

Mobility Management Schemes for Heterogeneity Support in Next Generation Wireless Networks

Tsunehiko Chiba, Hidetoshi Yokota, Akira Idoue
{t-chiba, yokota, idoue}@kddilabs.jp, KDDI R&D Laboratories, Inc.
Ashutosh Dutta, Subir Das, Fuchun J. Lin
{adutta, subir, fjlin}@research.telcordia.com, Telcordia Technologies, Inc.
Henning Schulzrinne
hgs@cs.columbia.edu, Columbia University

Abstract – Seamless mobility support in a heterogeneous roaming environment poses several challenging issues in the choice of network architecture design and mobility protocol. Several standards organizations are designing next generation wireless network architectures with a suite of new network elements and protocols that provide service continuity for intra- and inter-provider roaming. However, each of these mobility solutions provides its own set of signaling mechanisms and methods of interaction with different functional network elements. Thus, it becomes a challenging task for the network operators and service providers to support roaming to the visited networks with diverse capabilities while supporting service continuity. In this paper, we first highlight some of the next generation standards and then describe the main functional components of a generic next generation wireless architecture as described in several evolving standards. We then focus on the operational usage of network layer mobility protocols such as Client Mobile IP, Proxy Mobile IP and application layer mobility protocol for next generation networks, and address the operational issues associated with roaming and service continuity. Finally, we propose comprehensive mobility solutions that support the heterogeneity associated with the intra- and inter-provider roaming.

Index term – Roaming, Mobility, Wireless Networks, Heterogeneity, IMS/MMD

I. INTRODUCTION

Ubiquitous roaming support for real-time traffic, such as interactive VoIP, streaming, and the non-real-time data transfer of FTP and e-mail in an access independent manner, is becoming increasingly important. The evolution of the mobility protocols of MIPv4 (Mobile IPv4) [1] and MIPv6 (Mobile IPv6) [2] has made it easier to support ubiquitous roaming. However, challenges remain for providing suitable mobility solutions with consideration of quality of service, security and charging. In this paper, we focus on the challenges involved with seamless mobility support during intra- and inter-provider roaming. A mobile node's (MN's) movement within next generation wireless networks can be confined to the home domain or the visited domain. When the mobile node is outside the home domain and within the visited domain, it is said to be in roaming status. When the mobile node is in the roaming mode, it can also move between two sub-networks within the same domain or it can move from one domain to another domain.

Roaming involves several levels of heterogeneity, such as the types of mobility supported in the network elements and in the mobile node, the type of application supported on the

device, and the type of movement within both the home and visited domain. In a typical roaming environment, two domains can belong to two different carriers with different mobility support and security and authentication procedures. Also, we address the issues related to IP address hiding by adopting multiple-IP addressing approaches where media and SIP [3] signaling use different IP addresses. A combination of application layer, network layer, and local mobility protocol can be used, depending on the mobile node's movement pattern, the device and network mobility capability, and the type of application. We primarily consider mobility options that include CMIPv6 (Client Mobile IP) and PMIPv6 (Proxy Mobile IPv6) [4] for a generic next generation wireless network architecture that could be applicable to different types of roaming scenarios.

The remainder of the paper is organized as follows. In Section II, we provide examples of some of the mobility architectures being standardized and illustrate the functional components of a generic architecture for our analysis. Section III discusses some of the mobility protocol candidates used for the next generation architecture and the relative advantages and disadvantages. Section IV describes many important issues and the requirements related to mobility support for diverse roaming. Section V cites the related work that addresses some of the heterogeneity issues related to mobility, and then we provide a few comprehensive solutions for a generic network architecture. Finally, Section VI concludes the paper.

II. NEXT GENERATION WIRELESS NETWORK ARCHITECTURE

Several existing standards bodies are attempting to define the core network architecture for next generation wireless networks. 3GPP (Third Generation Partnership Project) defined an IMS (IP Multimedia Subsystem) [5] architecture, and 3GPP2 defined the MMD (Multimedia Domain) [6] architecture. Recently, A-IMS (Advances to IMS) [7] architecture, which enhances existing IMS and MMD networks, has been proposed to support a variety of services such as SIP-based and non-SIP-based applications. SIP-based applications are typically set up by SIP and provide services such as VoIP. On the other hand, non-SIP-based applications provide services such as IPTV and FTP without using SIP. Similarly, ITU-T (International Telecommunication Union Telecommunication Standardization Sector) is working on defining the Next Generation Network (NGN) under the premises of NGN-GSI (Global Standards Initiative). All these

architectures include heterogeneous access networks, such as CDMA, WiMAX, and 802.11 technologies, and include support for roaming. In this section, we briefly discuss the mobility protocols used by each standards body and then illustrate how our proposed comprehensive mobility solutions support the heterogeneity associated with a variety of mobility protocols.

3GPP IMS defines the framework for supporting real-time and non-real time IP multimedia services in an access agnostic manner. For seamless mobility management, however, it depends upon 3GPP data network mobility standard such as GTP (Generic Tunneling Protocol), which supports IP mobility. Recently, new efforts have started on Long Term Evolution (LTE) for 3GPP access technologies. In particular, new System Architecture Evolution (SAE) [8] is currently under discussion within the SA2 Work Group to enhance the 3GPP network capability to cope with the rapid growth in IP data traffic. This architecture focuses on the important mobility performance aspects of reduced latency, higher user data rates, improved system capacity and coverage, and reduced overall cost for the operator. Additionally, SAE assumes that IP-based 3GPP services will be provided through heterogeneous access technologies. To address mobility management in such a heterogeneous environment, both the CMIP and PMIP extensions to GTP and IETF mobility management protocols are being considered.

3GPP2 MMD architecture is a slight variation on the IMS architecture and supports both Simple IP [9] and Mobile IP while offering roaming support over a CDMA2000 network. Simple IP does not mandate a mobility stack in the mobile node. Thus, it cannot provide seamless mobility by itself, unless an application layer mobility protocol, such as SIP-based mobility [10], is used. However, A-IMS architecture plans to use a combination of CMIPv6 and a network-based localized mobility protocol, PMIPv6, when the mobile node moves between sub-networks in the visited network.

ITU-T's Handover Management Framework (HMF) [11], currently being discussed under NGN-GSI, describes the need to support both inter-carrier network mobility and intra-carrier network mobility. ITU-T defines mobility at the link layer, network layer, and application layer and recommends using CMIPv6, mSCTP [12], and SIP as potential protocols to take care of mobility.

All of these architectures have certain functions in common. They all try to provide ubiquitous services that need mobility support along with quality of service, security and charging. Without describing the details of each of these architectures, we can list the basic functional components required by any generic architecture. Our mobility solutions illustrated in later sections are composed of the following basic components.

- Functional components hHA (home Home Agent) and vHA (visited Home Agent) provide media packet transfer in the home domain and visited domain, respectively. The HAs map the home addresses with the temporary care-of-addresses and route the media and signaling messages to the mobile node.
- SIP servers, such as S-CSCF (Serving-Call Session Control Function) and P-CSCF (Proxy-CSCF), take care of routing SIP signaling messages from and to the mobile

node. S-CSCF is always located in the home network and helps user registration regardless of the user location. In MMD network, a user can use either the P-CSCF located in the home network or in the visited network. DHCP servers in each network help assign the P-CSCF address to the mobile node.

- AAA (Authentication, Authorization, and Accounting) servers in both the home network and visited network are used for user profile verification. However, each of the visited networks and the home network can have different mobility capabilities and requirements depending on the policy defined by the operators.
- There are both SIP-based and non-SIP-based application servers (ASs) that are responsible for providing advanced multimedia services beyond VoIP.
- PCRF (Policy Control and Charging Rules Function) controls the media based on the policy in the network, and helps to provide feature interaction between SIP-based and non-SIP-based services.
- Based on the type of access network (e.g., CDMA, 802.11, etc.), the architecture has the access gateways (AGWs) that may act as GGSN (Gateway GPRS Support Node), PDSN (Packet Data Serving Node) or PDF (Packet Data Interworking Function).

III. CANDIDATE MOBILITY PROTOCOLS

When the mobile node changes its network point of attachment, traffic is disrupted due to the handover process. As defined in RFC 3753 [13], a handover can be mobile-controlled or network-controlled. The mobility protocol is supposed to take care of handover by reducing traffic disruption during the handover. Depending upon the type of movement, mobility can be handled at the link layer, network layer, or application layer. Although a carrier is free to choose either IPv4 or IPv6, most next generation networks are developing solutions based on IPv6. Thus, we briefly introduce a few mobility protocols that work over IPv6-based networks. Since link layer mobility is access specific and cannot solve the problem of heterogeneity, we will not discuss the link layer mobility but stress upper layer mobility.

A. Network Layer Mobility

In this case, mobility is handled in the network layer and involves heterogeneous access technologies and could either be mobile-controlled or network-controlled. In a mobile-controlled scenario, the mobile node is usually equipped with a mobility stack and interacts with a remote entity such as HA. When the mobility protocol is network-controlled, other networking elements in the middle of the network interact with HA and perform handoff-related functions. The cellular mobility protocols of IS-41 and GSM (Global System for Mobile Communications) are actually network-controlled [14]. In this scenario, the call is anchored at the serving MSC (Mobile Switching Center). Based on the measurement from the mobile node, the serving MSC determines the likely target MSC for the handoff and instructs the mobile node to initiate the handoff. Thus, even if the mobility protocol is network-controlled, the mobile node can still assist in the mobility functions by providing specific information, such as signal-to-noise ratio or any other measurement-related information. We

provide examples of two types of the network layer mobility protocols: mobile-controlled mobility and network-controlled mobility.

A.1 Mobile-controlled Mobility

Primarily, there are two mobile-controlled mobility protocols, MIPv4 and MIPv6 designed for IPv4 and IPv6 networks, respectively. Figure 1 shows the different network elements of CMIPv6. The mobility stack within a mobile node interacts with the HA and sets up a tunnel between the mobile node and HA. Thus, any traffic destined for the mobile node is tunneled via the HA. During a handoff, the mobile node sends a binding update to both the HA and the correspondent node (CN) that maps the new care-of-address for the mobile node with its home address. In the case of route optimization, the correspondent node updates its cache and starts sending traffic directly to the mobile node instead of via the HA. Maintaining a tunnel between the mobile node and the HA may not always be desirable as it adds to the overhead of the already scarce bandwidth.

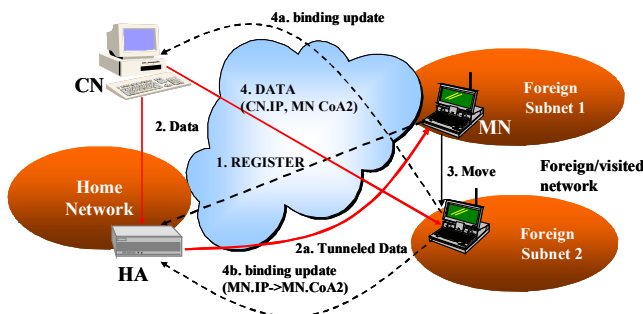


Figure 1: Mobile-controlled mobility - CMIPv6

A.2 Network-controlled Mobility

In order to avoid the overhead associated with tunneling over the air, few micro mobility protocols, namely Cellular IP [15] and HAWAII [16], have been proposed in the past. These protocols use host-based routing techniques and forwarding-cache-based techniques, respectively, to redirect traffic to the new point-of-attachment for the mobile node. These protocols are suitable for handling mobility when the mobile node's movement is limited within a domain. Although these protocols use the underlying networking components to a great extent and are suitable for local mobility, they still require a mobility stack on the mobile node. In order to reduce the load on the mobile node and handle local mobility, the IETF (Internet Engineering Task Force) has been developing network-based localized mobility management protocols. A few candidate protocols are currently being discussed, such as network-controlled local mobility [17] and PMIPv6. These protocols are designed to take care of local mobility and are controlled by the network elements in the edge routers. We will briefly describe one of these protocols, PMIPv6.

PMIPv6 does not use any mobility stack on the mobile node but rather uses the proxies on the edge routers to help perform the mobility functions, such as the binding update to the HA. These functions are called PMA (Proxy Mobile Agents) and can co-locate with the edge routers. As long as the mobile node moves within the same domain that has PMAs, the mobile node assumes that it is in a home link. The PMA is

responsible for sending the proper mobile prefix as part of the router advertisement for stateless auto-configuration, or it can also act as a DHCP relay agent for stateful auto-configuration. Figure 2 describes the network elements associated with PMIPv6 operation. After the mobile node connects to the new point-of-attachment as part of the initial bootstrapping process or after the movement to a new domain, access is authenticated with the designated AAA server. During this process, PMA sends the binding update to the HA with the address of the PMA that is specific to the home prefix of the mobile node. In the absence of a pre-existing tunnel, this process helps to set up a tunnel between the HA and the respective PMA. The mobile node configures its address using the prefix included in the router advertisement and interface-id, which can be assigned by PMA or created by itself. The PMIPv6-based mobility protocol is preferred when mobility is confined within a domain and wireless service providers do not want to overload the mobile node's stack by setting up a tunnel between the mobile and the HA. A tunnel is not desirable on the mobile node because it adds extra processing and bandwidth constraints to the wireless hop.

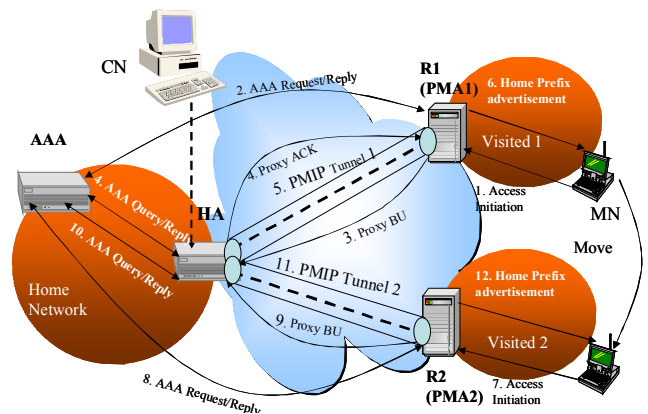


Figure 2: Network-controlled mobility - PMIPv6

B. Application Layer Mobility

Mobility can also be handled using application layer signaling such as SIP. Application layer mobility eliminates the need for a mobility stack on the mobile node and does not need any other mobility elements in the network. This is also suitable for such services as VoIP continuity, which switches the call between cellular and packet networks. However, application layer mobility also has shortcomings. Application layer mobility may take more time than network layer mobility because of application layer processing. In addition, it only supports mobility for SIP-based applications. If the application between the communicating hosts is SIP-based, then mobility support can be provided by using SIP signaling between the hosts. SIP can be used to support both RTP- and TCP-based applications [10] and [18], respectively, during handoff and takes care of the change in mid-session host parameters. However, application layer mobility cannot be used to support any non-SIP-based application, such as FTP and Telnet. Thus, if one needs to support mobility for all kinds of applications during handoff, the application layer mobility protocol for SIP-based mobility may not be appropriate. Figure 4 shows the protocol interaction between different networking components when application layer mobility is used.

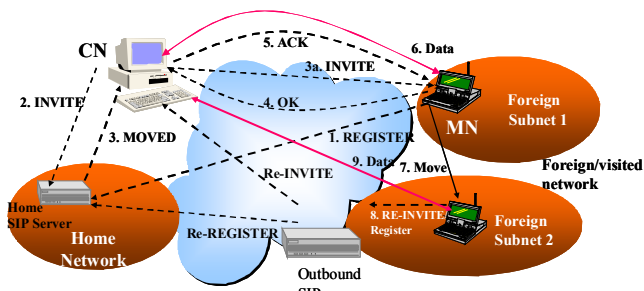


Figure 3: Application layer mobility – SIP

C. Advantages and disadvantages of Mobility Protocols

Each of these candidate protocols has advantages and drawbacks, and each is suitable for a specific type of environment. We will provide a qualitative comparison of these three protocols and compare the relevant high-level parameters that might be important considerations for deployment. For example, operators may be interested in factors that affect the performance and ease of deployment. Depending upon the priority of the application and policies, carriers can choose one mobility protocol or a combination.

Table 1: Qualitative difference in mobility protocols

Mobility Protocols	Mobility Stack on mobile	MIP Tunnel over the Air	Application independent	HA/PMA requirement
CMIPv6	Yes	Yes	Yes	HA
PMIPv6	No	No	Yes	HA/PMA
Application Layer	No	No	No	N/A

Thus, the challenge is to come up with a mobility scheme when carriers support different mobility protocols. We describe some of the solutions in Section V.

IV. MOBILITY REQUIREMENT IN HETEROGENEOUS NETWORKS

In general, roaming involves formal agreements between operators that allow a mobile node to connect to a visited network. Roaming includes, for example, the functionality by which users can communicate their identity to the local AN (Access Network) so that inter-AN agreements can be activated and service and applications in the mobile node's home network can be available locally to the user. We consider mobility support and network access as different while roaming in next generation networks.

In this section, we describe a few issues and requirements that need to be addressed in order to support mobility in diverse networks involving roaming. These issues arise because of diverse characteristics, requirements and capabilities in multiple networks and mobile nodes. We also propose a few solutions for these requirements.

A. 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 to the SIP server, and the address is private user information. In general, after the completion of SIP signaling, each communicating node knows each other's IP address for media and can send traffic directly or via HA. Thus, there is a chance of denial of service attacks if the media address is permanent. Therefore, carriers should avoid exposing private information to others. Since SIP URIs (Uniform Resource Identifiers) are used for setting up a call, the SIP signaling address is not exposed to the other user. The IPv6 addressing scheme has the inherent advantage of assigning multiple addresses to the same interface. We take advantage of the 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.

B. Expedited Media Delivery

Second, when the mobile node is in the visited domain and if the home address is used for media, the media must travel via the HA in the home network giving rise to media delay. We propose using the home address of the mobile node to set up the SIP session but we assign temporary addresses to the mobile node for media communication. 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 than the SIP signaling address, media traversal can be limited to the visited domain when both the communicating nodes are away from the home domain. The mobile needs to generate these addresses during the bootstrapping process or when entering a new visited domain. We provide several examples of how these features can be utilized for different roaming scenarios in Section V.

C. Avoidance of Media Packet Encapsulation over the Air

It is desirable to avoid the encapsulation of media packets over the air. Thus, it is important to choose a mobility protocol that can avoid the tunneling of media packets on the last hop, which is often wireless. A comprehensive roaming solution should implement mobility protocols that try to achieve this desired effect. We propose using a network-based localized protocol to handle media re-routing whenever possible to take care of this problem.

D. Mobility Types

A mobile node can experience different types of mobility based on movement within the home domain or in the visited domain. A carrier needs to be able to provide seamless mobility to the mobile node in the visited network and in the home network. We illustrate the types of mobility during its roaming in Figure 4. We primarily define mobility as local mobility and global mobility. Local mobility can be defined as home local mobility and visited local mobility.

Home local mobility is defined as a scenario when the mobile node moves between two different access routers within a home domain. A similar type of movement in the visited domain is called visited local mobility. Similarly, there can be several types of global mobility. The first form of global mobility is when the mobile node moves from its home network to a new carrier network. The second form of global

mobility involves the mobile node moving from one visited domain to another visited domain within the same carrier network. The third form of global mobility involves the mobile node moving from one carrier network to another carrier network while away from the home domain.

In this paper, we will focus on the solutions for home local mobility and visited local mobility.

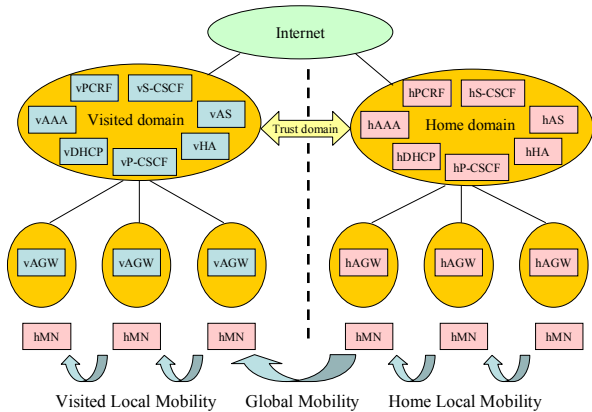


Figure 4: Mobility in a generic roaming architecture

E. Mobility Heterogeneity

Mobility diversity while supporting roaming between heterogeneous networks is an important issue that needs to be addressed. The issue of mobility diversity arises because of the different types of mobility. It is highly likely that the target network may not support the same type of mobility as in the home domain.

We will primarily consider three different kinds of mobility: Simple IP, CMIPv6, and PMIPv6 for roaming. In the Simple IP case, we will assume that there is no mobility stack on the mobile node except for the application layer mobility stack for SIP-based mobility. Since each mobile node is assumed to have an SIP stack, no additional stack is needed to support application layer mobility. In the CMIPv6 case, the mobile node has the MIP stack, in addition to HA support in the network, and has the responsibility of sending the binding update to the HA as its care-of-address changes. In order to realize CMIPv6, the network components should support the required mobility-related signaling. Mobile nodes can use two different IP addresses, one for SIP signaling and one for media. The third kind of mobility support is PMIPv6. In this case, the HoA (Home Address) of the mobile node does not change, but the care-of-address may change as well as CMIPv6 case when the mobile node moves between access routers. Also, static HoA is used for SIP signaling, and two different temporary HoAs may be used for SIP and non-SIP-specific media. Although there is no MIP stack on the mobile node, there is a PMA on each of the access routers.

In a roaming environment, the mobile and the network may have different mobility protocols. For example, (a) the mobile node may support just Simple IP without any mobility stack, (b) it could be equipped with application layer mobility, such as SIP-based mobility, or (c) it may be equipped with a MIPv6 stack. In order to support the mobility functionality of the mobile node, the network also needs to complement mobile

node’s capability. Thus, for Simple IP on the mobile node, the network may not have any other mobility support except basic routing. Similarly, the network may need to be equipped with either CMIPv6 or PMIPv6 support. As an example, in order to take advantage of CMIPv6 support in the network, the mobile node also needs to be equipped with a MIPv6 stack. On the other hand, if the network has PMIPv6 support, the mobile does not need to have a MIPv6 stack.

Table 2: Mobility movement matrix

MN Stack	Home Domain	Visited Domain
Simple IPv6	Simple IPv6 (Case I)	Simple IPv6
		PMIPv6 (Case V)
		CMIPv6
	PMIPv6 (Case II)	Simple IPv6
		PMIPv6
		CMIPv6
CMIPv6	Simple IPv6	Simple IPv6
		PMIPv6
		CMIPv6
	PMIPv6 (Case III)	Simple IPv6
		PMIPv6
		CMIPv6
CMIPv6 (Case IV)	Simple IPv6	
	PMIPv6 (Case VI)	
	CMIPv6	

□ This case may not happen.

Table 2 shows the possible combination of movement patterns that involve different types of mobility support in the home domain and in the visited domain. The mobile stack itself can either have Simple IP or CMIPv6 and can move from home domain to the visited domain, where the home domain and visited domain may offer different mobility support. CMIPv6 and PMIPv6 are used interchangeably during the discussion in the paper. We will discuss the details of different cases in Section V.

F. Application Types

Primarily, application in next generation wireless networks can be categorized as real-time and non-real-time services. Real-time services are categorized as interactive traffic such as VoIP, or streaming traffic such as IPTV. On the other hand, non-real-time services can be the packet transfer protocols such as FTP or Telnet. According to the transport type, the application can be split into two types: TCP/IP and RTP/UDP. Examples of SIP-based session control are VoIP and Chattcp. While VoIP is RTP/UDP based, Chattcp is TCP based. Similarly, there are non-SIP-based RTP/UDP applications, such as IPTV, which could be initiated using RTSP [19]. Non-real-time applications, such as FTP and Telnet, are also non-SIP-based. Thus, the choice of the mobility protocol is largely determined by the application supported in the network.

V. MOBILITY SOLUTIONS FOR ROAMING SCENARIOS

Analyzing some of the roaming issues involved, it appears that there is a need to develop a mobility management scheme that can take care of problems with the heterogeneity associated with roaming between intra- and inter-provider domains. We will primarily focus on a mobility management scheme that can handle the heterogeneity of mobility protocols in both the home domain and visited domain.

Some of the existing efforts use a combination of mobility protocols to provide a multilayered mobility management solution adapted to the type of application. For example, Wong et al. [20] suggested a multi-layer mobility management architecture using SIP-based mobility for real-time traffic and MIP for non-real-time traffic during the mobile node's movement between two domains. However, as long as the movement is limited within its domain, the mobile node uses a micro mobility management protocol, such as Cellular IP or HAWAII. Politis et al. [21] described hybrid multi-layered mobility management with AAA context transfer capabilities. Wang et al. [22] described how loose coupling or tight coupling between the application layer mobility protocol and network mobility layer protocol can affect overall system performance. However, many of these solutions assume similar types of networks in both domains, and none actually considered network-controlled mobility as an option. These solutions also do not consider roaming scenario. The A-IMS mentions roaming architecture between A-IMS networks and between A-IMS and non-A-IMS network. However, A-IMS does not address the situation where each domain has a different mobility capability. Work Group 13 and 19 within ITU-T are defining a mobility management framework for next generation networks. However, this architecture has not defined solutions for different kinds of roaming or addressed the heterogeneity problems associated with roaming.

For the sake of simplicity, we will analyze only two kinds of mobility: home local mobility and visited local mobility. For home local mobility and visited local mobility, we will illustrate two cases only.

A. Home Local Mobility

A combination of mobility protocols can be used to support home local mobility based on the mobile node's capability. In particular, there can be four different cases of home mobility. Case I does not include any mobility support in the home domain, neither does it mandate any mobility support on the mobile node. Thus, both the network and the mobile node have only Simple IP support. Case II involves mobile nodes without a network layer mobility stack and a network with PMIPv6 support. We assume that the network provides the relevant MIPv6-related networking components, such as HA in the network, when is the network supports PMIPv6. Case III involves a MIPv6 stack on the mobile node and a network with PMIPv6 support. Case IV involves CMIPv6 support for both the mobile node and the network. For simplicity, we will describe the call flows associated with Case II and IV.

A.1: Case II

Figure 5 shows Case II with home local mobility when the mobile node has a Simple IP stack, and the network is equipped with PMIPv6. We consider the generic network architecture and assume the access routers will behave as 3GPP2 PDSN. As the mobile node initially bootstraps in PDSN#1, it goes through an access authentication phase. With a PPP (Point-to-Point Protocol) link, access authentication takes place at the lower layer during the LCP and PAP/CHAP phase. Since the PDSNs are equipped with PMA, the NAI (Network Access Identifier) [23] is passed to the HA as part of the binding update. PMA may also receive the home prefix

and the interface-id for the specific mobile node from the HA. These are used for creating the hHoA#1 address.

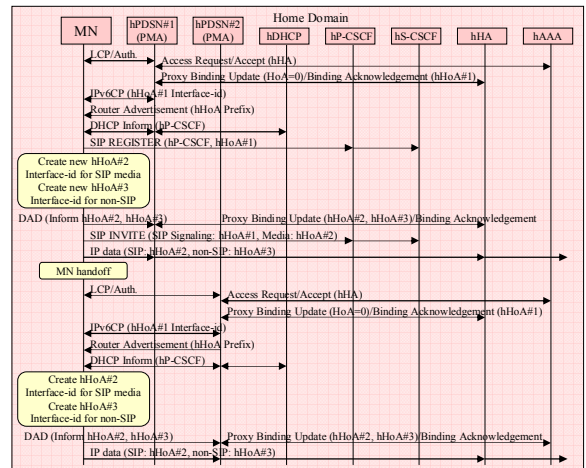


Figure 5: MN=Simple IP, Home Domain=PMIPv6 (Case II)

The mobile node interacts with the DHCP server to obtain the address of the P-CSCF as well. It then sends a SIP registration to the P-CSCF, and the P-CSCF sends it to S-CSCF. Since hHoA#1 is used for the SIP signaling purpose, the mobile node uses the HoA prefix and locally generated random interface-id to generate the new media addresses hHoA#2 and hHoA#3 for SIP-based and non-SIP-based traffic, respectively. At this time, DAD (Duplicate Address Detection) is used to inform the PDSN of hHoA#2 and hHoA#3 addresses. The mobile node uses hHoA#2 as the media contact address in its SDP (Session Description Protocol) when it invites another user. This way the mobile node receives media for the SIP-based application using a different IP address than for SIP signaling. Since there is already a tunnel established between the HA and PMA, any SIP signaling traffic destined for hHoA#1, SIP media destined for hHoA#2, and non-SIP media destined for hHoA#3 are tunneled via the PMIPv6 tunnel setup between the PMA and HA. Even if the mobile node moves to a new PDSN#2, and hence changes to a new PMA, hHoA#1, hHoA#2, and hHoA#3 do not change.

A.2: Case IV

Figure 6 shows Case IV for home local mobility, the mobile node has CMIPv6 support, and the network supports CMIPv6 but not PMIPv6. Since the mobile node is equipped with the CMIPv6 stack, it can send a binding update to the HA and maps its home address hHoA#1 with the care-of-address hTemp#1. The mobile node also sends a SIP registration message to P-CSCF, and P-CSCF sends it to S-CSCF to update the P-CSCF information obtained via the DHCP server. The contact address in the SIP header is hHoA#1. When inviting another user, the mobile node uses hTemp#1 as the media contact address in its SDP. Similarly, the mobile node creates a new address hTemp#2 to support non-SIP-based applications. As handoff is executed to a different PDSN#2, the mobile node goes through a similar access authentication procedure and obtains a new set of temporary addresses, such

as hTemp#3 and hTemp#4, to support SIP and non-SIP-based applications, respectively.

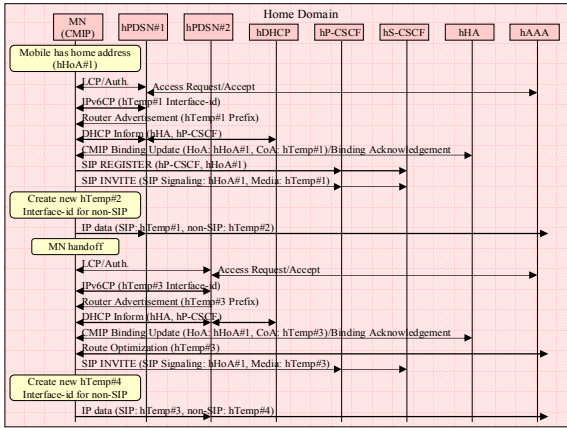


Figure 6: MN=CMIPv6, Home Domain=CMIPv6 (Case IV)

As part of its binding update to the HA, the mobile node uses hTemp#3 as the mapping address to the HA because CMIPv6 cannot be used for media traffic due to the limited wireless bandwidth. Since the media is sent directly to the mobile node, it is imperative that the correspondent node be notified about the change in IP address. Thus, the mobile node may have to use the route optimization procedure to get the media to the new IP address. Filtering functionality in PDSN can be achieved by using the new media address carried in the SDP of re-INVITE. Since P-CSCF will have access to this SDP parameter, it can use it to notify the PDSN to open the gate.

B. Visited Local Mobility

As explained in Figure 5, it is possible for the home domain and visited domain to have different mobility support. Thus, when moving from one domain to another domain, the mobile node may have to adapt accordingly if the mobility support is different. Out of several possible cases, where the mobility support in visited domain could be different than the mobility support in the home domain, we only describe two cases for visited local mobility to illustrate how mobility might work when the mobile node moves to a domain that has different mobility support than the home domain.

B.1: Case V

Figure 7 shows the flows associated with Case V when the mobile node has a Simple IP stack and the home domain has Simple IP support, but the visited domain supports PMIPv6.

When the mobile node is within the home domain, it needs to use application layer mobility to support seamless services; however, as it moves to the visited domain, the mobile node has the option of using either application layer mobility or PMIPv6. The first time the mobile node moves to the visited domain, access is authenticated along with the PMIPv6 binding update procedure with PMA. PMA sends the interface-id during the IPv6CP procedure, and sends the vHoA prefix as part of the router advertisement. Based upon these

two parameters, the mobile node generates a new vHoA#1 used for SIP signaling. At this time, the mobile node obtains the address of vP-CSCF from the vDHCP server. The mobile node then sends SIP registration to the vP-CSCF, and the vP-CSCF forwards it to hS-CSCF to update the contact address for SIP signaling and reports the address of vP-CSCF.

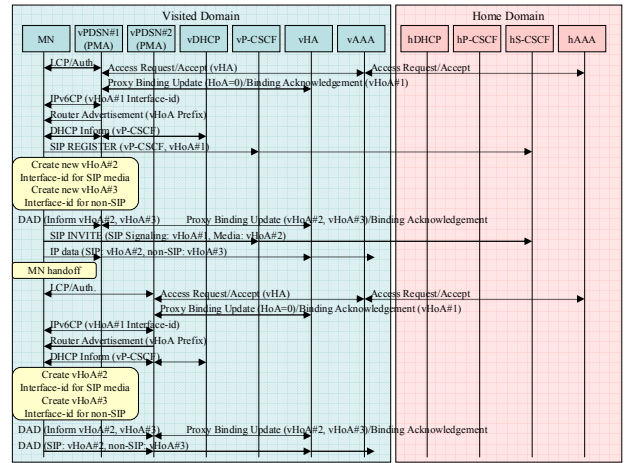


Figure 7: MN=Simple IP, Home Domain=Simple IP, Visited Domain=PMIPv6 (Case V)

In order to send the SIP and non-SIP media, the mobile node creates two more new addresses using a self-generated interface-id and vHoA prefix. After a successful SIP signaling setup, the mobile node receives traffic using the addresses, vHoA#2 and vHoA#3 for SIP and non-SIP-related media, respectively. During handoff, the mobile node obtains the same prefix and interface-id from the vHA. Therefore, the mobile node does not have to send a SIP registration message unless the assigned P-CSCF changes.

B.2: Case VI

Figure 8 shows Case VI where the mobile node has a MIPv6 stack, the home domain is equipped with PMIPv6, and the visited domain is equipped with CMIPv6. This is a typical scenario showing mobility heterogeneity between the home domain and visited domain.

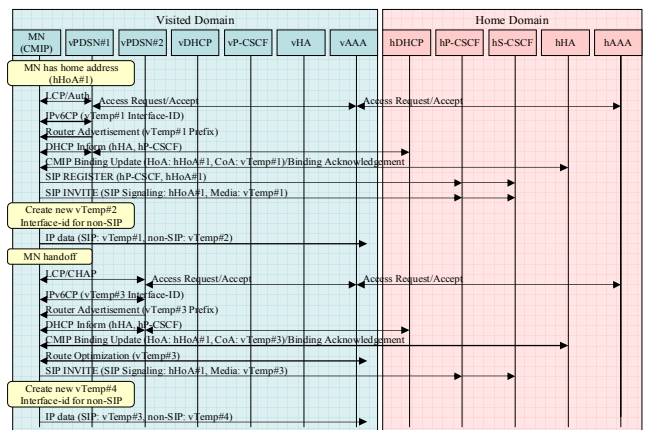


Figure 8: MN=CMIPv6, Home Domain=PMIPv6, Visited Domain=CMIPv6 (Case VI)

Since the visited domain does not support PMIPv6, there is no PMA in the PDSNs. For the sake of simplicity, PDSNs or associated PMAs are not shown in the home domain. As the mobile bootstraps in the visited domain, it sets up the PPP connection with vPDSN#1. During the access authentication procedure, the vPDSN#1 communicates with vAAA and hAAA and may obtain the interface-id and prefix. The vPDSN#1 informs the mobile node of the interface-id and prefix using IPv6CP and router advertisement, respectively. Thus, the mobile node creates a new care-of-address vTemp#1 using the prefix and interface-id and then obtains the address of hP-CSCF from the hDHCP server. The home address of the mobile node can be statically configured. The mobile node sends the binding update to the hHA mapping hHoA#1 with vTemp#1 and then sends SIP registration to hP-CSCF, and the hP-CSCF sends it to S-CSCF to update the P-CSCF information. Once SIP registration and CMIPv6 update are completed, the mobile node sends a SIP INVITE message to the correspondent node to set up the call. As shown in the diagram, the media address is vTemp#1, and the SIP contact address is hHoA#1. By using the same prefix, the mobile node also creates new temporary address vTemp#2 to handle the non-SIP-based application.

During the handoff in the visited network and connection to the new vPDSN#2, the mobile node creates a pair of new temporary media addresses to support SIP-based and non-SIP-based applications. The mobile node sends a binding update to the hHA and SIP registration to the hP-CSCF and then hP-CSCF sends it to hS-CSCF for proper routing of any incoming call. However, in order to maintain continuity of the current media stream, the mobile node has to make use of the route optimization process and updates the correspondent node using the visited temporary address for both SIP-based and non-SIP-based applications. The associated handoff also results in a SIP re-INVITE that takes care of any changes in mid-session parameters. The media address in the SDP, which is sent as part of the SIP re-INVITE, opens the filtering gate in the PDSN. In order to support non-SIP-based applications, one either needs to have route optimization support on the server or may have to use application layer mobility.

VI. CONCLUSIONS

A carrier can choose a specific candidate mobility protocol within its own network, based on the type of application supported, the mobile node's movement pattern, and any other policy. However, the heterogeneity of mobility protocols for roaming services adds to the operational complexity. We proposed comprehensive analyses that address the mobility issues for roaming in next generation wireless networks. These analyses could be useful for carriers that plan to provide mobility support to roaming users across networks with diverse mobility protocol support. It appears that a carrier may need to support policy-based multi-layer mobility solutions and use specific mobility protocols based on the application used, type of movement by the mobile node, and available mobility support in the network. We plan to report the experimental results for optimized mobility in roaming cases in future papers.

REFERENCES

- [1] C. Perkins et al, "IP Mobility Support for IPv4," IETF RFC 3220, Jan. 2002
- [2] D. Johnson et al, "Mobility Support in IPv6," IETF RFC 3775, June 2004
- [3] J. Rosenberg et al, "SIP: Session Initiation Protocol," IETF RFC3261, June 2002
- [4] S. Gundavelli et al, "Proxy Mobile IPv6," IETF draft-sgundave-mip6-proxymip6-01, Jan. 2007
- [5] 3GPP, "IP Multimedia Subsystem (IMS)," TS23.228 V6.6.0, June 2004
- [6] 3GPP2, "All-IP Core Network Multimedia Domain - IP Multimedia Subsystem Stage 2," X.S0013-002-A, Nov. 2005
- [7] K. Bogineni et al, "Advances to IP multimedia subsystem," Cisco News Release, July 2006
- [8] 3GPP, "Technical Specification Group Services and System Aspects; 3GPP System Architecture Evolution: Report on Technical Options and Conclusions (Release 7)," TS23.882 V1.6.1, Nov. 2006
- [9] 3GPP2, "cdma2000 Wireless IP Network Standard: Simple IP and Mobile IP Access Services," X.S0011-002-D, Feb. 2006
- [10] E. Wedlund, H. Schulzrinne, "Mobility Support using SIP," ACM WoWMOM'99, 1999
- [11] ITU-T, "Framework of Handover Management for Next Generation Networks," version 0.3, Oct. 2006
- [12] M. Riegel et al, "Mobile SCTP," IETF draft-riegel-tuexen-mobile-sctp-07.txt, Oct. 2006
- [13] J. Manner et al, "Mobility Related Terminology," IETF RFC 3753, June 2004
- [14] L. Yi-Bing et al, "Mobility Management for Cellular Telephony Networks," IEEE Parallel & Distributed Technology: Systems & Technology, Dec. 1996
- [15] A. Valko et al, "Cellular IP: A Local Mobility Protocol," IEEE 13th CCW, Oct. 1998
- [16] Ramjee et al, "Hawaii: A Domain-based Approach for Supporting Mobility in Wide-area," ICNP'99, 1999
- [17] J. Kempf et al, "Goals for Network-based Localized Mobility Management," IETF draft-ietf-netlmm-nohost-req-05.txt, Oct. 2006
- [18] Hseuh et al, "Application Mobility Proxy for Real-time Communication," 3G Wireless Conference, CA, 2002
- [19] H. Schulzrinne et al, "Real Time Streaming Protocol (RTSP)," IETF RFC2326, Apr. 1998
- [20] K. D. Wong et al, "A multilayered Mobility Management Scheme for Auto-Configured Wireless IP Networks," IEEE Wireless Communications, Oct. 2003
- [21] Politis et al, "Hybrid Multilayer Mobility Management with AAA Context Transfer Capabilities for All-IP Networks," IEEE Wireless Communications, Aug. 2004
- [22] Q. Wang et al, "Mobility Management Architectures based on joint Mobile IP and SIP protocols," IEEE Wireless Communications, Dec. 2006
- [23] B. Aboba et al, "The Network Access Identifier," IETF RFC2486, Jan. 1999