

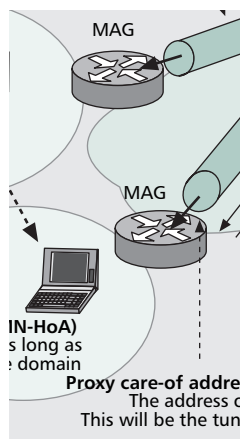
MOBILITY MANAGEMENT FOR ALL-IP MOBILE NETWORKS: MOBILE IPv6 vs. PROXY MOBILE IPv6

KI-SIK KONG AND WONJUN LEE, KOREA UNIVERSITY

YOUN-HEE HAN, KOREA UNIVERSITY OF TECHNOLOGY AND EDUCATION

MYUNG-KI SHIN, ELECTRONICS AND TELECOMMUNICATIONS RESEARCH INSTITUTE (ETRI)

HEUNGRYEOL YOU, KOREA TELECOMMUNICATION (KT)



The authors present the qualitative and quantitative analyses of the representative host-based and the representative network-based mobility management approaches.

ABSTRACT

Recently, a network-based mobility management protocol called Proxy Mobile IPv6 (PMIPv6) is being actively standardized by the IETF NETLMM working group, and is starting to attract considerable attention among the telecommunication and Internet communities. Unlike the various existing protocols for IP mobility management such as Mobile IPv6 (MIPv6), which are host-based approaches, a network-based approach such as PMIPv6 has salient features and is expected to expedite the real deployment of IP mobility management. In this article, starting by showing the validity of a network-based approach, we present qualitative and quantitative analyses of the representative host-based and network-based mobility management approaches (i.e., MIPv6 and PMIPv6), which highlight the main desirable features and key strengths of PMIPv6. Furthermore, a comprehensive comparison among the various existing well-known mobility support protocols is investigated. Although the development of PMIPv6 is at an early stage yet, it is strongly expected that PMIPv6 will be a promising candidate solution for realizing the next-generation all-IP mobile networks.

INTRODUCTION

With the rapid growth in the number of mobile subscribers and mobile devices such as cellular phones, personal digital assistants (PDAs), and laptop computers, the demand for “anywhere, anytime, and any way” high-speed Internet access is becoming a primary concern in our lives. Recent advances in various wireless access technologies such as IEEE 802.16d/e and wideband code-division multiple access (WCDMA) and the incessant efforts of several standards bodies such as the Internet Engineering Task

Force (IETF), Third Generation Partnership Project (3GPP), and International Telecommunication Union — Telecommunication Standardization Sector (ITU-T) appear to increase the possibility of realizing mobile and ubiquitous computing environments. However, many challenges still remain to be solved for achieving such a goal.

The recent fundamental networking trend has been focused mostly on realizing all-IP mobile networks. All-IP mobile networks, which are expected to combine the Internet and telecommunication networks tightly together, are networks in which IP is employed from a mobile subscriber to the access points (APs) that connect the wireless networks to the Internet. One of the most important and challenging issues for next-generation all-IP mobile networks is mobility management. Mobility management enables the serving networks to locate a mobile subscriber’s point of attachment for delivering data packets (i.e., location management) and maintain a mobile subscriber’s connection as it continues to change its point of attachment (i.e., handover management).

Mobile IPv6 (MIPv6) [1] is one of the most representative efforts on the way toward next-generation all-IP mobile networks. However, although MIPv6 is a well-known mature standard for IPv6 mobility support and solves many problems seen in Mobile IPv4 (MIPv4) [2], it has still revealed some problems such as handover latency, packet loss, and signaling overhead. Furthermore, despite the reputation of this protocol, it has been slowly deployed in real implementations over the past years, and does not appear to receive widespread acceptance in the market [3, 4]. Recently, a network-based mobility management protocol called Proxy Mobile IPv6 (PMIPv6) [5] is being actively standardized by the IETF NETLMM working group, and is starting to attract considerable attention

among the telecommunication and Internet communities. Unlike the various existing protocols for IP mobility management such as MIPv6, which are host-based approaches, a network-based approach such as PMIPv6 has salient features and is expected to expedite the real deployment of IP mobility management. To the best of our knowledge, this article is the first to present qualitative and quantitative analyses on MIPv6 and PMIPv6. In addition, this article provides a comprehensive comparison and summary that addresses the main strong and weak points of PMIPv6 against various existing well-known mobility support protocols.

The remainder of this article is organized as follows. First, we briefly present overviews and discuss problems of host-based mobility management approaches and then identify several key strengths of the network-based mobility management approach. Then we present an overview of the network-based mobility management approach (i.e., PMIPv6) to providing IP mobility support. Qualitative and quantitative comparisons of PMIPv6 against various existing mobility support protocols are thoroughly investigated, highlighting the main desirable features and key strengths of PMIPv6. Finally, concluding remarks are given.

WHY NETWORK-BASED MOBILITY MANAGEMENT?

Mobile IP is probably the most widely known IP mobility support protocol. Two versions of Mobile IP have been standardized for supporting host-based mobility on the Internet: MIPv4 and MIPv6. They support the mobility of IP hosts by allowing them to utilize two IP addresses: a home address (HoA) that represents the fixed address of a mobile node (MN) and a care-of-address (CoA) that changes with the IP subnet to which an MN is currently attached. In terms of the fundamental architectural aspects, these two mobility support standards follow the same concept. However, there are slight differences with regard to some important details. MIPv6 comprises three components: the MN, the home agent (HA), and the correspondent node (CN). The role of the foreign agent (FA) in MIPv4 was replaced by the access router (AR) in MIPv6. In addition, although route optimization extensions were proposed for both MIPv4 and MIPv6, they were only standardized for MIPv6. A detailed description of MIPv6 route optimization as well as details of MIPv4 and MIPv6 can be found in [1, 2].

Although MIPv6 is a mature standard for IP mobility support and solves many problems, such as triangle routing, security, and limited IP address space, addressed in MIPv4, it still has some problems such as handover latency, packet loss, and signaling overhead. Besides, the handover latencies associated with MIPv4/v6 do not provide the quality of service (QoS) guarantees required for real-time applications. Therefore, various MIPv6 enhancements such as hierarchical Mobile IPv6 (HMIPv6) [6] and fast handover for Mobile IPv6 (FMIPv6) [7] have been reported over the past years, mainly focused on perfor-

mance improvement in MIPv6. However, MIPv6 and its various enhancements basically require protocol stack modification of the MN in order to support them. In addition, the requirement for modification of MNs may cause increased complexity on them. On the other hand, in a network-based mobility management approach such as PMIPv6, the serving network handles the mobility management on behalf of the MN; thus, the MN is not required to participate in any mobility-related signaling. Compared to host-based mobility management approaches such as MIPv6 and its enhancements, a network-based mobility management approach such as PMIPv6 has the following salient features and advantages.

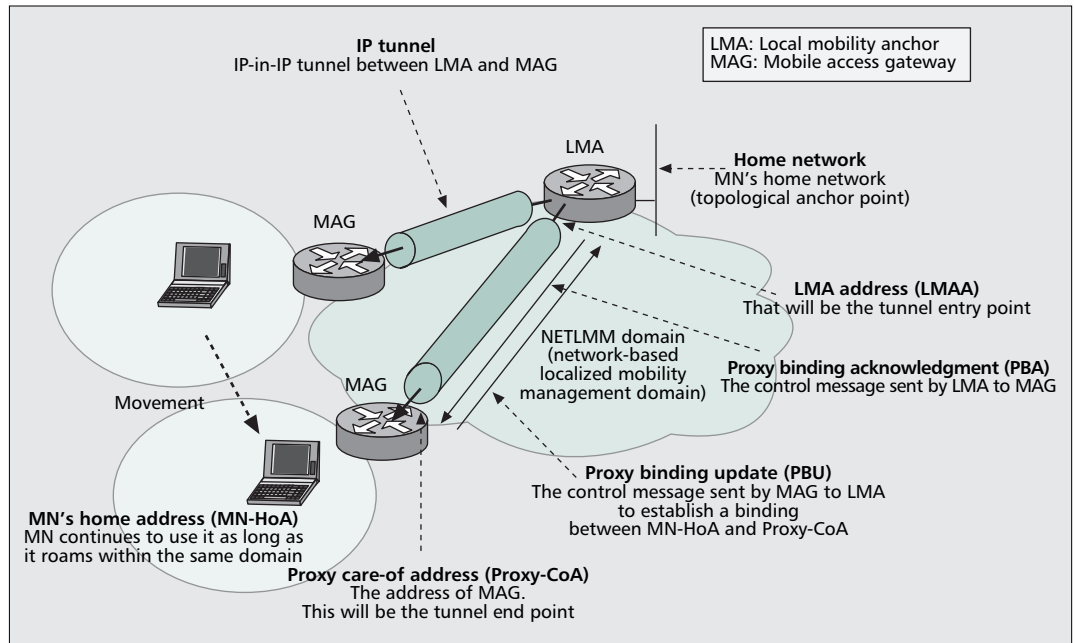
Deployment perspective: Unlike host-based mobility management, network-based mobility management does not require any modification of MNs. The requirement for modification of MNs can be considered one of the primary reasons MIPv6 has not been widely deployed in practice, although several commendable MIPv6 enhancements have been reported over the past years [3, 4]. Therefore, no requirement for modification of MNs is expected to accelerate the practical deployment of PMIPv6. Such an expectation can easily be demonstrated by the fact that in the WLAN switching market, no modification of the software on MNs has been required to support IP mobility, so these unmodified MNs have enabled network service providers to offer services to as many customers as possible [8].

Performance perspective: Generally, wireless resources are very scarce. In terms of scalability, efficient use of wireless resources can result in enhancement of network scalability. In host-based network layer approaches such as MIPv6, the MN is required to participate in mobility-related signaling. Thus, a lot of tunneled messages as well as mobility-related signaling messages are exchanged via the wireless links. Considering the explosively increasing number of mobile subscribers, such a problem would cause serious performance degradation. On the contrary, in a network-based network layer approach such as PMIPv6, the serving network controls the mobility management on behalf of the MN, so the tunneling overhead as well as a significant number of mobility-related signaling message exchanges via wireless links can be reduced. Generally, the signaling latency introduced by an MN can be significantly affected by the performance parameters such as wireless channel access delay and wireless transmission delay. The latencies incurred by such performance parameters can be considerable compared to those of the wired link; thus, the signaling latency introduced by the MN could result in increasing handover failures as wireless channel access and wireless transmission delays get larger (more details on handover latency can be found later in this article).

Network service provider perspective: From the perspective of a network service provider, it is expected that network-based mobility management would enhance manageability and flexibility by enabling network service providers to control network traffic and provide differentiated services and so on. Such a possibility can easi-

Compared to host-based mobility management approaches such as MIPv6 and its enhancements, a network-based mobility management approach such as PMIPv6 has several advantages.

The fundamental foundation of PMIPv6 is based on MIPv6 in the sense that it extends MIPv6 signaling and re-uses many concepts such as the HA functionality. However, PMIPv6 is designed to provide network-based mobility management support to an MN in a topologically localized domain.



■ Figure 1. Overview of PMIPv6.

ly be expected from legacy cellular systems such as IS-41 and Global System for Mobile Communications (GSM), which can be considered network-based (i.e., network-controlled) systems. Note that PMIPv6 has some resemblance to General Packet Radio Service (GPRS) in that they are both network-based mobility management protocols and have similar functionalities. However, PMIPv6 is an Internet protocol that is not dependent on any access-technology-specific protocol, so it could be used in any IP-based network, while GPRS is an access-technology-specific protocol closely coupled with the signaling protocols used in legacy cellular systems.

NETWORK-BASED MOBILITY MANAGEMENT: PMIPv6

In a network-based approach such as PMIPv6, the serving network controls mobility management on behalf of the MN; thus, the MN is not required to participate in any mobility-related signaling. The design goals the IETF NETLMM working group aims to cover are very extensive. The primary features of such goals are as follows (more details are provided in [4, 8]):

- **Support for unmodified MNs:** Unlike a host-based approach, a network-based approach should not require any software update for IP mobility support on MNs.
- **Support for IPv4 and IPv6:** Although the initial design of a network-based approach uses an IPv6 host, it is intended to work with IPv4 or dual-stack hosts as well.
- **Efficient use of wireless resources:** A network-based approach should avoid tunneling overhead over a wireless link; hence, it should minimize overhead within the radio access network.
- **Link technology agnostic:** A network-based approach should not use any wireless-link-specific information for basic routing manage-

ment, and should support any type of wireless link technology.

- **Handover performance improvement:** A network-based approach should minimize the time required for handover.

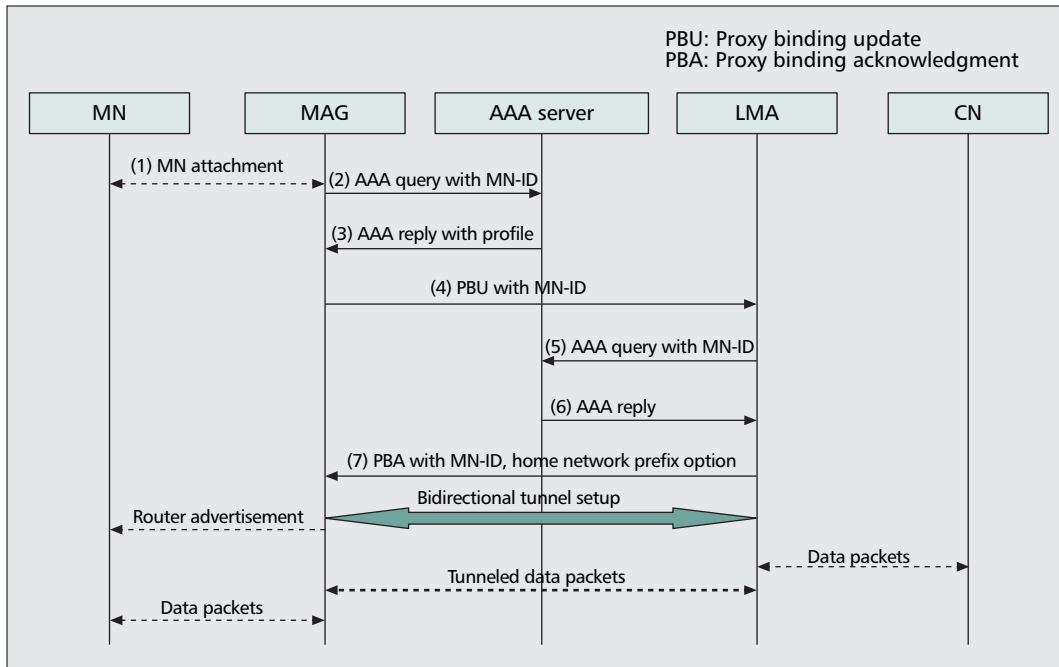
OVERVIEW OF PMIPv6

The fundamental foundation of PMIPv6 is based on MIPv6 in the sense that it extends MIPv6 signaling and reuses many concepts such as the HA functionality. However, PMIPv6 is designed to provide network-based mobility management support to an MN in a topologically localized domain. Therefore, an MN is exempt from participation in any mobility-related signaling, and the proxy mobility agent in the serving network performs mobility-related signaling on behalf of the MN. Once an MN enters its PMIPv6 domain and performs access authentication, the serving network ensures that the MN is always on its home network and can obtain its HoA on any access network. That is, the serving network assigns a unique home network prefix to each MN, and conceptually this prefix always follows the MN wherever it moves within a PMIPv6 domain. From the perspective of the MN, the entire PMIPv6 domain appears as its home network. Accordingly, it is needless (or impossible) to configure the CoA at the MN.

The new principal functional entities of PMIPv6 are the mobile access gateway (MAG) and local mobility anchor (LMA). The MAG typically runs on the AR. The main role of the MAG is to detect the MN's movements¹ and initiate mobility-related signaling with the MN's LMA on behalf of the MN. In addition, the MAG establishes a tunnel with the LMA for enabling the MN to use an address from its home network prefix and emulates the MN's home network on the access network for each MN. On the other hand, the LMA is similar to the HA in MIPv6. However, it has additional capabilities required to support PMIPv6. The

¹ Typically, there are various link-layer-specific events on which the MAG can depend for detecting the MN's attachment and detachment within a PMIPv6 domain. For example, the help of layer 2 triggers such as MN_ATTACH and MN_DETACH may be needed [9].

Unlike MIPv6, a tunnel in PMIPv6 is established between the LMA and the MAG, and not an MN. This could be desirable because the tunneling increases the bandwidth constraints on the wireless link and the processing burden on the MN.



■ Figure 2. Message flow in PMIPv6.

main role of the LMA is to maintain reachability to the MN's address while it moves around within a PMIPv6 domain, and the LMA includes a binding cache entry for each currently registered MN. The binding cache entry maintained at the LMA is more extended than that of the HA in MIPv6 with some additional fields such as the MN-Identifier, the MN's home network prefix, a flag indicating a proxy registration, and the interface identifier of the bidirectional tunnel between the LMA and MAG. Such information associates an MN with its serving MAG, and enables the relationship between the MAG and LMA to be maintained.

Figure 1 illustrates an overview of how PMIPv6 works within a localized domain. The brief descriptions of the basic terminology are also shown in this figure.

MESSAGE FLOW OF PMIPv6

Figure 2 shows the message flow of the overall operations in PMIPv6. Each step shown in Fig. 2 is described as follows:

Steps 1 and 2: When an MN first attaches to an access network connected to the MAG, the access authentication procedure is performed using an MN's identity (i.e., MN-Identifier) via the deployed access security protocols on the access network.

Step 3: After successful access authentication, the MAG obtains the MN's profile, which contains the MN-Identifier, LMA address, supported address configuration mode, and so on from the policy store (e.g., authentication, authorization, and accounting [AAA] server).

Step 4: Then the MAG sends a proxy binding update (PBU) message including the MN-Identifier to the MN's LMA on behalf of the MN.

Steps 5 and 6: Once the LMA receives the PBU message, it checks the policy store to ensure that the sender is authorized to send the PBU

message. If the sender is a trusted MAG, the LMA accepts the PBU message.

Step 7: Then the LMA sends a proxy binding acknowledgment (PBA) message including the MN's home network prefix option, and sets up a route for the MN's home network prefix over the tunnel to the MAG.

Unlike MIPv6, a tunnel in PMIPv6 is established between the LMA and the MAG, and not an MN. This could be desirable because the tunneling increases the bandwidth constraints on the wireless link and the processing burden on the MN. Once the MAG receives the PBA message from the LMA, it has obtained all the required information to emulate the MN's home network on the access network, and it then starts to send a router advertisement (RA) message to the MN. It is noted that the RA message contains the MN's home network prefix. After receiving the RA message, the MN configures its home address by combining the home network prefix included in the RA message and its interface address, which is based on the supported address configuration mode (e.g., stateless or stateful address configuration mode) from the policy store. It must be noted that since PMIPv6 only supports the per-MN-prefix model and not the shared-prefix model, a unique home network prefix is assigned to each MN. Therefore, unlike MIPv6 and its various enhancements, the MN always obtains its unique home address while it moves within a PMIPv6 domain.

After the bidirectional tunnel is successfully set up, all traffic sent from the MN gets routed to its LMA through the tunnel. The LMA receives any data packets sent by the CN to the MN. The LMA forwards the received packet to the MAG through the tunnel. After receiving the packets, the MAG on the other end of the tunnel removes the outer header and forwards the packets to the MN.

Category	MIPv6	PMIPv6
Mobility management type	Host-based mobility management	Network-based mobility management
Mobility scope	Global mobility	Localized mobility
Functionally correspondent entity	HA	LMA (i.e., HA functionality with additional capabilities)
Topologically correspondent entity	AR	MAG
MN modification	Yes	No
Location registration message	Binding update message	Proxy binding update message
MN address	HoA or CoA	HoA (always)
Relation between tunnel and binding cache entry	1:1 relation (i.e., HA-MN tunnel)	1:m relation (i.e., LMA-MAG tunnel)
Tunneling over wireless link	Required	Not required
Router advertisement type	Broadcast	Unicast
Lookup key in binding cache	HoA	MN identifier
Addressing model	Shared-prefix model	Per-MN-prefix model
Supported link type	Any type of link	Point-to-point link
Route optimization	Supported	Not supported
Movement detection	Required (performed by RS/RA)	Not required (performed by layer 2)
Duplicate address detection (DAD)	Performed at every subnet movement	Performed only one time (at initial movement into the domain)
Return routability	Required	Not required

■ **Table 1.** Comparison between MIPv6 and PMIPv6.

QUALITATIVE ANALYSIS

In this section we qualitatively investigate PMIPv6 based on various evaluation criteria and compare it with various existing well-known mobility support protocols as well as MIPv6. A synopsis of the main characteristics, including the strong and weak points of PMIPv6 compared to the various existing well-known mobility support protocols, is provided in Tables 1 and 2.

COMPARISON BETWEEN MIPv6 AND PMIPv6

We first compare MIPv6 and PMIPv6 in terms of some high-level characteristics and performance aspects, which are shown in Table 1. MIPv6 is a host-based solution for handling the global mobility of hosts in IPv6 networks. This means that a host is involved in mobility-related signaling; thus, a modification of the host protocol stack is required for operating MIPv6 (i.e., an MN sends the BU message for location registration). In contrast, PMIPv6 provides a network-based solution for handling the localized mobility of hosts in IPv6 networks (i.e., a network entity, the MAG, sends the PBU message for location registration). Therefore, no requirement of the hosts is needed. Moreover, PMIPv6 can also support IPv4 as well as IPv6 by specifying

some extensions for supporting the IPv4 tunneling mechanism and specific encapsulation modes.

Basically, PMIPv6 attempts to reuse MIPv6 because MIPv6 is a considerably mature protocol with several implementations that have been realized through interoperability testing. Thus, the functionality of the LMA in PMIPv6 can be considered as an enhanced HA with additional capabilities. In MIPv6 a bidirectional tunnel is established between the HA and each MN, whereas a bidirectional tunnel in PMIPv6 is established between the LMA and MAG, not each MN. This is because the MN is not involved in any type of mobility-related signaling. As in MIPv4 [2], the bidirectional tunnel between the LMA and MAG is typically a shared tunnel, and can be employed for routing traffic streams for different MNs attached to the same MAG. It extends the 1:1 relation between a tunnel and an MN's binding cache entry to a 1:m relation, reflecting the shared nature of the tunnel.

MIPv6 employs the shared-prefix model in which multiple MNs in the same subnet are configured with a common IPv6 network prefix. In contrast, PMIPv6 employs the per-MN-prefix

Protocol criteria	MIPv4	MIPv6	HMIPv6	FMIPv6	Cellular IP	SIP	SCTP	PMIPv6
Operating layer	Network layer	Network layer	Network layer	Network layer	Network layer	Application layer	Transport layer	Network layer
Mobility scope	Global	Global	Local	Local/global	Local	Local/global	Local/global	Local
Location management	Yes	Yes	Yes	No	Yes	Yes	No	Yes
Handover management	Yes (limited)	Yes (limited)	Yes	Yes	Yes	No	Yes	Yes
Required infrastructure	HA, FA	HA	HA, MAP	HA, enhanced AR	Enhanced BS	Registrar	None	LMA, MAG
MN modification	Yes	Yes	Yes	Yes	Yes	No	Yes	No
Handover latency	Bad	Bad	Moderate	Good	Good	Bad	Good	Good ¹
Route optimization	No	Yes	Yes	—	No	Yes	Yes	No

¹ Stateless address autoconfiguration is assumed.

■ **Table 2.** Comparison between PMIPv6 and various well-known mobility support protocols.

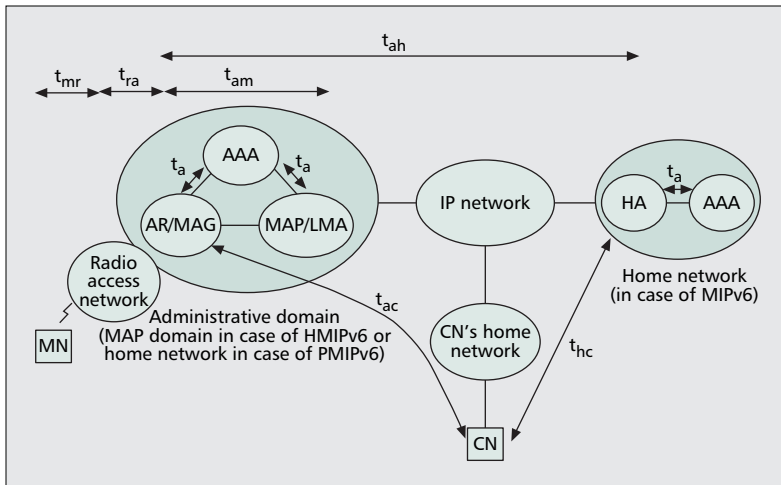
model. Hence, a unique home network prefix is assigned to each MN, and no other MN shares this prefix. Therefore, the prefix follows the MN while the MN moves within a PMIPv6 domain, so the network layer movement detection and duplicate address detection (DAD) processes are not required within a PMIPv6 domain (note that for inter-PMIPv6 domain movement, network layer movement detection and DAD are performed) [9]. In contrast, for MIPv6, movement detection and DAD, which are time-consuming operations that can degrade handover performance significantly, are essential during every subnet movement. With regard to some aspects such as movement detection, DAD, and return routability [1], it can easily be deduced that PMIPv6 is superior to MIPv6, as shown in Table 1. However, for route optimization, PMIPv6 does not have a corresponding capability. In PMIPv6 an individual RA message should be unicast to the MN because PMIPv6 only supports the per-MN-prefix model. However, MIPv6 supports the shared-prefix model; thus, the RA message is broadcast in the same network. The choice of the per-MN-prefix model in PMIPv6 conflicts with the use of a shared link layer (e.g., Ethernet, IEEE 802.11) as the last hop in a PMIPv6 domain. Hence, the type of supported link in PMIPv6 is simply point-to-point. Detailed descriptions are provided in [9].

COMPARISON BETWEEN PMIPv6 AND VARIOUS WELL-KNOWN MOBILITY SUPPORT PROTOCOLS

In Table 2 we provide a summary of the main characteristics of PMIPv6 compared to various other existing well-known mobility support protocols such as MIPv6 enhancements (e.g., HMIPv6 and FMIPv6), IP micromobility protocols (e.g., Cellular IP) [10], transport layer mobility support protocol (e.g., SCTP), and

application layer mobility support protocol (e.g., SIP). A detailed description of each of these mobility support protocols is provided in [3, 6, 7, 10]. In this article we assume that readers are reasonably familiar with these protocols. Basically, MIPv4/v6 and their enhancement protocols except FMIPv6 support location and handover management functionalities to some extent. On the other hand, SCTP does not support location management, and SIP does not support handover management. Therefore, in terms of mobility management, these protocols might not be entirely suitable by themselves. Realizing successful deployment of MIPv4/v6 and their enhancement protocols basically requires the addition or modification of some functionality in both the network and MN. In contrast, PMIPv6 requires no modification of the MN's protocol stack.

Generally, most of existing mobility support protocols have been developed for their own characteristic purposes and suitable environments. For example, Cellular IP, HMIPv6, and PMIPv6 have been proposed to reduce handover and registration latencies in a localized domain. Similar to PMIPv6, Cellular IP maintains a single IP address while changing subnets within a domain. However, it has some inherent drawbacks, such as lack of scalability, incurred by establishing host-specific routes. For HMIPv6, although it is an efficient localized mobility management protocol that can reduce handover latency significantly compared to MIPv6, it still requires movement detection and DAD because the MN's on-link CoA (LCoA) should be newly assigned whenever the MN moves to another subnet within a domain. However, the performance of handover latency in PMIPv6 appears to be better than that of HMIPv6 because the MN within a PMIPv6 domain always uses the same home address, and hence does not perform movement detection and DAD.



■ **Figure 3.** A simple analytical model for performance analysis.

QUANTITATIVE ANALYSIS

From the viewpoint of the network layer approach, mobility management protocols can be classified into three types of approaches. MIPv6 and HMIPv6 can be considered representative host-based global mobility management and representative host-based localized mobility management protocols, respectively. They have been standardized by the IETF, which is the organization for defining Internet protocols. Similarly, PMIPv6 can be considered a representative network-based localized mobility management protocol. It is also being standardized by the IETF. Currently, a network-based global mobility management protocol is not available and does not appear to be developed, because only the MN rather than the network can detect and select a new serving network. Instead, in order to develop a globally deployable Internet-based easy-to-use mobility management architecture, a combination of host-based global mobility management and network-based localized mobility management would be a good choice [11]. In this section we focus on a quantitative analysis among MIPv6, HMIPv6, and PMIPv6 on handover latency, which is one of the most critical factors in next-generation all-IP mobile networks.

BASIC ASSUMPTIONS AND HANDOVER LATENCY ANALYSIS

For performance analysis, similar to [12], we consider a simple analytical model shown in Fig. 3. We use the following notations:

- The delay between the MN and AP is t_{mr} , which is the time required for a packet to be sent between the MN and AP through a wireless link.
- The delay between the AP and AR/MAG is t_{ra} , which is the time between the AP and the AR/MAG connected to the AP.
- The delay between the AR/MAG and MAP/LMA (i.e., the delay between the AR and MAP in HMIPv6 or between the MAG and LMA in PMIPv6) is t_{am} .
- The delay between the AR/MAG and HA is t_{ah} .

- The delay between the AR/MAG and CN is t_{ac} , which is the time required for a packet to be sent between the AR/MAG and the CN, and not via the HA.
- The delay between the HA and CN is t_{hc} .
- The delay between the mobility agents and AAA is t_a .

For simplicity, we make the following assumptions:

- For a fair analysis of these protocols under the same network structure, the administrative domain can be applied as follows. From the perspective of MIPv6, the administrative domain is assumed to be simply a foreign network. From the perspective of HMIPv6, it is assumed to be a foreign MAP domain. Similarly, for PMIPv6, it is assumed to be a home network domain because the MN always moves around within a home network regardless of its point of attachment.
- Based on the above assumption, the mobility agents of each protocol follow the mapping scenario shown in Fig. 3. For example, if PMIPv6 is considered, the location of the LMA is assumed to be the same as that of the MAP in HMIPv6 because they both have functionalities similar to the HA in MIPv6 within a localized administrative domain.
- For a fair analysis, we assume that the MNs are allowed to access a serving network after the AAA procedure is completed, and these access delays are assumed to be all the same for MIPv6, HMIPv6, and PMIPv6.
- Address configuration is only performed by means of stateless address autoconfiguration, and the time required to combine the network prefix obtained from the RA message to its interface is negligible in the case of address configuration delay.
- All the delays mentioned above are symmetric.
- The delay between the MN and CN is shorter than the sum of the delays between the MN and HA and between the HA and CN.
- For simplicity, router solicitation (RS) messages are not considered here. Thus, only RA messages can affect the movement detection of the MN.

Generally, IP handover latency can be expressed as the sum of the movement detection delay (T_{MD}), address configuration delay (T_{DAD}), the delay involved in performing the AAA procedure (T_{AAA}), and location registration delay (T_{REG}). In this article, more specifically, *handover latency* is defined as the time that elapses between the moment the layer 2 handover completes and the moment the MN can receive the first data packet after moving to the new point of attachment.

In order to estimate the movement detection delay, based on the above assumptions, we only consider the delay caused by the reception of an unsolicited RA message without considering an RS message. Therefore, in this case the movement detection delay depends on the period of the RA message. In [1] it is specified that the routers for supporting mobility should be able to be configured with a smaller `MinRtrAdvInterval` ($= \text{MinInt}$) value and `MaxRtrAdvInterval` ($= \text{MaxInt}$) value in order to allow sending unsolicited RA messages more often. The mean

time between unsolicited RA messages can be expressed as $(\text{MinInt} + \text{MaxInt})/2$. Therefore, for simplicity, we assume that the mean value of movement detection delay (T_{MD}) in MIPv6 and HMIPv6 is half of the mean time between unsolicited RA messages; thus, $T_{MD} = (\text{MinInt} + \text{MaxInt})/4$. More detailed analysis of movement detection delay can be found in our previous study [13]. After an MN detects network layer movement, new prefix information of the network (or subnet) becomes available to the MN. From the prefix information, a new CoA is generated by means of IPv6 stateless (or stateful) address autoconfiguration. In order to verify the uniqueness of this CoA, it performs the DAD process before combining the network prefix to its interface. During this process, the MN cannot use the CoA for communication. Therefore, according to [13], the DAD delay in MIPv6 and HMIPv6 can be simply expressed as $T_{DAD} = R \times D$, where R and D denote `RetransTimer` and `DupAddrDetectTransmits` specified in [14], respectively. From the perspective of network service providers, in order to make mobile services feasible in public wireless Internet, AAA functions performed by AAA protocols such as DIAMETER must be implemented. Based on the above assumption, these access delays (T_{AAA}) are all the same; thus, $T_{AAA} = 2 \times 2t_a = 4t_a$ for the three protocols (i.e., one access is performed between AR/MAG and AAA, the other between HA/MAP/LMA and AAA).

On the other hand, the registration delay in MIPv6 (T_{REG}^{MIPv6}) requires the time equivalent to the sum of the HA registration delay (i.e., $2(t_{mr} + t_{ra} + t_{ah})$) and the CN registration delay (i.e., $2(t_{mr} + t_{ra} + t_{ac})$). Moreover, in order to register with the CN, the delay for return routability (i.e., $2(t_{mr} + t_{ra} + t_{ah} + t_{hc})$) [1] is additionally required prior to the CN registration. Therefore, including all the factors mentioned above, the handover latency in MIPv6 (D_{HO}^{MIPv6}) can be expressed as follows:

$$D_{HO}^{MIPv6} = T_{MD} + T_{DAD} + T_{AAA} + T_{REG}^{MIPv6} \quad (1)$$

$$\text{where } T_{REG}^{MIPv6} = 6(t_{mr} + t_{ra}) + 4t_{ah} + 2(t_{ac} + t_{hc}).$$

Unlike MIPv6, the registration delay in HMIPv6 (T_{REG}^{HMIPv6}) only requires the MAP registration delay (i.e., $2(t_{mr} + t_{ra} + t_{am})$) without the requirement of the CN registration delay within a MAP domain. This is because the MN's movement within a MAP domain is transparent outside of the MAP domain. Therefore, including all the factors mentioned above, the handover latency in HMIPv6 (D_{HO}^{HMIPv6}) within a MAP domain can be expressed as follows:

$$D_{HO}^{HMIPv6} = T_{MD} + T_{DAD} + T_{AAA} + T_{REG}^{HMIPv6} \quad (2)$$

Unlike MIPv6 and HMIPv6, PMIPv6 does not require movement detection and DAD except when the MN first enters a PMIPv6 domain. In addition, the MN's movement within a PMIPv6 domain is also transparent outside of the PMIPv6 domain because PMIPv6 is a localized mobility management protocol similar to HMIPv6. Therefore, the handover latency in

PMIPv6 can be composed of the sum of the AAA access delay (T_{AAA}), the registration delay between the MAG and LMA (T_{REG}^{PMIPv6}), and the packet transmission delay from the MAG to the MN (i.e., $(t_{mr} + t_{ra})$). Finally, the handover latency in PMIPv6 (D_{HO}^{PMIPv6}) within a PMIPv6 domain can be simply expressed as follows:

$$D_{HO}^{PMIPv6} = T_{AAA} + T_{REG}^{PMIPv6} + t_{mr} + t_{ra} \quad (3)$$

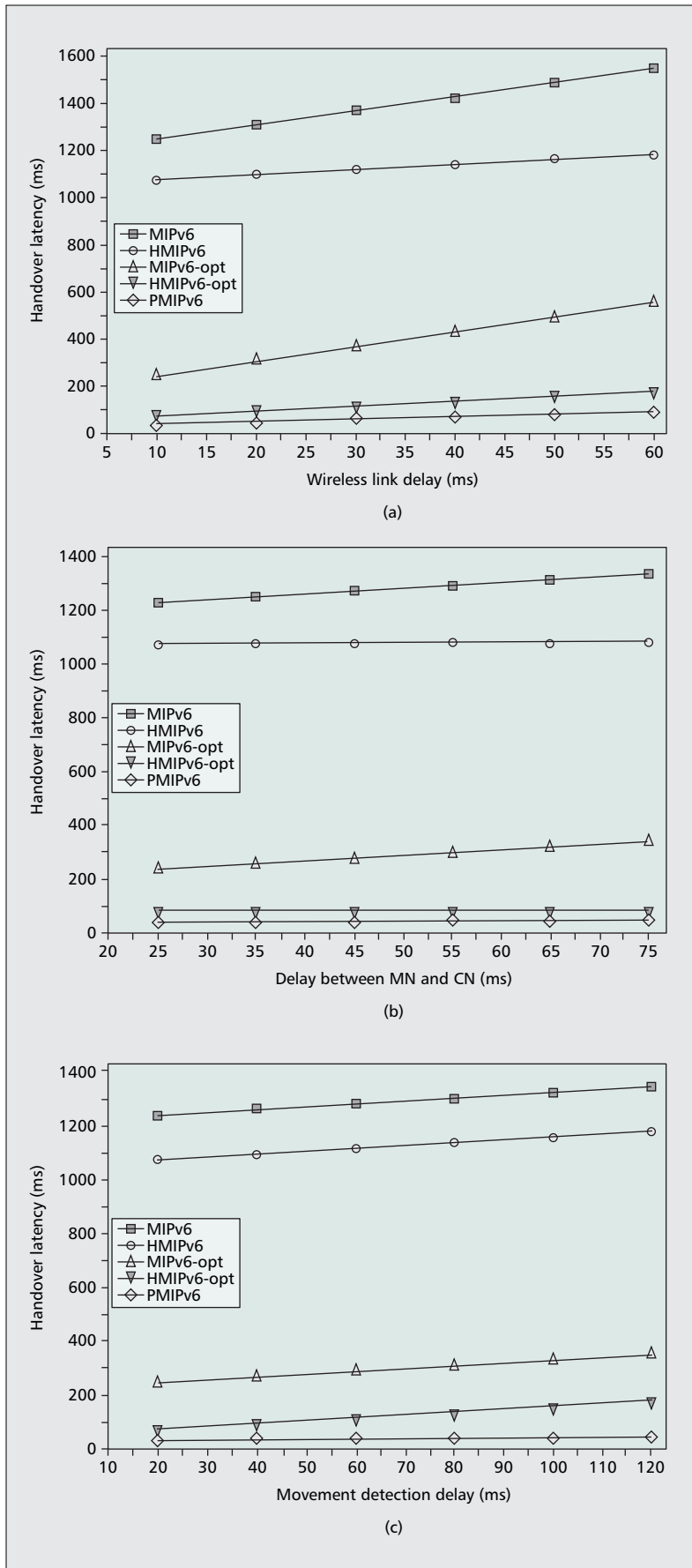
where $T_{REG}^{PMIPv6} = 2t_{am}$.

NUMERICAL RESULTS

Here, we show the numerical results based on the analysis derived in the previous subsection. Although we only focus on analyzing the handover latency within a domain in order to simplify the analysis because there are various possible scenarios [15] for interdomain movement, we believe that this analysis could fully reflect the main features of each protocol. For our analysis, t_{mr} is assumed to be 10 ms, considering the relatively low bandwidth in the wireless link, and the other parameters used are as follows: $t_{ra} = 2$ ms, $t_{am} = t_{hc} = 10$ ms, $t_{ah} = t_{ac} = 20$ ms, and $t_a = 3$ ms, respectively. All these values are the same or similar to the parameter setting values given in [12]. We set $\text{MinInt} = 30$ ms and $\text{MaxInt} = 70$ ms [1], and $R = 1000$ ms and $D = 1$ [13, 16], respectively.

Impact of Wireless Link Delay — Figure 4a shows the impact of t_{mr} on handover latency. For all of the mobility support protocols, it can be observed that handover latencies increase with the wireless link delay even if the slopes of each graph are different from each other. MIPv6 is most affected by the change in wireless link delay because it requires the largest number of messages (e.g., the message exchanges for the BU or binding acknowledgment (BA) to/from the HA, the return routability procedure, and the BU for the CN) to be exchanged over the wireless link. In contrast, PMIPv6 is least affected because the MN is not involved in mobility-related signaling. In particular, it must be noted that the handover latencies of MIPv6 and HMIPv6 based on RFC 2462 [14] are significantly larger than that of PMIPv6. This is because the time required for the DAD process in MIPv6 and HMIPv6 is considerably larger than the delays caused by other factors that may affect handover latency. As mentioned earlier, the DAD process is very time consuming. Hence, several efforts to optimize DAD latency have been undertaken. For example, the IETF IPv6 working group has attempted to revise RFC 2462, which specifies that the IPv6 DAD process consumes at least 1000 ms, and some enhancements such as optimistic DAD (oDAD, RFC 4429 [17]) have been made recently. Based on the premise that DAD is far more likely to succeed than fail, oDAD provides an approach to eliminate the DAD delay. Although oDAD reduces the handover latency in the non-collision case, it can incur some penalty for both the optimistic MN and the rightful owner of the address if address collision occurs. Hence, for our analysis of handover latency in MIPv6 and HMIPv6, we evaluated the handover latencies based on both RFC 2462 and RFC 4429, respectively.

Unlike MIPv6 and HMIPv6, PMIPv6 does not require the movement detection and the DAD processes except when the MN first enters a PMIPv6 domain. In addition, the MN's movement within a PMIPv6 domain is also transparent to the outside of the PMIPv6 domain.



■ **Figure 4.** Comparison between handover latencies in MIPv6, HMIPv6, and PMIPv6: a) impact of wireless link delay; b) impact of delay between MN and CN; c) impact of movement detection delay.

Impact of Delay between MN and CN — Figure 4b shows the impact of $(t_{mr} + t_{ra} + t_{ac})$ on handover latency. Since we evaluate handover latency only for intradomain movement, HMIPv6 and PMIPv6 do not require registration to the CN because the MN's movement within a domain is transparent outside the domain. That is, the delay between the MN and CN does not affect the handover latency of each protocol within a domain. However, for MIPv6, the handover latency increases with the delay between the MN and CN. This is because MIPv6 requires registration to both the HA and CN whenever the MN moves across subnets; thus, the increase in the delay between the MN and CN affects the increase in handover latency in MIPv6.

Impact of Movement Detection Delay — Figure 4c shows the impact of T_{MD} on handover latency. As mentioned earlier, in PMIPv6 movement detection does not occur except when the MN moves across a PMIPv6 domain. This is due to the fact that since PMIPv6 only supports the per-MN-prefix model, a unique home network prefix is assigned to each MN. That is, from the perspective of the MN, the entire PMIPv6 domain appears as its home network. In other words, the MN is not related to movement detection delay in intradomain movement. On the contrary, the graphs for MIPv6 and HMIPv6 increase with the same slope as the movement detection delay does. In MIPv6 and HMIPv6, whenever the MN moves across subnets, it configures the different CoAs via stateless (or stateful) address autoconfiguration. Therefore, in MIPv6 and HMIPv6, movement detection should be performed as quickly as possible in order to minimize handover latency and packet loss. Increased movement detection delay results in increased handover latency, and this could cause significant degradation to be experienced by the MNs.

CONCLUDING REMARKS

To the best of our knowledge, this article is the first to provide qualitative and quantitative analyses of MIPv6 and PMIPv6. In this article our analysis results demonstrate the superiority of PMIPv6. Although various IP mobility support protocols have been proposed, from the perspective of the practical deployment of each protocol, a confrontation has existed between the telecommunications and Internet communities for a long time. However, PMIPv6 could be considered a promising compromise between them. It is a practical derivative of MIPv6 rather than a new idea, and could be considered a turn for the better because it reflects telecommunication operators' favor, enabling them to manage and control their networks more efficiently.

Although we have chiefly focused on the comparison between MIPv6 and PMIPv6 in this article, the interactions between them would also be possible. For example, similar to the HMIPv6-MIPv6 interaction, PMIPv6 could be used as a localized mobility management protocol, whereas MIPv6 could be used as a global mobility management protocol. Details on the various interaction scenarios and related issues can be

found in [15]. Future research will explore cross-layering issues (e.g., PMIPv6 over IEEE 802.11 or 802.16e networks) as well as route optimization and fast handover issues in PMIPv6.

ACKNOWLEDGMENTS

This work was supported in part by the Korea Research Foundation Grant funded by the Korean Government (MOEHRD) [KRF-2006-331-D00539], and in part by the Ministry of Information and Communication (MIC), Korea, under ITRC IITA-2007-(C1090-0701-0046).

REFERENCES

- [1] D. Johnson, C. Perkins, and J. Arkko, "Mobility Support in IPv6," IETF RFC 3775, June 2004.
- [2] C. Perkins, "IP Mobility Support for IPv4," IETF RFC 3344, Aug. 2002.
- [3] N. Banerjee, W. Wu, and S. K. Das, "Mobility Support in Wireless Internet," *IEEE Wireless Commun.*, vol. 10, no. 5, Oct. 2003, pp. 54–61.
- [4] J. Kempf, "Problem Statement for Network-Based Localized Mobility Management (NETLMM)," IETF RFC 4830, Apr. 2007.
- [5] S. Gundavelli *et al.*, "Proxy Mobile IPv6," IETF Internet draft, draft-ietf-netlmm-proxymip6-01.txt, June 2007, work in progress.
- [6] H. Soliman, C. Castelluccia, K. E. Malki, and L. Bellier, "Hierarchical Mobile IPv6 Mobility Management (HMIPv6)," IETF RFC 4140, Aug. 2005.
- [7] R. Koodli, "Fast Handover for Mobile IPv6," IETF RFC 4068, July 2005.
- [8] J. Kempf, "Goals for Network-Based Localized Mobility Management (NETLMM)," IETF RFC 4831, Apr. 2007.
- [9] J. Laganier and S. Narayanan, "Network-Based Localized Mobility Management Interface Between Mobile Node and Mobility Access Gateway," IETF Internet draft, draft-ietf-netlmm-mn-ar-if-02, May 2007, work in progress.
- [10] P. Reinbold and O. Bonaventure, "IP Micro-Mobility Protocols," *IEEE Commun. Surveys & Tutorials*, vol. 5, no. 1, 3rd qtr. 2003, pp. 40–56.
- [11] P. Roberts and J. Kempf, "Mobility Architecture for the Global Internet," *Proc. MobiArch '06*, Dec. 2006, pp. 23–28.
- [12] H. Faithi and R. Prasad, "Mobility Management for VoIP in 3G Systems: Evaluation of Low-Latency Handoff Schemes," *IEEE Wireless Commun.*, vol. 12, no. 2, Apr. 2005, pp. 96–104.
- [13] Y. Han, J. Choi, and S. Hwang, "Reactive Handover Optimization in IPv6-Based Mobile Networks," *IEEE JSAC*, vol. 24, no. 9, Sept. 2006, pp. 1758–72.
- [14] S. Thomson and T. Narten, "IPv6 Stateless Address Autoconfiguration," IETF RFC 2462, Dec. 1998.
- [15] H. Soliman and G. Garetta, "Interactions Between PMIPv6 and MIPv6: Scenarios and Related Issues," IETF Internet draft, draft-garetta-netlmm-mip-interactions-00, Apr. 2007, work in progress.
- [16] T. Narten, E. Nordmark, and W. Simpson, "Neighbor Discovery for IP Version 6," IETF RFC 2461, Dec. 1998.
- [17] N. Moore, "Optimistic Duplicate Address Detection (DAD) for IPv6," IETF RFC 4429, Apr. 2006.

BIOGRAPHIES

KI-SIK KONG (kisik.kong@gmail.com) received his B.S., M.S. and Ph.D. degrees in computer science and engineering from Korea University in 1999, 2001, and 2005, respectively. From 1999 to August 2005 he was a researcher in the Research Institute of Computer Information and Communication at Korea University. From September 2005 to

August 2007 he was a research professor at Korea University and Ewha Womans University. Currently, he is a research professor in the Department of Computer Science and Engineering at Korea University. His research interests include IP mobility/QoS support, performance modeling, and optimization issues in next-generation wireless mobile networks. He was listed in Marquis *Who's Who in Science and Engineering* (2006–2007, 2008–2009), *Who's Who in the World* (2008), and *Outstanding Scientists of the 21st Century* (2007–2008), respectively.

YOUN-HEE HAN [M] (yhhan@kut.ac.kr) received his B.S. degree in mathematics from Korea University in 1996. He received his M.S. and Ph.D. degrees in computer science and engineering from Korea University in 1998 and 2002, respectively. From March 4, 2002 to February 28, 2006 he was a senior researcher in the Communication and Network Group of Samsung Advanced Institute of Technology. Since March 2, 2006 he has been a professor in the School of Internet-Media Engineering at Korea University of Technology and Education, CheonAn. His primary research interests include theory and application of mobile computing, including protocol design and performance analysis. Since 2002 his activities have focused on IPv6, IPv6 mobility, media-independent handover, and cross-layer optimization for efficient mobility support in IEEE 802 wireless networks. He is a member of IEICE. He has also made several contributions to IETF and IEEE standardization. Currently, he is chair of the IPv6 over WiBro working group of TTA IPv6 Project Group in Korea.

MYUNG-KI SHIN (mkshin@etri.re.kr) is currently a senior researcher at the Protocol Engineering Center of the Electronics and Telecommunications Research Institute (ETRI), Korea. He is a technical leader of the Mobile Router project in ETRI. He has been working on IP protocols since 1994. His research interests include IPv6, Mobile IPv6, multicast, and future network technologies. He was also a guest researcher at the U.S. National Institute of Standards and Technology in 2004–2005. He is actively involved in IETF IP related WGs (IPv6, multicast, mobility). He is an author of several IETF RFCs (RFC 3338, RFC 4038, RFC 4489, etc.). He is also a member of the CTO Executive Committee of the IPv6 Forum. He received a Ph.D. degree in computer engineering doing research on IPv6 multicast and mobility from Chungnam National University in 2003.

HEUNG-RYEOL YOU (hryou@kt.com) received B.S., M.S., and Ph.D. degrees in electronic engineering from Yonsei University, Seoul, Korea, in 1985, 1987, and 2002, respectively. He has been a research engineer with Korea Telecom Authority (now KT), Seoul, Korea, since 1987 and is currently director of the Infra Laboratory, KT. His research interests are in the areas of mobility management, seamless mobility, wireless communication network and system design, and position location technologies.

WONJUN LEE [SM] (wlee@korea.ac.kr) received B.S. and M.S. degrees in computer engineering from Seoul National University in 1989 and 1991, respectively, an M.S. in computer science from the University of Maryland, College Park in 1996, and a Ph.D. degree in computer science and engineering from the University of Minnesota, Minneapolis in 1999. In 1998 he was a research associate at Stanford Research International (SRI), Menlo Park, California. In March 2002 he joined the faculty of Korea University, where he is currently an associate professor in the Department of Computer Science and Engineering. He has published over 45 journal papers with IEEE, Elsevier, and Springer-Verlag. His research interests include mobile communications and protocol engineering applied to wireless systems.

A confrontation has existed between the telecommunication and the Internet communities for a long time. However, PMIPv6 could be considered as a promising compromise between them. It is a practical derivative of MIPv6, rather than a new idea.