Technical University Berlin

Telecommunication Networks Group

QoS-aware authorization for mobile devices

T. Chen, G. Schäfer
[chen,schaefer]@ee.tu-berlin.de

Berlin, 26.03/2002, Version 1.5

TKN Technical Report TKN-03-009

TKN Technical Reports Series

Editor: Prof. Dr.-Ing. Adam Wolisz

Abstract

This document[1] analyzes the requirements and issues of QoS-aware authorization in mobile networks in the perspectives of authorization perception, authorization expression, security consideration and efficient handover support. It surveys the state of the art techniques in the current IETF and IRTF approaches and some substantial research activities. At last it presents two QoS-aware authorization schemes in hierarchical mobile IPv6 integrating with the QoS-conidtionalized BU approach: either the MAP or an AR authorizes MN's QoS requests. In the two schemes, authorization information is expressed in its service contract or service level agreement (SLA) with its home-domain service provider and is mapped to the QoS option in MIPv6 binding update message. Efficient handover support is achieved in the visited access network whenever possible not involving AAAH for authorization service since after the first registration MN's authorization information is already available in the visited network. A cookie mechanism is employed to prevent denial of service (DoS) and reduce the registration latency.

[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" (responsible project manager: Dr. Changpeng Fan in Siemens AG, ICM N PG SP RC PN).

Contents

Chapter 1

Introduction

The proliferation of mobile computing devices and wireless networking products over the past decade has made host mobility on the Internet an important research issue. Based on the fact that QoS capabilities will play a very important role in the future, we believe that the merging of mobility and QoS will be a very hot topic and also raise many new challenges.

This work discusses authorization issue in QoS-capable mobile networks, that is what network resources an attaching mobile node is allowed to use.

1.1 Relation of this report to other works at TKN

This report has been written in the context of the project *Mobility in Multi-Domain, Multi-Technology, IP-based Networks* that is funded by Siemens AG, department Information and Communication Network (ICM N MC ST 3). The focus of this project is to investigate the suitability of IP-based networks for support of mobility under the perspective of advanced mobility mechanisms, security, and Quality of Service (QoS). Integrating these three components into an overall secure, QoS-capable mobility architecture (SeQoMo architecture) based upon IP protocol is the ultimate goal of this project.

The work on authentication has been finished [19]. Another security aspect is SeQoMo is the topic of this work: QoS-aware authorization of mobile devices in All-IP network. This work has two prerequisites: Hierarchical Mobile IP (HMIP) and QoS-conditionalized binding update approach.

- HMIP: This mobility mechanism can be used to avoid the frequent local handoff problem and it has been selected as the micro mobility approach for this project. In SeQoMo, the mobility component aims to provide non-interrupted connectivity for MNs and to restrict QoS signaling to the minimum necessary part of the network. The relevant security issues are mainly discussed in this scenario.
- QoS-conditionalized binding update approach: In this approach, QoS information is piggybacked in the binding update message and verified by each entity along the route from the access router (AR) to the mobility anchor point (MAP) where the old and new paths meet (this kind of MAP is called switching MAP in the rest of the paper) so that the switching MAP can

decide whether to perform a handover based on the evaluation results from every entity along the route including the switching MAP itself.

We assume that authorization information is always handled by an AAA server (AAAL) in the visited network. Most likely, the authorization information is obtained originally from a AAA server in MN's home network (AAAH).

1.2 Overview of the Report

This report is organized as follows: the next chapter illustrates the requirements and issues for QoS-aware authorization in mobile networks. Chapter 3 describes how some related works solve the issues mentioned in Chapter 2. Chapter 4 presents our proposal to meet the discussed requirements and address the identified issues. Chapter 5 summarizes the key findings and draws some conclusions.

Chapter 2

The Requirements and Issues

The general requirements for authorization in mobile networks are discussed in [14, 33]. To clarify the QoS-aware authorization requirements and main issues in this work, we classify them into the following aspects: QoS-aware authorization phases, the mapping of authorization expression to QoS, security considerations and efficient handover support.

2.1 QoS-aware authorization phases

When an MN node registers in a visited access network, the network needs to learn the amount of QoS the MN is allowed to use in it.

Concerning the procedures for QoS-aware authorization, two phases can be distinguished: a learning phase and a verifying phase.

- The learning phase: The visited network needs to learn what is the maximum amount of QoS it should give to the MN. The learning phase should be integrated with the joint AAA/HMIP registration procedure. According to the previous work on authentication [19], the authorization information is transmitted to the visited network with the authentication check result.
- The verifying phase: When the MN roams and registers with another access router (AR) in the visited network requesting for resources, it should be checked that its QoS request does not exceed its credit limit. This verification should be integrated with the processing of QoS-conditionalized binding update (BU) messages.

The following questions need to to answered related to the learning phase:

- *Who will be responsible to learn the authorization information at the authorization learning phase?*
  There are two mobility entities to initiate authorizing the MN's QoS request: the MAP and an AR.

- *What will be the content of the authorization response from the MN's home domain?*
  There are two principal mechanisms to learn an MN's authorization information: An aggregate QoS description of the services is transmitted to his AAAH who approves or disapproves this specific request; or the overall service contract of the MN is transmitted to the visited network regardless what amount of QoS is requested.

The former one has the advantage to avoid unnecessary distribution of MN's private information and to prevent from potential abuse of the MN's authorization. However, re-authorization with AAAH has to be done when the MN requests a better quality of service. The latter mechanism is convenient for the visited network to handle the MN's various QoS requests. However, this mechanism always exposes overall content of the MN's service contract in the visited network.

There is one issue for the verifying phase: *Who will verify the MN's QoS request based on the MN's authorization information?*
We need to answer the question whether it is enough that one entity performs verification on behalf of the whole access network or it is necessary that each entity along a BU route from AR to the MAP needs to verify QoS requests.

2.2 Mapping of authorization information expression to QoS

An authorization specification language is required to ensure an unambiguous mapping of the QoS requests to authorization actions in order to make the QoS requests understandable and verifiable at an authorization entity.

The authorization information may be stored and transmitted by the use of policies and attribute certificates [34]. The exact content of QoS-aware authorization varies to fit in different applications and scenarios [6, 22, 31].

2.3 Security considerations

Threat models introduced by Mobile IPv6 are explained in details in [25]. In this section we stress on several threats in this work:

- *Masquerade attacks*: When an attacker masquerades as the MN, it could to consume MN's legally paid services without paying for the usage; when an attacker pretends to be AR, it could easily cause the MN to switch to the new AR and a different network and thereby impair the MN's reachability. To get things worse, if an attacker masquerades as AAAL, it could bring fake authorization information of the MN to the visited network so that the MN can abuse the resources more than its genuine authorization indicates.

- *Man-in-the-middle(MITM) attacks*: If a malicious node stays between the MN and an AR or between the entities which takes care of registration and AAAL or between AAAL and AAAH, it could possibly eavesdrop or modify the traffic.

- *MN's misbehavior*: An MN could possibly attach to multiple ARs at the same time and try to use more resources that it is entitled to. Even if the requested QoS over each link meets the MN's authorization limits, it could eventually happen that the total amount of QoS requested in the visited network exceeds the the MN's authorization limit.
- *Disclosure of authorization data*: If the overall service contract for this MN is distributed to the visited network with the authentication or authorization acknowledgment, an attacker could be able to learn confidential information about the MN's service profile, which might enable the attacker to reconstruct or reuse the credentials for future authorization processes. Furthermore, the service profile itself of an MN can be considered as a confidential information which should not be disclosed unnecessarily in order not to violate the MN's owner's privacy.
- *Non-repudiation*: The MN should not be able to falsely deny that it originated a QoS request at a later time.
- *Denial of service:* If there is no check on whether the BU sender is credible in the visited access network before reserving the resources according to the QoS request in the BU message, repeated BU requests from attackers can reserve all the available resources in a path so that the path runs out of resources fro any legitimate requests. It is unfavorable to hold the QoS-conditionalized BU process waiting for the results of re-authentication and re-authorization processes.

Digital signatures or message authentication codes should be used to prevent the the above-mentioned threats. Distribution and exchange of encryption key information between communicating peers to establish a security association (SA) might be required.

2.4 Efficient handover support

Generally, there are two kinds of delay during a handover: the movement detection delay and the registration delay. The signaling for authorization information contributes to the registration delay.

It is necessary that the authorization specific procedure adds minimal latency to the registration and handover procedures. The authorization-related communications should avoid getting the AAAH involved if it is possible.

2.5 Summary

We summarize the discussion on requirements and issues of the QoS-aware authorization for mobile devices into the following points:

- Authorization learning entity: who should be responsible to learn the authorization information in the visited access network;
- Authorization verifying entity: who should be responsible to verify that the QoS request to ensure that it doesn't exceed the authorization limit.

- Content of authorization information: whether the entire service contract will be transmitted to the access network or a specific evaluation result upon each specific QoS request will be transmitted;
- Mapping of authorization information expression to QoS: the MN's QoS request should be understandable in the access network based on the knowledge of the MN's authorization information;
- Monitoring the MN's resource utilization: how to prevent the MN's misbehavior to use more resources than what it's allowed to use;
- Efficient handover support: how to minimize the authorization-related registration delay.

In the next chapter, we bring out the state of the art analysis to explain how these issues are addressed in some related works.

Chapter 3

The State of the Art Analysis

In this chapter, we will analyze the solutions in some related works to the issues pointed out in Chapter 2.

3.1 Introduction to related works

3.1.1 Mobile IP / AAA

The Mobile IP registration [28] works well when all mobile nodes belong to the same administrative domain. In this subsection, we introduce a multi-domain model for Mobile-IP authorization and present it based on the AAA authorization framework [34].

Figure 3.1 depicts the trust model in AAA infrastructure according to [32].

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.

Figure 3.2 provides an example of a MIP network that includes an AAA infrastructure. It has a trust model like the one mentioned above.

Following is the registration actions after MN appears within the a foreign network:

- MN issues a registration to FA.
- FA 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.

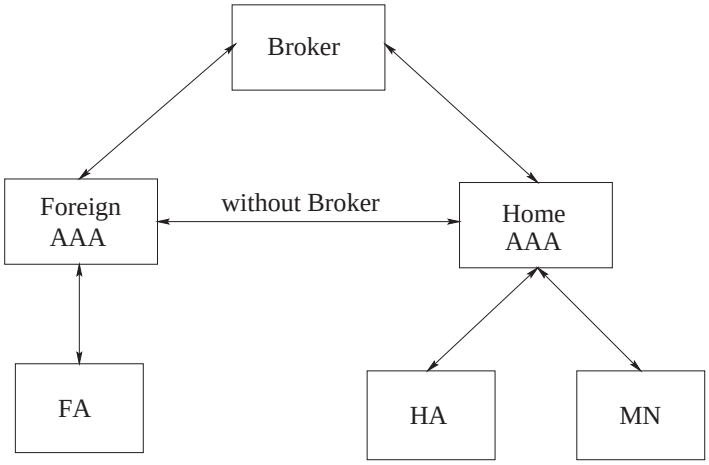


Figure 3.1: Trust Model in AAA Infrastructure [32]

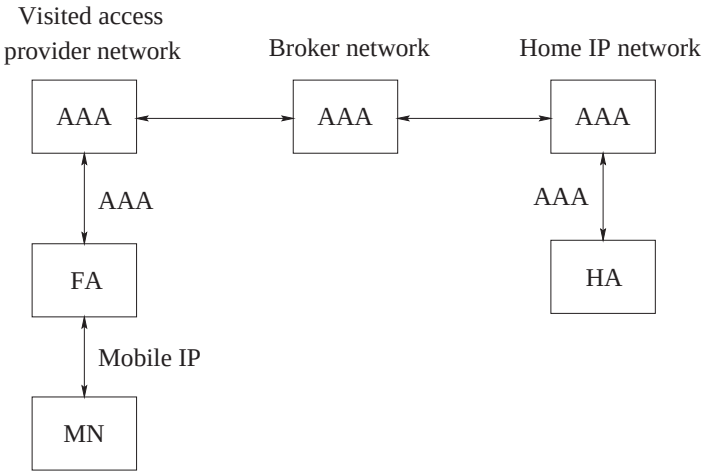


Figure 3.2: Mobile IP AAA [32]

- 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 [20].
- 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 re-

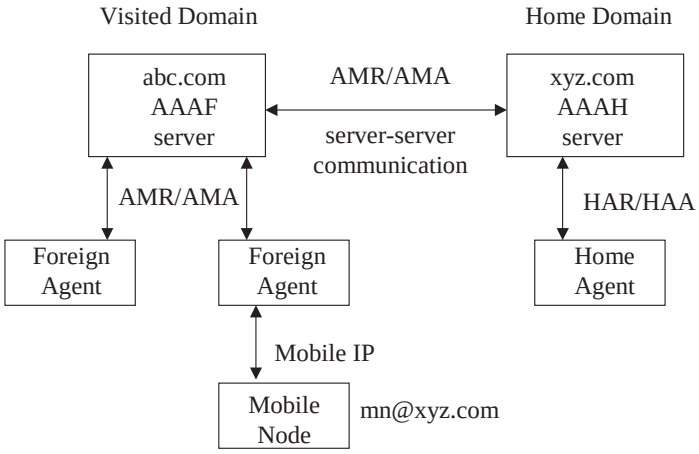


Figure 3.3: Inter-Domain Mobility [5]

sponse. The message is forwarded to AAAL via the broker and finally arrives at the FA 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.

3.1.2 Diameter Mobile IP applications

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 Operations Working Group (ROAMOPS). The Diameter mobile IP applications [5] (namely "Diameter" in the rest of this paper) enables a Diameter server to provide authentication, authorization and accounting services to an MN. While it has been described in detail in [19] as its fundamental work, this section introduces Diameter Mobile IP applications regarding to the requirements and issues for this work.

Figure 3.3 shows an example for inter-domain mobility in Diameter Mobile IPv4 application.

In Diameter, the inter-domain mobility actions are listed as follows:

- *FA's advertisement and MN's registration request:* The FA may provide a challenge in its advertisement messages in order to allow for replay protection in the Mobile IP registration process. The MN wishing to register includes the challenge, its network access identifier (NAI) and MN-AAA authentication extension to enable authorization by AAAH in its registration message and sends it to the FA;

- *AMR message initiation:* When the FA receives the registration request, it creates the AA-Mobile-Node-Request (AMR) message, which includes necessary Attribute Value Pairs (AVP). The MN's home address, home agent, NAI and other important fields are extracted from the registration messages for possible inclusion as Diameter AVPs. The AMR message is then forwarded to the local Diameter server, known as the AAA-Foreign, or AAAF.

- *AMR message forwarding:* Upon receiving the AMR, the AAAF determines whether the AMR should be processed locally, or if it should be forwarded to another Diameter Server, known as the AAA-Home, or AAAH. Figure 3.3 shows an example in which a mobile node (mn@xyz.com) requests service from a foreign provider (abc.com). The request received by the AAAF is forwarded to xyz.com's AAAH server.

- *Authentication and home agent selection:* The AAAH performs the authentication check and locates the home agent. The home agent could be either in the foreign or in the home domain. The AAAH checks the Home-Agent-In-Foreign-Network flag of the MIP-Feature-Vector AVP to perceive whether the home agent was located in the foreign domain. If the flag is enabled, then the home agent is located in the foreign domain then AAAH sends an HAR message to AAAF which contains a MIP-Reg-Request AVP. If the home agent was not located in the foreign domain, the AAAH checks for the MIP-Home-Agent-Address AVP. If one was specified, the AAAH checks that the address is that of a known home agent, and one that the MN is allowed to request, and the home agent's identity is included in the Destination-Host AVP. If no home agent was specified, and if the MIP-Feature-Vector has the Home-Agent-Requested flag set, and if allowed by policy in the home domain, the AAAH should allocate a home agent on behalf of the MN. This can be done in a variety of ways, including using a load balancing algorithm in order to keep the load on all home agents equal.

- *HAR message initiation:* The AAAH then sends an Home-Agent-MIP-Request (HAR), which contains the Mobile IP registration request message data encapsulated in the MIP-Reg-Request AVP, to the assigned or requested home agent. The AAAH may allocate a home address for the mobile node, and include it in a MIP-Mobile-Node-Address AVP within the HAR, or else leave this allocation responsibility for the home agent.

- *HAR message receipt and HAA initiation:* Upon receipt of the HAR, the home agent first processes the Diameter message. It processes the MIP-Reg-Request AVP and creates the registration reply, encapsulating it within the MIP-Reg-Reply AVP. If a home address is needed, the Home Agent must assign one and include the address in both the registration reply and within the MIP-Mobile-Node-Address AVP. The Accounting-Multi-Session-Id AVP in the HAR must be included in the HAA, which is then forwarded to the AAAH.

- *HAA message receipt and AMA initiation:* Upon receipt of the HAA, the AAAH creates the AA-Mobile-Node-Answer (AMA) message, includes the Accounting-Multi-Session-Id that was present in the HAA, and the MIP-Home-Agent-Address, MIP-Mobile-Node- Address AVPs in the AMA message, enabling appropriate firewall controls for the penetration of tunneled traffic between the Home Agent and the Mobile Node. The AAAF is responsible for ensuring that the AMA message is properly forwarded to the correct FA.
- *Registration Reply:* After receiving the AMA message, the FA sends a registration reply message to the MN.

Some key points related the requirements and identified issues in this work are:

- *Session identifier:*
  During the creation of the HAR, the AAAH must use a different session identifier than the one used in the AMR/AMA. Of course, the AAAH must use the same session identifier for all HARs initiated on behalf of a given MN's session. That means the session ID should be unique for a session in order to indicate a continuation of an existing session.
- *Authorization expression:* When a service makes use of the authentication and/or authorization portion of an application, and a user requests access to the network, the Diameter client issues an "auth request" to its local server. The "auth request" is defined in a service specific Diameter application (e.g. NASREQ). The base Diameter protocol does not include any authorization request messages, since these are largely application-specific and are defined in a Diameter application document [2].

  In the Diameter Mobile IPv4 application [5], the MN includes the Challenge and MN-AAA authentication extension in AMR to enable authorization by AAAH.

  The FA (or HA in the case of a co-located MN) uses information found in the Registration Request to construct the following AVPs that are to be included as part of the AMR:

  – home address (MIP-Mobile-Node-Address AVP)
  – home agent address (MIP-Home-Agent-Address AVP)
  – mobile node NAI (User-Name AVP)
  – MN-HA Key Request (MIP-Feature-Vector AVP)
  – MN-FA Key Request (MIP-Feature-Vector AVP)
  – MN-AAA Authentication Extension (MIP-MN-AAA-Auth AVP)
  – Foreign Agent Challenge Extension (MIP-FA-Challenge AVP)

  There is no more information on authorization-related AVPs in Diameter IPv6 application.

  The Diameter NASREQ Application [3] includes the Authorization AVPs that are needed for the various services offered by a NAS, such as PPP dial-in, terminal server and tunneling applications, such as L2TP.

  Since the Diameter protocol is designed to be extensible, it's possible to create new AVPs for the QoS-awareness authorization work.

- *Minimized round trip concerns:*
  It is not required that the FA invokes AAA services every time a registration request originated by the MN, but rather only when the prior authorization from the AAAH expires. The expiration time of the authorization (and registration keys, if allocated by the AAA server) is communicated through the Authorization-Lifetime AVP in the AMA from the AAAH.

  The Mobile IP Working Group is currently investigating fast handoff proposals, and the Seamoby WG is looking at creating a protocol that would allow AAA state information to be exchange between foreign agents during a handoff. These proposals may allow future enhancements to the Diameter protocol, in order to reduce the amount of Diameter exchanges required during a handoff.

- *Key distribution:*
  If registration keys are requested, the AAAH must create them after the MN is successfully authenticated and authorized. Three keys needed to be distributed to two communicating parties respectively are the key for MN and FA, the key for MN and HA, and the key for FA and HA.

  Once the registration keys have been distributed, subsequent Mobile IP registrations need not invoke the AAA infrastructure until the keys expire.

- *SA establishment:*
  The Diameter base protocol [2] leverages either IP Security IPsec (IPSec) [1] or Transport Layer Security (TLS) [10] for integrity and confidentiality between two Diameter peers. Diameter clients, such as Network Access Servers (NAS) and Mobility Agents must support IPSec and may support TLS. Diameter servers must support TLS and IPSec. To an establish SA between two peers through agents, the Diameter CMS (Cryptographic Message Syntax) Security Application [4] can be used.

  The authentication work [19] assumes to use Encapsulating Security Payload (ESP), one of the IPSec protocols to protect messages between all involved entities including Diameter clients and servers and mobility agents.

3.1.3 AAAC design in Moby Dick project

Authentication, authorization, accounting and charging design in the Moby Dick project (AAAC) [36] 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 3.4 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.

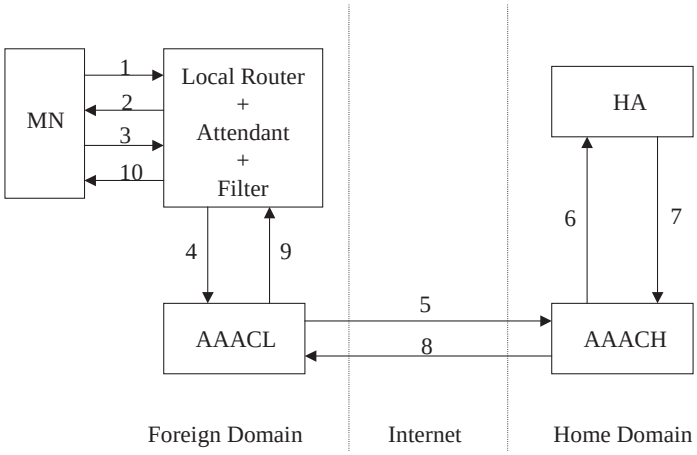


Figure 3.4: Registration message exchange [36]

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.

According to [36], it is still not clear in this AAAC that how the HA-MN binding updates and acknowledgment and replay protection will be performed after the session key is distributed.

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.

3.1.4 Akenti

Akenti [26] provides access control, enabling distributed management of access rights for resources. Akenti works on access control to distributed resources which is the first 2 AAs related to the quite huge AAAARCH picture. Different from the policy-based approaches, Akenti is an attribute certificate approach, using public/private key signed certificates to express user identity, resource use conditions, and user attributes; Public Key Infrastructure (PKI) certificate authorities (CA) and Lightweight Directory Access Protocol (LDAP) servers manage the certificates. It is a module that can be used

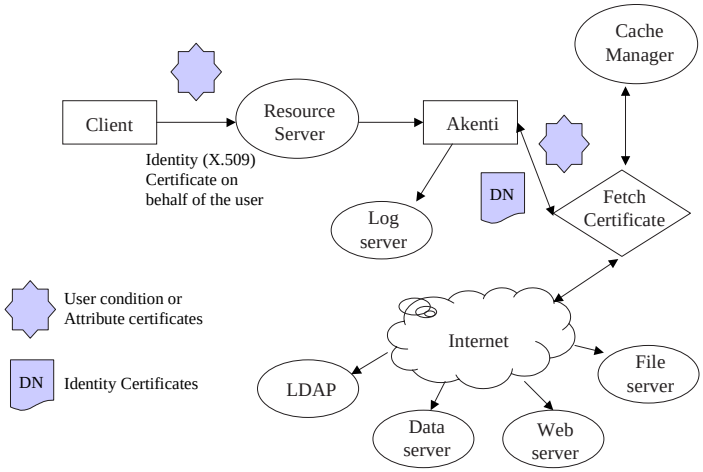


Figure 3.5: How Akenti works

with any application to provide access control. Once mutual authentication between communicating systems is established over SSL, Akenti is called to exercise access control on the resource accessed, to give out capabilities (actions allowed on that resource) for the remote system.

The component of the Model are:

- Identity (X.509) Certificate Authorities (CA) are used to issue and digitally sign the identity certificates for the user. These certificates associate an entity's name with a public key, and bind them together through the digital signature of the CA. They are stored in LDAP servers.
- Use-condition certificates are signed documents, remotely created and stored by resource owners that specify the conditions for access to the resource;
- Attribute certificates are signed documents, remotely created and stored that certify that a user possesses a specific attribute. If corresponding attribute certificates can be found for the user, then the use-conditions are satisfied, and the user's client is allowed access.

Figure 3.5 shows how Akenti works.

- A mutual authentication between the client/user and the server;
- The policy engine gathers use-condition certificates from the own servers;
- The attributes required by the use-conditions are verified by obtaining attribute certificates from trusted directories;
- If the user satisfies all the requirements, a secure connection is established between the client and server. Otherwise, the policy engine denies access to the server's resource.

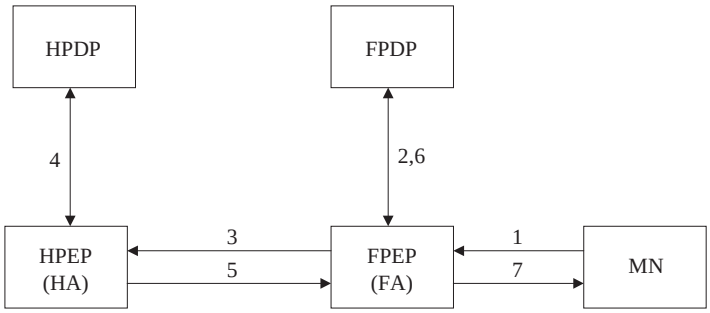


Figure 3.6: A typical policy control registration

3.1.5 COPS usage for Mobile IPv4

The COPS (Common Open Policy Service) protocol is a simple client/server model for supporting policy control over QoS signaling protocols [11]. COPS usage for Mobile IPv4 describes how COPS is used to control Mobile IP registration based on policies. It defines the interactions between the PEP (policy enforcement point) and the PDP (policy decision point) to handle Mobile IPv4 registration messages.

Figure 3.6 illustrates policy framework for mobile IPv4 [23].

The policy-enabled registration steps are the following:

1. MN sends a registration request to FA
2. FPEP (PEP client attached to FA) and FPDP (PDP client attached to FA) interact for policy decisions for the registration request
3. FA relays the registration request to HA
4. HPEP (PEP client attached to HA) and HPDP (PDP client attached to HA) interact for policy decisions
5. HA sends registration reply to FA
6. FPEP and FPDP interact for policy decisions for registration reply
7. FA forwards registration reply to MN

In this example, before relaying a registration request to the HA or relaying a registration reply to the MN, the FA may apply policies defined for the MN. Similarly, before responding to the registration request, the HA may apply policies for user roaming within the foreign domain.

In this typical COPS application, COPS is used to communicate policy information between a PEP and a remote PDP within the context of a particular type of client. Not every policy aware node in an infrastructure should be expected to contact a remote PDP because this would cause potentially long delays in verifying requests that must travel up hop by hop [35]. Therefore, the optional local PDP can be used by the device to make local policy decisions in the absence of a remote PDP.

With respect to QoS, the COPS protocol is targeted to support policy control over QoS signaling protocol such as RSVP [11]. Moreover, as one of requirements the COPS should allow for QoS which might be expressed in precise specifications of level of service requirements in the PEP requests forwarded to the PDP [35]. COPS is being developed within the RSVP Admission Policy Working Group (RAP WG) of the IETF, primarily for use as a mechanism for providing policy-based admission control over requests for network resources. The COPS usage for RSVP [18] is based on and assumes prior knowledge of the RAP framework [RAP] and the basic COPS [COPS] protocol. It provides specific usage directives for using COPS in outsourcing policy control decisions by RSVP clients (PEPs) to policy servers (PDPs).

Of particular importance is the “language” used to specify the policies implemented by the PDP. In order to handle the complexity of policy decisions and to ensure a coherent and consistent application of policies network-wide, the policy specification language should ensure unambiguous mapping of a specification profile to a policy action.

The PEP-PDP interaction may contribute significantly to the overall registration latency. Therefore, the PEP should reduce the amount of interactions with the PDP. This warrants fewer decisions solicited by the PEP, and less number of installed states. One possible measure is that The PEP caches decisions and policies locally and make local decisions whenever possible. For example, when a MN sends a registration request to refresh registration after the lifetime of the previous registration request expires, the HPEP can use locally cached decisions to handle it.

Concerning security considerations, the COPS protocol provides an Integrity object that can achieve authentication, message integrity, and replay prevention. The security between the PEP and PDP may be provided by IP security (IPSec). The IPSec Authentication Header(AH) should be used for the validation of the connection; additionally IPSec Encapsulation Security Payload (ESP) may be used to provide both validation and secrecy. Transport Layer Security (TLS) may be used for both connection-level validation and privacy.

In a COPS application namely deployment work of network intelligence to IP networks [24], COPS is used in cooperation with Diameter for Mobile IPv4 scenarios 3.7.

In this architecture, the service control layer is separated from the IP packet transmission layer. the service control layer manages each service profile for each MN in a service profile database (DB). A service profile consists of a set of procedures and data to control customized IP services for a MN. The service control layer downloads each service profile copy to the IP packet transmission layer.

The policy-based network management systems (PBNMSs) is deployed to supervise and control a network based on the network operator’s policy to maintain overall performance of the network. An AAAH notifies PBNMSs about the MN’s customization demand (probably the QoS request) via the COPS. PBNMSs then send the AAAH an acknowledgment of the demand after confirming that none of the services to other users will be degraded. The AAAH then updates the service profile in the service profile DB and downloads a copy of the modified service profile to the HA and FA to update the old one.

Since this work integrates COPS with Diameter for Mobile IPv4 applications, it introduces no new concerns on the identified issues other than those discussed in the previous section of Diameter Mobile IP applications. It gives an example of service profile for an MN as the following figure shows:

How to map the service profile to AAA messages is not addressed in [24].

In the UMTS environment, COPS can be used for outsourcing policy services. Through the use of the UMTS Go PIB (Policy Information Base), defined in [16], COPS-PR (COPS Usage for Policy Provisioning) [7] is used for outsourcing over the Go interface.

Figure 3.9 presents the policy control model for UMTS [16].

- *UE (User Equipment):* The UE is the UMTS term for a device used by a subscriber to access network services.
- *SGSN (Serving GPRS Support Node):* The SGSN performs the necessary functions in order to

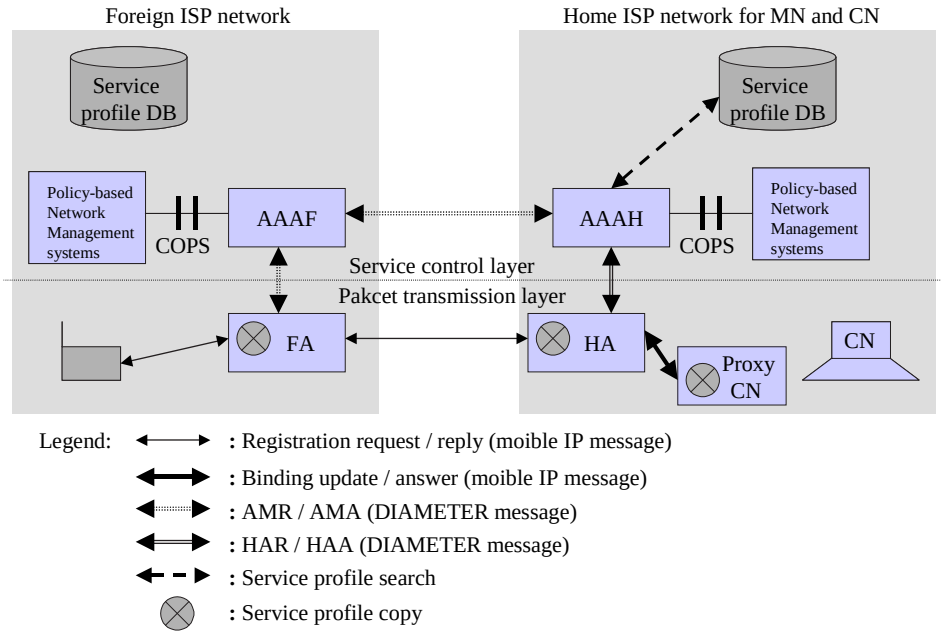


Figure 3.7: A Diameter and COPS joint architecture for Mobile IPv4

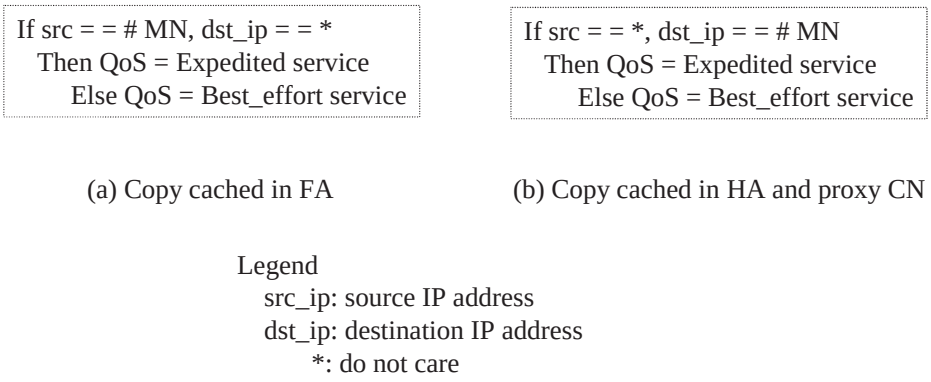


Figure 3.8: A example of policy-based service profile

handle the packet transmission to and from the UE.

- *PEP (Policy Enforcement Point):* The PEP is a logical entity that enforces policy decisions made by the PCF.
- *GGSN (Gateway GPRS Support Node):* The GGSN is a network element connecting the UE to the external network. The GGSN contains a PEP to enforce policies. It also contains a UMTS BS Manager for handling resource reservation requests from the UE (e.g. through PDP context signaling).
- *PCF (Policy Control Function) (PDP):* The PCF is a logical policy decision element which uses standard IP mechanisms to implement policy in the IP media layer. The PCF makes decisions in regard to network based IP policy using policy rules, and communicates these decisions to the PEP in the GGSN.
- *UMTS BS Manager:* The UMTS Bearer Service Manager handles resource reservation requests from the UE.
- *P-CSCF (Proxy Call Session Control Function):* The P-CSCF is a network element providing session management services (e.g. telephony call control).
- *Go interface:* Interface between the GGSN (PEP) and PCF (PDP).

Session authorization mechanism is in the following steps:

1. The UE issues a session set-up request (i.e. SIP INVITE) to the P-CSCF indicating, among other things, the media streams to be used in the session. As part of this step, the terminal may authenticate itself to the P-CSCF.

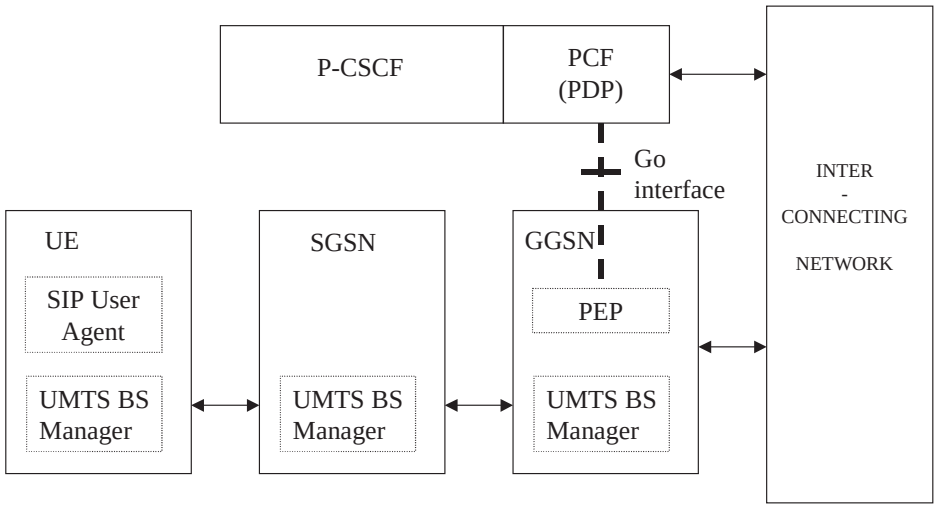


Figure 3.9: Policy control model for UMTS

2. The P-CSCF forwards the SIP INVITE to other CSCF functions in the network. However, the result of this will be that the P-CSCF receives a provisional SIP response from the other endpoint of the call. This will typically be a SIP 183 response message, also containing the relevant media information pertaining to the other half of the media to be used. Based on this information, the P-CSCF sends to the PCF the necessary information to authorize the request.

3. Based on the information received, containing information elements like bandwidth required, IP end points addresses and ports, the PCF authorizes the session and sends a decision to the P-CSCF. Included in this response is an "authorization token" that can subsequently be used by the PCF to identify the session and the media it has authorized.

4. The P-CSCF sends a response to the UE (e.g. by forwarding the SIP 183) indicating that session set-up is progressing. Included in this response is a description of the negotiated media along with the token from the PCF.

5. The UE issues a request (e.g. PDP context activation) to reserve the resources necessary to provide the required QoS for the media stream. Included in this request is the token from the PCF provided via the P-CSCF and flow identifier(s) that identifies the flow(s) on the PDP Context.

6. The GGSN receives the reservation request and sends a policy decision request (e.g. COPS REQ) to the PCF in order to determine if the resource reservation request should be allowed to proceed. Included in this request is the token and the flow identifier(s) provided by the UE. The PCF uses this token and flow identifier(s) to correlate the request for resources with the media authorization previously provided to the P-CSCF.

7. The PCF sends a decision (e.g. COPS DEC) to the GGSN.

8. The GGSN sends a response to the UE (e.g. PDP context activation response) indicating that resource reservation is complete.

In the terms of identified issues, P-CSCF initiates the authorization phase on behalf of the user, sending to the PCF the necessary information which contains information elements like bandwidth required, IP end points addresses and ports. Included in the response to UE is an "authorization token" that can be used later by the PCF to identify the session and the media it has authorized. Here ends the first round trip of negotiation. In the second round trip, the UE sends to the GGSN a request to activate the PDP context at PCF. The GGSN sends a policy decision request (e.g. COPS REQ) to the PCF. The PCF uses this token and flow identifier(s) to correlate the request for resources with the media authorization previously provided to the P-CSCF. The GGSN sends a response to the UE (e.g. PDP context activation response) based on the decision (e.g. COPS DEC) from PCF.

The information contained in the first request to PCF can be authorized at PCF based on certain policy-based mechanism. Details of QoS parameters and QoS parameter mapping in the 3GPP End-to-End QoS Concept and Architecture are for further study and not available yet [27].

3.2 Summary of the solutions in related works to the identified issues

In the terms of identified requirements and issues, we will compare the solutions in the mentioned related works.

3.2.1 Authorization learning and verifying phases

As a mobility entity in the MIPv4 infrastructure in MIP/AAA and Diameter AAA-extension, FA is responsible for learning the authorization information from AAAH via AAAL. However, there is no QoS support in MIP/AAA and Diameter.

In Akenti, an Akenti server will learn a user's authorization information and verify each access request to the resource.

In COPS usage of MIP, after receiving policy decision request which may contain one or more policy elements in addition to the admission control information (such as a flow-spec or amount of bandwidth requested) from the PEP, the PDP makes a decision based on the information stored in its local policy inventory and returns the policy decision to the PEP which enforces the PEP by appropriately accepting and denying the request from the MN. The PDP might optionally contact other external servers for the policy-based acknowledgment of the MN's request. Therefore, the PDP will learn an MN's authorization information which is carried by policies from either its local policy inventory or other external servers. The PEP will enforce and verify each MN's request.

3.2.2 Authorization expression

In Diameter authorization-related AVPs are used to transmit the information. The authorization information is contained in the Challenge and MN-AAA authentication extension in AMR message. No more detailed information is available so far.

In Akenti the authorization information is in attribute certificates such as Identity (X.509) Certificate Authorities (CA). In COPS the other way to store and transmit the authorization information is policies like the Figure 3.8.

3.2.3 Authorization content

In Akenti the overall authorization information will be transmitted to the visited access network with the MN's complete attribute certificate. In other related works a specific authorization response might be passed to the visited network upon a specific QoS request.

3.2.4 Security association establishment

In AAAC the session key for MN and AR is generated by AAAH to set up a dynamic SA between MN and AR. There is an assumption that the static SAs including the SA for MN-HA has already been established.

In MIPv4-based works three session keys are created by AAAH to set up dynamic SAs for FA-MN, FA-HA and MN-HA respectively. It is also assumed that static trust relationships among mobility entities already exist.

In Diameter security keys need to be set up and shared between the MN and other network entities such as the key between the MN and the AR. The AAA entities can play a major role in the computation and distribution of these security keys. Two key distribution methods, relying on this AAA infrastructure and allowing authenticated key distribution, are proposed: one is based on random numbers and the other is based on Diffie Hellman [12]. Similarly, the static trust relationships among network entities are assumed existing. IPSec is used to protect Diameter messages between mobility entities and AAA servers and either IPSec or TLS can be used to protect messages between Diameter servers such as AAA servers and brokers.

In COPS IPSec or TLS can be used to protect the communication between the PEP and the PDP as a static SA.

3.2.5 Efficient handover support

In all AAA related works handover support can be achieved within the scope of AAAL. That means when a handoff occurs within the AAAL domain, the AAAL will take care of the authentication and authorization check whenever possible to reduce involving the AAAH.

The Mobile IP Working Group is currently investigating fast handoff proposals, and the Seamoby WG is looking at creating a protocol that would allow AAA state information to be exchange between foreign agents during a handoff. These proposals may allow future enhancements to the Diameter protocol, in order to reduce the amount of Diameter exchanges required during a handoff [5].

In COPS it is possible for the PEP to cache policy-based authorization information locally to minimize the registration latency in cases of re-authorization.

We use the table 3.1 to summarize the above discussions.

Mobile IP has recently undergo some interesting transformations in order to be more suitable for use by existing cellular telephone operations and equipment manufacturers. Originally engineered as a solution for wireless LANs, Mobile IP enables a wireless network node to move freely from one point of connection to the Internet to another, without disrupting TCP end-to-end connectivity. Meanwhile, the AAA protocols aims to enable service providers to make a business case for supplying Mobile IP to their mobile customers. Therefore, this work is based on a joint architecture of the Mobile IP and Diameter which is an AAA protocol promoted by IETF.

Additionally considering the two conditions mentioned in Chapter 1, we will present our proposed architecture which integrates the Diameter and hierarchical Mobile IPv6 (HMIPv6) in the next chapter.

Table 3.1: Related Works

Issues	AAAC	MIP/AAA	Diameter	Akenti	COPS
Mobility mechanism	MIPv6	MIPv4	MIPv4/MIPv6	not addressed	MIPv4
QoS-capable	yes	no	no	no	yes
Authorization learning phase	QoS entity	FA	FA	Akenti server	PDP
Authorization verifying phase	AR	FA	FA	Akenti server	PEP
Authorization expression	user profile and policy	not addressed	authorization-related AVPs	attribute certificate	policy
Authorization content	specific response	not addressed	specific response	whole contract	specific response
Dynamic SAs	session key for MN-AR	session keys for MN-FA, FA-HA, MN-HA	session keys for MN-FA, FA-HA, MN-HA	not addressed	not addressed
Static SAs	established	established	established by IPSec and TLS	not addressed	established by IPSec and TLS
Handover support	Intra domain of AAACL	intra domain of AAAL	intra domain of AAAL	not addressed	registration handled by PEP

Chapter 4

QoS-aware Authorization in the SeQoMo Architecture

Figure 4.1 illustrates the architecture framework for the SeQoMo project. This architecture integrates single-level MAP hierarchical Mobile IP with an AAA structure.

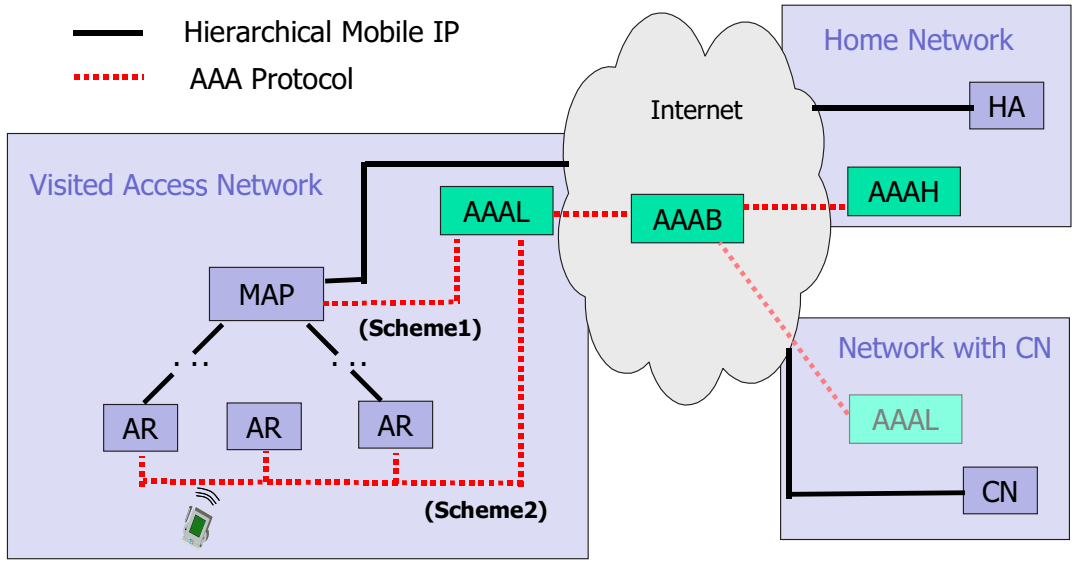


Figure 4.1: Architecture framework for the SeQoMo project

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

with CN to have an AAAL.

In Hierarchical Mobile IP, the mobility 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 (LCoA) [29]. In the QoS-conditionalized binding updates approach [13], each QoS request is to be checked and forwarded hop-by-hop from AR to the switching MAP. The hierarchy includes AR and the MAP.

In this HMIP environment, the MAP is already responsible to communicate with the AAAL for the authorization service. AAAH also needs to interface with the home agent (HA) to handle the registration message. Even though the HA needs not to be located in the same administrative domain as AAAH, we put them in the same home domain to simplify the picture.

The solid lines represent the paths for hierarchical Mobile IP flows while the dotted lines represent the AAA traffic. Figure 4.1 presents two schemes relying on which mobility entities have connections with AAAL. In Scheme 1 when the MAP authorizes the MN's QoS request, it should have a connection with AAAL for authorization service. Scheme 2 in which an AR is responsible to authorize the MN's QoS request requires that each AR has a connection with AAAL.

In the following we will discuss the two schemes in details.

4.1 Two schemes to authorize the QoS requests

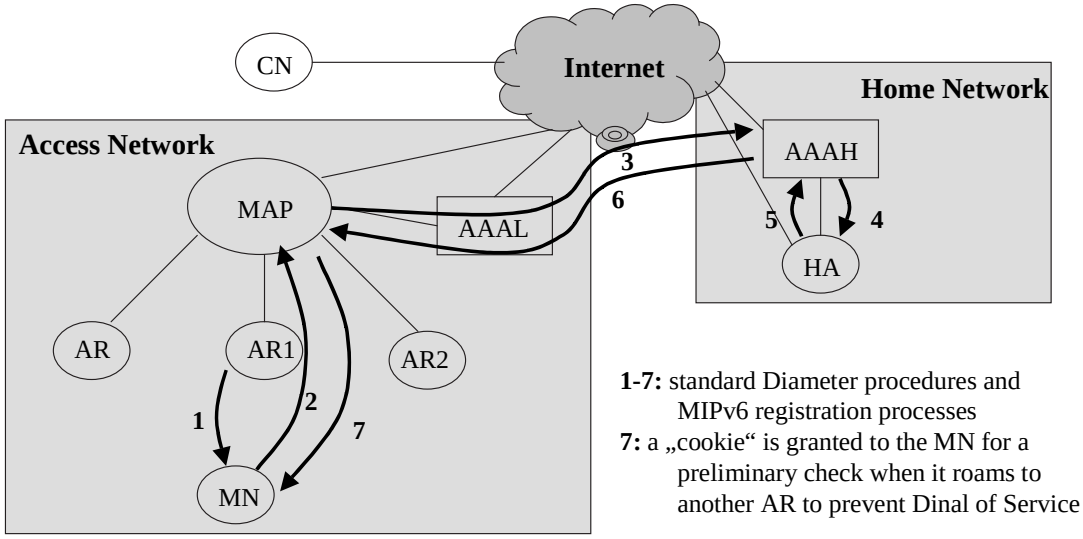
4.1.1 MAP authorizes the MN's QoS request

Figure 4.2(a) shows the steps of MN's registration with the MAP and its authorization procedures.

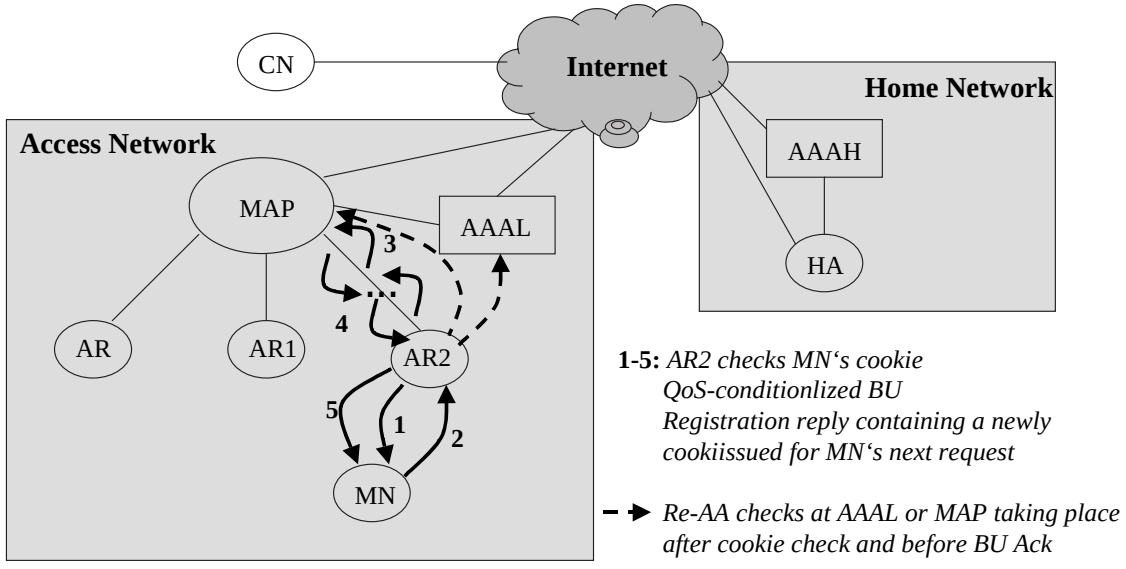
1. MN receives an advertisement from AR1 (an access router).
2. MN sends a registration request to the MAP including its QoS request.
3. The request is transmitted from the MAP to an AAAH in the MN's home domain for authentication and authorization services via AAAL.
4. If the authentication and authorization checks are passed, the AAAH sends the HA the BU message and session parameters such as session ID, session key and session lifetime etc.
5. The HA replies AAAH a BU acknowledgment.
6. The authorization check result, session parameters and BU acknowledgment are transmitted from the AAAH to the MAP via the AAAL. Then AAAL caches the authorization check result and the MAP performs the BU.
7. The MAP replies the MN's registration request with two BU acknowledgments, session parameters and a cookie which is used for a preliminary check when the MN roams in the visited access network.

The above procedure includes the standard Diameter procedures and MIPv6 registration processes. The initial motivation to introduce "cookies" is to save the time that otherwise would have to spend

on consulting AAAL for authenticating the MN in cases of handover. More detailed discussions on cookies refer to 4.3.



(a) Authorization processes



(b) Handover processes

Figure 4.2: MAP authorizes the MN’s QoS request

After registering successfully, the MN has access in the visited access network. When it performs a handover, the handover processes take place as Figure 4.2(b) presents.

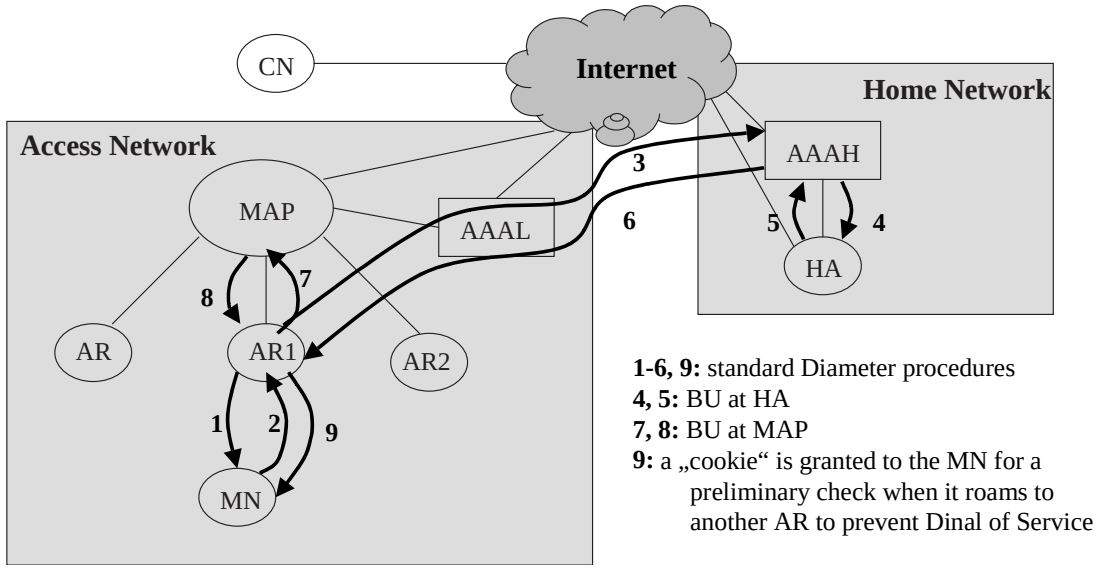
1. MN receives a new advertisement from AR2 (an access router).
2. MN sends a QoS-conditionalized BU message and its cookie to the AR2. AR2 checks the cookie to see if the MN is a credible user in the local domain. If it succeeds, it will start the QoS-conditionalized BU process and re-authentication and re-authorization process independently. The re-AA checks have to be performed with an entity such as MAP or AAAL before acknowledging the BU to the MN.
3. The QoS-conditionalized BU message is sent hop-by-hop upwards to the MAP. Each hop checks whether it can satisfy the QoS request for both uplink and downlink and reserves the resource if it can meet the request.
4. The MAP sends BU acknowledgment hop-by-hop backwards to the AR2. Whether or not the BU succeeds depends on check results of each hop including the MAP and the AR2.
5. The AR2 replies the MN with the BU acknowledgment and a new cookie which is used for its next request.

4.1.2 AR authorizes the MN's QoS request

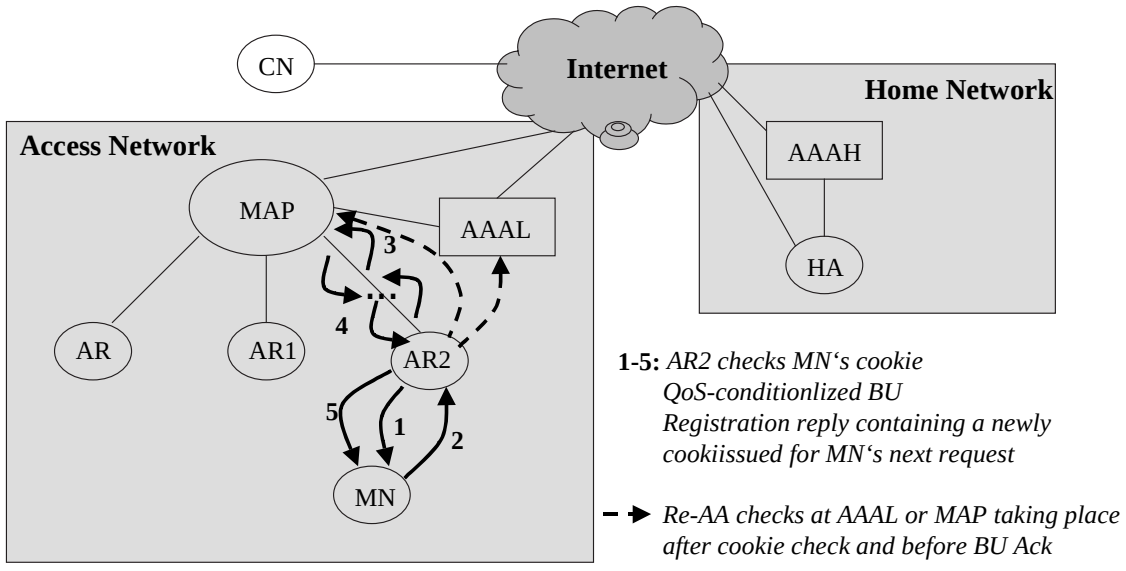
Another alternative entity to authorize the MN's QoS request is an AR. Figure 4.3(a) shows the joint steps of authorizing MN's QoS request by AR and registering with the MAP.

1. MN receives an advertisement from AR1.
2. MN sends a registration request to AR1 including its QoS request.
3. The request is transmitted from the AR1 to a AAAH in the MN's home domain for authentication and authorization services via AAAL.
4. If the authentication and authorization checks are passed, the AAAH sends the HA the BU message and session parameters such as session ID, session key and session lifetime etc.
5. The HA replies AAAH a BU acknowledgement.
6. The authorization check result, session parameters and BU acknowledgement are transmitted from the AAAH to the AR1 via the AAAL. Then AAAL caches the authorization check result.
7. AR1 sends the BU message to the MAP.
8. The MAP replies with the BU acknowledgement.
9. The AR1 replies the MN's registration request with two BU acknowledgements, session parameters and a cookie which is possibly generated by the MAP.

Step 1 to 6 and Step 9 contain the standard Diameter procedures and BU processes at HA. Step 7 and 8 is for BU at the MAP. It is noted that the procedures of BU at the MAP happen after the AA checks



(a) Authorization processes



(b) Handover processes

Figure 4.3: AR authorizes the MN’s QoS request

and BU at HA. This arises a problem that the MAP might reject the BU due to some reasons even though the BU has already successfully done at HA.

Figure 4.3(b) presents the processes when a handover occurs.

1. MN receives a new advertisement from AR2 (an access router).
2. MN sends a QoS-conditionalized BU message and its cookie to the AR2. AR2 checks the cookie with the temporal cookie key distributed by the MAP. If it succeeds, it will start the QoS-conditionalized BU process and re-authentication and re-authorization process independently.
3. The QoS-conditionalized BU message is sent hop-by-hop upwards to the MAP. Each hop checks whether it can satisfy the QoS request for both uplink and downlink and reserves the resource if it can meet the request.
4. The MAP sends BU acknowledgment hop-by-hop backwards to the AR2. Whether or not the BU succeeds depends on check results of each hop including the MAP and the AR2.
5. The AR2 replies the MN with the BU acknowledgment and a new cookie which is used for its next request.

The cookie will be detailed in 4.3. After the preliminary check with the cookie the re-AA checks have to be performed with an entity such as MAP or AAAL before acknowledging the BU to the MN.

4.1.3 Comparison between the two schemes

When MAP authorizes the QoS requests, it has an SA to AAAL through which it requests for authentication and authorization services. In contrast, when an AR initiates the authorization, each AR which is potentially responsible for the authorization has to have an SA with the AAAL for the same purpose in addition to the SA between it and the MAP. Therefore, there are much more SAs in Scheme 2 to be established and maintained than in Scheme 1.

However, Scheme 2 avoids the MAP to be the potential bottleneck for both HMIPv6 data flows and AAA traffics as in Scheme 1 by handling the authorization-related signaling by ARs.

4.2 Solutions to the identified issues

In this section we clarify our approaches to the identified issues.

4.2.1 QoS-aware authorization phases

Either the MAP (in Scheme 1) or an AR (in Scheme 2) initiates the authorization procedures and the registration processes. In both schemes AR is the gateway for the MN to access the visited network, verifying the MN's QoS request.

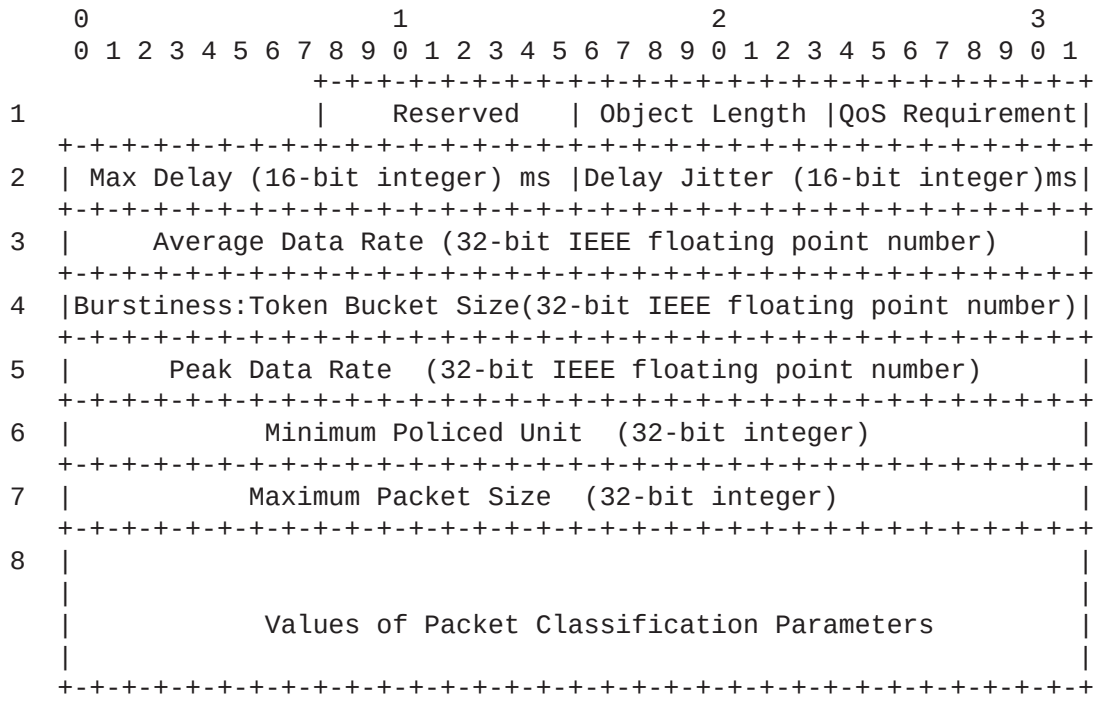


Figure 4.4: Composition of a QoS OBJECT Messages [8]

4.2.2 Mapping of authorization information to QoS object

To coordinate the QoS-conditionalized BU approach, authorization data design is based on the QoS option in MIPv6 BU message.

In the QoS-conditionalized BU approach, a QoS object is carried in the BU message as the format shown in Figure 4.4 [13].

The main fields in the QoS object are:

- QoS Requirement: This field describes the QoS requirement of the MN's packet stream in terms of traffic class. An example is the QoS specification in terms of delay sensitivity, such as interactive-delay sensitive, non-interactive delay sensitive or delay insensitive, as in UMTS QoS specification [27]. Another example is specification in terms of DiffServ Per-Hop Behavior (PHB) classes such as Expedited Forwarding (EF) or Assured Forwarding (AF). Yet another alternative is QoS specification in terms of IntServ classes such as guaranteed service or controlled load service.

  Some examples are,

  – 00000xxx: DiffServ EF PHB
  – 00001xxx: DiffServ AF PHB

  - 00010xxx: IntServ guaranteed service
  - 00011xxx: IntServ controlled load service
  - 00100xxx: UMTS traffic class

- Delay specification: The fields "Max Delay" and "Delay Jitter" specify the end-to-end values of respective quantities in milliseconds that the packet stream can tolerate.
- Traffic Volume: The fields Average Data Rate, Burstiness, Peak Data Rate, Minimum Policed Unit and Maximum Packet Size describe the volume and nature of traffic that the corresponding packet stream is expected to generate.
- Packet Classification Parameters: This field provides values for parameters in packet headers that can be used for packet classification. In particular, it specifies a subset of TCP/UDP port numbers, IPv6 flow label and SPI corresponding to particular packet stream. Typically, source and destination IP addresses to be used for packet classification can be inferred from header of packet carrying QoS OBJECT OPTION.

On the other hand, we classify the MN's authorization information which is stated in its service contract or service level agreement (SLA) with its home-domain service provider according to customer-perceived application services such as TELNET, FTP and SNMP. Some service level specifications are the following [15]:

- *Flow description:* The specifications of the authorization information contain one flow description which may be specified by providing one or more of the following attributes:

  - Differentiated services information = DSCP (Differentiated Services Code Point (DSCP) value XOR set of DSCP values XOR any
  - Source information = source address XOR set of source addresses XOR source prefix XOR set of source prefixes XOR any
  - Destination information = destination address XOR set of destination addresses XOR destination prefix XOR set of destination prefixes XOR any
  - Application information = protocol number XOR protocol number and source port, destination port XOR any

  The above flow description attributes can be mapped to the Packet Classification Parameters in Figure 4.4.

- *Traffic envelop:* The traffic envelop describes the traffic characteristics which might be peak rate, token bucket size, average rate, MTU and minimum packet size as the 32-bit lines from 3 to 7 in Figure 4.4 indicate.
- *Performance guarantees:* The performance parameters such as delay and jitter describe the service guarantees the network offers to the customer for the packet streams. A performance parameter can be quantified (its value is specified to a numeric value) or can be qualified by being marked as high, medium or low representing gold, silver or bronze service respectively.

Optionally, only one or some of the parameter values (e.g. Round-trip delay < 90 ms) can be specified for a type of service.

In the QoS requirement field in Figure 4.4, for instance, Best-Effort service which is currently used in the Internet is assigned “000000” and the service has the properties of no bandwidth guarantee and no QoS. For premium service which is understood as a Virtual Leased Line (VLL) service is defined as the EF PHB with the recommended code point “101110” in [9].

Following are a couple of authorization data examples expressed with the parameters from the QoS OBJECT OPTION.

- *VLL:*
  - QoS requirement = 101110 (EF PHB) [21]
  - Delay guarantee
  - Peak data rate
  - Packet classification parameter: IP-addresses=(source,destination), DSCP = EF
- *Real-time traffics:* e.g. video streaming which needs to specify a minimum rate and demands as the low loss rate as possible.
  - QoS requirement = 001010 (AF PHB, low drop and Class 1) [17]
  - Delay guarantee
  - Peak data rate
  - Burstiness Bucket Size
  - Packet classification parameter: IP-addresses=(multicast), DSCP = AF
- *Web-browsing and e-mail traffics:*
  - QoS requirement = 000001 (delay insensitive)
  - Average data rate
- *Emergency traffics:*
  - QoS requirement = 101110 (EF PHB)
  - Delay guarantee
  - Average data rate
  - Packet classification parameter: DSCP = TOP

4.2.3 Efficient handover support

In order to reduce the time spent on re-authorization by the AAAH, the MN's authorization information is transmitted to the visited access network and cached in AAAL. Thus the re-authorization is possible to be handled locally without involving AAAH.

During the first registration, a binary answer (yes or no) responding to a specific QoS request is given by the AAAH and the specific QoS request is cached by AAAL as the best QoS the MN is authorized currently. If the next QoS request exceeds the cached authorization limit, the AAAL has to consult AAAH for authorization and then it updates the cached authorization information. If the next QoS request doesn't exceed the cached authorization limit, the re-authorization can be done locally. Thus the QoS request which does not exceed the authorization limit can be re-authorized locally so as to minimize the re-registration latency, meanwhile the whole contract does not need to be transmitted to the visit access network.

Furthermore, a cookie is introduced for a preliminary check in order to start the QoS-conditionalized BU without having to wait for re-authentication and re-authorization results from the AAAL. More details are available in 4.3.

4.2.4 SA establishment

It's assumed that SAs for mobility agents and SAs for AAA entities are already established in the access network. To distribute session keys for MN-AR and MN-HA, the key distribution approach based on random numbers is used [12]. The AAAH generates one random number for each required security key. Then taking as inputs, to a key derivation algorithm shared with the MN, this random number, the long term key shared with the MN and optionally other data, the AAAH derives the desired security key which is securely transmitted to the network entity, the mobile node wants to share the key with. And the random number is sent to the MN which can derive the security session key thanks to the knowledge of the long term key and the key derivation algorithm shared with its home network.

The trust relationships are shown in Figure 4.5.

4.2.5 MN's misbehavior prevention

The AAAL or the MAP watches over MN's resource utilizations in the visited domain to prevent MN's any misbehaviors such as using more resources than it's entitled to by attaching to multiple ARs at the same time. In another words, the AAAL or the MAP acts as the resource manager in the domain.

4.3 Discussions on cookies

In this section, the initial motivation and ideas of the cookie mechanism is introduced first. Then the usage of cookies for the security purpose in this work is described. At last, some issues are discussed.

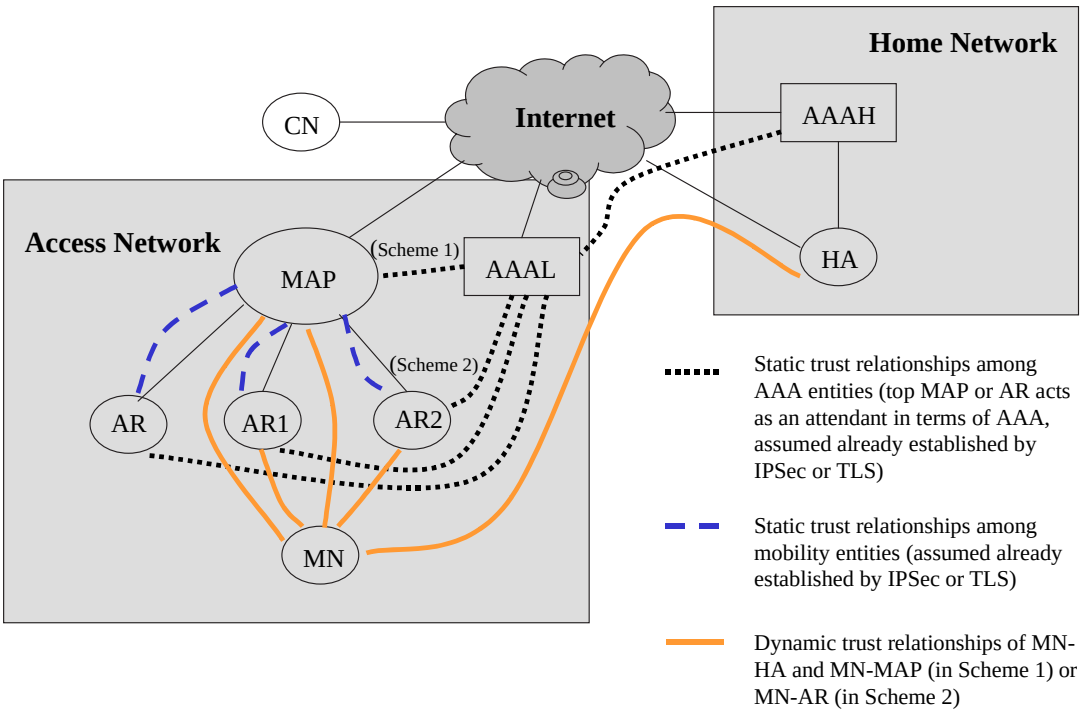


Figure 4.5: Trust relationships in the proposed architecture

4.3.1 Introduction of cookies

Originally, a mechanism known as cookies is used for key exchange and it can thwart clogging attacks. In this attack, an opponent forges the source address of a legitimate user and sends a public Diffie-Hellman key to the victim. The victim then performs a modular exponentiation to compute the secret key which is an expensive process. Repeated messages of this type can clog the victim's system with useless work. The cookie exchange requires that each side sends a pseudo-random number, the cookie, in the initial message, which the other side acknowledges. This acknowledgment must be repeated in the first message of the Diffie-Hellman key exchange. If the source address was forged, the opponent gets no answer. thus, an opponent can only force a user to generate acknowledgments and not to perform the Diffie-Hellman calculation [30].

The following scheme is used in the mechanism:

- The initiator generates an initiator cookie:

$$CKY - I = H(Secret_{Initiator}, Address_{Responder}, t_{Initiator})$$

- The responder generates an responder cookie: CKY-I = H

$$CKY - I = H(Secret_{Responder}, Address_{Initiator}, t_{Responder})$$

Both the initiator and the responder include both cookies in their messages, and check their own cookie before performing the expensive computation. The attacker who can not receive a response from the responder is unable to cause the denial of service (DoS) in the targeted network.

4.3.2 Usage of cookies

In our proposed architecture, we use cookies to prevent denial of service attacks in the access network. If there were no checks (if the BU sender is credible in the visited access network) before the expensive QoS-conditionalized BU process when the MN roamed to a new 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 halt the QoS-conditionalized BU process for the results of re-authentication and re-authorization from AAAL. Therefore, at a new AR (e.g. AR2 in Figure 4.2(a) and Figure 4.3(a)) a preliminary check on the MN's cookie which is issued by the MAP during its first registration is introduced aiming at the above two concerns.

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 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.

4.3.3 Issues of cookies

Based on the discussion above, a couple of issues arise:

- Since a cookie is used only once, all the ARs in the visited access network should be informed to reject the attempt to use a cookie second time.
- The re-authentication and re-authorization have to be done at AAAL sooner or later before the BU acknowledgment is replied to the MN. Even though the BU process and re-AA process may happen independently, it is possible of the re-AA process to introduce some registration latency. That means the BU acknowledgment potentially has to wait for the re-AA results before it goes to the MN.
- An attacker can suppress the MN's request and rob its cookie for its only use.
- An attacker can masquerade as an AR to make the MN unreachable in the access network.

4.4 Summary and discussions

In this chapter we explained two schemes to authorize the MN's QoS requests - either the MAP or an AR does it. We compared briefly advantages and disadvantages of the two schemes.

We discussed our solutions to the identified issues in the terms of QoS-aware authorization phases, authorization expression, efficient handover support, SA establishment and the MN's misbehavior prevention.

We stressed on the "cookies" which is used to prevent DoS and reduce the registration latency. We described the usage of this mechanism and some incidental issues.

With the respect to resource management in the visited access network, policy mechanisms need to be introduced to grant resource access based on both authorizing QoS requests and leveraging resource upon local network conditions so that traffic to and from Emergency Services can have precedence over all other types of traffic under all circumstances such as normal, degraded and catastrophic ones. That means in any emergency cases, a limited scope of resource utilization is committed without any authorization check.

Chapter 5

Summary and Conclusions

This report has studied overall requirements for the Mobile IP QoS-aware authorization design and identified the requirements in four aspects: QoS-aware authorization phases, QoS and expression of authorization information, security considerations and efficient handover support.

Based on the IETF's and IRTF's generic AAA architectures and some guideline documents, several research activities in this area have been discussed. Some works are heading to the direction of integrating AAA functions along with charging and auditing functions into mobility environment. Other efforts focus on distributed service management.

After analyzing the requirements and issues of the topic of QoS-aware authorization in Mobile IPv6 networks, we propose the SeQoMo architecture which applies in HMIPv6 networks and joins the QoS-conditionalized BU work.

The proposed SeQoMo architecture has the following characteristics:

- The AAA framework integrates into a hierarchical mobile IPv6 architecture. The functions of main components such as AR and MAP have been extended to meet QoS-aware authorization requirements.
- The MAP which is responsible for the MN's registration is the entity to learn MN's authorization and verify if MN's QoS request meets its authorization information.
- Efficient handover support is achieved in the visited access network. The AAAL which is unique in the domain will respond to any authentication and authorization services for a MN within a MN's session lifetime, without contacting MN's AAAH. When the session lifetime is expired, AAAL needs to communicate with MN's AAAH to get MN's authentication and authorization information like a new registration.
- The AAAL or the MAP watches over MN's resource utilizations in the visited domain to prevent MN's any misbehaviors such as using more resources than it's entitled to by attaching to multiple ARs at the same time. In other words, the AAAL acts as the resource manager in the domain.
- Authorization expression is based on the QoS option in MIPv6 BU message. We classify the

MN's authorization information which is stated in its service contract or service level agreement (SLA) with its home-domain service provider according to customer-perceived application services.

- Key distribution based on random numbers is used for SA establishments for MN-AR and MN-HA according to [12]. The AAAH generates one random number for each required security key. Then taking as inputs, to a key derivation algorithm shared with the MN, this random number, the long term key shared with the MN and optionally other data, the AAAH derives the desired security key which is securely transmitted to the network entity, the mobile node wants to share the key with. And the random number is sent to the MN which can derive the security session key thanks to the knowledge of the long term key and the key derivation algorithm shared with its home network .
- In the access network, it is assumed that SAs for mobility agents and SAs for AAA entities are already established.
- A cookie mechanism is employed to prevent DoS and reduce the registration latency.

Two schemes to authorize the MN's QoS requests are introduced and their advantages and disadvantages are briefly compared.

The future work will be:

- Refine the authorization procedures, required protocol messages
- Design authorization data structure, criteria to check QoS requests and identify hooks and interfaces to integrate with the QoS-conditionalized BU work
- Undertake the prototype implementation
- Figure out solutions to the identified issues mentioned in the cookie discussion section

Bibliography

[1] R. Atkinson and S. Kent. Security Architecture for the Internet Protocol, November 1998. RFC 2401.

[2] P. R. Calhoun, H. Akhtar, J. Arkko, E. Guttman, A. C. Rubens, and G. Zorn. Diameter Base Protocol, March 2002. Internet-Draft, draft-ietf-aaa-diameter-09.txt.

[3] P. R. Calhoun, W. Bulley, A. C. Rubens, J. Haag, G. Zorn, and D. Spence. Diameter NASREQ Application, March 2002. Internet-Draft: draft-ietf-aaa-diameter-nasreq-09.txt.

[4] P. R. Calhoun, S. Farrell, and W. Bulley. Diameter CMS Security Application, March 2002. Internet-Draft, draft-ietf-aaa-diameter-cms-sec-04.txt.

[5] P. R. Calhoun, T. Johansson, and C. E. Perkins. Diameter Mobile IPv4 Application, March 2002. Internet draft, draft-ietf-aaa-diameter-mobileip-09.txt.

[6] G. Carle, S. Zander, and T. Zseby. "policy-based accounting", internet draft draft-irtf-aaaarch-pol-acct-03.txt, August 2001.

[7] K. Chan, J. Seligson, D. Durham, S. Gai, K. McCloghrie, S. Herzog, F. Reichmeyer, R. Yavatkar, and A. Smith. COPS Usage for Policy Provisioning (COPS-PR), March 2001. RFC 3084.

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

[9] B. Davie and al. An Expedited Forwarding PHB, September 2001. Internet Draft: draft-ietf-diffserv-rfc2598bis-02.txt.

[10] T. Dierks and C. Allen. The TLS Protocol Version 1.0, January 1999. RFC 2246.

[11] D. Durham, Ed, J. Boyle, R. Cohen, S. Herzog, R. Rajan, and A. Sastry. The COPS (Common Open Policy Service) Protocol, January 2000. RFC 2748.

[12] S. Faccin, B. Patil, and C. Perkins. Diameter Mobile IPv6 Application, November 2001. Internet-Draft: draft-le-aaa-diameter-mobileipv6-01.txt.

[13] A. Festag, X. Fu, G. Schaefer, C. Fan, C. Kappler, and M. Schramm. "qos-conditionalized binding update in Mobile IPv6", internet draft draft-tkn-mobileip-qosbinding-mipv6-00.txt, July 2001.

[14] S. Glass, T. Hiller, S. Jacobs, and C. Perkins. "Mobile IP Authentication, Authorization, and Accounting Requirements", rfc 2977, October 2000.

[15] D. Goderis and al. Service Level Specification Semantics and Parameters, November 2000. Internet Draft: draft-chaskar-mobileip-qos-01.txt.

[16] L-N. Hamer, K. Chan, H. Syed, H. Shieh, and R. Zwart. COPS-PR for outsourcing in UMTS: UMTS Go PIB, November 2001. Internet-Draft: draft-hamer-rap-cops-umts-go-00.txt.

[17] J. Heinanen, F. Baker, W. Weiss, and J. Wroclawski. Assured Forwarding PHB Group, June 1999. RFC 2597.

[18] S. Herzog, J. Boyle, R. Cohen, D. Durham, R. Rajan, and A. Sastry. COPS usage for RSVP, January 2000. RFC 2749.

[19] A. Hess and G. Schaefer. Performance evaluation of AAA/Mobile IP authentication. Technical report, TU Berlin TKN, 2001.

[20] T. Hiller. cdma2000 Wireless Data Requirements for AAA, June 2001. RFC 3141.

[21] V. Jacobson, K. Nichols, and K. Poduri. An Expedited Forwarding PHB, June 1999. RFC 2598.

[22] S. Jajodia, P. Samarati, and V. S. Subrahmanian. A logical language for expressing authorizations. In *Proceedings of the IEEE Symposium on Research in Security and Privacy*, pages 31–42, Oakland, CA, May 1997. IEEE Computer Society, Technical Committee on Security and Privacy, IEEE Computer Society Press.

[23] M. Jaseemuddin and A. Lakas. COPS usage for Mobile IP (MIP), October 2000. Internet Draft: draft-jaseem-rap-cops-mip-00.txt.

[24] M. Kakemizu, M. Wakamoto, and A. Orita. Unified IP Service Control Architecture Based on Mobile Communication Scheme. *FUJITSU Sci. Tech.*, 37(1):81–86, June 2001.

[25] A. Mankin, B. Patil, E. Nordmark, P. Nikander, P. Roberts, and T. Narten. "threat models introduced by Mobile IPv6 and requirements for security", internet draft draft-ietf-mobileip-mipv6-scrty-reqts-02.txt, November 2001.

[26] S. Mudumbai, M. Thompson, G. Hoo, A. Essiari, K. Jackson, and W. Johnston. "akenti", `http://www-itg.lbl.gov/security/Akenti/`.

[27] 3GPP Organization Partners. 3GPP TS 23.207: End-to-End QoS Concept and Architecture (Release 5), January 2002. `ftp://ftp.3gpp.org/Specs/latest/Rel-5/23_series/23207-520.zip`.

[28] C. Perkins. IP Mobility Support, October 1996. RFC 2002.

[29] H. Soliman, C. Castelluccia, K. El-Malki, and L. Bellier. "Hierarchical MIPv6 mobility management (HMIPv6)", internet draft draft-ietf-mobileip-hmipv6-05.txt, July 2001.

[30] W. Stallings. *Cryptography and Network Security: Principles and Practice*. Prentice Hall, second edition edition, 1998. Hardcover, 569 pages.

[31] M. Thompson. Certificate-based access control for widely distributed resources. In *Proceedings of the Eighth Usenix Security Symposium*, pages 215–228, August 1999.

[32] 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", rfc 2905, August 2000.

[33] J. Vollbrecht, P. Calhoun, S. farrell, L. Gommans, G. Gross, B. de Bruijn, C. de Laat, M. Holdrege, and D. Spence. "AAA authorization requirements", rfc 2906, August 2000.

[34] J. Vollbrecht, P. Calhoun, S. Farrell, L. Gommans, J. Gross, B. Bruijn, C. Laat, M. Holdrege, and D. Spence. "AAA authorization framework", rfc 2904, August 2000.

[35] R. Yavatkar, D. Pendarakis, and R. Guerin. A Framework for Policy-based Admission Control, January 2000. RFC 2753.

[36] S. Zander. AAAC design. Technical report, GMD Fokus, January 2002. Deliverable for IST-2000-25394 Project Moby Dick.