

# A-IMS Architecture Analysis and Experimental IPv6 Testbed

A. Dutta, F.J. Lin, S. Das, D. Chee, B Lyles  
Telcordia Technologies, Piscataway, New Jersey, 08854  
T.Chiba, H. Yokota, KDDI R&D Labs, Japan  
H. Schulzrinne, Columbia University, New York

*Abstract*— Advances to IMS (A-IMS) architecture extends the existing IMS/MMD architecture currently being defined in 3GPP/3GPP2 respectively so that it can support both SIP and non-SIP-based services. We describe the key strength of A-IMS architecture, compare the benefits over MMD architecture, and then describe an enhanced MMD experimental testbed to demonstrate many of the A-IMS features. We highlight many of the functional components of the testbed that perform several operations such as signaling, location management, security, and mobility. We experiment with two different mobility management techniques and analyze the associated delays and packet loss for both 802.11 networks and PPP networks. We illustrate the service interaction between SIP-based services such as VoIP and non-SIP-based services such as IPTV. Analysis from these experimental results and testbed implementation can be useful to any service provider that plans to deploy IMS/MMD architecture over IPv6.

*Index Terms*— A-IMS, IPTV, IPv6, MMD, Mobility, Testbed

## I. INTRODUCTION

Wireless service providers strive to preserve the quality of service and user experience for the mobile users. However, in order to make a successful transition from current cellular-based architecture to next generation IP-based networks, they need advanced architecture and operations support systems. 3GPP (Third Generation Partnership Project) [1] and 3GPP2 (Third Generation Partnership Project 2) [2] are defining the IP Multimedia Subsystem (IMS) and Multimedia Domain (MMD) architecture respectively, that can be used as a platform to provide secured and seamless services to these roaming users over IPv6 network. In order to be able to provide variety of services in a roaming environment, a carrier has to investigate the deployment issues, such as type of application supported, roaming agreement between the carriers, and heterogeneity of the mobility protocols. In order to take care of some of the gaps in the current version of IMS/MMD architecture, a new design specification is being proposed called advances in IMS (A-IMS) [3]. Many of the wireless carriers who are currently implementing MMD networks, can easily implement A-IMS but initially may like to map only some of the A-IMS functionality to MMD whenever required. Thus, it is important to analyze the benefits of the

proposed A-IMS architecture compared to existing IMS/MMD networks. Testbed realization of this standardized architecture can help to investigate the underlying networking issues that might affect the end user performance. In this paper, we analyze the A-IMS architecture, study the gap and then provide a guideline of what A-IMS components can be used to enhance the existing IMS/MMD architecture and testbed [4]. We also describe the experimental testbed where we have demonstrated both application layer and network layer mobility over heterogeneous networks and feature interaction between VoIP and IPTV service.

This paper is organized as follows. Section II provides the overview of A-IMS and its key strengths compared to MMD. Section III discusses the recommended A-IMS functions that could be applied to an existing MMD architecture. We describe an experimental A-IMS testbed and realization of advanced features in Section IV. Finally, Section V concludes the paper.

## II. A-IMS OVERVIEW

IMS (Advances to IMS) [3] is an architecture proposed by few carriers and equipment manufacturers. A-IMS offers certain benefits over IMS and MMD architecture currently being defined in 3GPP and 3GPP2 respectively. According to the specification, A-IMS takes care of a number of shortcomings and deficiencies with the existing IMS/MMD standards. A-IMS is an enhanced evolution of existing IMS/MMD standards and provides a level of control and security superior to that of the IMS/MMD approach. To understand A-IMS, it is important to know what shortcomings and deficiencies of the existing IMS/MMS standards that A-IMS intends to address.

Figure 1 shows the overview of A-IMS architecture. Key A-IMS components include: Application Manager (AM), Service Broker (SB), Policy Manager (PM), Bearer Manager (BM), IP Gateway (IPGW), Service Data Manager (SDM), Security Manager (SM), Key Management Function (KMF). We describe the details of some of these functional components:

**Policy Manager:** It coordinates overall network resource usage for both SIP and non-SIP applications. The PDF (Policy Decision Function) or PCRF (Policy Control Rules Function) defined in IMS/MMD is tied closely to the SIP services. A-IMS decouples this tie and designates a Policy Manager to support both SIP and non-SIP applications. The PM implements both subscriber specific policies and network specific policies for both SIP and non-SIP applications.

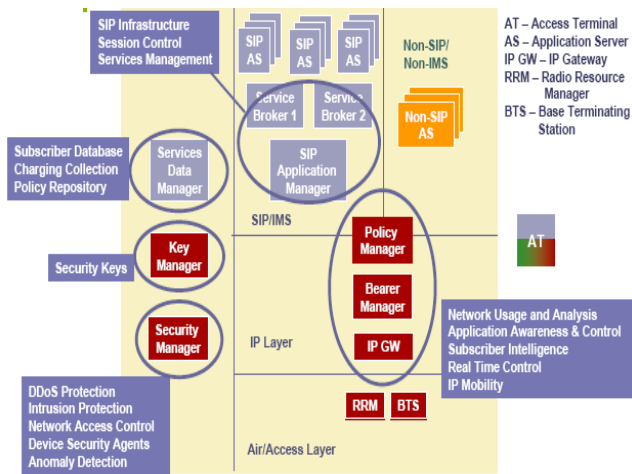


Figure 1. A-IMS Architecture Overview

**IP Gateway (IPGW):** The IPGW is the first network layer component in the network. It enables a unified way to handle multiple types of access networks, in an access independent way. It provides the following IP functions: Layer 3 authentication of the Access Terminal (AT), IP address assignment, accounting and QoS functions, handoff and context transfer, policing, marking, and gating of IP packets and flows.

**Security Manager:** In existing IMS/MMD, there is no dedicated network component for security management; security management and procedures are distributed in the network and carried out by S-CSCF, HSS, P-CSCF, and AT. In A-IMS, Security Manager is designated as a dedicated server that manages security policies. Also, all security keys are separated from the HSS and kept in a separate Key Management Function (KMF). One of the Security Manager's functions is MSA-MC (MSA Master Controller) that interacts with the MSAs on IATs (Intelligent ATs) to detect and prevent potential attacks from intelligent devices. The SM gathers security events information from all A-IMS components including Access Terminals (ATs). It owns the security policies (different from functional policies managed by the PM) for the network, pushing these policies to various A-IMS components. It provides intrusion detection, network infrastructure security, and traffic anomaly detection.

**Bearer Manager:** The BM (Bearer Manager) is the IP anchor point (home or visited) for Mobile IP that acts as the enforcement point for both network and subscriber specific policies. The BM provides the following bearer related services: Mobile services, Admission control, Packet classification for services and for security, QoS policy enforcement services, Network security enforcement services, Charging/accounting services, Lawful intercept services, Location and presence services. Unlike existing IMS/MMD, the A-IMS adopts the concept of dual anchoring and dual IP addresses via the use of Bearer Managers (BMs) in home and visited networks. For an AT roaming to a visited network, it has the option of anchoring its address on the Home BM or Visited BM.

**Application Manager (AM):** The AM performs similar functions as Call Session Control Functions (P-CSCF, S-CSCF, I-CSCF) and PSTN Routing (BGCF) defined in IMS. The AM interfaces with Policy Manager, Service Broker, SIP Application Server, Service Data Manager, Media Server, and PSTN Gateway. The AM supports SIP services but allows interactions with non-SIP services.

**Service Broker (SB):** The SB works with the Application Server, Application Manager, Policy Manager, and Security Manager to manage service interactions. The SB handles service interactions that cannot be resolved by Application Manager. The SB works with Policy Manager to resolve service interactions resulting from conflicting resource requirements among SIP and non-SIP applications. The SB works with Security Manager to resolve service interactions resulting from conflicting security policies between applications.

**Service Data Manager (SDM):** The SDM is the central repository of subscriber data in the network, providing, HSS services, Layer-3 and optional Layer-2 AAA services, Network/subscriber policy database, Capabilities for online & offline charging, Interfacing with Provisioning Systems to allow storage and retrieval of subscriber data into and out of it.

**Key Management Function:** The KMF is responsible for the storage of subscriber and network keys for the implementation of A-IMS authentication services. It typically resides within the Security Manager or the Service Data Manager.

### III. A-IMS FUNCTIONS FOR ENHANCED MMD ARCHITECTURE

This section provides a description of A-IMS functions that can be added to enhance the current MMD architecture.

#### A. Interaction between SIP and non-SIP applications:

The lack of support for non-SIP-based applications and products is the biggest concern for the current IMS/MMD architecture. A-IMS architecture not only accommodates both SIP and non-SIP services but also allows interactions and integration of both types of services. To support a wide range of applications over the MMD, both SIP and non-SIP applications should be included in the MMD architecture. To accomplish this goal, network components equivalent to the A-IMS Policy Manager and Service Broker need to be added to the MMD architecture and the P-CSCF, S-CSCF in MMD that correspond to the AM in A-IMS have to be enhanced as indicated in the example in Section 2. To support non-SIP applications, new application interfaces need to be defined between P-CSCF and non-SIP applications such as IPTV. The P-CSCF and S-CSCF in MMD need to interact with both the PCRF and the Service Broker to manage service interactions among SIP and non-SIP applications. It communicates with the PCRF for admission and preemption control between SIP and non-SIP applications. It also communicates with the Service Broker in order to know how to invoke SIP and non-SIP applications and manage their interactions.

### B. Dual Anchoring and Dual Addresses for the Access Terminal:

A-IMS allows dual anchoring and dual addresses for an Access Terminal in order to reduce mobile VoIP latency over CDMA 1xEV-DO Rev.A networks. This technique can be adopted into the MMD architecture to improve the quality of mobile VoIP services in the CDMA2000 network. The A-IMS assumes that the AT can support client MIPv6 or Simple IP, and both the home network and the visited network may support Client MIPv6 and Proxy MIPv6. Nevertheless, these assumptions may not be true in the existing MMD networks. As a result, the dual anchoring and dual addresses approach defined by A-IMS need to be modified and adjusted accordingly. One example could be what if the AT doesn't support the MIPv6 but only Simple IPv6 and what if both the home network and the visited network don't support CMIPv6 or PMIPv6 etc.

**C. IPTV Architectures and Services:** A-IMS architecture can offer both SIP-based and non-SIP-based services. Ideally, non-SIP-based services do not use SIP signaling and do not need to traverse through any of the SIP-based components such as P-CSCF, I-CSCF, S-CSCF. However, non-SIP-based services also have to interact with other IMS components such as PCRF to control the interaction between SIP and non-SIP based services. Some of the examples of non-SIP-based services are: ftp, email, telnet, IPTV.

**D. Home Address Anonymity:** In most mobility protocols, the same address is used for both SIP signaling and media traffic. However, this represents a potential security risk because the mobile node registers its home address with the SIP server while the address is supposed to be a private user information. In general, after the completion of SIP signaling, each communicating node knows the IP address of the media and can send traffic directly or via HA. Thus, there is a chance of denial of service attack if a permanent address, such as home address is used. Since SIP URIs (Uniform Resource Identifiers) are used for setting up a call, the home address that is used for SIP signaling address is not exposed to the communicating user. We take advantage of the multiple addressing scheme associated with IPv6 and resolve this security concern to avoid the risk of denial of service attacks. Thus, the home address is not used for media traffic. SIP signaling and media use different IP addresses.

**E. Expedited Media Delivery:** We propose using the home address of the mobile node for SIP signaling but we assign temporary addresses to the mobile node for media communication. When both the mobiles are in a roaming mode and away from home, using the temporary addresses from visited networks as the media address, media traversal delay is reduced. Thus, if a different IP address is used for media and the SIP signaling address, media traversal can be limited to the visited domain when both the communicating nodes are away from the home domain.

### IV. A-IMS EXPERIMENTAL IPV6 TESTBED

In this section, we describe the experimental A-IMS testbed and many of the supported features including mobility, SIP-based, and non-SIP-based services. Figure 2 shows the experimental IPv6 testbed with different functional components. We have prototyped many of the IMS components such as P-CSCF, I-CSCF, and S-CSCF for signaling, HSS for registration function, Home Agent for the bearer manager functions, PCRF for policy control functions, PDSN and PDIF for access networks, IPTV server for non-SIP-based services. We briefly explain the functional components of the testbed and then explain more details about the mobility features. Current testbed has one home network and two visited networks. The experiments are based on mobile's movement between the visited networks.

**Radio Access Networks:** Currently, we have configured two kinds of radio access networks in the A-IMS testbed, such as WiFi (802.11) and CDMA2000. In the absence of real CDMA networks, we have emulated CDMA2000 using PPPoE and RAN emulator. Thus, the current testbed provides the ability to support the handoff between WiFi and PPP networks.

**Address Configuration:** Since the end hosts are IPv6-enabled, we have implemented both PPP and stateless modes of auto-configuring the IP addresses. In stateless mode, the mobile configures its IP address based on the prefix of the router advertisement. In PPPoE mode, the prefix is provided to the mobile by the PDSN.

**Server Discovery:** Server discovery is a process of discovering the addresses of the outbound SIP servers in each subnet. P-CSCFs are the outbound SIP servers in each network. After configuring an IP address, the mobile uses DHCP INFORM message to obtain the IP address of the server. As the mobile changes its network, it rediscovers a new P-CSCF in each subnet.

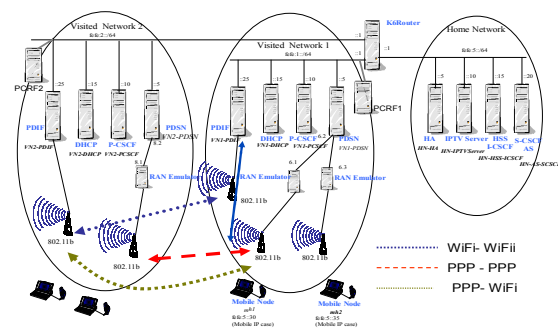


Figure 2: Enhanced IMS/MMD Mobility Testbed

SIP registration (re-registration), SIP INVITE (re-INVITE) use the newly discovered proxy to send these messages.

**Registration:** Registration is a process by which the mobile communicates with the network to establish its new association

with the network. The mobile is a SIP client that has a unique URI (Universal Resource Identifier). It registers with the HSS (Home Subscriber System), via the current P-CSCF in the subnet. Registration message actually travels via I-CSCF and S-CSCF. S-CSCF and HSS communicate with each other using Diameter protocol.

**Multimedia Call setup:** Since SIP is used as the signaling protocol, the mobile users can communicate with each other using SIP URI. Both the mobile users update their updated address-of-records and care-of-proxy servers with the S-CSCF in the home domain. If MIP is used, home address is used as the address-of-record and the mobile just uses the new outbound proxy server. Thus, any new call gets routed via S-CSCF, HA, and P-CSCF before reaching the callee. But, if application layer mobility is used, then the mobile uses new care-of-address as the new address-of-record during SIP registration. In the absence of HA, the new call gets routed to P-CSCF directly without being routed to home.

**Security Association:** AKA (Authentication and Key Exchange) is a way of making sure that the mobile is authenticated and there is a security association between the mobile and the P-CSCF. AKA procedure is performed during mobile's SIP registration with S-CSCF. During the AKA procedure, the IPSEC SA is established between MN and P-CSCF. Once the security association is established, PCRF is informed and the gating on the PDSN or PDIF is turned on.

**Mobility Support:** Current version of A-IMS testbed can provide both network layer and application layer mobility support. As part of network layer mobility support, we have implemented MIPv6 [5], and as part of application layer mobility we have implemented SIP-based mobility [6]. The mobile can either be connected to a PDIF over 802.11 network or PDSN over PPPoE (PPPoE over Ethernet). We describe both the network layer mobility and application layer mobility and evaluate their performance.

**Network Layer Mobility:** Figure 3 shows the protocol flow for MIPv6-assisted handover between WiFi networks. There are several stages of operation involved during the handover from one visited network to another. Initially, mobile discovers the new network resources, and attempts to connect to the new network. After the layer 2 association is complete, the mobile sends a Router Solicitation (RS) to the router that triggers the router advertisement. The mobile learns the prefix from the router advertisement. The mobile then configures its interface with a new address. The mobile performs a Duplicate Address Detection [6] before it can start communicating successfully. Upon completion of the new IP address, the mobile sends a binding update to the Home Agent and also to the correspondent node. After learning the new P-CSCF address via DHCP, the mobile also registers with S-CSCF and notifies its new outbound proxy server. If there is any other SDP related changes such as Codec parameters, then the mobile also sends a re-INVITE to the correspondent host. In our experiment, since media and signaling addresses are split, we

also send new IP address for the media as part of the re-INVITE.

Mobility using MIPv6 can be used in two ways. In one case, both signaling and media addresses are split and in another case, the mobile uses the home address both as the signaling and media address. In split case, the mobile has assigned two IPv6 addresses, IP0 and IP1 to its interface using stateless auto-configuration [10]. Both IP0 and IP1 however have the same prefix. Mobile has a home address IP<sub>h</sub> that is configured using the home agent prefix. The mobile uses IP<sub>h</sub> as its contact address for SIP REGISTER and SIP INVITE messages during registration and call setup respectively. But the mobile uses IP1 as part of its SDP address in the INVITE. After the mobile moves to the new visited network, it auto-configures the two new addresses, IP2 and IP3. Using the new prefix, MN sends a binding update to HA that associates IP1 with the mobile's home address IP<sub>h</sub>. The mobile could use the new IP address IP3 in the SDP as part of Re-INVITE or MIPv6 route optimization. We have shown the results of non-split case in our experiment.

**Application Layer Mobility:** In some situations, application layer mobility is the preferred way of taking care of handoff. SIP-based mobility [7] is one way of providing the application layer mobility. In this case, there is no additional home agent in the home network and thus there is no indirection. Similar to MIPv6, we prototyped the application layer mobility involving handoff between WiFi networks and point-to-point (PPP) networks.

It takes advantage of the underlying SIP-layer signaling to take care of the session continuity between the mobile and correspondent node. Figure 4 shows an example call flow of SIP-based mobility involving two 802.11 networks. In the absence of MIPv6, there is no layer 3 binding update here.

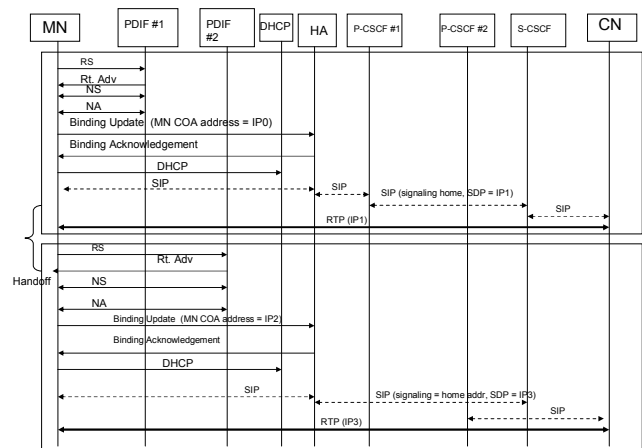


Figure 3: Network layer mobility over WiFi networks

We have also prototyped network layer mobility and application layer mobility over PPPoE. However, in case of PPP, interface-id will be assigned through IPv6CP by the

PDSN and prefix will be assigned through router advertisement over the PPP link.

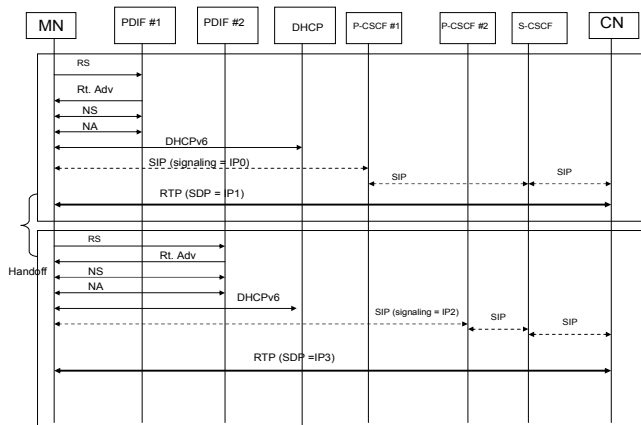


Figure 4: Application layer mobility over WiFi networks

In case of PPP networks, the mobile does not need to perform DAD (Duplicate Address Detection) [7] procedure to determine the uniqueness of the address assigned. In the absence of DAD the mobile does not suffer from extra delay associated with NUD (Neighbor Unreachability Detection). Unlike MIPv6, during SIP-based mobility over PPPoE, there is no permanent home address. Thus, the mobile uses IP0 as the signaling address for SIP INVITE and REGISTER and uses IP1 as the SDP address for media transmission.

Similarly, after the mobile has moved to the new network, it auto-configures two new addresses (IP2 and IP3) with the new prefix. It however uses IP2 as the signaling address and IP3 as the new media address that is conveyed to the CN via re-INVITE. We needed to add support for fast router selection mechanism [11] so that the delay due to network detection can be reduced during handoff from one network to another in case of SIP-based mobility. Figure 4 shows the results from handoff operation when network layer and application layer mobility protocols are used to support handoff for both 802.11 and PPP networks. Figure 4 illustrates time taken to complete several primitive functional operations during each handoff.

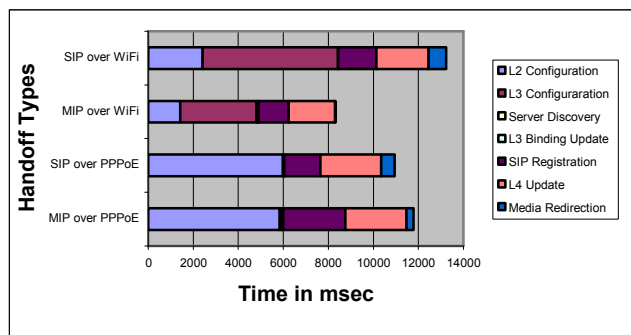


Figure 4: Time taken for various mobility functions

Handoff delay in either case will depend upon whether gating is applied on the access gateway or not. Layer 2 delay for PPPoE is inclusive of the delay of 802.11 delays. SIP-based

mobility does not have layer 3 binding update, so the mobile will need to wait until the layer 4 update is complete as part of re-INVITE process. It appears layer 4 update takes more time because it deals with application layer processing. However, in case of MIPv6, media can flow right after the layer 3 binding update is complete. But MIPv6-based mobility can use Layer 4 update (i.e. re-INVITE) to provide additional functionalities, such as QoS gating and Codec negotiation of the end points. Layer 3 configuration is negligible in case of PPP network compared to WiFi case, since there is no duplicate address detection. Optimization techniques for operations at each layer can further reduce the delay to an acceptable level.

## V. CONCLUSIONS

In order to be able to provide cellular-like dependable but more flexible services, current carriers will need to upgrade their existing infrastructure to an IPv6-based network. 3GPP and 3GPP2 in collaboration with the IETF are defining architectures and operation support systems (OSS) to support the next generation IPv6 networks. However, A-IMS proposed recently provides many of the added benefits and support for non-SIP-based services. We provided a functional analysis of A-IMS and its added benefits. The experimental IPv6-based mobility testbed based on A-IMS architecture shows how both network layer and application layer mobility protocols can be used to support mobility between 802.11 and cellular type PPP networks. This testbed also implements how SIP-based (e.g., VoIP) and non-SIP-based (e.g., IPTV) services can be supported and can coexist using standards-based IETF protocols such as SIP, MIPv6, RTSP, and Diameter.

## REFERENCES

- [1] 3GPP TS 23.218: 3rd Generation Partnership Project: Technical Specification Group Core Network; IP Multimedia Session handling; IM call Model
- [2] 3GPP2 X.S0013-004-0 v2.0: All-IP Core Network Multimedia Domain: IP Multimedia Call Control based on SIP and SDP
- [3] K. Bogineni et al, "Advances to IP multimedia subsystem," Cisco News Release, July 2006
- [4] A. Dutta et al, "Mobility Testbed 3GPP2 MMD Networks," IEEE Communication Magazine, July 2007
- [5] D. Johnson, C. Perkins and J. Arkko, "Mobility Support in IPv6, RFC 3775," June 2004
- [6] H. Schulzrinne and E. Wedlund, "Application Layer Mobility using SIP," vol 4, ACM MC2R, July 2000
- [7] T. Narten et al, "Neighbor Discovery for IPv6," RFC 2461, Dec 1998
- [8] H. Schulzrinne et al, "Real Time Streaming Protocol," RFC 2326, April 1998
- [9] P. Calhoun et al, "Diameter Base Protocol," IETF RFC 3588, Sep. 2003.
- [10] S. Thomson and T. Narten, "IPv6 Stateless Auto-configuration of IPv6 networks," RFC 2462, Dec 1998
- [11] N. Nakajima et al, "Handoff Delay analysis and measurement for SIP-based mobility in IPv6," IEEE ICC 2003 Anchorage.