AAA Working Group
John Wang
Motorola

Internet Draft
Rong Wang
Motorola
Document: <draft-wang-aaa-cel-req-00.txt>

Expire: April 20, 2000
October 20, 1999

Cellular Network Authentication, Authorization, and Accounting Requirements
<draft-wang-aaa-cel-req-00.txt>

Status of this Memo

1. Abstract

The AAA Working group is currently looking at defining the requirements for Authentication, Authorization and Accounting. This document contains the requirements that should be supported within AAA to aid in providing next generation cellular services.

2. Conventions used in this document

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC-2119 [2].

3. Background

There is a trend in the cellular industry to support next generation cellular services based on IP technology.

The current IP network is designed for stationary or portable commuting. There are fundamental differences between portable commuting and cellular applications. In cellular industry the following issues are of great concern: the limited over-the-air capacity, the restricted computing power and power supply of Mobile Station (MS), the latency consideration for real time applications, and the mobility behavior of MS etc. These lead to some stringent requirements on the IP network as a whole.

Next generation cellular applications will raise the requirements on IP network even higher. There are two fundamental factors that clearly differentiate the new generation from the current cellular applications: global coverage and multi-mode MS with integrated service.

AAA functionality, among with others such as mobility management and call control, is an integral part of system management. To ensure efficient system implementation, the architecture and functionality of the overall system management functions must be compatible.

This document defines AAA requirements for the next generation cellular services targeting an integrated system management architecture with high quality and overall system efficiency.

4. Terminology

Access Network
: The access network provides the basic transmission, local control and management functions needed for the terminal device to access the resources of the Core Network.

Core Network
: The next generation core network should provide the transmission, switching, control and management functions needed to connect the Access Network to other networks. The intent is that Core Network hide all nuances specific to a given network technology from the Access Network.

Foreign Agent (FA)
A router on a mobile node's visited network which provides routing services to the mobile node while

registered. The foreign agent de-tunnels and delivers datagrams to the mobile node. For datagrams sent by a mobile node, the foreign agent may serve as a default router for registered mobile nodes.

Home Agent (HA)
A router on a mobile node's home network which, when the mobile node is away from home, receives traffic for the mobile node, tunnels these datagrams for delivery to the mobile node, and maintains current location information for the mobile node.

Home Location Register (HLR)
The functional entity that provides the primary database repository of subscriber information used to provide control and intelligence in cellular and wireless networks.

Integrated Service
A service that is capable of supporting multiple access technologies in a resource, cost and latency efficient way.

Mobile Node (MN)
A host that changes its point of attachment from one network or sub-network to another.

Mobile Station (MS)
The mobile of portable subscriber radio-telephone equipment.

Multi-mode MS
MS capable of accessing multiple access networks (possible simultaneously).

5. Utilization of AAA Functions in Current Cellular Networks

In cellular network, authentication is a set of functions used to prevent fraudulent access to cellular networks by devices illegally programmed with counterfeit Mobile Identification Number (MIN) and Electronic Serial Number (ESN) information [3]. A successful mobile-to-network authentication occurs when the MS demonstrates its possession of assigned secret authentication information to network.

This can be achieved by showing calculation results based on the authentication information in such a way that the network can verify its correctness. A centralized Authentication Center (AC) is the primary functional entity in the current cellular network responsible for managing the authentication information, although the serving system may also be allocated certain responsibilities.

The authentication process can be invoked by many events. It is performed most often in the following situations:

- Registration
- Call Origination
- Call Termination

6. AAA Considerations in Next Generation Cellular Network

As cellular networks migrate to an integrated architecture, there are new situations that must be considered when designing the AAA solution.

6.1 Integrated Mobility Management and AAA

Mobile IP [3] enables a mobile node to change its attachment point on the Internet while maintaining its IP address as well as network connectivity. As a mobility management protocol, Mobile IP is suitable for portable computing but it is not efficient enough for cellular applications. Tromboning is one major issue in Mobile IP when used in a cellular network [4].

There have been many efforts to make Mobile IP more efficient. Some of the leading efforts include the route optimization [5] and Mobile IP regional tunnel management [6] techniques. These technologies are based on a hierarchical location database architecture to provide ways to update the MN location information and to make it possible to connect a call based on local information rather than reference to the Home Agent(HA).

The mobility management functions (e.g. registration, handoff functions) tie directly with the AAA functions. It is preferable that AAA and mobility management functions are integrated together.

6.2 Integrated AAA Architecture for Integrated Access Networks

Currently, each access network technology has its own authentication and authorization process. For example, access authentication/authorization in a cellular network is carried out through messages between MS, its Home Location Register (HLR) and a

centralized Authentication Center. Meanwhile, access authentication/authorization in Mobile IP is done through messaging between the Mobile Node (MN), its HA, Foreign Agent (FA) and AAA server(s).

An integrated AAA architecture cross access technology provides an opportunity for creating a unified AAA interface for integrated services.

6.3 Addressing

To function properly in an integrated network, it is indispensable to have an unique address to identify the end user or the customer device.

It is a general practice in existing cellular industry to adopt a topology dependent address that is directly routable without consulting any centralized global database. It is of crucial importance for IP network to maintain this feature for cellular or other real time applications due to efficiency and latency considerations. Consequently, AAA solution must be able to support topology dependent address as well.

6.4 Independent of Radio Access Technologies

Multiple radio access technologies (e.g. Global System for Mobile Communication and Code-Division Multiple Access) exist in the cellular network. AAA functions should be independent of the air interface protocol used to access the network.

7. Cellular Service Requirements on AAA

Based on the above scenarios of cellular networks/services, the following specific requirements for AAA can be ascertained.

- The AAA server SHOULD be able to support mobility management with a layered and distributed architecture efficiently.

- AAA SHOULD be able to work in an integrated mobility management and AAA framework to offer the most efficient solution.

- AAA SHOULD be able to offer an integrated and efficient solution for a customer with multi-mode capable MS.

- AAA MUST be able to provide mutual authentication functionality for MS and the network(s). And the AAA solution MUST be scalable.

- AAA MUST support mutual authenticated key agreement to provide keys for message privacy and integrity.

- AAA MUST be able to work with the topology dependent address.

- AAA MUST support message privacy and integrity.

- The AAA solution MUST be able to support device roaming.

- The AAA solution SHOULD be able to support user roaming.

- AAA MUST support the option for AC to share some temporary secret information about a MS or subscriber with serving system in a secure and efficient way.

- AAA SHOULD provide flexible period key update.

- There SHOULD NOT be any assumptions on the access network technologies for AAA solutions.

8. Security Considerations

This draft defines the AAA requirements for the next generation cellular services. As AAA is security driven, most of this document addresses the security considerations AAA must make on behalf of cellular services.

9. References

1 Bradner, S., "The Internet Standards Process -- Revision 3", BCP 9, RFC 2026, October 1996.

2 Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997

3 Perkins, C., editor, "IP mobility support", RFC 2002, October 1996

4 Gallagher M. and Snyder R., "Mobile Telecommunications Networking with IS-41", McGraw-Hill, 1997

5 Perkins, C. et. al., "draft-ietf-mobileip-optim-08.txt: Route Optimization in Mobile IP", Internet Draft, February 1999

6 Gustafsson, E. et. al., "draft-ietf-mobileip-reg-tunnel-01.txt: Mobile IP Regional Tunnel Management", Internet Draft, August 1999

10. Acknowledgement

Many thanks to Phil Roberts, Dan Brown and Lily Chen at Motorola for their valuable comments and support.

11. Author's Addresses

John Wang
Motorola Inc.
1501 W. Shure Dr.
Arlington Heights, IL 60004, USA
Phone: (847) 435-2710
Email: ezw001@email.mot.com

Rong Wang
Motorola Inc.

1501 W. Shure Dr.
Arlington Heights, IL 60004, USA
Phone: (847) 632-2647
Email: rwang1@email.mot.com