# AAA for Mobile IP, Autumn 2002

Thalainayar Balasubramanian Ramya
Helsinki University of Technology, Espoo

Mobility, the buzzword of wireless generation has paved the way to invent significant features that makes communication more easier. Mobile Internet Protocol (Mobile IP) is a standard protocol used in mobile computing and networking making the dream of seamless connection to the net a reality.

This paper gives a brief functional description of Mobile IP based on the International Engineering Task Force (IETF) standards and current implementations. The architectural description and requirements of Authentication, Authorization and Accounting (AAA) for Mobile IP, specifically for IPv6 is discussed in detail. The paper concludes with a brief on the merits and the prospects for the future of AAA using Mobile IPv6.

## 1. INTRODUCTION

Mobile IP assists the mobile terminals to move from one link to another without changing its home address [12]. This concept is an emerging technology in the field of wireless communications. The successful transition from wired to wireless mobile phones has clearly shown the overwhelming response from the end users for wireless technology. This success has contributed to the increase in research in the area of Mobile IP. Based on the concept of Mobile IP, the services provided by these applications can roam among different wireless networks. Therefore, it is important to study about the authentication, authorization and accounting services involved in Mobile IP. The following concepts are discussed in detail in this paper. The terminologies involved in Mobile IP, the concepts of Mobile IPv4, Mobile IPv6 and the advantages of Mobile IPv6 are described in detail in Section. 2. Introduction to AAA with the terminologies and architecture is analysed in Section. 3. Section. 4 presents the AAA requirements for Mobile IP. The subsections include the implementation of AAA for both the versions of Mobile IP and compares the features of existing protocols. Finally, Section. 5 details the implementation issues and the future of AAA for Mobile IP, specifically for Mobile IPv6.

## 2. OVERVIEW OF MOBILE IP

Mobile IP is a proposed standard protocol that builds on the Internet protocol by making mobility transparent to applications and higher level protocols like Transmission Control Protocol (TCP)[13].

### 2.1 Terminologies involved in Mobile IP

*Mobile Node (MN):* The terminal which roams within and among networks without changing its home address [12]. Personal Data Assistant (PDA), mobile phones are examples of mobile node.

*Home Agent:* A router on the home network of mobile node that maintains the identity of mobile node. It tunnels the data packets to the mobile node when it is away from the home network[12].

*Foreign Agent:* A router on the visited network. It decapsulates and delivers the data packets to the mobile node that were tunneled by mobile node's home agent[12].

*Correspondent Node:* A peer with which the mobile node is communicating. The correspondent node can be either mobile or stationary[12].

*Mobility Binding:* The association of a home address with a care-of-address, along with the remaining life time of that association.

*Home Address:* IP address assigned to a mobile node, used as the permanent address of the mobile node [12].

*Home Subnet Prefix:* The IP subnet prefix corresponding to a mobile node's home address[7].

*Home Link:* The link on which a mobile node's home subnet prefix is defined[7].

*Foreign Subnet Prefix:* IP subnet prefix other than the mobile node's home subnet prefix [7].

*Foreign Link:* Link other than mobile node's home link.

*Binding Update:* This is used by a mobile node to the correspondent node or the mobile node's home agent to

Author's contact information: ramya@cc.hut.fi
Telecommunications and Multimedia Laboratory
Helsinki University of Technology, Finland
Acknowledgment of support: Tuomas Kivinen

Published in *I*nternet Protocols for Mobile Computing - Seminar on Internetworking, Autumn 2002, by Helsinki University of Technology, Telecommunications Software and Multimedia Laboratory. The complete publication can be found at http://www.tml.hut.fi/Studies/T-110.551/2002/papers/December/index.html. Permission to make digital/hard copy of all or part of this material without fee for personal or classroom use provided that the copies are not made or distributed for profit or commercial advantage, a copyright/server notice, the title of the publication, and its date appear.
ISBN 951-22-6272-X - ISSN 1455-9749 - HUT - TML - TML-C9

inform about its current binding.

*Binding Acknowledgement:* Acknowledgement message used to acknowledge the receipt of Binding Update.

### 2.2 Basic concept of MobileIPv4

The mobile node does not use the mobility services when it is within the home network. The mobile node determines its movement to a foreign network with the help of the agent advertisements[1][12]it receives. Once the mobile node discovers that it is attached to a foreign network it obtains a care-of-address(COA). This care-of-address can be obtained from any of the two methods, namely, foreign agent care-of-address or co-located care-of-address.

Foreign agent care-of-address is assigned by the foreign agent as a result of the solicitation request sent to it by the mobile node. This request is forwarded to the home agent through the foreign agent. When the home agent accepts the request, it sends a reply message to the mobile node through the foreign agent. This reply message is often termed as mobile binding.

Co-located care-of-address is assigned by some external services like Dynamic Host Control Protocol (DHCP). In this method, the mobile node directly contacts the home agent for registration. When the home agent accepts the registration request it sends a reply message with the mobile binding to the mobile node.

After registration, the data packets sent to the home address of the mobile node are receieved by the home agent. The home agent tunnels the data packets and sends it to the tunnel endpoint. The tunnel endpoint can be either a foreign agent or the mobile node itself, based on the care-of-address. This process of tunneling data packets is called encapsulation. It is used to hide the home address of the mobile node. In the tunnel endpoint the data packets are decapsulated and forwarded to the mobile node.

The data packets from the mobile node are sent to the correspondent node through foreign agent. This process need not involve the home agent. The routing method in Mobile IPv4 is generally termed as triangular routing.

Whenever the mobile node returns back to the home network it has to deregister with the home agent. Before the time period for the particular association expires, the mobile node should renew the registration.

### 2.3 Basic Concept of Mobile IPv6

In Mobile IPv6, when the mobile node is in its home link the packets sent to the home address are transferred using the usual Internet routing procedures. The subnet prefix of the mobile node's home address will be the same, in Mobile IPv6, as that of one in the home link's subnet prefixes.

When the mobile node detects that it is in a foreign network, it gets a care-of-address through the stateless or stateful address autoconfiguration methods based on IPv6 neighbour discovery[7],[10]. The mobile node requests a router in the home link to be its home agent. Thus it sends a binding update to the home agent for registration, which is acknowledged with the binding acknowledgement. If a mobile node has more than one care-of-address, it registers any one care-of-address with the home agent as primary care-of-address. Fig. 1 explains the data transfer between mobile node, correspondent node and the home agent. After registration, the packets coming from the correspondent node to the mobile node's home address is tunneled to its care-of-address by the home agent. When the mobile node receives the tuneled packets, it sends a binding update to the correspondent node. The correspondent node acknowledge the binding update to the mobile node. The data packets are then directly sent to the mobile node's current care-of-address. A return routability test is performed to authorize the establishment of binding[7].

If the home agent is reconfigured it is detected by the mobile node using 'dynamic home agent discovery' in IPv6[13].

### 2.4 Advantages of Mobile IPv6 over Mobile IPv4

(1) There is no need for a separate foreign agent in Mobile IPv6.

(2) Tunneling of data packets from the home agent to mobile node's current care-of-address is highly reduced.

(3) The data packets are directly sent to the mobile node's current care-of-address.

(4) Mobile IPv6 uses the mechanism of dynamic home agent discovery.

(5) Security is ensured using IPv6.

(6) Ipv6 has an increased address size upto 128 bits and it supports auto-configuration.

(7) It efficiently uses the return routability test to confirm the flawless data transfer between the mobile and correspondent nodes.

## 3. OVERVIEW OF AAA

AAA is a concept that includes authentication, authorization and accounting for networks. This helps to have a control over the activities of users on the network.

### 3.1 Terminologies involved in AAA

*Subscriber:* The end user who is paying for the services provided.

*Authentication:* The procedure of verifying and validating user credentials to confirm whether they are the entitled subscriber for the service.

*Authorization:* The procedure of identifying and confirming the level of services allowed for a particular user.

*Accounting:* It involves maintaining log of service utilization by the user, cost allocation, auditing and trend analysis. Billing the user is done based on the service utilization.

*AAA Home Server (AAAH):* The server associated with the home agent.

*Foreign AAA Server (FAAA):* The server associated with the foreign agent.

[1] Agent advertisements are transmitted by mobility agents to advertise its services on link. Mobile node uses these advertisements to determine their current point of attachment to the Internet

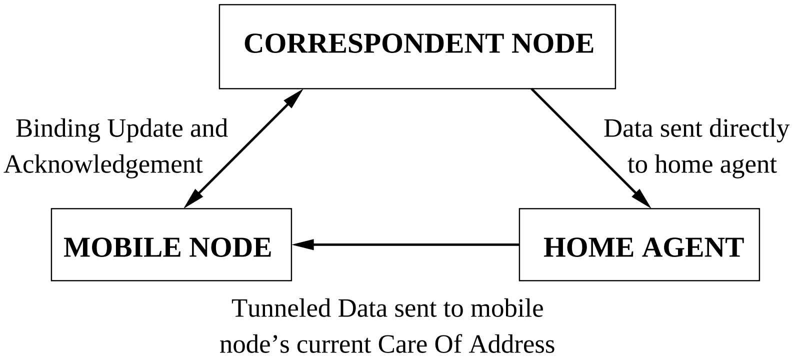

CORRESPONDENT NODE
Binding Update and Acknowledgement
Data sent directly to home agent
MOBILE NODE
HOME AGENT
Tunneled Data sent to mobile node's current Care Of Address

Fig. 1. Concept of Mobile IPv6.

*Attendant:* A node designed to provide the service interface between a client and the local domain [8].

*Client:* A node requests a service from an attendant within a administrative domain.

*Local domain (AAAL):* Administrative domain containing the AAA infrastructure of immediate interest to Mobile IP client when it is away from home.

*Broker :* A trusted intermediary agent between two AAA servers to obtain and provide valid authorizations and user credentials[8].

*Network Access Identifier (NAI):* The userID submitted by the client during Point-to-Point Protocol (PPP) [15] authentication. In roaming, the purpose of the NAI is to identify the user as well as to assist in the routing of the authentication request[1].

### 3.2 Architecture of AAA

AAA architecture is divided into two main types, namely, generic and Application Specific. Generic architecture can perform the operations of authentication, authorization and accounting. As the applications using AAA are unique, the application specific knowledge is essential. Application Specific Modules (ASM) perform this function, and it is interfaced with the generic AAA server.

The components involved in the Generic AAA architecture include:

*Event Log:* This is maintained for the auditing purposes. It is also used for authorization as certain authorization decisions depends on the previous logs.

*Policy Repository:* Database used to store the policy rules based on which the decisions are taken.

*Request Forwarding:* Mechanism used to handle the multiple administrative domain.

Using these components the AAA server interactions is explained as follows:

(1) As AAA does not know how to handle the application specific part, the request submitted by the user should be well structured.

(2) The ASM interfaced with AAA takes care of application specific part.

(3) Authorization decision is made based on the event log and policy rules in the repository.

(4) The components are then forwarded to another AAA server for evaluation.

### 3.3 Basic requirements for AAA

The basic requirements depend on all the three interdependent modules of AAA.

(1) The authentication procedure should be strict to avoid the replay attacks and man-in-the-middle attacks.

(2) Authorization procedure accepts a trusted third party to transact the details between AAA servers for evaluation of user's request. In such a case, an end to end security should be provided.

(3) In accounting, consideration should be given for fault tolerance, resource consumption and data collection model[3].

## 4. AAA FOR MOBILE IP

Mobile IP is becoming a popular concept. As the users are allowed to connect to any network at any time using Mobile IP, it is essential to have a well organized AAA procedure. This helps to have a good control over the services received by the user from foreign domain.

Fig. 2 describes the ouline of AAA for Mobile IP.

### 4.1 AAA implementation for Mobile IPv4

When the mobile node roams within the home link, the AAA architecture is implemented simliar to that of the normal wired networks. Once the mobile node starts roaming among networks, it should be authenticated and authorized before it starts getting a service from the foreign domain. For approving the request received from the user, the foreign domain depends on the home domain of the mobile node to get the user credentials. The agent(attendant) in the local domain receives the request and forwards it to the local authority which is also in the same domain of the agent. As the local authority does not have the user details to authorize, it contacts the home domain of the mobile node. The home domain sends the user details through the secure interaction between these two domain. Broker can also be used between two servers.[8]

When the Mobile IP agents are involved in the procedure, the foreign agent acts as a translation agent between the Mobile IP and AAA.

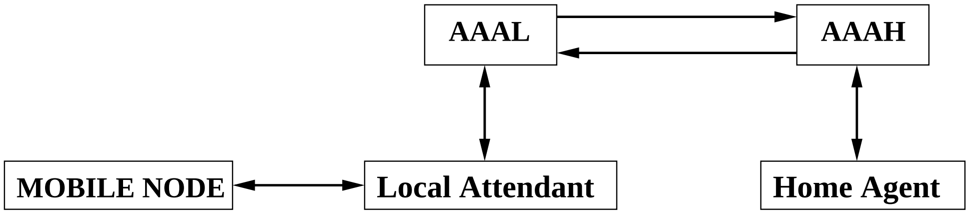


Fig. 2. AAA and Mobile IP.
[5]

### 4.2 AAA implementation for Mobile IPv6

Fig. 3 shows the basic steps involved in the implementation of AAA for Mobile IPv6. Mobile IP with dynamic IP addresses have more simpler and secure methods than Mobile IPv4 in implementing the AAA architecture. In a mobile node using the stateless address configuration of IPv6 version, NAI is used to obtain the dynamic address in the foreign domain linking the AAA authorization to it. The router itself acts as the agent (attendant) for AAA. When the host (IPv6) is connected to the network, it sends a router solicitation request with extensions to carry NAI and AAA. The router accepting the request extracts the user credentials for itself, and also forwards the same to AAAL. In AAAL, the authorization is validated, and the reply is sent to the router with AAA reply. The router adds the host address in its neighbour cache if the authorization succeeds. The advantage of this method is that, the number of transactions made for messages is reduced.[4]

For a stateful address autoconfiguration, like DHCP the clients first send DHCP solicitation request to the DHCP servers in the network. When the AAA authorization is required, the DHCP request message with the MN-NAI extension containing the AAA data is sent to the DHCP server by the DHCP client. The DHCP server extracts the NAI and AAA data from the extensions and sends to AAAL. From AAAL, the data is forwarded to AAAH through the AAA network, where the user credentials are processed. AAAH creates a reply message based on the processed user credentials and it is sent to AAL, DHCP server and to the DHCP client. The reply received by AAAL from AAAH is interpreted to separate the required details, and determine the details to be delivered to the DHCP server and to the local network. The reply from AAAL, is used by the DHCP server to create a DHCP reply message containing the acceptance or rejectance of the lease with MN-AAA extension and the encrypted data received from the DHCP client. [4]

### 4.3 Existing AAA protocols

The Remote Authentication Dial In User Service (RADIUS)[14] and DIAMETER[11] are popular among the existing AAA protocols.

RADIUS is not a perfect architecture as it is vulberable to security attacks. Confidentiality during transfer of data is not guaranteed in RADIUS as it does not provide end-to-end security. Therefore, it is subjected to attribute editing, password theft, account modification and action replay attacks. Also, it does not support notification or retransmission of lost data.

DIAMETER is designed to overcome the inefficiencies of RADIUS. It uses the extensions for application specific implementations. It guarantees data integrity and confidentiality. It has the ability to notify the server in case of lost data and error messages could be sent to the client.

## 5. CONCLUSION

The implementation of AAA for Mobile IP involves complex issues such as security, message transaction and decision making. Comparing the implementation issues in IPv4 and IPv6 versions, IPv6 has desirable merits namely, IPSec and address management. Therefore, standardising and implementing the AAAv6 architecture will be helpful when the complete transition from IPv4 to IPv6 occurs.

Moreover, the three modules of AAA are interdependent. Hence, all the three modules has to be defined and designed clearly such that it should be transparent to the end users, irrespective of the IP version used. The number of data transactions involved in the authorization procedure has to be reduced. The AAA server should be prepared to handle any number of requests at the same time.

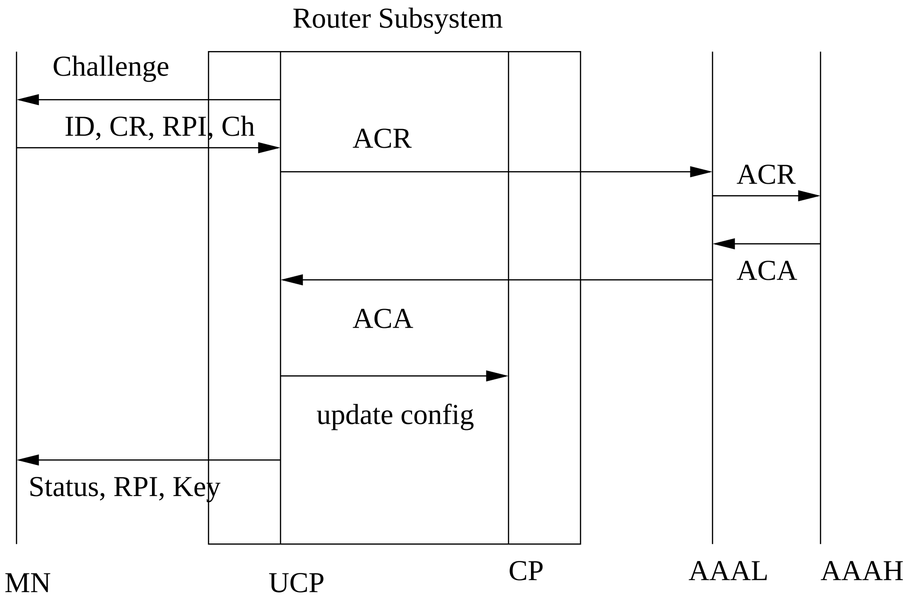
The future work of AAA for Mobile IPv6, needs more study on the policy rules, to determine the authentication and authorization of the subscriber. To ensure confidentiality and to avoid the security attacks as discussed in subsection. 4.3, end-to-end security should be guaranteed. The use of digital signatures can be efficiently implemented to overcome the security issues. Once the mobile networking becomes a user friendly technology, AAA will have its powerful role to play.

## REFERENCES

[1] Aboba, B., and Beadles, M., The Network Access Identifier, RFC 2486. Online, January 1999, referred to 24.10.2002.
URL:http://www.faqs.org/rfcs/rfc2486.html

[2] Aboba, B., and Vollbrecht, J., Proxy chaining and Policy Implementation in Roaming, RFC 2607. Online, June 1999, referred to 27.10.2002.
URL:http://www.zvon.org/tmRFC/RFC2607/Output/frontpage.html

[3] Aboda, B.,Arkko, J., and Harrington, D., Introduction to Accounting Management, Internet Draft. Online January 2000, referred to 30.9.2002.



UCP-Uncontrolled Part; CP-Controlled Part;
ACR-Acknowledgement Request; ACA-Acknowledgement Acceptance.

Fig. 3. General AAAv6 Overview
[5]

URL: http://www.ietf.org/internet-drafts/ draft-ietf-aaa-acct-00-txt

[4] Asokan, N.,Patrik, F., Charles, E.P., and Thomas, E., AAA for IPv6 Network Access, Internet Draft. Online, 10.3.2000, referred to 24.10.2002. URL:http://people.nokia.net/~charliep/txt/ aaav6/aaav6.txt

[5] Charles, E.P., Patrik, F., and Thomas, E., AAAv6. Online, September 2001, referred to 23.10.2002. URL:http://www.ietf.org/proceedings/01aug/slides/ urp-8/s1d003.html

[6] Cisco Systems, Overview Authentication, Authorizing and Accounting. Online, November 2001, referred to 28.10.2002. URL:http://www.cisco.com/warp/public/cc/pd/iosw/ prodlit/aaans_ov.html

[7] David, B.J., Charles, E.P., and Arkko, J., Mobility Support in IPv6, Internet Draft. Online, Updated June 2002. referred to 28.9.2002. URL:http://www.ietf.org/internet-drafts/ draft-ietf-mobileip-ipv6-18.txt

[8] Glass, S., Hiller, T., Jacobs, S., and Perkins, C., Mobile IP Authentication, Authorization, and Accounting Requirements. RFC 2977, Online, October 2000, referred to 15.10.2002. URL:http://www.faqs.org/rfcs/rfc2977.html

[9] Marc Danzeisan, Secure Mobile IP Communication. Der Philosophisch- naturwissensschaftlichen Fakultt, Diplomarbeit,der Universitt Bern Online 2001, 56 p, referred to 6.10.2002. URL:http://www.iam.unibe.ch/~rvs/publications/ SecMIP.pdf

[10] Narten, T., Nordmark, E., and Simpson, W., Neighbor Discovery for IP Version 6 (ipv6), RFC 2461. Online, December 1998, referred to 30.9.2002. URL:http://www.faqs.org/rfcs/rfc2461.html

[11] Pat, R.C., Comparison of DIAMETER Against AAA Network Access Requirements. Internet Draft. Online, April 2000, referred to 27.10.2002. URL:http://www.diameter.org/drafts/latest/ draft-calhoun-aaa-diameter-comp-00.txt

[12] Perkins, C., IP Mobility Support, RFC 2002. Online, Updated October 1996, referred to 24.9.2002. URL:http://www.ietf.org/rfc/rfc2002.txt

[13] Perkins, E.P, Mobile Networking Through Mobile IP. Online, referred to 26.9.2002. URL:http://www.computer.org/internet/ v2n1/perkins.html

[14] Rigney, C., Rubens, A., Simpson, W., and Willens, S., Remote Authentication Dial In User Service (RADIUS), RFC 2138. Online, April 1997, referred to 27.10.2002. URL: http://www.ietf.org/rfc/rfc2138.txt

[15] Simpson, W., The Point-to-Point Protocol, RFC 1661. Online, July 1994, referred to 24.10.2002. URL:http://www.cis.ohio-state.edu/cgi-bin/ rfc/rfc1661.html

[16] Tuomas Kivinen, Authentication methods for Mobile IP, Master's Thesis, Helsinki University of Technology, Presented March 2001, referred to 3.10.2002.