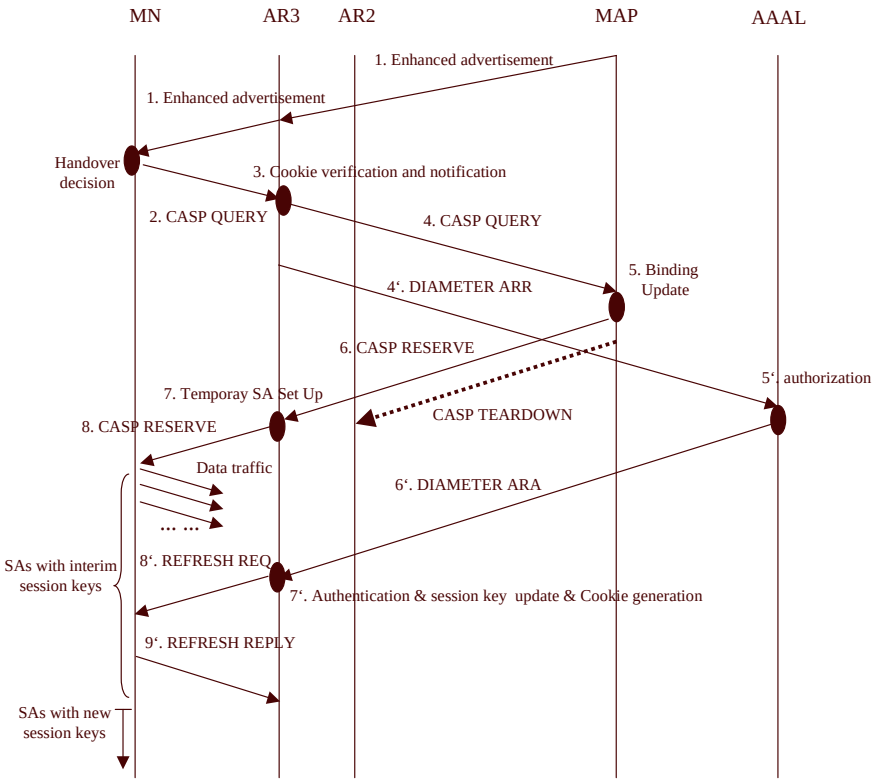


Figure 5.4: The signaling procedure in the intra-domain handover case

protect the message exchanges for the setup of the temporary security association, to protect not only the data exchange but also the involved infrastructure and to reduce the possible points of attack. The scheme is especially suitable for local mobility, where the signaling overhead is reduced and fast messages exchanges with low latency and short interruptions are required. This scheme applies particularly in the intra-domain handover cases where it is efficient to reduce handover latency by combining mobility, QoS and security signaling and perform it in parallel.

Problem Statement

When an MN moves from one access router (old AR) to another AR (new AR) in the access network (namely intra-domain handover), it wants to keep access to the network without interruption, neither for mobility support, QoS provisioning nor security.

The scheme addresses several problems. The aim is to protect the data exchange between MN and new AR in the time slice from the first answer of an AR to the initial registration message from a MN up to replacement of the temporary SA by a definite one after the answer from an AAA entity. By transmitting all relevant information, a temporary security association will be established with a minimum of latency and required message exchanges in this time interval. Afterwards, all data can

be transmitted via this association.

The exchange of the signaling messages for the SA setup needs additional protection. Different values are included in the messages to guarantee confidentiality and data integrity.

The access network is very vulnerable to DoS attacks. In order to avoid them, a cookie is included in the initial registration request by a mobile node. The access router is able to perform a preliminary authentication check of the mobile node based on the cookie without having to communicate with an AAA entity.

The exchange of the messages is combined with the signaling data for QoS reservation and actions which have to be executed for the mobility management, e.g. renew the registration information at the responsible entity, e.g. mobility anchor point (HMIPv6). This is required to reduce the handover latency and to make IP based mobility supporting networks even suited for real time sensitive applications.

The State of the Art Analysis

Up to now, there is no solution which explicitly addresses the security of data exchanges during a handover. A combination of general mobility management and security signaling data which can provide nearly seamless handovers does not exist. Currently both have been dealt with separately in different scenarios with different techniques.

Several efforts have been made to secure the connection of a mobile node to the access network after a handover. MIP+diameter destruction derby? One possible solution might be to transfer the information about existing security associations from the old access router to the new one. This is referred as context transfer [42]. In this case, an existing security association can be reused after the handover. This process has some disadvantages. It assumes that the old access router knows the new one in order to transfer the relevant information to it. To determine the new AR is a non-trivial task which assumes the availability of e.g. special data link layer mechanisms. Additionally, the other signaling message exchanges, e.g. for mobility management, which are part of the proposed procedure have to be performed supplementary.

Mechanism Description

Figure 5.5 shows the message exchanges of the mechanism.

1. During the prior registration procedure with the old access router all relevant information is exchanged to establish an SA with key

   $$K_{MN,ARi}$$

   between the MN and the (old) access router ARi. Under protection of the key

   $$K_{MN,AN}$$

   the mobile node is also communicated an encrypted version of the temporary session key

   $$TK_{MN,ARi+1}$$

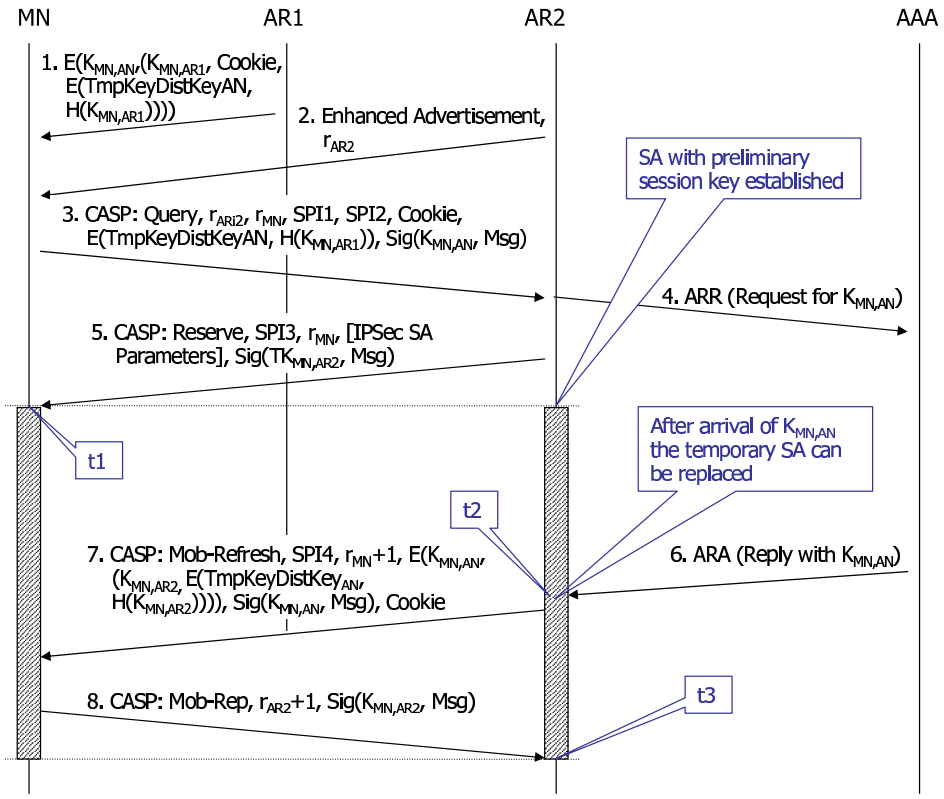


Figure 5.5: Message exchanges of the crypto aspects of the intra-domain handover cases

for later communication with the new access router ARi+1 (The details of how the keys are transmitted to the MN are out of the scope of the patent). The encryption of this key is performed with the key

$$TmpKeyDistKey_{AN}$$

that is known to all access routers in the access network, but not to the mobile nodes. For reasons explained below, we choose the new temporary session key

$$TK_{MN,ARi+1}$$

to be equal to

$$H(K_{MN,ARi}),$$

with H(X) denoting the computation of a one-way hash function over value X, so that all in all this part of the message can be written as

$$E(TmpKeyDistKey_{AN}, H(K_{MN,ARi})),$$

with E(K, X) denoting encryption of X with key K. Additionally, a cookie is included in the message. It serves as the preliminary authentication check when a request is send to a new access router.

2. Later on, when the MN moves, it will receive enhanced advertisements from new access routers. These advertisements contain the information, which enables the MN to make a handover decision if necessary. See Chapter 4.2.3 for details. Additionally, the advertisements contain a random number

   $$r_{ARi+1},$$

   which is used as the challenge in a challenge response mechanism to check the validity and currentness of the following response of the MN.

3. When performing a handover to the new access router ARi+1, the mobile node sends a CASP Query message together with the random number

   $$r_{ARi+1}$$

   provided by the new access router in his advertisement, an own random number

   $$r_{MN}$$

   and the encrypted temporary session key

   $$E(TmpKeyDistKey_{AN}, H(K_{MN,ARi}))$$

   to the new access router. The cookie from step 1 is used for the preliminary authentication of the message. Afterwards, the new access router decrypts the temporary session key with the key

   $$TmpKeyDistKey_{AN}$$

   known to it and can then locally set up the temporary security association that will use the key

   $$TK_{MN,ARi+1} = H(K_{MN,ARi}).$$

   Additionally, information is included in the message on how the temporary IPSec security association (SPI1) and the definite one (SPI2) should be called in direction to the mobile node. The message is signed with a hash value computed over the message and the key

   $$K_{MN,AN}.$$

4. Furthermore the new access router communicates after the mobile node's handover request with the appropriate entities in the access network, that is the MAP for mobility and QoS handling and the local AAA server for checking the authenticity of the request. The request for this is sent via an Diameter ARR message and contains the signature of the mobile node with the key

   $$K_{MN,AN}.$$

5. As soon as the mobility and QoS setup has been finished, the new access router answers to the mobile node with a CASP Reserve message containing the mobile nodes random number

   $$r_{MN}$$

and additional information on how the temporary security association should be called in direction to the access router (SPI3) as well as other potentially required parameters. This message is signed with a hash value computed over the message and the temporary session key

$$TK_{MN,ARi+1}.$$

After the mobile node has checked the hash value and the random number

$$r_{MN},$$

it can locally setup the security association and start secure data exchange with the new access router.

6. Upon successful verification of the authenticity of the MN's request the answer (Diameter ARA message) from the local AAA server will arrive at the new access router with the key

$$K_{MN,AN}.$$

7. Upon reception of this message the new access router randomly selects a new definite session key

$$K_{MN,ARi+1}$$

and the new encrypted key for the next temporary SA

$$E(TmpKeyDistKey_{AN}, H(K_{MN,ARi+1}))$$

and encrypts both with the key

$$K_{MN,AN}.$$

Then it selects a new local identifier for the new definite SA and transmits this information together with the encrypted session key, the value

$$r_{MN} + 1$$

and a hash value over the whole message and the key

$$K_{MN,AN}$$

with a CASP Mob-Refresh message to the mobile node. Also, a cookie is included for a registration procedure with a new AR.

8. After the MN has received this message it checks the contained hash value and random number, decrypts the new definitive session key and sets up the new definitive SA. A CASP Mob-Reply is send to the ARi+1 as acknowledgement. Afterwards communication between the MN and the new AR is secured with the new definitive SA.

Chapter 6

CASP Mobility Client Protocol

In high mobility scenarios, frequent handovers may result in a significant degradation of QoS provisioning if the access network is unable to provide enhanced solutions for prompt QoS re- establishments. Most of the current approaches for signaling protocols consider only the actions which have to be taken after a handover occurs. Some newly proposed protocols use various ideas to speed up the re-establishment of the reservation paths and handle the specific mobility related events, e.g. changes of the IP address of a mobile node. However, none of the protocols introduces mechanisms for the preparation of a handover.

In CASP, signaling and discovery message delivery are separated. The Scout protocol is used to discover the next suitable CASP node and the required soft-state refresh interval if the next CASP node is more than one network-layer hop away. It is only needed in case that no other suitable means of discovering the next CASP node are available. In environments with high mobility, however, the discovery process with scout will increase a considerable overall handover latency.

To address the issue identified in 4.1.5, we describe our design of CASP Mobility Client protocol [33], which enables seamless QoS provisioning support for mobile nodes.

6.1 Overview of the General Architecture of CASP

The modular CASP framework includes a general purpose messaging layer (M-layer) and a number of client layers for various signaling applications.

An M-layer session state consists of a session identifier, a flow identifier, a previous and next CASP hop, a refresh interval and a branch identifier. The session identifier is independent from the IP address of the sender and is therefore suited to identify the message flow from a mobile node even after a change of the care-of address due to a handover. The support by the CASP hops for different client layers is optional. An intermediate node is not required to support the client layers.

The CASP messaging layer belongs to the NTLP (NSIS Transport Layer Protocol), in combination with a standard transport protocol like TCP or UDP. The different CASP clients are allocated to the NSLP (NSIS Signaling Layer Protocol).

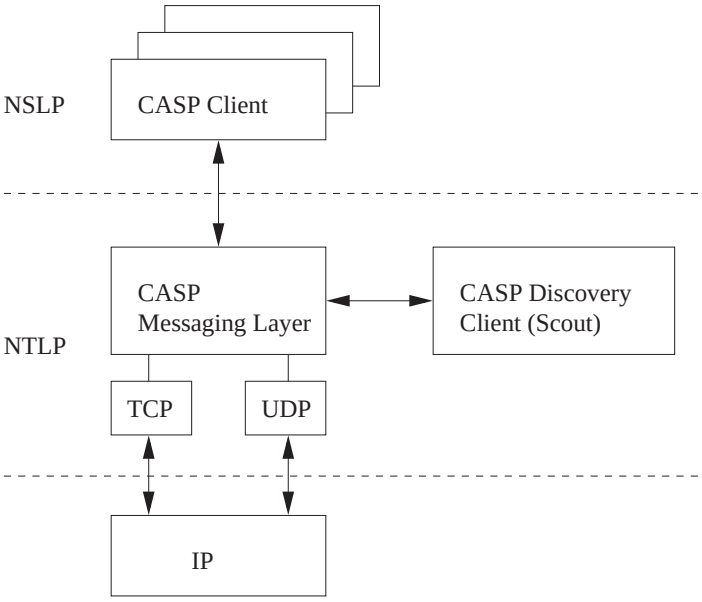


Figure 6.1: The CASP framework

Each CASP message has one basic format. It consists of a common header, a Flow ID and optionally the following fields: Length Header, CASP Timeout, a Scout Cookie R and the client data error code.

The length header must only be present, if the deployed transport protocol is stream-based.

The common header consists of 4 flags for reverse routing, tear-down of all CASP M-layer states, discovery if a new next-hop may be required and an insecure flag, which indicates that a hop without channel security has been traversed [1]. Furthermore it contains a TTL, Hop count, Type and the session identifier field. The Type field distinguishes between CASP messages and Scout messages.

To treat a message flow according to particular rules, the Flow ID is used. It allows policy based forwarding and NAT and contains typically the IP addresses of the senders and receivers and some demultiplexing information.

6.2 Operations

The operations of CASP Mobility Client Protocol are illustrated in cases of power-up, inter-domain handover and intra-domain handover (see Chapter 5).

The CASP Mobility Client PDU structure is shown in Figure A.2. It is designed based on the general format of a CASP message as shown in Figure A.1.

Table 6.1 shows the message types of the Mobility Client messages.

The message formats of objects of refreshment, security content, SA parameter, IPSEC SPI, binding

[1] The applicability and benefit of this flag need to be investigated if it has the same use as the bit which is proposed in [3]

Table 6.1: Mobility Client Message Types

Value	Message Type	Flow Identifier
1	QoS Reserve	From message flow
2	QoS Commit	From message flow
3	QoS Release	From message flow
4	QoS Success	From message flow
5	QoS Error	From message flow
6	QoS Query	From message flow
10	Refresh Request	0
11	Refresh Reply	0

update, bandwidth and cookie are shown in Appendix A.

6.3 Comparison of the CASP Mobility Client with CASP QoS Client

A general message exchange of CASP QoS Client protocol is shown in Figure 6.2; The message exchange of CASP Mobility Client protocol is shown in Chapter 5.

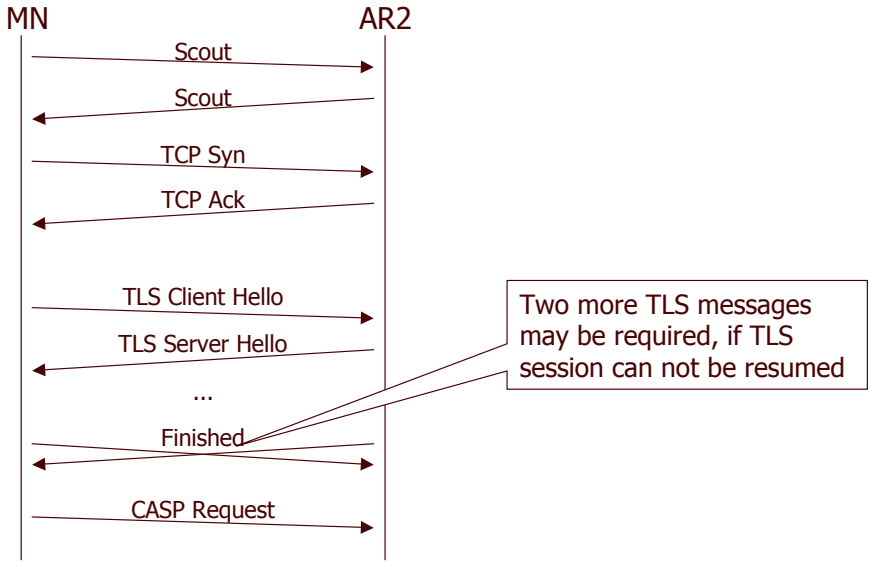


Figure 6.2: The general message exchange of the CASP QoS Client protocol

The general message exchange of the CASP QoS Client protocol proceeds as follows:

- a CASP node detects its next CASP node by using the scout protocol;
- two CASP nodes establish a TCP connection;
- Two nodes set up a TLS connection with 4-6 message exchanges.

Therefore, it requires 8 or 10 message exchanges before CASP request can be sent. Moreover, it does not allow to make handover decision dependent on the QoS information; it does not address the threat of DoS attacks.

In contrast, the proposed CASP Mobility protocol makes the message exchanges especially in intra-domain handovers much more easier. As shown in Figures 5.4 and 5.5, after receiving the enhanced advertisement, which contains all the information for MN to make a handover decision, MN requires only two message exchanges to locate the next CASP node and set up a security association.

Obviously, the CASP Mobility Client protocol is much more beneficial in secure and optimized handover scenarios.

Chapter 7

Conclusions

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

During the last 3.5 year the SeQoMo project investigated the suitability of IP based networks for mobility support under the perspective of security and QoS provisioning.

At the beginning of the project it could only be estimated that the Internet protocol would be the network layer protocol of the future for those scenarios. During the period of the project the technical development clarified that this project was heading in the right direction and in some parts it was one of the most notable leaders of the research and investigation.

Starting with the investigation of solutions and the improvements of existing schemes the SeQoMo generated own solutions for the specific problems which come along with the extraordinary requirements of the given scenario. In the early days of the project we realized that the aim of nearly seamless mobility support could only be achieved with an integrated solution for all the occurring problems and not by a simple combination of single solutions for the three SeQoMo parts.

In summary, the specific developed concepts and mechanisms are listed as follows:

- making handover decision based on availability of resources;
- protecting the access network against DoS attacks;
- signaling security and protection on wireless links;
- Protections of signaling and data traffic in a separate manner;
- Optimizing re-registration procedure in local movements by parallelizing resource reservation process and re-authorization process;
- practical authorization processes in the HMIPv6 architecture.

They are integrated in handover procedures of the cases of power-up, inter-domain HO, intra-domain HO and session refreshment as shown in Chapter 5 5.

Especially, the emphasis and the main achievement of the SeQoMo project lie in the optimization of the intra-domain HO in micro-mobility scenarios. All the measures of combining the signalings of the mobility, QoS re-establishment processes, parallelizing the QoS-aware re-authorization process with the QoS re-establishment process, performing a preliminary check with a cookie, enhancing the advertisements with QoS information and securing user and signaling data with a temporary session key aim at optimizing the intra-domain handover procedure.

At the end of the project, the result of the SeQoMo is an overall solution which is deployable in a real access network.

The principal achievements (Detailed list refers to B) consist of

- integrated signaling procedure with built-in security mechanisms for confidentiality, integrity and DoS protection;
- Prototypical implementation in experimental testbed; (see details in [12])
- 2 patent applications, 6 Internet drafts and 12 conference papers. (see Appendix: publication list)

Appendix A

Packet Formats

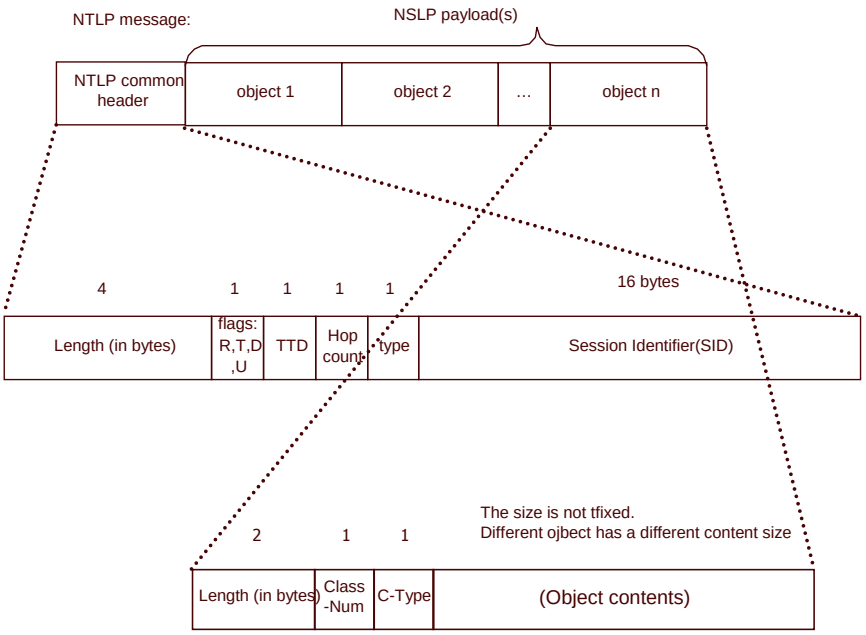


Figure A.1: General CASP Message Format

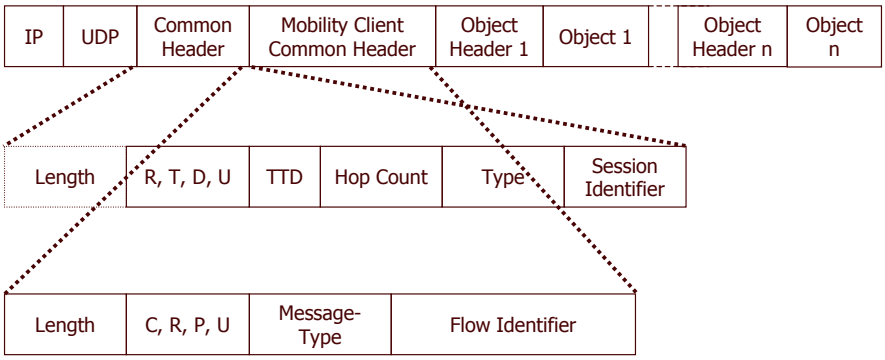
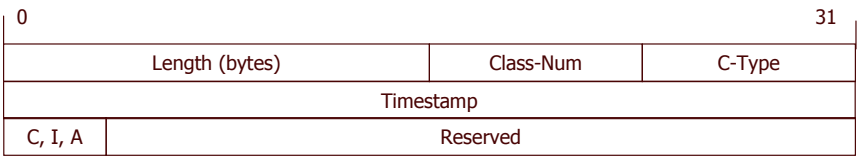
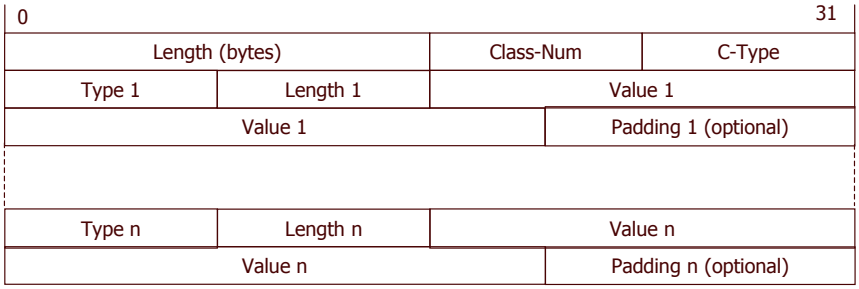


Figure A.2: CASP Mobility Client PDU Structure



C: New Cookie (Cookie Object will be included in the message)
I: IPSec SA (+ IPSec SPI Objects)
A: AAA Key (+ Security Content Object)

Figure A.3: CASP Mobility Refreshement Object



- Carries hash values, signatures and random numbers

Figure A.4: CASP Mobility Security Content Object

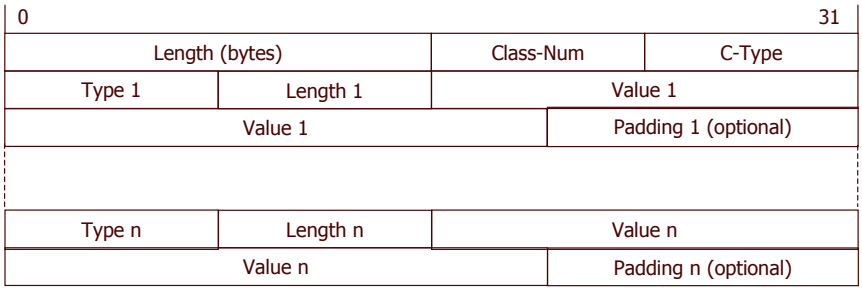


Figure A.5: CASP Mobility SA Parameter Object

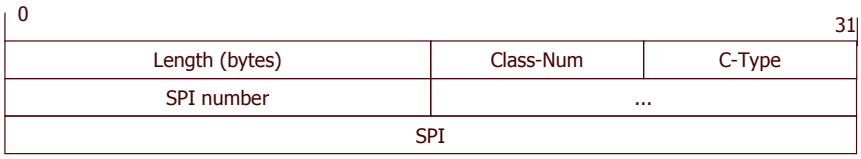


Figure A.6: CASP Mobility IPSEC SPI Object

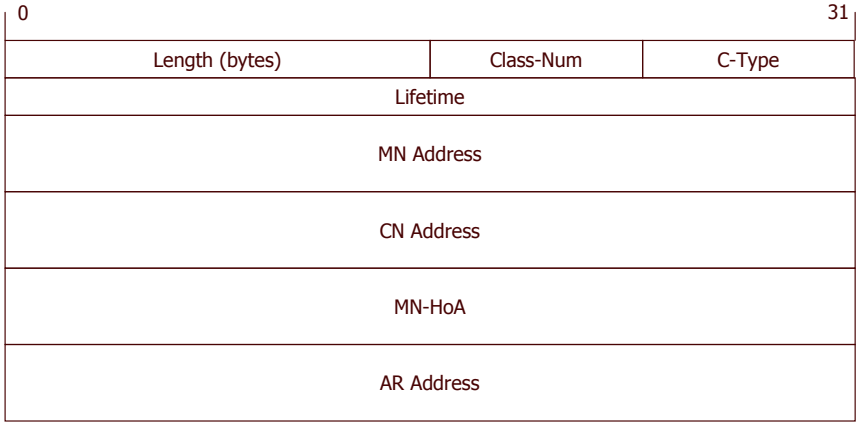


Figure A.7: CASP Mobility Binding Update Object

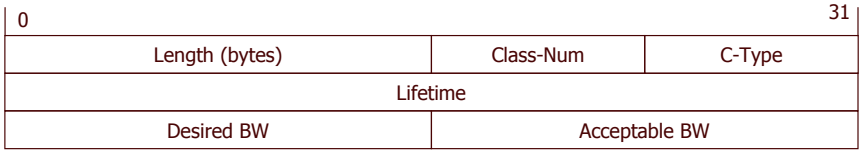


Figure A.8: CASP Mobility Bandwidth Object

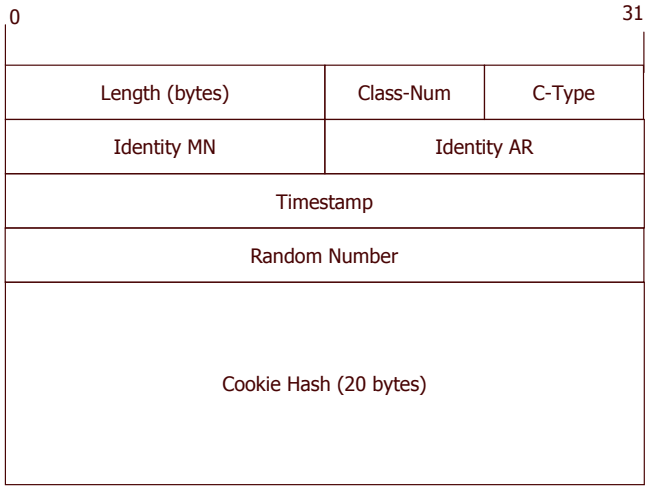


Figure A.9: CASP Mobility Cookie Object

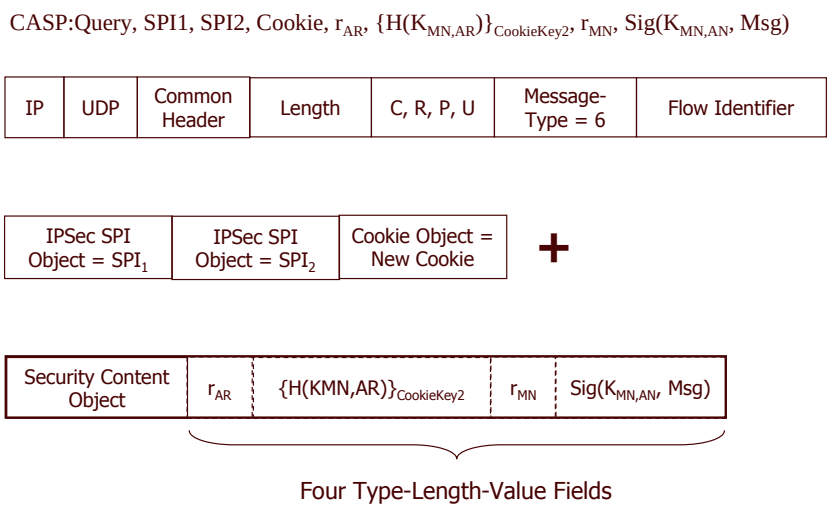


Figure A.10: The first message from the crypto HO message exchange

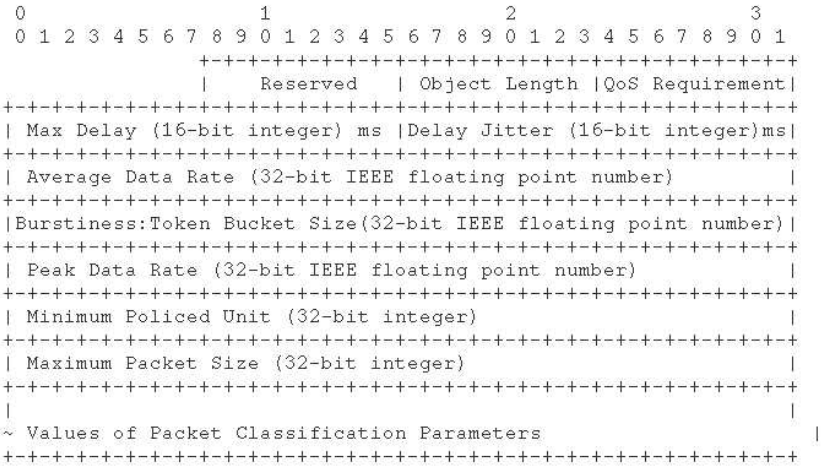


Figure A.11: Composition of a QoS OBJECT

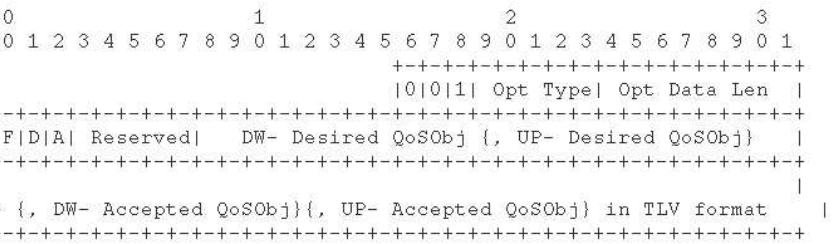
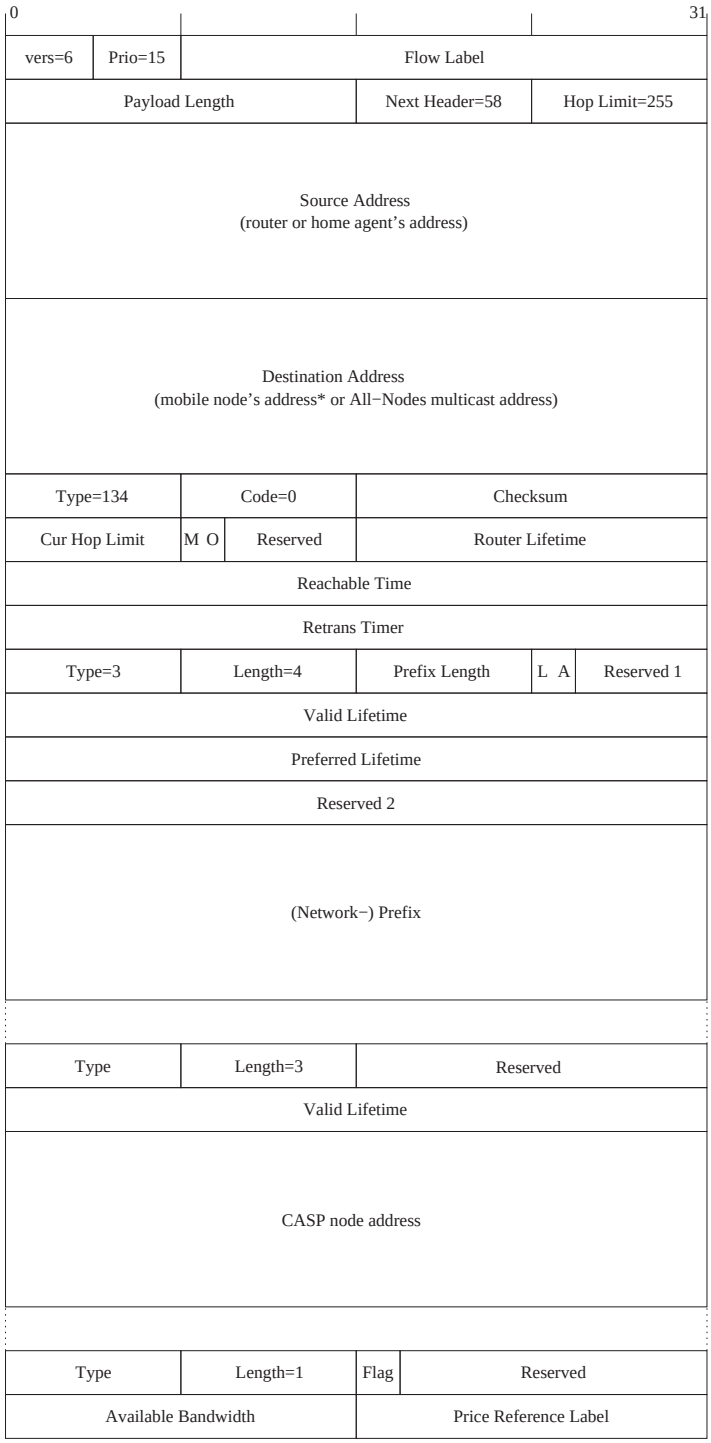


Figure A.12: Composition of a QoS OPTION



* The mobile node's address is used as the destination address only when the advertisement corresponds to the mobile node's solicitation message.

Figure A.13: Message format of an enhanced advertisement

Appendix B

Achievements

B.1 Project Deliverables

About 50 intermediate project reports are delivered during the project for internal use.

- T. Chen, S. Hermann, and G. Schaefer, "Final Architecture Description", D-Arch-3, September, 2003.
- T. Chen, S. Hermann, and G. Schaefer, "Update on Architecture with respect to CASP", D-Arch-2, May, 2003.
- T. Chen, A. Festag, A. Neumann, S. Hermann, H. Karl, G. Schaefer, "Retionale, Design and Functionality for Secure, QoS-enabled Mobility Support in All-IP Network - the SeQoMo Approach", D-Arch-1, March, 2003.
- T. Chen, S. Hermann, and G. Schaefer, "Report on CASP Mobility Client Protocol Implementation Design and First Prototype Functionality", D-Prot-1, June, 2003.
- T. Chen, S. Hermann, and G. Schaefer, "CASP Mobility Client Protocol sepcification", D-CASP-Mob, March, 2003.
- T. Chen, S. Hermann, and G. Schaefer, "Demonstrator of the SeQoMo Architecture prior to CASP Integration", D-Demo, March, 2003.
- T. Chen, A. Neumann, A. Festag, G. Schaefer, "Secure, QoS-enabled Mobility Support for IP-based Networks", D-Security-4, December, 2002
- T. Chen and G. Schaefer, "QoS-aware Authorization In Mobile IP Networks - Intermediate Implementation Report", D-Security-3, September, 2002
- T. Chen and G. Schaefer, "Design of QoS-aware Authorization for Mobile Devices", D-Security-2, May, 2002
- T. Chen and G. Schaefer, "QoS-aware Authorization for Mobile Devices", D-Security-1, March, 2002

- A. Festag, "Optimization of Handover Performance by Link-layer Triggers in IP-based Networks; Parameters, Protocol Extensions, and APIs for Implementation", D-LL-1, July, 2002
- G. Schaefer, "Paper on Improved Authentiation Protocol that Separates the Two Tasks of Session Key Distribution and Timeliness Check of the Mobile Node's Response", D-Auth-3, September, 2001
- A. Hess and G. Schaefer, "Performance Evaluation of AAA / Mobile IP Authentication", D-Auth-2, July, 2001
- G. Schaefer, H. Karl, and A. Festag, "Current Approaches to Authentication in Wireless and Mobile Communications Networks", D-Auth-1, February, 2001
- A. Festag, "Current Development and Trends in Handover Design for All-IP Wireless Networks", D-MM-1, Auguest, 2000
- A. Festag, "Update on Current Development and Trends in Handover Design for All-IP Wireless Networks", D-MM-1, March, 2002
- A. Festag, "Uitilization of Multicast for Support of Host Mobility in IP-based cellular Networks", D-MM-2, January, 2002
- A. Festag, "Performance Evaluation of MIP w and w/o Hierarchical FAs: Goal, Metrics, Parameters and Testbed Setup", D-MM-3, February, 2002
- A. Festag, "Report on Measurements of Mobile IP w/ and w/o Hierarchical Foreign Agents", D-MM-4, December, 2001
- A. Festag, "Investigation of Link Layer trigger in HMIPv4", D-MM-4-Update, July, 2002
- A. Festag, "Protocol Specification of MOMBASA Software Environment", D-MM-5, October, 2001
- A. Festag, "Report on Description and Specification of MEP Supporting Multicast (MMEP)", D-MM-5-Update, December, 2001
- A. Festag, "Implementation Design of MOMBASA Software Environment", D-MM-6a, November, 2001
- A. Festag, "Testing of MOMBASA Software Environment", D-MM-6b, December, 2001
- A. Festag, "Design, Implementation and Performance of Multicast-based Paging for IP Mobility", D-MM-7, December, 2001
- A. Festag, "Performance Evaluation of Multicast-based Handover: Goal, Metrics, Parameters and Testbed Setup", D-MM-8, February, 2002
- A. Festag, "Performance Evaluation of an Approach for Multicast-based Handover", D-MM-9, February, 2002
- A. Festag, "Performance Comparison of HMIPv4 and MOMBASA", D-MM-10, March, 2002

- A. Festag, "Simulative Study of Multicast-enhanced MIP and HMIP", D-MM-11, July, 2002
- X. Fu, "QoS-Support in Mobile Networks: Some Thougts and Future Steps", D-QoS-1, January, 2001
- X. Fu, "QoS Signaling and Mobility Support for Differentiated Service Networks: An Overview", D-QoS-2, March, 2001
- X. Fu, "An Analysis of Two Approaches for QoS Support in All-IP Mobile Networks", D-QoS-3, April, 2001
- A. Festag, X. Fu, H. Karl, G. Schaefer, "Technical Report on QoS-Conditionalized Binding Update in Mobile IPv6", D-QoS-4, July, 2001
- X. Fu, "Description of the Objectives of the Design of a Proof-of-concept Realization of the Proposal: QoS Metric and Measurement", D-QoS-5, July, 2001
- X. Fu, "Description of Feasibility of the Design - Environment and Principle Ideas", D-QoS-6, June, 2001
- X. Fu, "Preliminary Report on Some Results of Measurements of the Implementation Based on D-QoS-5",D-QoS-7, August, 2001
- X. Fu, "Evaluation of the Proposed Approach: Possible Modifications for D-QoS-4 and Possible Directions for Policy-based QoS Control",D-QoS-8, September, 2001
- X. Fu, "Design of the Prototype Implementation of QoS-conditionalized BU in MIPv6",D-QoS-9, October, 2001
- X. Fu, "HMIPv6 Testbed Setup",D-QoS-10, December, 2001
- A. Festag, X. Fu, H. Karl, G. Schaefer, C. Fan, C. Kappler, and M. Schramm, "QoS-Conditionalized Binding Update in Mobile IPv6", D-QoS-11, January, 2002
- X. Fu, "Status Report for the Prototype Implementation of QoS-conditionalized BU in Mobile IP",D-QoS-12, March, 2002
- X. Fu, "Revised I-D on NSIS Framework",D-QoS-13, June, 2002
- X. Fu, "Analysis on RSVP Regarding Multicast",D-QoS-14, June, 2002
- A. Neumann and X. Fu, "Report on QoS-Conditionalized BU Prototype Implementation",D-QoS-15, August, 2002
- A. Neumann and X. Fu, "Final Report on Prototype Implementation and Documentation",D-QoS-16, September, 2002
- X. Fu, "Assumptions on Architecture and Parameters in the Project "Mobility in Multi-Domain, Multi-Technology, IP-based Networks", D-Comm-1, February, 2001
- T. Chen, X. Fu, H. Karl, G. Schaefer, A. Festag, "An Introduction to the SeQoMo Architecture and its Conceptual Framework", D-Comm-2, December, 2001

- X. Fu, T. Chen, A. Festag, G. Schäfer, and H. Karl, "SeQoMo Architecture: Interactions of Security, QoS and Mobility Components", D-Comm-3, April, 2002
- A. Festag, X. Fu, H. Karl, G. Schaefer, C. Fan, C. Kappler, and M. Schramm, "Revised I-D on QoS-Conditionalized Binding Update in Mobile IPv6", D-QoS-11, July, 2002

B.2 Invention Reports

Three invention reports have been written. Two of them have lead to patent applications. The third one is still under Siemens internal evaluation.

B.3 Internet Drafts

- A. Festag, X. Fu, H. Karl, G. Schäfer, C. Fan, C. Kappler, M. Schramm, "QoS-Conditionalized Binding Update in Mobile IPv6", Internet Draft: draft-tkn-monileip-qosbinding-v6-00.txt
- M. Brunner, "Requirements for Signaling Protocols", Internet Draft: draft-ietf-nsis-req-09.txt
- X. Fu, C. Kappler, and H. Tschofenig, "Analysis on RSVP Regarding Multicast", Internet Draft: draft-fu-rsvp-multicast-analysis-00.txt
- H. Schulzrinne, H. Tschofenig, X. Fu, and A. McDonald, "CASP - Cross-Application Signaling Protocol", Internet Draft: draft-schulzrinne-nsis-casp-00.txt
- H. Schulzrinne, H. Tschofenig, X. Fu, and J. Eisl, "A Quality-of-Service Resource Allocation Client for CASP", Internet Draft: draft-schulzrinne-nsis-casp-qos-00.txt
- S. Hermann and T. Chen and G. Schaefer and C. Fan, "QoS Resource Allocation in Mobile Networks with CASP", Internet Draft: draft-hermann-casp-qos-mobility-00.txt

B.4 Conference Papers

[FCF+03] X. Fu, T. Chen, A. Festag, H. Karl, G. Schaefer and C. Fan, "Secure, QoS-Enabled Mobility Support for IP-based Networks" IP-based Cellular Networks, Paris, France, December 2003, To appear.

[NFK03] A. Neumann, X. Fu, and H. Karl, "Prototype Implementation and Performance Evaluation of a QoS-Conditionalized Handoff Scheme for Mobile IPv6 Networks", IEEE Computer Communications Workshop (CCW), Laguna Niguel, CA, October 2003, To appear.

[SK03] S. Sroka and H. Karl, "Performance Evaluation of a QoS-Aware Handover Mechanism", 8th IEEE Symp. on Computers and Communications, Kemer, Turkey, July 2003.

[FKW03] A. Festag, H.Karl, and A. Wolisz, "Classification and Evaluation of Multicast-Based Mobility Support in All-IP Cellular Networks", In Proc. Of Kommunikation in Verteilten Systemen (KiVS), pp. 233-244, Leipzig, Germany, February 2003.

[HS02] A. Hess and G. Schaefer, "Performance Evaluation of AAA / Mobile IP Authentication", 2nd Polish-German Teletraffic Symposium (PGTS'02), Gdansk, Poland, September 2002.

[FKT02] X. Fu, C. Kappler, and H. Tschofenig, "Analysis on RSVP regarding Multicast", 54th IETF Meeting, Yokohama, Japan, July 2002.

[FKK02] X. Fu, H. Karl, and C. Kappler, "QoS-Conditionalized Handoff for Mobile IPv6", 2nd IFIP-TC6 Networking Conf. (Networking2002), pp. 721-730, Pisa, Italy, May 2002 Springer-Verlag.

[FWW02] A. Festag, L. Westerhoff, and A. Wolisz, "The MOMBASA Software Environment – A Toolkit for Performance Evaluation of Multicast-Based Mobility Support", Performance Tools 2002, pp. 212-219, London, GB, April 2002.

[FW01] A. Festag and A. Wolisz, "Performance Evaluation of Mobile IP: Investigating the Concept of Hierarchical Foreign Agents", Mobility for All-IP Networks - Mobile IP (MAIN 2001), Berlin, Germany, April 2001.

[FW00] A. Festag and A. Wolisz, "MOMBASA: Mobility Support - A Multicast-based Approach", European Wireless 2000 together with ECRR 2000 (EW'2000), pp. 491-499, Dresden, Germany, September 2000.

[Fes00] A. Festag, "Mobility Support in IP-based Networks - A Multicast-Based Approach", Eighth Workshop of the HP OpenView University Association, Berlin, Germany, June 2000.

[FAW+00] A. Festag, T. Assimakopoulos, L. Westerhoff, A. Wolisz, "Rerouting for Handover in Mobile Networks with Connection-Oriented Backbones: An Experimental Testbed", IEEE Conf. on High Performance Switching and Routing (ICATM'2000), pp. 491-499, Heidelberg, Germany, June 2000.

Appendix C

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] Analysis of Existing Quality of Service Signaling Protocols, June 2003.

[2] T. Aura, P. Nikander, and J. Leiwo. DOS-Resistant Authentication with Client Puzzles. *Lecture Notes in Computer Science*, 2133:170, 2001.

[3] S. Bellovin. The Security Flag in the IPv4 Header, April 2003.

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

[5] J. Boyle, R. Cohen, D. Durham, and R. Rajan A. Sastry, January 2000.

[6] M. Brunner. Requirements for QoS Signaling Protocols, August 2003.

[7] P. Calhoun, T. Johansson, and C. Perkins. Diameter Mobile IPv4 Application, April 2003.

[8] P. R. Calhoun, H. Akhtar, J. Arkko, E. Guttman, A. C. Rubens, and G. Zorn. Diameter Base Protocol, December 2002.

[9] H. Chaskar. Requirements of a QoS Solution for Mobile IP. RFC 3583, September 2003.

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

[11] T. Chen, A. Festag, A. Neumann, S. Hermann, H. Karl, and G. Schaefer. Rationale, Design and Functionality for Secure, QoS-enabled Mobility Support in All-IP Networks - the SeQoMo Approach. D-Arch-1, March 2003.

[12] T. Chen, S. Hermann, and G. Schaefer. CASP Prototypical Implementation Software Report - Integration of SeQoMo and CASP Concepts , oct 2003.

[13] T. Chen, S. Hermann, and G. Schaefer. SeQoMo Architecture With Respect to CASP. D-Arch-2, May 2003.

[14] G. Chiruvolu, A. Agrwal, and M. Vandenhoute. Mobility and QoS support for IPv6 Based Real-time Wireless Internet Traffic. In *IEEE Int'l Conf. Commun.*, volume 1, pages 334–338, 1999.

[15] E. Dahlmann, M. Gudmundsson, M. Nilsson, and J. Skold. UMTS/IMT-2000 Based on Wideband CDMA. *IEEE Communications Magazin*, September 1998.

[16] S. Deering and R. Hinden. Internet Protocol, Version 6 (IPv6) Specification, December 1998.

[17] C. Perkins (ed.). IP Mobility Support for IPv4. RFC 3220, January 2002.

[18] H. Einsielder and et al. The Moby Dick Project: A Mobile Heterogeneous All-IP Architecture.

[19] 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.

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

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

[22] 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.

[23] A. Festag. *Mobility Support in IP Celluar Networks - A Multicast-Based Approach*. PhD thesis, TKN, TU-Berlin, Germany, 2003.

[24] 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.

[25] 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.

[26] D. Forsberg, J. T. Malinen, J. K. Malinen, and H. H. Kari. Increasing Communication Availability With Signal-Based Mobile Controlled Handovers. In *Proceedings of IP based Cellular Networks (IPCN2000)*, may 2000.

[27] D. Forsberg, J. T. Malinen, T. Weckstroem, and M. Tiusanen. Distributing Mobility Agents Hierarchically under Frequent Location Update. In *Proceedings of Sixth IEEE International Workshop on Mobile Multimedia Communications (MOMUC'99)*, 1999.

[28] 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.

[29] X. Fu, H. Schulzrinne, and H. Tschofenig. Mobility Support in NSIS, June 2003.

[30] J. Haartsen, M. Naghshineh, J. Inouye, O. Joeressen, and W. Allen. Bluetooth: Vision, Goals, and Architecture. *Mobile Computing and Communications Review*, 1998.

[31] L-N. Hamer, B. Gage, B. Kosinski, and H. Shieh. Session Authorization Policy Element, April 2003.

[32] D. Harkins and D. Carrel. The Internet Key Exchange (IKE), November 1998.

[33] S. Hermann, T. Chen, G. Schaefer, and C. Fan. QoS Resource Allocation in Mobile Networks with CASP, jun 2003.

[34] 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.

[35] T. Hiller. cdma2000 Wireless Data Requirements for AAA, June 2001.

[36] IEEE 802.11 (ISO/IEC 8802-11:1999). IEEE Standards for Information Technology, 1999.

[37] D. Johnson, C. Perkins, and J. Arkko. IP Mobility Support for IPv6. Internet-Draft: draft-ietf-mobileip-ipv6-24.txt, June 2003.

[38] S. Kent and R. Atkinson. IP Authentication Header, Novemeber 1998.

[39] S. Kent and R. Atkinson. IP Encapsulating Security Payload (ESP), Novemeber 1998.

[40] R. Koodli(ed.). Fast Handovers for Mobile IPv6. INTERNET DRAFT draft-ietf-mobileip-fast-mipv6-09.txt, September 2003.

[41] H. Krawczyk. SKEME: A Versatile Secure Key Exchange Mechanism for Internet. IEEE Proceedings of the 1996 Symposium on Network and Distributed Systems Security, 1996.

[42] J. Loughney, M. Nakhjiri, and C. Perkins. Context Transfer Protocol, June 2003.

[43] P. Maniatis, M. Roussopoulos, E. Swierk, M. Lai, G. Appenzeller, X. Zhao, and M. Baker. The Mobile People Architecture. *ACM Mobile Computing and Communications Review (MC2R)*, 1999.

[44] J. Manner, T. Suihko, M. Kojo, M. Liljeberg, and K. Raatikainen. Localized RSVP. Internet Draft, January 2003.

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

[46] H. Moeland and M. Trompower. Inter-Access Point Protocol Wireless Networking Distribution System Communication, March 1998.

[47] B. Moon and H. Aghvami. RSVP Extensions for Real-Time Services in Wireless Mobile Networks. *IEEE Communications Magazine*, pages 52–59, December 2001.

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

[49] T. Narten, E. Nordmark, and W. Simpson. Neighbor Discovery for IP Version 6 (IPv6), December 1998.

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

[51] A. Neumann, X. Fu, and H. Karl. Prototype Implementation and Performance Evaluation of a QoS-Conditionalized Handoff Scheme for Mobile IPv6 Networks. In *Proc. IEEE Computer Communications Workshop (CCW)*, Laguna Niguel, CA, October 2003.

[52] H. Orman. The OAKLEY Key Determination Protocol, November 1998.

[53] R. Ramjee and T. LaPorta. Paging Support for IP Mobility, July 2000.

[54] R. Ramjee, T. LaPorta, S. Thuel, and K. Varadhan. IP Micro-Mobility Support Using HAWAII, July 2000.

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

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

[57] C. Shen. Several Framework Issues Regarding NSIS and Mobility, January 2003.

[58] R. Singh, Y. C. Tay, W. T. Teo, and S. W. Yeow. RAT: A Quick (And Dirty?) Push for Mobility Support. In *Proceedings of the Second IEEE Workshop on Mobile Computing Systems and Applications*, february 1999.

[59] H. Soliman, C. Castelluccia, K. El-Malki, and L. Bellier. Hierarchical Mobile IPv6 mobility management (HMIPv6). Internet-Draft: draft-ietf-mobileip-hmipv6-07.txt, June 2003.

[60] P. Srisuresh and K. Egevang. Traditional IP Network Address Translator (Traditional NAT), January 2001.

[61] 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.

[62] A. Talukdar, B. Badrinath, and A. Acharya. MRSVP: A Resource Reservation Protocol for an Integrated Services Network with Mobile Hosts. *Wireless Networks*, 7(1):5–19, 2001.

[63] H. Tschofenig. NSIS Authentication, Authorization and Accounting Issues, March 2003.

[64] H. Tschofenig. RSVP Security Properties, June 2003.

[65] H. Tschofenig and D. Kroeselberg. NSIS Threats, June 2003.

[66] A. Valko. Cellular IP - A New Approach to Internet Host Mobility. *ACM Computer Communication Review*, 1999.

[67] J. Vollbrecht, P. Calhoun, S. farrell, L. Gommans, G. Gross, B. de Bruijn, C. de Laat, M. Holdrege, and D. Spence. AAA Authorization Application Examples, August 2000.

[68] H. J. Wang, B. Raman, C. Chuah, R. Biswas, R. Gummadi, B. Hohltand X. Hong, E. Kiciman, Z. Mao, J. S. Shih, L. Subramanian, B.Y. Zhao, A. D. Joseph, and R. Katz. ICEBERG: An Internet-Core Network Architecture for Integrated Communications. *IEEE Personal Communications*, 2000.

[69] E. Wedlund and H. Schulzrinne. Mobility Support Using SIP. In *Proceedings of Second ACM/IEEE International Conference on Wireless and Mobile Multimedia WoWMoM99*, August 1999.

[70] S. Zander. AAAC Design. Technical report, GMD Fokus, January 2002.

[71] L. Zhang, S. Berson, S. Herzog, and S. Jamin. Resource ReSerVation Protocol (RSVP) — Version 1 Functional Specification. RFC 2205, September 1997.

[72] X. Zhao, C. Castelluccia, and M. Baker. Flexible Network Support for Mobile Hosts. *MONET Special Issue on Management of Mobility in Distributed Systems*, 2001.