Proceedings of the IP Based Cellular Network Conference (IPCN 2003),
December 2003, Paris, France.

Secure, QoS-Enabled Mobility Support for IP-based Networks

X. FU
Telematics Group
Universität Göttingen
Lotzestrae 16-18
37083 Göttingen, Germany
fu@cs.uni-goettingen.de

T. CHEN, A. FESTAG, H. KARL, G. SCHÄFER
Telecommunication Networks Group
Technische Universität Berlin
Einsteinufer 25
10587 Berlin, Germany
[chen, festag, karl, schaefer]@ee.tu-berlin.de

C. FAN
ICM N PG SP RC PN
Siemens AG
Siemensdamm 62
13627 Berlin, Germany
changpeng.fan@siemens.com

***Abstract*—The rising number of mobile users, the advent of various radio access technologies, and the increasing importance of IP services over wireless as well as wired networks pose a number of new challenges. While Mobile IP has been designed for mobility management in IP networks, it may result in high latency and signaling overhead during handoff. Thus, advanced mobility mechanisms improving Mobile IP are desired to perform efficient handoffs. Also, appropriate Quality-of-Service (QoS) support is needed for mobility-enhanced IP in order to meet end users' expectations. Furthermore, security measures are required to protect the network infrastructure.**

This paper[1] describes the Secure, QoS-enabled Mobility (SeQoMo) architecture addressing these issues. In particular, optimization of handoff operations, low-latency QoS re-establishment for IP-level handoff, authentication, and QoS-aware authorization for mobile nodes are investigated and integrated in a unified framework. We also describe how the SeQoMo architecture as a whole supports efficient handoff processing especially during local movements, with optimized QoS support and authentication and QoS-aware authorization services.

I. 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. First, while Mobile IP (MIP) [9] and MIPv6 [6] are designed for mobility management in IP networks, they may result high latency and signaling overhead during handoff. Therefore, advanced mobility mechanisms improving Mobile IP are desirable to perform efficient handoffs. Also, appropriate QoS support is needed for mobility-enhanced 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 handoff. However, this is not supported by current Mobile IP. In this context, the IETF is developing the requirements for a QoS solution for MIP [2]. Furthermore, security measures are required to protect the network infrastructure. The provision of the Authentication, Authorization and Accounting (AAA) service in a mobile environment [4] will require inter-domain exchange of AAA information, which is essential to provide access services and resource usages within the visited domain.

This paper describes the Secure, QoS-enabled Mobility (SeQoMo) architecture addressing the above issues concerning IP mobility. The goals of SeQoMo are:

- Optimization of handoff operations. In addition to basic mobility support (location management and handoff), support of horizontal (intra-technology) as well as vertical (inter-technology) handoff is desired.[2] Furthermore, signaling overhead caused by mobility support as well as service interruption and packet losses caused by handoff should be minimized.
- Low-latency QoS re-establishment for IP-level handoff. Traffic flows should obtain QoS treatment as soon as the packet flow as such has been (re-) established after a handoff, while additional signaling traffic overhead should be kept low. In addition, a handoff to a particular access router (AR) should not be performed if minimal QoS requirements, defined by the user, can not be met along such a new path. It is also desirable for higher layers to know if a path is unable to provide required QoS.
- Authentication and QoS-aware authorization for mobile users. The visited network should verify the MN has the identity it claims to have. Also, the visited network needs to learn what kinds of services or how many QoS resources the MN is allowed to use and verify the resource usage of the MN to ensure that the total resource consumption does not exceed what the MN is entitled to use. To support efficient handoffs, it is also necessary to minimize the registration latency introduced by authentication and authorization (AA) procedures in handoffs taking place both within an administrative domain and between such domains. Furthermore, all AA messages should be transmitted securely to prevent both passive and active attacks.

Our proposed SeQoMo architecture consists of an IP-level mobility assistant, a QoS-conditionalized handoff controller and a QoS-aware security entity, based on extensions to the ex-

[1] This work has been supported in part by a research contract with Information and Communication Mobile, Siemens AG.

[2] An alternative way of defining horizontal and vertical handoff is the crossing of administrative boundaries. With respect to mobility management, a handoff between different administrative domains is naturally slower than an intra-domain handoff, while it is still a challenge for the *mobility* management to provide fast intra-domain, inter-technology handoff.

isting proposals for Hierarchical MIPv6 (HMIPv6), QoS Support for Mobile IP and Diameter Extensions for Mobile IPv6. These proposals are briefly described in Section II. The functional description of the SeQoMo architectural components is presented in Section III. By comparing with RSVP, we show in Section IV how the SeQoMo architecture as a whole supports efficient handoff processing during local movements, with optimized QoS support and authentication and QoS-aware authorization services. Section V concludes the paper and outlines our future work.

II. Related Work

A. Hierarchical Mobile IPv6

Hierarchical MIPv6 (HMIPv6) [11] is a protocol developed by the IETF that tries to overcome the shortcomings of MIPv6 on signaling load and potentially long handoff latencies. HMIPv6 introduces a new entity, the Mobility Anchor Point (MAP). When an MN moves into a new MAP domain (i.e., its MAP changes), it gets two new CoAs: a Regional CoA on the MAP's subnet (RCoA) and an on-link address (LCoA). The MN then sends a binding update (BU) to the MAP specifying its RCoA in the Home Address field, using its LCoA as its source address; it also requests a BU (RCoA, Home Address) from its home agent (HA) and correspondent nodes (CNs). If the MN moves locally, only the LCoA is changed and a registration packet is sent to the MAP. While this enhancement is more efficient for mobility support, it is unable to provide QoS support and QoS-aware authorization for mobile users.

In practical deployment, the MAP would usually be located in a gateway of an administrative domain; such an arrangement will be assumed in the remainder of this paper.

B. QoS Support for Mobile IP

In order to provide end-to-end QoS, IntServ and DiffServ have been designed; RSVP [12] has been developed as a signaling protocol. However, RSVP is difficult to use in mobility scenarios, e.g., due to its inability to build proper reservation state over the tunnel between the HA and the visited network.

Shen et al. [10] extended RSVP by proposing a "flow transparency" concept, i.e., identifying the flow address (source and destination address) with the MN's home address, regardless of the change of the MN's CoA. Paskalis et al. [8] proposed putting a "mobility proxy" at the edge of the access domain (e.g., a MAP domain) on behalf of RSVP messages: inside and outside the access domain, LCoA and RCoA of the MN will be used to identify the same session. The mobility proxy will either change the session information in Path/Resv messages accordingly and forward it (inter-domain handoff), or generate a Path toward the mobile node/respond with a Resv message upon receipt of a Path message from the mobile node (intra-domain handoff).

These RSVP-based approaches still have problems regarding latency for QoS signaling ($\geq$ two round-trip times) and signaling overhead. Chaskar and Koodli [3] proposed a QoS option that allows to include QoS-related data within existing mobility management messages. This approach allows to trigger a one-pass check for the required resources along the path toward the destination node in MIPv6. QoS option is a hop-by-hop IPv6 header option containing one or more so-called QoS objects, which code the QoS desired by a flow and is attached to the Mobile IPv6 Binding Update. This approach allows a one-pass check for the required resources along the path toward the destination node, simultaneously with the binding update. Its drawback is that the MN does not receive any feedback on whether the desired QoS is available at all along the new path.

This problem is solved in [5], where a handoff is conditionalized upon the ability of providing the required QoS along the new path. If a router along this path cannot provide adequate QoS, a handoff request will be returned as unsuccessful and another QoS-conditionalized handoff process could be initiated afterwards (if there is yet another potential path available). Furthermore, the QoS object does not need to be transmitted by every host, but could be obtained by the new access router from the old AR, e.g., by way of Context Transfer [7].

C. Diameter Extensions for Mobile IPv6

Mobile IPv6 in itself does not provide sufficient security support for mobility across different administrative domains, which limits the applicability of MIPv6 for large scale deployments. In order to grant a mobile node access to network resources, the mobile node needs to be authenticated and authorized. Diameter applications in Mobile IPv6 [4] precisely enable mobile users to roam and obtain service in networks that may not necessarily be owned by their home service provider.

Diameter is a follow-up AAA protocol to RADIUS, which is a method of managing the exchange of AAA information in the network. Existing extensions to the Diameter base protocol are intended to provide an AAA framework to applications such as Mobile IP. All data delivered by Diameter and its applications are in the form of Attribute Value Pair (AVP) and new AVPs can be created to meet some specific usage.

Diameter extension for Mobile IPv6 allows a Diameter server to authenticate, authorize, and collect accounting information for IP data traffic under mobility management by MIPv6. However, this proposal does not specify explicitly how to support QoS-enabled mobility in an efficient way; it also does not specify the way to extend to HMIPv6.

III. The Secure, QoS-Enabled Mobility Architecture

The Secure, QoS-enabled Mobility (SeQoMo) architecture is a conceptual description of components in routers, access points, mobile nodes, etc., and their behaviors (namely, interfaces and communication protocols to be used among these components). As the standardization of MIPv6/HMIPv6 is not yet completed, there are still some open problems regarding security issues and the lack of a fast handoff detection mechanism. These protocols also do not provide a means to signal QoS for the mobile hosts. To provide these functionalities, the SeQoMo architecture introduces the following capabilities: 1) enhanced mobility management by using layer-2 trigger; 2) QoS signaling for mobile hosts through the QoS-conditionalized handoff scheme; and 3) protection for mobile

communications by amending the Diameter MIPv6 extension with QoS-enabled mobility support in HMIPv6.

By means of piggybacking QoS signaling and data for security checks in the mobility signaling, the SeQoMo approach aims to propose a (re-)registration procedure with minimum latency. The detailed re-registration procedure of a local movement refers in Section IV-A.

As shown in Fig. 1, the SeQoMo architecture consists of three functional components: 1) an IP-level handoff assistant (IHA), which improves the handoff performance by a layer-2 trigger and initiates a secure, QoS-aware handoff process upon detection of an MN movement; 2) a QoS conditionalized-handoff controller (QHC), which performs an efficient QoS signaling by way of piggying-back QoS object(s) in the binding messages and QoS-conditionalizes the handoff process; and 3) a QoS-aware security entity (QSE), which provides authentication and QoS-aware authorization services when an MN sends QoS requests to the visited network. Instances of the same component might be located in different nodes in the network topology, jointly accomplishing their task (where the instances are of course suitably modified to reflect their various positions).

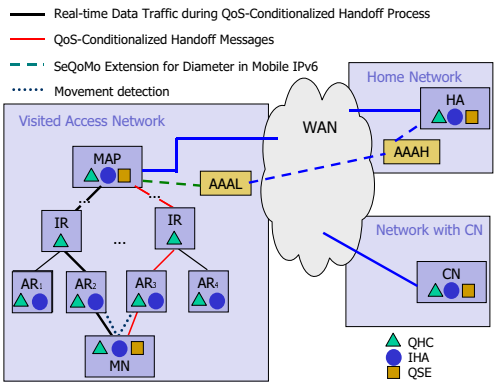

Fig. 1. The SeQoMo Architecture

A. IP-Level Handoff Assistant

The IP-level handoff assistant (IHA) in the SeQoMo architecture extends HMIPv6 with fast detection of MN movements based on layer-2 information to assist the IP-level handoffs. It also provides the MN with the detected movement information: local or global movement.

After the IHA obtains the knowledge of layer-3 information (the IPv6 address of the new AR as well as of the MAP) assisted by the layer-2 trigger, it initiates the QHC and the QSE processes (as described below) and will finalize a handoff upon positive results from the QHC and the QSE processes.

B. QoS-Conditionalized Handoff Controller

When several access points are available to an MN, it would be desirable for the MN to maintain an existing QoS assurance during handoff but at the same time to conditionalize its handoff upon the availability of sufficient QoS resources along a new network path through another access point.

This is done by the QoS-conditionalized handoff controller (QHC). Triggered by the IHA, the QHC transfers QoS information required by mobile nodes along the new potential path and ensures that QoS requirements can be met after a handoff (if this is at all possible, depending on the network situation the mobile is faced with after moving around). Note that the QHC design goal is to provide a generic means for signaling a mobile's QoS requirements to the QoS-aware routers during handoffs; the actual resource reservation process is out of scope and relies on underlying QoS provisioning models such as IntServ or DiffServ. Along the new path, QoS signaling messages are inspected by QoS controllers (entities within routers responsible for interpreting QoS messages) that invoke local QoS provisioning mechanisms [1] and that optionally inserting/modifying the signalled QoS parameters according to local network QoS management policies. A detailed description of QoS-conditionalized handoff scheme can be found in [5].

The QHC in the MAP (in case of local movement) performs a handoff provided that the following conditions are met: QoS requirements in the new path are met and the local QSE agrees to use requested QoS. If this succeeds, the QHC in the MAP will initiate a tear-down process (regarding QoS reservations) in the old path (optionally after some small delay, in order to allow the MN to smoothly switch to the new path) and the actual handoff is performed, i.e., packets now travel along the new path along with an acknowledgement of the successful handoff. Otherwise, a negative acknowledgement will be and returned to the MN in the registration acknowledgement along the same path as the registration request message traveled.

C. QoS-Aware Security Entity

The QoS-aware security entity (QSE) provides authentication and authorization services when mobile nodes demand services with different QoS requirements in a visited network.

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

In the local movement case, since it is assumed that the authentication and authorization data are already cached in the AAAL after its first registration in the visited domain, the re-authentication and re-authorization can be done locally at the AAAL without involving the AAAH to reduce the latency caused by traversing through the WAN as shown in Fig. 1. In addition to existing approaches, these checks also take into account if the mobile node has sufficient authorization to obtain the requested QoS.

IV. Comparison with the case using RSVP as QoS signaling protocol in local movements

The integration of the IP-level handoff assistant, the QoS-conditionalized handoff controller, and the QoS-aware security entity in the SeQoMo framework necessitates information exchange between these entities, varying between local and global movements.

Since mobile users are more likely to move locally, it is very important to reestablish their real-time traffic with QoS and security protection at the earliest possible moment after a local movement is detected.

In this section we compare the SeQoMo approach with the case using RSVP as the QoS signaling protocol in local movements in order to show how this architecture improves the efficiency of mobility with optimized QoS and security support in the local movement cases.

A. Procedure of Local Movement

When the IHA in the MN detects a local movement (based on layer 2 and 3 information it obtains from the AR), it initiates a secure, QoS-enabled handoff request. To expedite the whole handoff process, the data for security checks are also piggybacked in the mobility signaling package. As shown in Fig. 2, the registration (i.e., handoff request) message sent by the MN includes BU, QoS option, and AA information.

In the QoS-conditionalized handoff process, QoS availability information is checked along the path and correspondent QoS resources are reserved. In this way, the uplink of data transmission is guaranteed with QoS more quickly. If in a router in the path no sufficient QoS resources are available to meet the MN's "least acceptable" QoS request, the normal handoff procedure will not be performed, but the QoS-conditionalized handoff process will return the MN with a negative information, which also releases the QoS reservation (if any) along the path toward the MN.

Even if the routers along the path can meet the MN's QoS requirement, it is still necessary for the infrastructure to protect itself against misbehavior or attack. Authentication and authorization is hence needed. However, the latency of a local registration and additional signaling overhead has to be kept minimal. This is achieved in the SeQoMo architecture by a cache of AA information in the AAAL (close to the MAP) for mobile users recently joining the MAP domain.

In case the security entity (QSE) associated with the MAP agrees to the MN using the requested QoS, a handoff in the MAP will be made. Before sending the binding acknowledgement (BA) message to MN, MAP needs to contact AAAL for re-authentication and re-authorization (re-AA). When the check is passed, the downlink transmission will propagate. The data for re-AA are also piggybacked in the mobility signaling so that MAP can perform the re-AA check on behalf of the QoS path. The scheme is beneficial in minimizing the re-registration latency since normally MAP locates close to AAAL.

During the downlink transmission of the binding acknowledgement message, the QoS reservation will be adapted or released depending on whether the handover in the MAP has succeeded.

B. Performance Analysis

An alternative architecture for the secure, QoS-enabled mobility for IP-based networks could be combining HMIPv6, extended Diameter, and RSVP extension for mobile IPv6. In this section we analyze the performance of the two schemes, following the same way as described in [3]. In the QoS perspective,

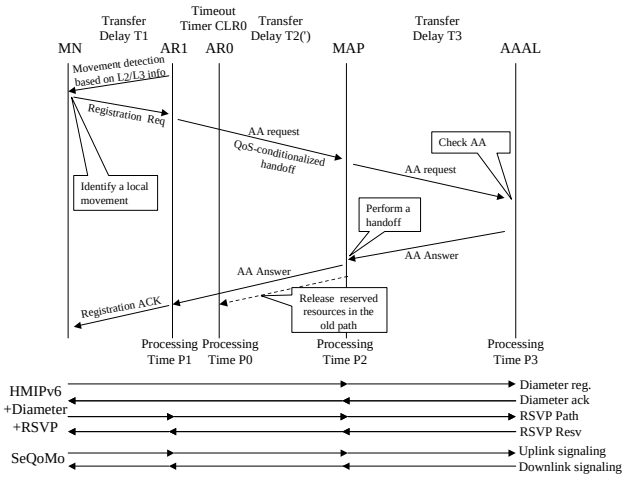

Fig. 2. Handoff Procedure for a Local Movement

having the intermediate routers in the new path get appropriate QoS provisioning is very important, therefore, the metrics we used are the resulting QoS-state (re-)establishment (after successful security check) latency and the required processing for intermediate routers after the MN is ready to use the new CoA/LCoA and RCoA.

Let CLR denote the QoS soft-state timeout timer for a router, P denote the CPU processing time of a signaling message in a router, T denote the transfer delay between two routers, and assume there are no other routers for the scenarios illustrated in the examples described above (see Fig. 2). Table I shows the latency of QoS re-establishment (or release for the old AR) in the intermediate routers by two schemes.

Assuming CLR >> T >> P, one can easily see that our proposed SeQoMo architecture re-establishment latency for routers is less than HMIPv6+Diameter+RSVP (RSVP++) scheme; the CPU processing (the sum of P's) for the signaling messages needed in the routers is also much less.

TABLE I

LATENCY AND PROCESSING TIME FOR QOS RE-ESTABLISHMENT/ RELEASE IN INTERMEDIATE ROUTERS DURING A LOCAL MOVEMENT

	RSVP++	SeQoMo
AR1	3T1+4T2 +4T3 +2P1+4P2 +2P3	T1+2T2 +2T3 +2P1+2P2 +P3
AR2 (Release)	CLR0	T1+T2 +T2'+2T3 +P1+2P2+P3
MAP	3T1+3T2 +4T3 +P1+2P2 +P3	T1+T2 +2T3 +P1+2P2 +P3

V. SUMMARY AND OUTLOOK

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

a unified framework. We motivated and described the architectural components and their interactions, namely the IP-level handoff assistant, the QoS-conditionalized handoff controller and the QoS-aware security entity. We specifically presented the procedure of local movements to address the difficult problem of efficient (low latency and low overhead with QoS-enabled security protection) handoff for mobile IPv6. This architecture can meet the requirements described in [2].

We are currently developing a layer-2 triggering mechanism and are undertaking a prototype implementation demonstrating the ideas and advantages of the integral SeQoMo architecture. In summary, SeQoMo works mainly for optimization of local movements. To meet the requirements of a real network, we use the SeQoMo approach for local movements while we employ the RSVP approach for global movements. Future work includes investigations on wireless link layer QoS support for the QoS-conditionalized scheme and incorporation of fast handoff and context transfer mechanisms. Moreover, enhancing access routers' advertisement messages with additional information such as currently available bandwidth or cost could be used to rank potential access routers in order to make an educated choice when attempting a QoS-conditionalized handoff.

REFERENCES

[1] M. Brunner. Requirements of QoS Protocols. Internet draft, work in progress, April 2002.

[2] H. Chaskar. Requirements of a QoS Solution for Mobile IP. Internet draft, work in progress, February 2002.

[3] H. Chaskar and R. Koodli. QoS Support in Mobile IP Version 6. In *IEEE Broadband Wireless Summit (Networld+Interop'2001)*, Las Vegas, USA, May 2001.

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

[5] X. Fu, H. Karl, and C. Kappler. QoS-Conditionalized Handoff for Mobile IPv6. In E. Gregori, M. Conti, A. Campbell, G. Omidyar, and M. Zukermann, editors, *Networking 2002*, LNCS 2345, pages 721–730. Springer-Verlag, 2002.

[6] D. Johnson, C. Perkins, and J. Arkko. Mobility Support in IPv6. Internet draft, work in progress, May 2002.

[7] J. Kempf. Problem Description: Reasons For Performing Context Transfers Between Nodes in an IP Access Network. Internet draft, work in progress, May 2002.

[8] S. Paskalis, A. Kaloxylos, and E. Zervas. An Efficient QoS Scheme for Mobile Hosts. In *Proc. of IEEE LCN'01*, Tampa, Florida, November 2001.

[9] C. Perkins. IP Mobility Support. RFC 3220, January 2002.

[10] C. Shen, W. Seah, A. Lo, H. Zheng, and M. Greis. An Interoperation Framework for Using RSVP in Mobile IPv6 Networks. Internet draft, work in progress, July 2001.

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

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