Review on Mobility Management for Future-IP-based Next Generation Wireless Networks

Ibrahim Al-Surmi*, Mohamed Othman*, Borhanuddin M. Ali**

*Dept of Communication Tech and Network

**Dept of Computer and Communications Systems Engineering

University Putra Malaysia

43400 UPM Serdang, Selangor D.E., Malaysia

iaa_a@yahoo.com, mothman@fsktm.upm.edu.my, borhan@eng.upm.edu.my

***Abstract*— The mobility support protocols are separated by two categories; First, Host-based mobility management protocols such as Mobile IPv6, and its enhancements (HMIPv6 and FMIPv6) which all basically requires protocol stack modification of the mobile node in order to support them. That modification may increase the complexity on them and wasting of air resource. Besides, some drawbacks that still suffers such as high handover latency, energy consumption, packet loss, and signaling overhead. Secondly, Network-based localized mobility management such as Proxy Mobile IPv6 that attract a fair amount of critical attention in the Internet communities. The serving network handles the mobility management on behalf of the mobile node. Thus the mobile node is not required to participate in any mobility related signaling. In this paper we investigate the two categories and explore the technology aspects. Description of IEEE 802.11 access network handover management was also reviewed. In addition, a comparison for existing mobility management protocols was presented for a better analysis. Furthermore, related research issues and challenges that facing mobility management are also identified.**

***Keywords*—IPv6, Host-based Mobility, Network based Mobility, MIPv6, PMIPv6, Handover latency.**

I. INTRODUCTION

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 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 that 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). The Host-based mobility protocol called Mobile IPv6 [5] 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 [2], it has still revealed some problems such as handover latency, power consumption, high packet loss and signalling overhead Furthermore, despite the reputation of this protocol, it has been slowly deployed in real implementations [3]. Therefore, various enhancements such as FMIPv6 [6] and HMIPv6 [7] focused on performance improvements of MIPv6. However, they require protocol stack modification of the mobile node (MN). In addition, the requirement for modification of MN's may cause increased complexity on them and introduce battery problem and waste of air resource. Recently, a network-based mobility management protocol called Proxy Mobile IPv6 (PMIPv6) [1] is being actively standardized by the IETF NETLMM working group, and it has salient features and is expected to expedite the real deployment of IP mobility management. It handles the mobility management on behalf of the MN. Thus, the MN is not required to participate in any mobility-related signaling, it is easy deployment and low installation cost. The mobility management categories illustrate in the Figure 1. This paper focuses on review the mobility management categories, provides a compression and related research issues.

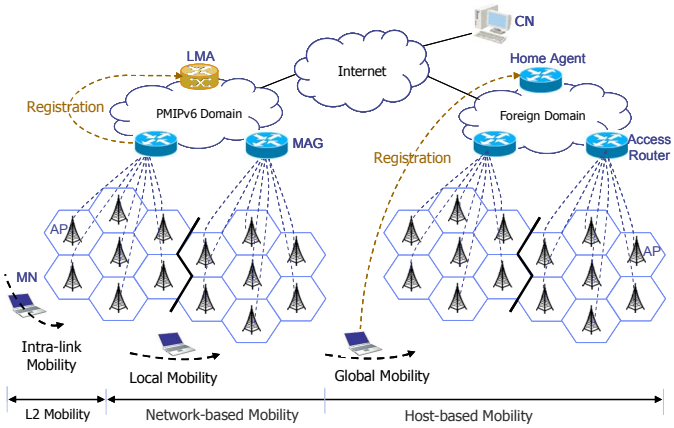

Figure 1. Mobility Managemnet's categories

The rest of the paper is organized as follows: Section II introduce mobility management protocols. In the section III an overview of IEEE 802.11 access network handover management. Section IV provides a comparison between host-based mobility management and network-based mobility management protocols. Research issues and challenges in Section V. Last section VI, the paper is concluded.

II. Overview on Mobility Management protocols

In this sections an overview of IPv6, Host-based mobility and Network-based mobility management protocols.

A. *Internet Protocol Version6*

The new version of IP that is make mobility easier to handle by defines some new features, as below:

1) ***IPv6 Addresses:*** There are different scopes of IPv6 addresses that can be differentiated by looking at certain bit patterns of the address prefix. The most important scopes in IPv6 are: First Link local address that can be used to communicate within the node's link and its packets address will not be routed outside the link. Second Site local address these addresses within a site are unique, A network administrator will define the size of a site depend on it is need. Third is the Global Address, an address with a global scope is globally unique, so its packets address can be routed anywhere. IPv6 define three types of addresses:

- **Unicast:** The most used addresses, every unicast address belongs to only one interface.
- **Multicast:** This address belongs to more than one interface. A node with multicast address will receive all packets sent to this multicast address.
- **Anycast:** It is the new types of address, and it is also assigned to more than one interface like the multicast address, but if a packet is sent to such an address, it will only be delivered to one of the interfaces.

2) ***Neighbour Discovery:*** Neighbour Discovery [9] works per link which means that such messages will not be routed out of a link. It is done by sending ICMPv6 messages. The cases for which the Neighbour Discovery can be used are:

- Link layer independent that is the way of finding link layer address for nodes. This is similar to the Address Resolution Protocol in IPv4.
- Discover default routers on a link therefore routers advertise there address in a regular time interval.
- Neighbour Unreachability Detection can be used to check whether a particular neighbour is still on the link.
- Duplicate Address Detection (DAD) is used to determine the uniqueness of the configured addresses on a particular link.
- Address Autoconfiguration for a node to obtain or generate its own addresses by using stateful or stateless address autoconfiguration respectively.

3) ***IPv6 Address Autoconfiguration:*** The address autoconfiguration in IPv6 [12] creates a link local address, verifies its uniqueness on the link and determines whether the addresses should be obtained through stateful or stateless methods. The Stateful Address Autoconfiguration allows an IPv6 node to obtain interface addresses and configuration information from a server; that maintains a database to checks which addresses have been assigned to which nodes. This case can be recognized through mechanisms such as DHCPv6. and Stateless Address Autoconfiguration allows an IPv6 node to generate its own addresses, by deduce an IPv6 address from the link prefix that usually gets advertised by routers on that link. An address is formed by combining the link prefix and the node interface identifier. In the absence of routers, a host can generate only link local addresses that are only sufficient for allowing communication among nodes that are attached to the same link. It is important to note that if a MN can configure a Care-of Address in the stateless manner, the whole address configuration process takes less time than if the node would use DHCPv6 or listen for router advertisements.

B. *Host-Based Mobility Management*

In this section, a general overview over Mobile IPv6 is given and its two major extensions Fast Handover and Hierarchical Mobile IPv6 are presented in more detail.

1) ***Mobile IPv6 (MIPv6):*** MIPv6 enable a MN to move within the internet domain without loosing current connection [5]. In order for a MN to be reachable at any time by a corresponding node (CN), the MIPv6 supports mobility of MN by providing them at two addresses: First is a fixed address called Home Address (*HoA*) provided by its home agent (HA). If the MN1 as shown in Figure2 is in its home network, packets destined to it will not have to be altered and can reach the MN through the normal routing process.

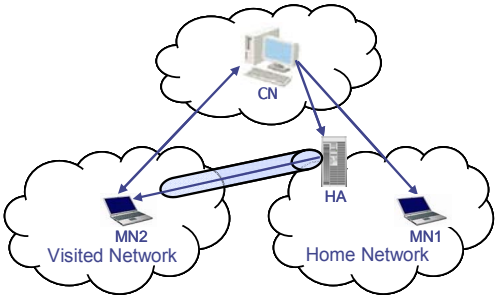

Figure 2. Mobile IPv6 Overview

Second address is Care-of-Address (CoA), which is provided by a visited network and it changes as the MN moves to a new network. Now, it will not be reachable through its HoA. Therefore, the HA in the home network is now responsible to receive packets which are destined to the MN's HoA if the MN2 is in a visited network. Whenever it receives such a packet, it will tunnel it to the MN's current CoA. The MN2 therefore has to update it's HA about his current CoA. This means for the HA to forward any packets destined to the MN's HoA to its current CoA. The packets are tunnelled through a tunnel begins at the HA and ends at the MN2 at visited network. If the MN2 wants to send packets to the CN, it can send them directly to the CN's address. As MN1 a packet would take the already shown path backwards. For MN2 the path goes directly from MN2 to CN. MIPv6 has shows that it has some well-known drawback such as, high handoff latency and packet loss. Furthermore handling MN's local mobility in the same way as it handles the global mobility, that is when MN move to new subnet, it will update its new point of attachment to it's HA and CN each time it move, without any locality consideration, will increase signalling traffic overhead, thereby causing user perceptible

deterioration of real time traffic. These weaknesses have led to the investigation of other enhancement to for MIPv6 performance [10].

2) *Fast Handover for MIPv6 (FMIPv6):* Fast Handover for MIPv6 was proposed to reduce handoff latency and minimize service disruption during handovers pertaining to MIPv6 as described in [6]. For a mobile technology such as MIPv6 it is very important that whenever the MN moves to a new link the update of information necessary to route packets to it is done as fast as possible. The loss of packets should be minimized as well as the overhead of sending duplicates of packets. If the whole handover process takes too much time, it can happen that connections will be terminated because the transport layer assumes that the connection is broken. At this point we have to differentiate between two kinds of Handovers; L2 Handovers caused by link layer whenever a MN changes its Access Point (this happens when the MN receives a stronger signal from another Access Point (AP) that it is currently connected to), and L3 Handover caused by network layer Handovers whenever a MN moves out of its current subnet range. The overall time needed for a Handover depends on three factors: movement detection, configuration of new CoA and Binding Updates. The basic idea behind FMIPv6 is that a MN can anticipate the Handover process and inform the new Access Router (newAR) about the Handover. This would shorten the time needed by the MN to detect movement. Figure 3 shows the signaling for FMIPv6.

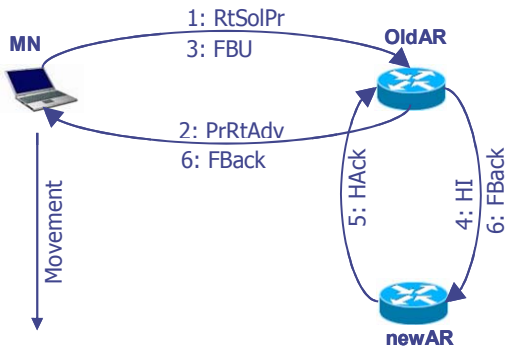

Figure 3. FMIPv6 signaling scenario for fast handover

As the first two messages, the *PrRtAdv* message that can be sent by oldAR in a periodical manner or it is sent after oldAR received an *RtSolPr* from the MN. This message can also contain a new CoA for the MN to use on newAR's link. The MN can initiate the L3 Handover by sending a *FBU* message to inform oldAR that packets should be forwarded to newAR. This message also contains the MN's new *CoA*. To forward packets, a tunnel is established between oldAR and newAR. However, the MN does not know yet if the new *CoA* is unique on the new link. Therefore, oldAR sends a *HI* message to newAR for address duplication check on the new link and it sets up the temporary tunnel to redirect packets between oldAR and newAR. The newAR responds with *HAck* message if the tunnel is set up successfully and there is no address duplication. After oldAR received the *HAck*, it sends an *FBack* message to the MN on both oldAR and newAR. After newAR received both the *FBU* and the *HAck* it starts forwarding packets using the tunnel to the MN's old CoA. It's important to note that this tunnel starts at oldAR and ends at newAR. It does not end at the MN. This allows the MN to still use its old CoA while verifying the new one. Packets sent by the MN from its old CoA will also be tunnelled back from newAR to oldAR. This goes as long as the MN has verified its new CoA and updated the HA and all CN's. After that MN will inform newAR about its movement to its link. Probably newAR buffered some packets for the MN and it can now forward them to the MN.

3) *Hierarchical MIPv6 (HMIPv6):* Hierarchical MIPv6 is another important improvement for MIPv6, which adds an indirection for locating a MN [7]. Depending on where the CN and HA are located in the Internet topology it tunnels packet to a Mobility Anchor Point (MAP), which is addressed by a regional CoA (RCoA). The MAP in turn tunnels these packets to the MN, addressed by a local CoA (LCoA). The local handovers of the MN only have to be signalled to the MAP thus avoiding high latencies and overhead for the local binding updates Figure 4 show HMIPv6 whole procedure.

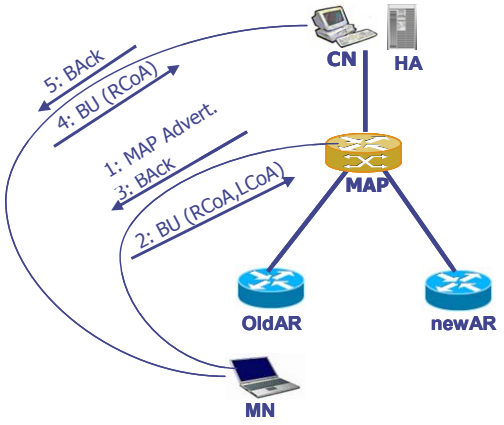

Figure 4. HMIPv6 signaling scenario

It is assumed that a MN is currently connected to oldAR and will do a Handover to newAR, Whenever the MN wants to update the CN or HA about its new CoA, it will send them a *BU*. The *BU* will travel from the MN to MAP and to the CN or HA. The acknowledgment for the BU from the CN/HA will travel the same way back. If link between CN/HA to MAP is a long link which means that it would take a significant amount of time for the *BU* to travel from MAP to the CN/HA and back, it would make sense to have kind of a temporary HA on MAP. A MN then just has to update the MAP as long as the same MAP is located between the MN and CN/HA. The MN's address in this case is *LCoA*. The extra time for sending a BU over link between CN/HA and MAP is saved. An MN can find out about a MAP Addresses by the routers advertisement. A MN will then form an *RCoA* from the MAP. The MN then has to update the CN/HA with this *RCoA*. After that, the CN/HA send their packets to the *RCoA*. The MAP tunnels them to the MN's *LCoA*. The MAP can also buffer packets destined to the MN and will resend the buffered packets when the MN has sent it a *BU* through the newAR.

C. *Network-Based Mobility Management*

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.

1) *Proxy Mobile IPv6 (PMIPv6):* PMIPv6 [1] is designed to provide network-based mobility management support to an MN in a topologically localized domain. Therefore, an MN is not performing any mobility related signaling, and the proxy mobility agent performs that signaling on behalf of the MN. Once an MN enters its PMIPv6 domain and performs access authentication, the serving network assigns a unique home network prefix (HNP) to each MN, and conceptually this prefix always follows the MN wherever it moves within a PMIPv6 domain, to ensure that the MN is always on its home network and can obtain its HoA on any access network. From the perspective of the MN, the entire PMIPv6 domain appears as its home network. Accordingly, it is no need to configure the CoA at the MN. A brief description of the basic terminology and overview of PMIPv6 within a localized domain illustrates in the Figure 5. The new principal functional entities of PMIPv6 are the local mobility anchor (LMA) and mobile access gateway (MAG), the LMA is similar to the HA in MIPv6. However, it has additional capabilities required to support PMIPv6 such as:

- Maintain reachability to the MN's address while it moves around within a PMIPv6 domain.
- Maintain a binding cache entry for each currently registered MN. That is has some additional information associates an MN with its serving MAG, and maintain enabled the relationship between the MAG and LMA, such as MN-ID, MN's home network prefix HNP, etc.

The MAG typically runs on the AR and it is main role to:

- Detect the MN's movements
- Initiate mobility-related signaling with the MN's LMA on behalf of the MN.
- Establish a tunnel with the LMA for enabling the MN to use an address from its home network prefix.
- Emulate the MN's home link on the access link by advertising the MN's home network prefix to the MN.

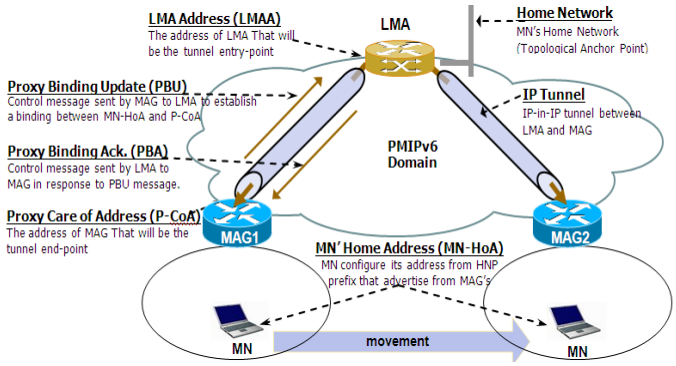

Figure 5. Basic terminology overview of PMIPv6 domain

The overall operations in PMIPv6 signaling flow include two phases, First is Attachment phase that include steps (1-6), as shown in the Figure 6, which describes the MN initial attachment to the network until it can send/receive a data packet to/from CN. Each step is described as follows:

1. MN initially attaches to MAG1 in a PMIPv6 domain by present MN-ID to perform access authenticated.
2. MAG1 request AAA server for access authentication.
3. AAA servers respond by send MN's profile to MAG1 if successful authentication, which contains MN-ID, LMA Address (LMAA), address configuration mode.
4. MAG1 sends a *PBU* message to the MN's LMA on behalf of the MN, to update current location of the MN.
5. LMA will replay by sends a *PBA* message including the MN-HNP and creates a *Binding cache Entry (BCE)* that binds the MN-HNP to MAG address (*PCoA1*), also establishes a bidirectional tunnel to MAG1.
6. MAG1 setup a tunnel to the LMA and adds a default route over the tunnel to the LMA, upon receiving the *PBA* message. It also creates a *Binding Update List (BUL)* that binds the MN-HNP and *LMAA*. The MAG1 then sends *RtrAdv* messages to the MN on the access link to advertise the MN-HNP as the hosted on-link-prefix. When the MN receives these *RtrAdv* messages, the MN configures the IP address using either a statefull or stateless address configuration modes (as mention in section II-A-3). After successfully completing the address configuration procedure, the MN now can use this address for packet delivery to/from CN.

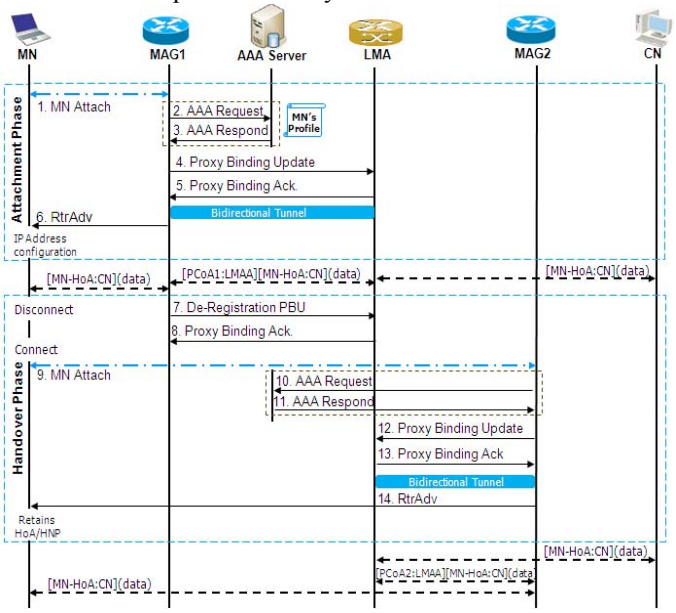

Figure 6. Overall operations signaling flow in PMIPv6

Second phase is the Handover procedure that include steps (7-14) as shown in the Figure 6 above, which describes a MN movement from MAG1 to MAG2 until it can resume send/receive data packets to/from CN, as follow:

7. When MAG1 detects MN movement away from its access link (to MAG2), it send *De-Registration PBU* message to the LMA with the zero value for lifetime.
8. LMA sends a *PBA* message back to MAG1 and waits for a *MinDelayBeforeBCEDelete* amount of time, before it deletes the BCE for the MN.

9. MN initially attaches to MAG2 in a PMIPv6 domain by present MN-ID to perform access authenticated.
10. MAG2 request AAA server for access authentication.
11. AAA servers respond by send MN's profile to MAG2 if successful authentication.
12. MAG2 will update the MN's LMA about current location of the MN, by sending *PBU* message.
13. Within a wait period *MinDelayBeforeBCEDelete*, if the LMA then receives a *PBU* message for the same MN with a lifetime value greater than zero, it will update its the *BCE* with a new value, which is the address of MAG2 (PCoA2).Otherwise the LMA deletes the MN's *BCE* and removes the routing state for the MN-HNP. After updating the BCE, the LMA sends a *PBA* to MAG2.
14. MAG2 after receive *PBA* from LMA send *RtrAdv* messages to the MN with same MN-HNP.

Upon receiving the *RtrAdv*, the MN believes it is still on the home link and can continue sending/receiving packets to/from the CN. All data traffic in PMIPv6 sent from the MN gets routed to LMA through the tunnel between its MAG and LMA. The LMA forwards the received packet from the CN 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.

III. IEEE 802.11 ACCESS NETWORK MANAGEMENT

PMIPv6 [1] and IEEE 802.11 [11] standard are the most discussed topics among handover procedures; L2 (that is when the MN attaches to a new access point) and L3 (that when the MN change its attachment point to the new MAG). PMIPv6 enables a MN to continuously attach to the network while IEEE 802.11 keeps a MN connecting to the wireless link. When a MN wants to access an existing Access Point (AP) or entering new area it needs to get synchronization information from the AP. The handover procedure in the IEEE 802.11 involves Scanning, Authentication and Re-association phase, as shown in Figure 7.

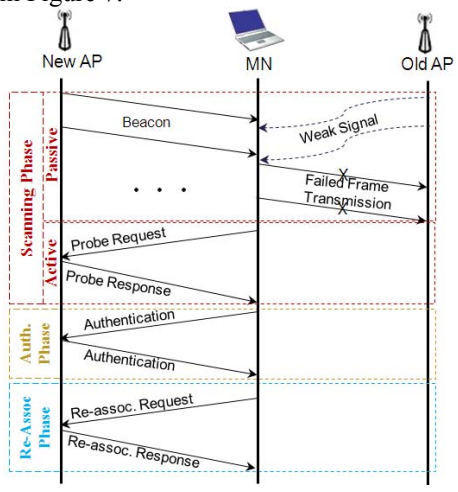

Figure 7. Handover latency phases for IEEE 802.11

In the scanning phase, two types of scanning defined: Active and Passive. In active scan, the MN tries to locate an AP by transmitting Probe Request Frames, and waits for Probe Response if any AP is available on certain channel. In Passive scan, a MN just waits for possible Beacon Frames, which sent out periodically by the AP containing synchronization information. The handover time in active scan is usually less than in passive scan. The passive scan of operation depends strictly on the period of beacon generation interval. However, this can provide better battery saving than active scan of operation.

Once the MN has located an AP, it goes through the Authentication phase for interchange of authentication information between the AP and the MN. If the MN is authenticated, it then starts the Re-association Phase, which is the exchange of information about the MN and AP capabilities, and then a MN is able to receive and transmit data packet after the Re-association phase is completed.

The whole handover latency cased by IEEE 802.11 is called as link switching delay and In order to improve the total handover latency and provide an optimization during MN's handover within PMIPv6 domain, a novel approach is needed to be integrated into both L2 and L3 handover procedure schemes. In the current 802.11 implementations handover latency may vary from hundreds of milliseconds to several seconds depending on some factors such different hardware vendors and wireless environments [13].

IV. HOST BASED VS. NETWORK-BASED MOBILITY MANAGEMENT PROTOCOLS

We provide a summary of the main characteristics of Host-based mobility protocols [2], [5-7] with the comparison with Network-based mobility protocol [1], as shown in Table 1.

Table 1. Mobility Management Protocols Comparison

Protocol Characterize	MIPv4	MIPv6	FMIPv6	HMIPv6	PMIPv6
Mobility Region	Global	Global	Global/Local	Local	Local
Required Infrastructure	HA ,FA	HA	HA,AR	HA,MAP	LMA,MAG
Location Management	Support	Support	Not Support	Support	Support
Route Optimization	Not Support	Support	-	Support	Not Support
Handover Latency	Bad	Bad	Good	Moderate	Good
Mobility Management	Host-based				Network-based
Type of Router advertisement	Broadcast				Unicast
Addressing Model	Shared-prefix				Per-MN-prefix
Maintaining L4 connectivity	No				Yes
MN Modification	Required				Not Required
MN Tunnel overhead	Yes				No
Packet Field Re-ordering	Sequence Number option				Time Stamp
Binding Cache Lookup key	MN-Home of Address				MN-ID/ MN-HNP

Generally, most of existing mobility support protocols has been developed for their own characteristic purposes and suitable environments. The most notable aspect of PMIPv6 is

the localize region and support Per-MN-prefix addressing model. The MN does not directly involve to the signaling process to support mobility handling compared to the host-based that has HA, CoA (Local, Global) to support the mobility in their region, those complicated signaling process cause the degradation of network performance specially handover latency. However, a PMIPv6 only has the role of LMA which is unique and assign a unique home network prefix (HNP) to each MN and this prefix follows the MN wherever it moves within the PMIPv6 domain, it will always have the same HNP. Therefore, the MN without any mobility stack can be supported mobility management. Therefore the L3 movement detection and duplicate address detection processes are not required within a PMIPv6 domain. Thus, PMIPv6 significantly can reduce the handover latency and at the same time keep the transport layer connectivity maintain due to not update the IP address during movement, which would enable services such as wireless voice-over IP (VoIP) and quality of service (QoS) support.

V. ISSUES IN MOBILITY MANAGEMENT PROTOCOLS

In the Host-based mobility management protocols, two versions of mobile IP have been standardized for supporting mobility on the Internet; MIPv4 and MIPv6, the MIPv6 is a mature standard for IP mobility support and solves problems, such as triangle routing, security, and limited IP address space, addressed in MIPv4 [2]. MIPv6 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 guarantees required for real-time applications. Therefore, various MIPv6 enhancements such as FMIPv6 [6] and HMIPv6 [7] have been reported over the past years, mainly focused on performance improvement in MIPv6. However, MIPv6 and its various enhancements basically require protocol stack modification of the mobile node in order to support them. In addition, the requirement for modification of mobile nodes may cause increased complexity on them and introduce battery problem and waste of air resource. Also the tunnelling that established between the Home Agent and Mobile Node increases the bandwidth constraints on the wireless link and the processing burden on the mobile node.

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, MN is not required to participate in any mobility-related signaling, for its easy deployment and low installation cost. It is noted that PMIPv6 [1] is used mainly for registration or binding update of the location of mobile nodes, and for the perspective of seamless handover, the PMIPv6 still needs to be for further study such as fast handover in PMIPv6. Also more study and standardization are needed for supporting route optimization in PMIPv6, Cross-layering Issues over IEEE 802.16/WiBro, Multi-Homing and fast handover with efficiency of IEEE 802.21. Also PMIPv6 is needed to interact with MIPv6 to support global mobility [4].

VI. CONCLUSIONS

In this paper, two mobility management categories; Host-based and Network-based mobility management protocols have been discussed. In addition, the requirement for modification of mobile node in the Host-based protocol may increase complexity on MN and waste of air resource beside remain drawbacks such as High handover latency, power consumption, packet loss, and signaling overhead. On the other hand Network-based protocol such as PMIPv6 has attracted a fair amount of critical attention in the Internet communities. A MN not require to participate in any mobility related signaling because the serving network will handles the mobility management on behalf of the MN, improving the handover performance for mobile communications and reduce unnecessary signalling and packet loss. Like many new technology PMIPv6 will evolve as it becomes more widely adapted and will be a necessity, because most handled device will be internet-enabled. In additions, this paper make description of IEEE 802.11 access network handover management to support mobile communication, beside a comparison between existing mobility management protocols, and illustrate an open issues and challenges for mobility management. Integration/Cross-layering mechanisms between PMIPv6 and underline technologies are necessary to overcome the overall drawbacks that remain unacceptable for Latency-sensitive services such as real-time and multimedia applications.

REFERENCES

[1] Gundavelli, S., Leung, K., Devarapalli, V., Chowdhury, K., and B. Patil, "Proxy Mobile IPv6", RFC5213, August 2008.

[2] C. Perkins, “IP Mobility Support for IPv4,” IETF RFC 3344, August2002.

[3] N. Banerjee, W. Wu, and S. K. Das, “Mobility Support in Wireless Internet”, IEEE Wireless communication, vol.10, no. 5, pp. 54-61, October. 2003.

[4] J. Kempf, “Problem Statement for Network-Based Localized Mobility Management (NETLMM),” IETF RFC 4830, April 2007.

[5] D. Johnson, C. Perkins, and J. Arkko, “Mobility Support in IPv6,” IETF RFC 3775, June 2004.

[6] R. Koodli, “Fast Handover for Mobile IPv6,” IETF RFC 4068, July 2005.

[7] H. Soliman, C. Castelluccia, K. E. Malki, and L. Bellier, “Hierarchical Mobile IPv6 Mobility Management (HMIPv6),” IETF RFC 4140, August 2005.

[8] K.Kong, W.Lee, Y.Han, M.Shin and H.You, “Mobility Management for all-IP mobile networks: Mobile IPv6 vs. Proxy Mobile IP6,” IEEE Wireless Communications, vol.15, no.2, pp.36-45, April 2008.

[9] T. Narten, E. Nordmark, and W. Simpson, “Neighbor Discovery for IP version 6 (IPv6),” IETF RFC 2461, July 2005.

[10] C.Makaya, S. Pierre,”An Analytical Framework for Performance Evaluation of IPv6-Based Mobility Management Protocols,” IEEE Transactions on wireless communications, vol. 7, no. 3, pp. 972-983,March 2008.

[11] Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specification, IEEE Std. 802.11, 1997.

[12] S. Thomson, T. Narten “IPv6 Stateless Address Autoconfiguration,” IETF RFC 2462, December 1998.

[13] Wu, H., Tan, K., Zhang, Y., Zhang, Q.”Proactive Scan: Fast Handoff with Smart Triggers for 802.11 Wireless LAN,” in *INFOCOM2007*, IEEE Computer Communications. 6-12 May 2007, p.749.