Technical University Berlin

Telecommunication Networks Group

SeQoMo Architecture: Interactions of Security, QoS and Mobility Components

X. Fu, T. Chen, A. Festag, G. Schäfer, H. Karl
[fu,chen,festag,schaefer,karl]@ee.tu-berlin.de

Berlin, April 2002

TKN Technical Report TKN-02-008

TKN Technical Reports Series

Editor: Prof. Dr.-Ing. Adam Wolisz

Abstract

This document describes the architectural framework of the SeQoMo (Secure, QoS-enabled Mobility support) architecture. After a review of the SeQoMo requirement, components and functionalities, protocol interactions of mobility, QoS and security components are described. Two use cases are presented to explain the typical behaviors of the overall system.

Contents

CONTENTS

Chapter 1

Introduction

With the advent of various radio access technologies and increasing deployment of sophisticated applications in mobile end systems, a set of technical challenges concerning mobile computing have been posed, among which the most important ones are: advanced mobility support, Quality of Service (QoS) and security issues.

The focus of the SeQoMo project is to investigate the suitability of IP-based networks for support of mobility under these perspectives. Integrating these three components into an overall secure, QoS-enabled mobility architecture (SeQoMo architecture [1]) based upon IP protocols is the ultimate goal of this project.

With respect to advanced mobility mechanisms, a conceptual overview of recent mobility approaches has been worked out, and hierarchical Mobile IP and multicast-based approaches have been selected as the most promising enhancements to standard Mobile IP. These approaches have so far been investigated with respect to their performance characteristics, especially during handover, taking into account the interdependence with higher layer protocols. To this end, a general software environment (MOMBASA) has been developed which allows to investigate a wide range of possible multicast-for-mobility approaches. A link layer trigger for mobility and QoS-enabled mobility will be identified and integrated in the SeQoMo architecture.

The objective of the Quality-of-Service part is to develop a mechanism that enables a mobile device to maintain an existing QoS assurance during handover. This mechanism lets a mobile device conditionalize its handover upon the availability of sufficient QoS resources along the new network path [4]. Hence, it is now possible to choose among several access points and to select the one access point which offers either a sufficient or the best QoS; this decision can be done by the mobile device if it so desires. This mechanism is designed for the case of hierarchical Mobile IPv6 (HMIPv6) [5] as underlying mobility mechanism. To demonstrate and evaluate this approach, a tested has been setup; a prototype has been designed; a proof-of-concept implementation for proposed QoS scheme together with an experimental hierarchical Mobile IPv6 implementation is ongoing. Link layer support for the QoS-conditionalized binding update (BU) scheme, i.e., how the link layer of the access router and the mobile node could make/release the requested QoS reservation, is expected to be investigated in the future stage.

In the context of security, the current phase of the project focuses on the aspect of authorization in order to work towards the integrated SeQoMo architecture in which mobile hosts will be verified that it's authorized to use the requested services in a visited network. Our work extends the Diameter for mobile IPv6 [3] to support QoS-enabled handover in hierarchical Mobile IPv6.

The rest of this document are organized as follows: after a review of the SeQoMo requirement, components and functionalities, protocol interactions of mobility, QoS and security components are described. Two use cases are then presented to explain the typical behaviors of the overall system.

Chapter 2

Requirements

The requirements of the three components are explained separately in the following sections.

2.1 Mobility

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

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

2.2 QoS

The requirements for QoS support for handover are as follows:

- Support for traffic flows to obtain QoS treatment as soon as the packet flow as such has been (re-) established after a handover;
- Minimal additional overhead (e.g., signaling traffic);
- Ability to inform higher layers in case of inability of QoS support in a path;
- Ability to choose an access point that is best suited from the QoS perspective.

2.3 Security

QoS-aware authorization service for Hierarchical Mobile IPv6 with QoS-conditionalized binding updates poses the following requirements [2]:

- A mapping is needed from the QoS information contained in authorization data to the QoS option which is carried in the binding update messages;
- There should be a means to learn and verify how much resources an MN is using in the visited domain so that the visited network can assure that the total resource utilization of the MN does not exceed what it is entitled to;
- To support efficient handovers, it's necessary that the authorization specific procedures add minimal latency to the registration and handover procedures;
- The visited network should prevent the Denial of Service (DoS) attack. That means if there is no check on whether the binding update sender is a registered and credible user before reserving the resources, attackers might repeat the QoS-conditionalized binding updates in a path to book out all available resources so that the path will run out of resources for any legitimate requests.

Chapter 3

Architecture Overview

The secure, QoS-enabled mobility (SeQoMo) architecture framework is a conceptual description of components (routers, access points, mobile nodes, etc.), and their behaviors (namely, communication protocols to be used among these components and interfaces among these components). The SeQoMo architecture allows enhanced mobility strategy (-ies) and plays a central role in QoS provisioning for mobile hosts; it also protects the communications for the QoS-enabled mobility. The following sections describe the SeQoMo components and their functionalities.

3.1 Mobility

The mobility support component is responsible for providing non-interrupted connectivity for mobile terminals by means of network-layer protocols. This component provides appropriate hooks to trigger the QoS support and security components upon (link layer detection of) movement. The results from the other two components are used to decide whether to do a handover.

In general, it is differentiated between global and local mobility support. Local refers to mobility support between access points belonging to the same access network, whereas global means mobility support between different access networks. The favored solution for mobility support is hierarchical Mobile IPv6. However, for local mobility other mobility solutions can be used as well. In particular, MOMBASA – a multicast-based approach – is considered.

3.2 QoS

The responsibility of the QoS support component in the SeQoMo architecture lies in carrying QoS information required by mobile terminals and ensures that QoS requirements can be met after a handover (if this is at all possible, depending on the network situation the mobile is faced with after moving around). In order to do so, the QoS component checks the resource availability in the QoS controllers (entities assumed to be responsible for resource reservation) along the path, influences handover decisions and security policies, and carried out by the mobility component's handover mechanisms. Here only the approach for QoS signaling in the all-IP mobile networks is considered; how the QoS controllers (QCs) interact with the internal resource reservation mechanisms (e.g., Integreted Services, Differentiated Services) deployed in the network elements is out of scope.

The QoS component in the MN initiates and completes the QoS-conditionalized binding update process. The registration request message also includes QoS and security information. If this process succeeds, the QoS component will initiate a tear-down process in the old path when necessary.

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

The QoS component in the Mobility Anchor Point (MAP) / Home Agent (HA) / Correspondent Node (CN) makes a handover decision provided that two conditions are met: QoS requirements in the route that QoS-conditionalized binding update message travels; security components agrees to use requested QoS. The QoS information carried in the registration acknowledge message will activate the correspondent entity to reserve, adapt the reservation or tear down the reservation along the downlink path toward the MN.

3.3 Security

The security component provides authentication and authorization services when mobile hosts demand services with different QoS requirements in a visited network.

To deal with the issue of Denial of Services (DoS), a cookie mechanism is employed in the framework. If there is no check on whether the BU sender is a registered and credible user in the visited access network before any expensive QoS-conditionalized BU process when the MN roams to a new Access Router (AR), repeated BU requests from attackers could reserve all the available resources along the new path so that this path runs out of resources for any legitimate requests. Moreover, it is unfavorable to keep the QoS-conditionalized BU process waiting for the results of re-authentication and re-authorization from AAAL. Therefore, at a new AR a preliminary check on the MN's cookie which is issued by the MAP during its first registration is introduced.

A cookie is granted to the MN after its first successful registration in the visited access network by the MAP. When the MN sends a registration request to a new AR, it includes the cookie in the message so that the AR can check this cookie with the temporal cookie key distributed from the MAP to it. If this simple check is passed, the AR regards the MN as a registered and credible user and starts its QoS-conditionalized BU process.

Since the cookie is transmitted in plain text from MN to the new AR, it is used only once to prevent eavesdropping. No matter whether the BU process succeeds or not, a new cookie is granted to the MN for its next request, but only if the MN's message was correctly signed.

Chapter 4

Component Interactions

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

4.1 Mobile Node

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

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

4.2 Access Router

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

4.3 Mobility Anchor Point

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

4.4 Home Agent / Correspondent Node

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

Chapter 5

Use Cases

This section describes specific use cases of the components of SeQoMo architecture and gives a set of potential interactions under these use cases.

5.1 Inter-Domain Handover

Figure 5.1 shows an inter-domain case. The mobility component in the MN detects an (inter-domain) movement and initiates a secure, QoS-enabled handover. QoS availability information is checked along the path and a sustainable QoS is forwarded on. In case the security component associated with the MAP or HA agrees the MN to use the requested QoS, a handover in the MAP or the HA will be performed; the MAP will send a cookie and AA check results to the MN. Only during the downlink direction transmission of the signaling message, requested QoS will be reserved; the uplink QoS reservation behavior is disabled to assure the security for this attempt. The handover process to the MAP and HA can be either parallel or sequential.

5.2 Intra-Domain Handover

Figure 5.2 shows the intra-domain cases. The mobility component in the MN detects an (intra-domain) movement and initiates a secure, QoS-capable handover. The AR checks the security information (cookie) and decides whether to forward the signaling message further. If this check returns "yes", QoS availability information is checked along the path and a correspondent QoS is reserved. In this way the uplink of data transmission is guaranteed with QoS more quickly. In case the security components associated with the MAP agrees for the MN to use the requested QoS, a handover in the MAP will be made; a cookie will be generated and delivered to the MN. During the downlink transmission direction of the signaling message, the QoS reservation will be adapted or released depending on whether the handover in the MAP has succeeded.

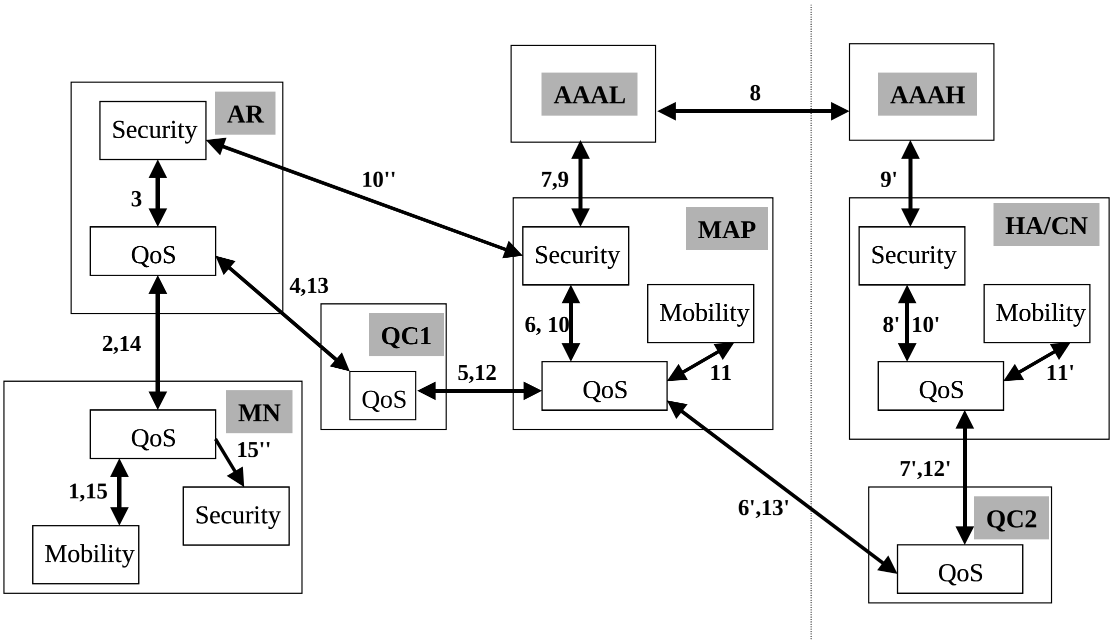

Figure 5.1: Inter-Domain Handover

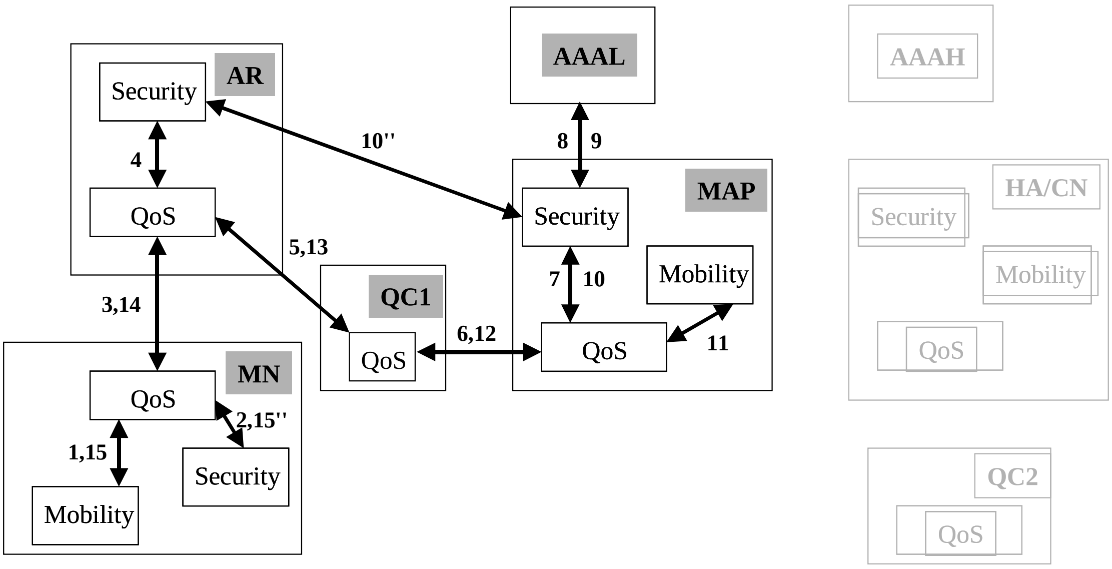

Figure 5.2: Intra-Domain Handover

5.3 Description of Interactions in Two Use Cases

A diagram of possible interactions for inter- and intra-domain handovers is summarized in Tab 5.1.

According to this diagram, the interaction sequence for inter-domain handover is:

- Registration to the MAP: 1-2-3-4-5-6-7-8-9-10-11-12-13-14-15(15”)
- Registration to the HA/CN: 1-2-3-4-5-6’-7’-8’-9’-10’-11’-12’-13’-12-13-14-15

The interaction sequence for intra-domain handover is:

- Registration to the MAP: 1-2-3-4-5-6-7-8-9-10-11-12-13-14-15(15”)
- Registration to the HA/CN: nothing

Note in the above sequences, 15(15”) means 15” can be done parallel or sequential to 15; the two registrations (to the MAP and to the HA/CN) can be either parallel or sequential; 10” is performed periodically and irrelevant to the handover process.

Table 5.1: Interactions of Inter-Domain and Intra-Domain Handovers

Steps (Inter-Domain)	Steps (Intra-Domain)	Node	Interactions	Data
1	1	MN	Mobility notifies QoS about a movement	BU(MAP); if necessary BU(HA/CN)
-	2	MN	QoS requests Security for cookie and authentication data; Security replies	whether a cookie is available, (if yes) cookie and authentication data
2	3	MN-AR	QoS(AR) obtains QoS and cookie from the registration message forwarded by the MN	QoS option, whether a cookie is available; if yes, cookie
3	4	AR	QoS requests Security to authenticate the cookie; Security replies	cookie / whether the cookie is accepted by the Security
4	5	AR-QC1	QoS(QC1) obtains QoS option from the registration message forwarded by the previous hop	QoS option
5	6	QC-MAP	QoS(MAP) obtains QoS option and authentication data from the registration message forwarded by the previous hop	QoS option and authentication data
6	7	MAP	QoS requests Security to authorize the registration request	authentication data
7	8	MAP-AAAL	Security(MAP) requests AAAL to authorize the registration request	authentication data
8	-	AAAL-AAAH-AAAL	AAAL requests AAAH to authorize the registration request; AAAH replies	authentication data / authentication result
9	9	AAAL-MAP	AAAL replies Security(MAP) with the authentication result	authentication result
10	10	MAP	Security replies QoS with authentication result and (if the result is positive) a cookie	authentication result, cookie
10”	10”	MAP-ARs	Security(MAP) distributes a cookie key to Security(all ARs in the MAP domain) periodically	a cookie key generated by Security(MAP)
11	11	MAP	QoS notifies Mobility for a handover; Mobility responds	BU / BAck
12	12	MAP-QC1	QoS(QC1) obtains QoS option from the registration message forwarded by the previous hop	QoS option
13	13	QC1-AR	QoS(AR) obtains QoS option from the registration message forwarded by the previous hop	QoS option

Steps (Inter-Domain)	Steps (Intra-Domain)	Node	Interactions	Data
14	14	AR-MN	QoS(MN) obtains QoS option and cookie from the registration message forwarded by the previous hop	QoS option and cookie
15	15	MN	QoS notifies mobility about the routing change	handover request / acknowledgement
15”	15”	MN	QoS delivers the cookie to Security	cookie / acknowledge
6’	-	MAP-QC2	QoS(QC2) obtains QoS option from the registration message forwarded by the previous hop	QoS option
7’	-	QC2-HA/CN	QoS(HA/CN) obtains QoS option and authentication data from the registration message forwarded by the previous hop	QoS option and authentication data
8’	-	HA/CN	QoS asks Security to authorize the registration request	authentication data
9’	-	HA/CN-AAAH-HA/CN	Security(HA/CN) asks AAAH to authorize the registration and AAAH replies with authentication result	authentication data
10’	-	HA/CN	Security replies QoS about the authentication result	authentication result
11’	-	HA/CN	QoS requests Mobility for a handover and Mobility responds	BU / BAck
12’	-	HA/CN-QC2	QoS(QC2) obtains QoS option from the registration message forwarded by the previous hop	QoS option
13’	-	QC2-MAP	QoS(MAP) obtains QoS option from the registration message forwarded by the previous hop	QoS option

Chapter 6

Summary and Future Work

The SeQoMo project investigates how to integrate advanced mobility mechanisms, security, and QoS components into an overall secure, QoS-enabled mobility architecture (SeQoMo architecture) based upon IP protocol. This document describes the interactions of the three components and elaborates two use cases deploying this architecture: inter- and intra-domain handovers. Further work of this project includes refining message flows, designing data structures, investigating on layer-2 triggering mechanism and undertaking a protypical implementation.

Bibliography

[1] T. Chen, X. Fu, H. Karl, G. Schäfer, and A. Festag. An Introduction to the SeQoMo Framework, SeQoMo project deliverable D-Comm-2, December 2001.

[2] T. Chen and G. Schäfer. Requirements and State of the Art Analysis for QoS-Aware Authorization of Mobile Devices in All-IP Networks, SeQoMo project deliverable D-Security-1, March 2002.

[3] S. Faccin, B. Patil, and C. Perkins. Diameter Mobile IPv6 Application. Internet draft, work in progress, November 2001.

[4] X. Fu, H. Karl, A. Festag, G. Schaefer, C. Fan, C. Kappler, and M. Schramm. QoS-conditionalized Binding Update in Mobile IPv6. Internet draft, work in progress, January 2002.

[5] H. Soliman, C. Castelluccia, K. El-Malki, and L. Bellier. Hierarchical MIPv6 Mobility Management (HMIPv6). Internet draft, work in progress, July 2001.