The final publication is available at

https://doi.org/10.1109/JSYST.2013.2297705

Additional Information

A Survey on Proxy Mobile IPv6 Handover

Hero Modares, Amirhosein Moravejosharieh, Jaime Lloret, *Senior Member, IEEE*, and Rosli Bin Salleh

Abstract—As wireless technologies have been improving in recent years, a mobility management mechanism is required to provide seamless and ubiquitous mobility for end users who are roaming among points of attachment in wireless networks. Thus, Mobile IPv6 was developed by the Internet Engineering Task Force (IETF) to support the mobility service. However, Mobile IPv6 is unable to fulfill the requirements of real-time applications, such as video streaming service and voice over IP service, due to its high handover (HO) latency. To address this problem, Proxy Mobile IPv6 (PMIPv6) has been introduced by the IETF. In PMIPv6, which is a network-based approach, the serving network controls mobility management on behalf of the mobile node (MN). Thus, the MN is not required to participate in any mobility-related signaling. However, the PMIPv6 still suffers from lengthy HO latency and packet loss during a HO. This paper explores an elaborated survey on the HO procedure of PMIPv6 protocols and proposed approaches accompanied by a discussion about their points of weakness.

Index Terms—Fast localized Proxy Mobile IPv6 (PMIPv6) handover (HO) procedure, HO in PMIPv6, PMIPv6, PMIPv6 with partial bicasting, predictive mode, reactive mode.

I. Introduction

THE future broadband wireless networks are quickly evolving toward all-IP networks. With an explosive growth in the number of users that are using the Internet in a wireless environment, the issue of IP mobility management technology is on the rise. Mobile IPv6 (MIPv6) [1], which is a host-based mobility management protocol, is one of the most representative efforts and proposed by the Internet Engineering Task Force (IETF) as the main protocol for mobility management at the IP layer. However, although MIPv6 is a well-known mature standard for IPv6 mobility, it has some well-known problems, such as handover (HO) latency, packet loss, and signaling overhead. Moreover, the MIPv6 requires protocol stack modification of the mobile node (MN) to support IP mobility [2]–[6]. Recently, Proxy MIPv6 (PMIPv6), which is one of the network-based mobility management protocols, has been standardized by the IETF Network-Based Localized Mobility Management Working Group [7]. Unlike the MIPv6, PMIP6 allows the serving network to control the mobility management on behalf of an MN, thereby eliminating the MN from any mobility-related signaling.

PMIPv6 is essentially based on MIPv6 in the sense that it extends MIPv6 signaling and reuses many concepts such as the functionality of the home agent (HA). However, PMIPv6 is also designed to provide network-based mobility management support to an MN in a topologically localized domain. Therefore, an MN is exempted from participation in any mobility-related signaling, and a proxy mobility agent in the serving network performs mobility-related signaling on behalf of the MN. However, a network-based mobility management protocol, such as PMIPv6, still suffers from HO latency and packet loss during a HO, such as in MIPv6. Although several fast HO schemes based on PMIPv6 have been already introduced to reduce the HO latency and packet loss [8]–[13], these schemes still experience some packet loss and packet-ordering problems during a HO [14]–[23]. In order to eventually come up with a robust and seamless HO procedure in PMIPv6 and its derived improved approaches, it is imperative to run as much comprehensive investigation as possible on previous related state of the arts. Here, we try to roughly examine various approaches in detail in the field of HO procedure improvement. Of course, it is obvious that the provided list of investigated approaches is not exhaustive.

This paper is organized as follows. Section II represents the background of PMIPv6 and the fundamental steps performed in the HO procedure. Section III discusses some of the schemes and approaches proposed in order to enhance the HO latency in the PMIPv6 network domain. The survey is concluded in Section IV, along with a discussion on future research opportunities in the PMIPv6 HO area.

II. Background

PMIPv6 is designed to provide network-based IP mobility management support to an MN in a topologically localized domain, without requiring the participation of the MN in any IP-mobility-related signaling. The core functional components used to support mobility in PMIPv6 are the policy store (PS), the local mobility anchor (LMA), and the mobile access gateway (MAG). The PS is the entity that manages the MN's authentication and maintains the MN's profile, which is a set of parameters configured for a given MN. The LMA is similar to the HA in MIPv6. However, it has additional capabilities required to support PMIPv6. The main role of the LMA is to maintain reachability to the MN's address, whereas the MN moves around within a PMIPv6 domain. The LMA includes a binding cache entry (BCE) for each currently registered MN. The main role of the MAG, which is typically the access router
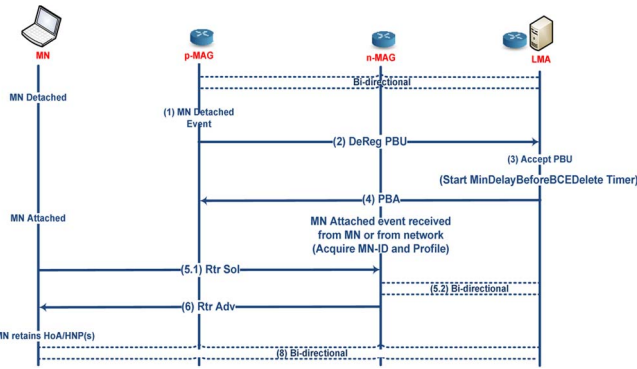
Fig. 1.   Signaling flow of PMIPv6.

(AR), is to detect the MN's movement and to send mobility-related signaling to the MN's LMA on behalf of the MN. Additionally, the MAG establishes a tunnel with the LMA for packet transmission. The MAG ensures that an MN can obtain an address from its home network prefix (HNP) and move anywhere within the PMIPv6 domain. Fig. 1 shows the signaling flow of the overall operations in PMIPv6 from the previously attached MAG (p-MAG) to the newly attached MAG (n-MAG). The HO procedure is described as follows [7].

Step 1: The HO procedure in PMIPv6 starts with MN's movement detection performed by the p-MAG along with the signaling LAM to report the MN's movement in order to update the BCE table inside the LMA.

Step 2: Upon receiving the update request sent from the p-MAG, the LMA identifies the sender of the request and waits for a certain amount of time to allow the n-MAG to request the binding update. However, the BCE will be deleted if the binding update request is not received within a certain amount of time.

Step 3: Upon detecting the MN on its access link, the n-MAG sends the PBU message to the MN's associated LMA.

Step 4: Upon receiving the PBU message, the LMA updates the related field in the BCE table and binds the MN-HNP to a Proxy Care-Of Address (proxy-CoA), which is the n-MAG address. Thereafter, a Proxy Binding Acknowledgement (PBAck) message containing the MN-HNP will be sent to the n-MAG.

Step 5: Upon (step 5.1) detecting the MN Router Solicitation (RS), (step 5.2) a bidirectional tunnel will be established between the LMA and the n-MAG.

Step 6: Upon receiving the PBAck sent from LMA, the n-MAG sets up the tunnel along by sending the Router Advertisement (RA) to the MN that contains updated MN-HNP and is sent from the LMA.

Step 7: When the MN receives the RA sent from the n-MAG, it starts to configure the new CoA address by utilizing either stateful or stateless address autoconfiguration procedures.

Step 8: By the completion of the address autoconfiguration procedure, data flows will be forwarded to the MN.

III. RELATED WORK

When an MN moves to a new access network in a PMIPv6 domain, it inevitably experiences packet loss or HO latency
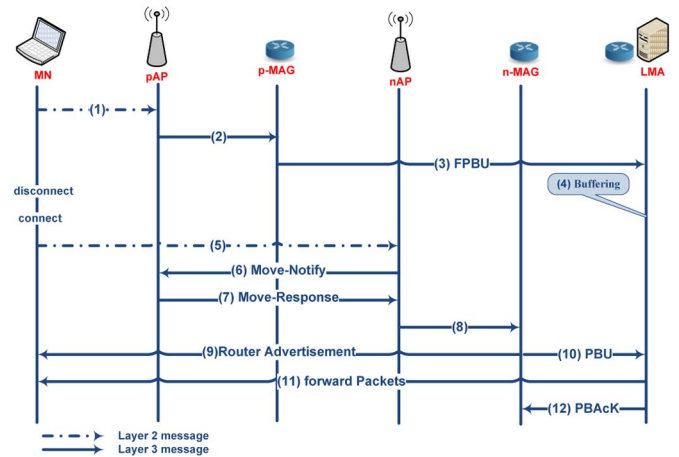

Fig. 2.   Message flow of fast HO in PMIPv6.

until it receives its MN-HNP advertisement from the n-MAG. Therefore, several fast HO mechanisms have recently been introduced to reduce the HO latency and packet loss with PMIPv6 [8]–[10].

A fast HO method was proposed [8] based on the 802.11 networks for the PMIPv6. Context information, such as the MN's authentication information and HNP, is transferred using the Inter-Access Point Protocol (IAPP) scheme.

Fig. 2 shows the sequence of message signaling related to the fast HO scheme for PMIPv6.

Step 1: *Sending the disassociation message (DM)*. The MN detects its movement by measuring the received signal strength (RSS) value, and it sends the DM that contains the MN's medium access control (MAC) address to its current connected AP when the RSS value exceeds the preconfigured threshold.

Step 2: *Forwarding the MN's ID*. Upon receiving the DM sent from MN, the associated AP [previous AP (pAP)] forwards the MN's ID (MAC address) to the current connected MAG (p-MAG).

Step 3: *Sending the fast PBU* (FPBU) *message*. The p-MAG then sends a FPBU message containing the MN's network access identifier (NAI) option to the LMA upon receiving the MN's ID.

Step 4: *Buffering*. Upon receiving the FPBU message, the LMA starts to buffer data flows destined to the MN.

Step 5: *Sending the reassociation (RA) message*. Once the MN attaches to the new point of attachment [new AP (nAP)], the RA message will be sent to the AP indicating the MN's MAC address and previous basic service set identification of the pAP.

Steps 6 and 7: *Exchanging MOVE-notify and MOVE response message*. Upon receiving the RA message, the MOVE-notify message will be transmitted from the nAP to the pAP via the distribution system (DS). Thereafter, context information that includes the HNP and authentication information, encapsulated in the MOVE-response message, will be replied from the pAP to the nAP.

Step 8: *Forwarding context information*. The nAP then forwards the context information of the MN to the n-MAG after the MOVE-response message is received.
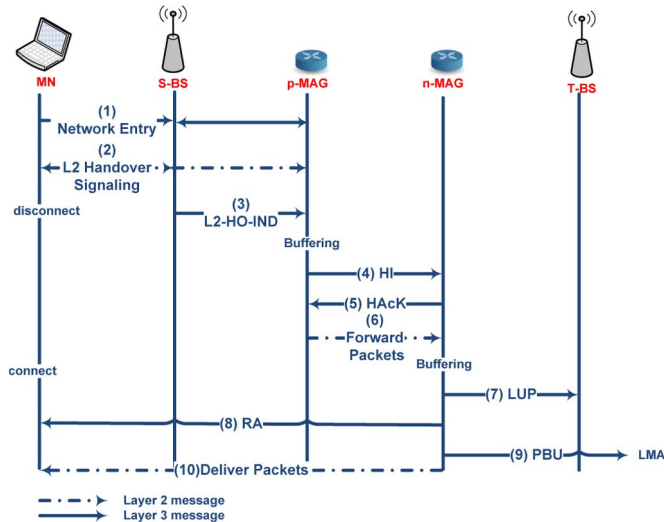
Fig. 3. Predictive mode.

Step 9: *Reconfiguring the default router for the MN*. When the MN's context information is delivered to the n-MAG, the RA message will be sent to the MN through the nAP in order to reconfigure the default router of the MN.

Step 10: *Configuring forwarding information*. Upon receiving the context information, the PBU message will be constructed by utilizing MN's context information and will be sent to LMA.

Step 11: *Forwarding buffered packets*. When the PBU message is received by the LMA, it then creates a route for the MN and begins to send the buffered data flows.

In a fast HO method [8], Lee *et al.* suggested adapting IAPP to reduce the "access authentication/obtaining MN's profile" time of the total HO delay. Nonetheless, the on-the-fly packets will be still lost during a HO.

An enhancement to the PMIPv6 protocol has been proposed in [9] to have the Layer 3 HO (L3 HO) performance and context transfer improved. This enhancement borrows a similar concept from fast HOs for FMIPv6. There are two modes of operation depending on whether the signaling of Layer 2 HO (L2 HO) is finished on the previous link or not: the predictive mode or reactive mode. During predictive mode, the HO initiation (HI) message is used by the p-MAG in order to transfer context to the n-MAG. While in reactive mode, an FBU message is used by the n-MAG instead of requesting MN's context information from the p-MAG. Eventually, a bidirectional tunnel will be established in order to transfer the packets buffered while performing the HO procedure.

A. Predictive Mode

In predictive mode, the L2 HO signaling finishes in the previous link. In this section, the MAG and the base station (BS) can be colocated using physical entities that are different (see Fig. 3). The procedure is described as follows.

Step 1: The network entry procedure is performed by the MN where access authentication and the configuration of the IPv6 are completed. After the IP connectivity is successful,

the mobility-related signaling of the MN will be done by the p-MAG on its behalf.

Step 2: When the MN is about to leave its associated BS coverage area, the MN and the associated BS negotiate through L2 HO signaling.

Step 3: The L2 HO-IND message, which includes the target BS ID (t-BS-ID), is sent by the serving BS (s-BS) to p-MAG once the L2 HO decision is made.

Step 4: The MAGs contain the [BS-ID, Proxy-CoA] tuples. Once the L2-HO-IND message is delivered, the p-MAG will then proceed to the following.

Step 4.1: Collect the related context of the MN with the following information: MN Identifier, MN Home Address (MN-HoA), MN-HNP, and MN's Proxy-CoA in the p-MAG and the MN's MAC.

Step 4.2: Determine the n-MAG's proxy CoA that will be retrieved by the p-MAG in order to send the HI message by utilizing the BS-ID field included in the L2-HO-IND message.

Step 4.3: Send the HI message to the n-MAG.

Step 5: Start the creation of the Binding Update List in the n-MAG side based on information retrieved from the HI message. Thereafter, the HAck message will be sent to the p-MAG, and once the HAck message is delivered to p-MAG, a bidirectional tunnel will be established between n-MAG's proxy-CoA and p-MAG proxy-CoA as the two ends of the tunnel.

Step 6: Packets from the p-MAG meant for the MN are tunneled to the n-MAG according to the MN-HoA. The packets received by the LMA are decapsulated by the p-MAG, encapsulate back into the p-MAG/n-MAG tunnel, and then sent to the n-MAG. The packets should be buffered by the n-MAG until the n-MAG and MN link is ready.

Step 7: Once the MN attaches to the t-BS, the network reentry is performed. To expedite the procedure, the context transfer from the p-MAG is used. The Link UP (LUP) message is sent to the n-MAG by the t-BS indicating that L2 link is established.

Step 8: The RA message containing the n-MAG's information is sent by the n-MAG to the MN that helps data transmission between the MN and the n-MAG feasible.

Step 9: The binding in LMA is updated when the n-MAG sends the PBU.

Step 10: Eventually, The MN receives the buffered packets from the n-MAG.

B. Reactive Mode

The reactive mode is shown in Fig. 4. The following steps are performed to process the HO procedure.

Step 1: The link layer is established after the network reentry process is performed by the MN. In order to expedite the link process, the context from the original session is needed.

Step 2: In order to reduce the loss of packets during HO, packets should be automatically buffered by the p-MAG for the MNs that are no longer in the link. Two cases need to be covered here. In the first case, the p-MAG did
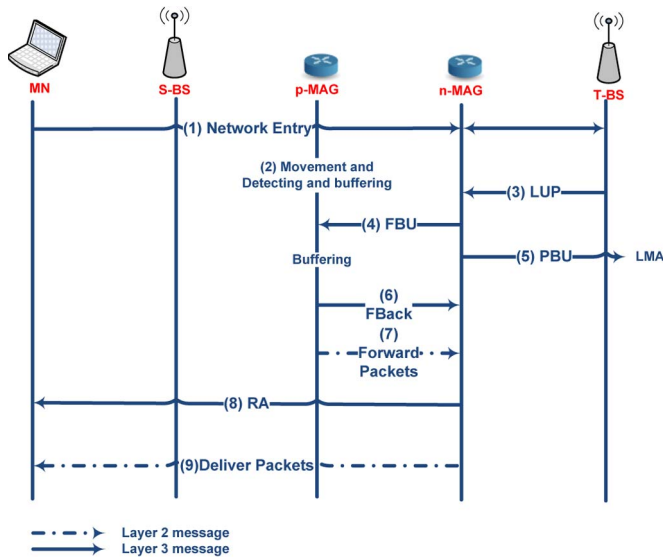
Fig. 4.   Reactive mode.

not know that the MN was handing over after it had just moved. In the second case, the MN knows that it is moving and that the procedure has not been completed yet, but the MN has already started exchanging L2 messages with the p-MAG. The packets will be automatically buffered (probably following a default period of time) by the p-MAG for every MN that is not within its link. The p-MAG could just buffer the packets because the chances of errors or denial-of-service attacks are very slim.

Step 3: Once the process of network reentry is completed, the n-MAG will receive the LUP message from the t-BS.

Step 4: The n-MAG immediately sends the FBU to the p-MAG once the previous BS-ID and MN's MAC becomes available after the network reentry process. The FBU contains the n-MAG's Proxy-CoA and the MAC of the MNs. By referring the [BS-ID, Proxy-COA] tuples in the n-MAG, the p-MAG's address can be determined. It is safe to assume that the previous BS-ID is exchanged during network reentry for this step, e.g., WiMAX links.

Step 5: The PBU is sent by the n-MAG to update the binding in LMA.

Step 6: The p-MAG identifies the MN's Binding Update List using the MN's MAC and retrieves the related context. The related context contains information such as the MN identifier, the MN-HoA, the MN-HNP, the MN's Proxy-CoA in the p-MAG, and the MN's MAC. The FBack message is used to transfer the context from p-MAG to n-MAG. The bidirectional tunnel will be established as soon as the n-MAG receives the FBack message. The tunnel will have the p-MAG's Proxy-CoA at one end and the n-MAG's Proxy-CoA at the other end.

Step 7: The p-MAG forwards the buffered packets to the n-MAG once the bidirectional tunnel is established.

Step 8: The RA and the n-MAG's information will be sent by the n-MAG to help MN send its packets.

Step 9: The MN receives the packets from the n-MAG.

The literature [9] utilizes the FMIPv6 signaling mechanism to improve the performance of the L3 HO. Before an MN

moves from the s-BS to the t-BS, the MN provides the t-BS information (t-BS ID) during the L2 HO signaling procedure. The MN then acquires the IP address of the n-MAG from a tuple incorporated in all the MAGs and performs the L3 HO based on this information. However, this scheme also has some limitations.

1) Each MAG needs to have a tuple that contains the BS-IDs and IP addresses for all the MAGs in the PMIPv6 domain.
2) After a HO, a packet-ordering problem occurs between the packets buffered at the p-MAG and the packets from the LMA after registration.
3) The MN should provide information about the target network to the p-MAG through L2 signaling.

The literature [24] proposed a hybrid mechanism to reduce the HO latency along with a reduction in signaling cost and packet delivery cost in PMIPv6 called hybrid-mode fast HO for PMIPv6 (HF-PMIPv6). In HF-PMIPv6, a decision table is utilized to determine the mode of mobility (i.e., predictive or reactive). If the mobility mode is determined to be in predictive mode, then the HF-PMIPv6 will be performed as the same as F-MIPv6 in which a tunnel will be established between p-MAG and n-MAG to alleviate packet loss. Otherwise, the mobility mode will be considered in reactive mode; therefore, the HF-PMIPv6 directly performs the HO procedure without setting up the tunnel in order to reduce the HO latency, tunnel transmission cost, and eventually, signaling cost.

Park *et al.* [10] proposed fast and local PMIPv6 (FLPMIPv6) to reduce the HO latency and packet loss. This scheme is based on FMIPv6 and uses the messages defined in IEEE 802.21. The MN provides information on the n-MAG using a media independent HO (MIH) message before the HO. The current connected MAG (p-MAG) then sends a HO-related message to the n-MAG. However, since this scheme is derived from host-based mobility and initiated by MNs, the network access devices need to perform L2 intelligently. In addition, since the p-MAG sends a BU message to the LMA before the L2 HO occurs, this means the L3 HO is performed before the L2 HO. Therefore, significant packet losses occur from the time the L3 HO is completed until the end of the L2 HO. In order to perform the HO procedure, predictive mode has been utilized in FLPMIPv6, and its related HO procedure is shown in Fig. 5.

Step 2: An MIH HI message will be transmitted to previous proxy mobile agent (PMA) (p-MAG) to inform of its movement. The new PMA (n-MAG)'s [AR-ID, AR-Info] tuples are included in this command message.

Step 3: Once the MIH HI message is received by the p-MAG, the HI message is sent to the n-MAG by that p-MAG. The HI message will have the MN's IP address (PCoA) and the MN's Identifier. The n-MAG will examine the existence of a tunnel to the LMA for PCoA after receiving the HI message. If such a tunnel is already present, there are two possibilities for this. One, the p-MAG's HI message is spurious, and the tunnel has been set up by the n-MAG when it saw the L2 being triggered earlier. The second possibility is that another node is already present and already using the PCoA address on the link. The MN's
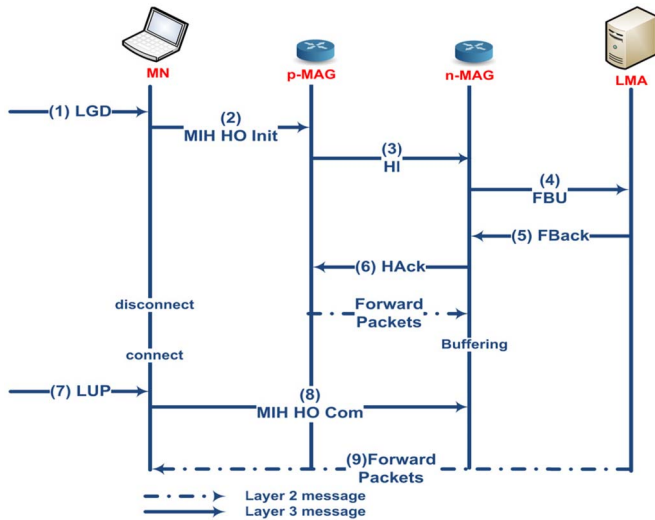
Fig. 5.   FLPMIPv6 HO procedure.

identifier is verified by the n-MAG to ensure if it is the same node. It will return a failure reply if the node is the same one, thus getting a Duplicate Address. However, if the HI message is accepted and processed by the n-MAG, the LMA will get the FBU message from the n-MAG. The tunnel from the p-MAG will then be redirected. The FBU message may contain the MN's unique identifier, which can be optionally included along with the PCoA as the HoA.

Step 4: The FBU message will be examined by the LMA to ensure whether there is a binding for the Regional Care-of Address (RCoA). A new binding entry will be created if such does not exist. If there is a binding, then the MN's identifier is verified with the one in the FBU to ensure it is similar. The binding information is updated if it matches and fails it if it does not. The tunnel is set (or updated) to the n-MAG after the FBU is successfully processed by the LMA. This tunnel is used to send and receive packets from the PCoA. Normally, the host route is added and points to the tunnel for the PCoA. The LMA will send an FBack message to the n-MAG if the MN's RCoA is updated successfully.

Step 5: The n-MAG will examine the FBU to ensure whether it has been processed successfully upon receiving the FBack message, and the HAck message will indicate a failure if it has not. Otherwise, a tunnel to the LMA is created. The forwarding is set up such that packets containing the PCoA's source address will be the one forwarded into the tunnel. States such as binding state is also maintained. This can be use as a verification method for any duplication or spurious indications of the MN or p-MAG. The host route is created to enable packets to be forwarded to the MN. A HAck message indicating a successful HO procedure will be sent back by the n-MAG to the p-MAG.

Step 6: Packets are forwarded to the n-MAG once the p-MAG receives the HAck message.

Step 7: The MN's MIHF will receive the LUP indicator from the MIHF when the MN connects to a new link. The n-MAG then receives the MIH HO Com message from the MN.
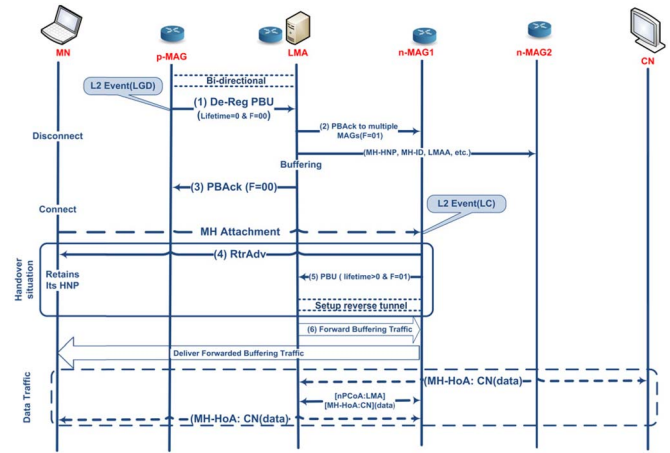

Fig. 6.   Latency low HO mechanism.

Step 8: Upon receiving the MIH HO Com message, the n-MAG will use this as an indication to begin packet forward to the MN. After which the buffered packets is forwarded.

In order to eliminate the connection failure and boost the HO performance up while the MN is roaming among PoAs, LMA plays a pivotal role as a context transfer node [25].

Whenever the LMA receives the link going down (LGD) message sent from p-MAG, it will multicast the MN's context information profile such as MN's ID and MN-HNP included in a modified PBAck message toward multiple neighboring MAGs. This is done based on a new MAG_Cache_Entry list configured at the LMA in order to perform the preregistration and preauthentication process closely together in advance before losing the connectivity with the associated MAG. The proposed mechanism enables the MN to quickly reconfigure its network interface immediately after receiving the RA message disseminated by n-MAG and resume its communication as quickly along with less connection failure as possible. Additionally, the buffering mechanism is offered to buffer outgoing data packets during the MN handing over procedure in order to be forwarded after the HO procedure completion. Fig. 6 illustrates the message signaling sequence of the proposed mechanism and the latency low HO mechanism.

Step 1: The p-MAG sends the deregistration request included in a PBU message to the LMA alerting the HO condition by LGD trigger. This notifies the LMA to update the BCE field related to MN and be ready for the proactive HO procedure.

Step 2: The LMA starts to multicast the PBAck message, which includes the MN's context information profile to multiple neighboring MAGs in order to enable the MN to perform the preregistration followed by the preauthentication process before a detachment event. Afterward, the LMA establishes a one-way tunnel to neighboring MAGs and starts to buffer the outgoing data packets.

Step 3: The PBAck message will be sent to the p-MAG in response to a PBU message.

Step 4: The MN's context information profile must be kept in neighboring MAGs for a certain amount of time. Therefore, upon detection of the Link Connect trigger, the new associated MAG sends the RA message with the same MN-HNP to the exact MN in order to enable the MN
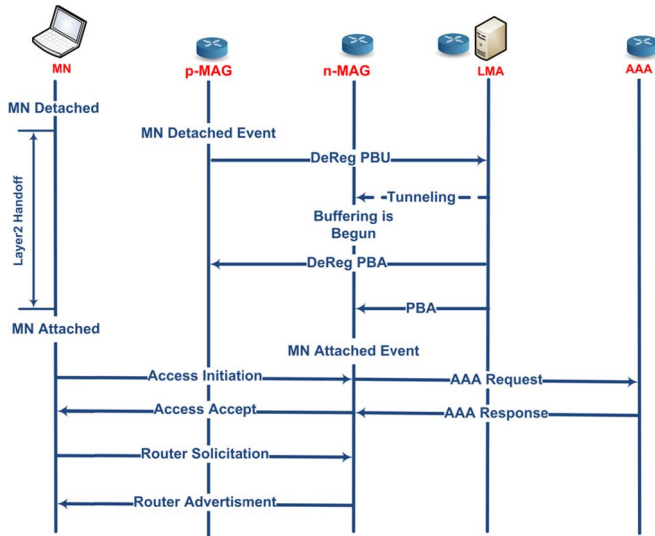
Fig. 7.   Signaling flow of PL-PMIPv6.

to reconfigure its network interface quickly. The prereg-
istration followed by preauthentication process enable the
n-MAG to bypass the registration and authentication pro-
cess by simply comparing the MNID and MN-HNP with
the received ones sent from the LMA.

Step 5: The n-MAG sends the PBU message to the LMA
requesting to update the current new location of the MN
and sets up the reverse endpoint of the bidirectional tunnel
in order to be able to retrieve the data packets destined for
the MN.

Step 6: Eventually, the LMA updates the BCE field related
to MN upon receiving the PBU sent from n-MAG and
forwards the buffered data packets toward the MN through
n-MAG.

However, multicating MN's context information profile to
all neighboring MAG and establishing the tunnels with all of
them not only violates the integrity of information forwarding
but also causes a huge amount of bandwidth consumption and
resource usage.

The literature [26] reported a reduction in data traffic loss for
PMIPv6 with authentication consideration. This is done using
Packet Lossless PMIPv6 (PL-PMIPv6), which is an analytical
model for lossless data traffic. In this model, the n-MAG
registration with LMA is performed by the p-MAG on behalf of
the n-MAG in advance in order to alleviate the L2 HO latency.
Thereafter, the buffering mechanism will be utilized by the
n-MAG to prevent the data packet loss. However, the success
of the whole HO procedure is based on the correct prediction
of the neighboring MAG that the MN is traveling to. More-
over, a large amount of the data packet will be lost since the
n-MAG buffers the data packets only after it receives the PBAck
message. Fig. 7 illustrates the HO procedure performed in
PL-PMIPv6.

The literature [27] proposed another scheme in which the
MN information, such as MN-identifier (MN-HNP), is stored in
an AAA server, enabling the n-MAG to request that information
upon receiving the reassociation request message sent from the
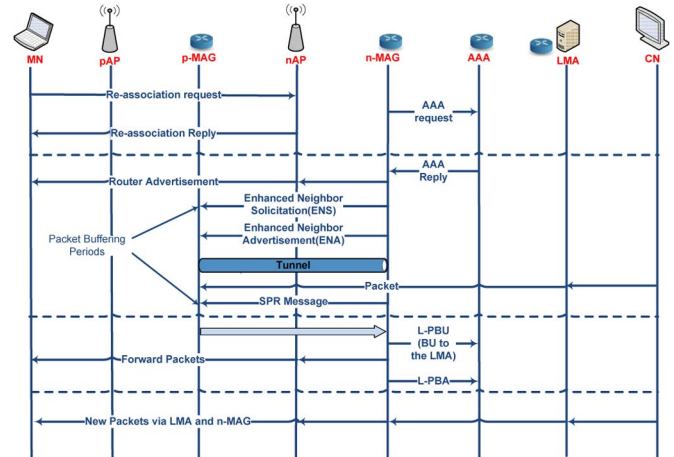MN to the n-MAG via the n-AP (see Fig. 8).

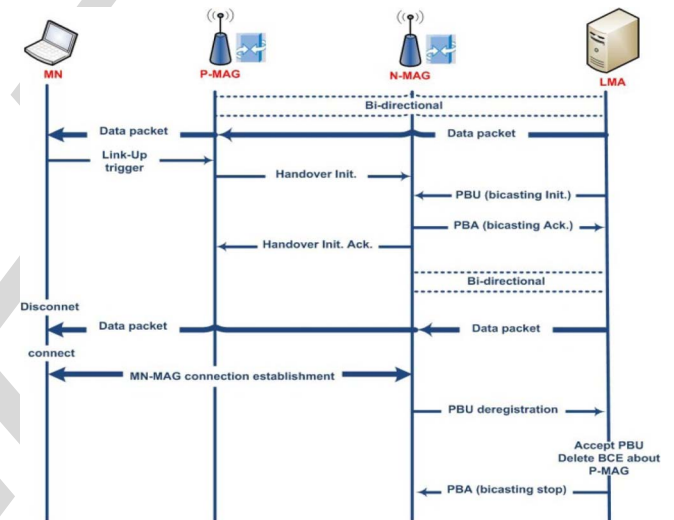Fig. 8.   Proposed fast HO scheme in the IEEE 802.11 network.

Fig. 9.   PMIPv6 with bicasting-enabled feature.

The RA reply message from n-MAG will be sent to the
n-AP that contains the MN-HNP. Based on the retrieved infor-
mation from the AAA server, the n-MAG informs the p-MAG
that the MN is about to leave the current connected network
(p-MAG network domain) by sending the Enhanced Neighbor
Solicitation message that contains the MN-HNP requesting
the performance of the HO procedure. Afterward, a bidirec-
tional tunnel will be established between the n-MAG and the
p-MAG upon stored packet request message transmission. At
this point, the MN is able to receive data packets forwarded
from the LMA to the n-MAG through a bidirectional tunnel
established between the p-MAG and the n-MAG. Eventually,
the LMA forwards data packets via the n-MAG upon receiving
the PBU message sent from the n-MAG. Analytical results
have shown that, although the proposed scheme reduced the
packet loss, utilization of a new entity accompanied with new
message signaling and large buffer capacity have made the
proposed scheme cost effective and inappropriate to be applied
on PMIPv6-based networks.

In PMIPv6 with bicasting [28] (see Fig. 9), upon receiving
the Link-Up trigger message, an HI message will be sent from
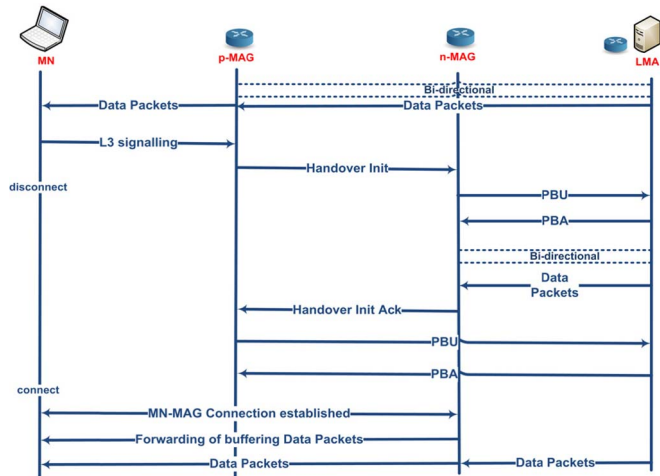the p-MAG to the n-MAG requesting to establish a new PMIP

Fig. 10. PMIPv6 with partial bicasting.

Fig. 11. Proposed PMIP-MHA operations.

tunnel with LMA. The HI message contains the MN's proxy-CoA and HoA (MN-HoA). Thereafter, the n-MAG establishes the tunnel with LMA by sending the MN-HoA and MN-identifier encapsulated in a PBU message. Upon receiving the PBU message, the LMA updates the binding cache entry and sets the tunnel with the n-MAG in order to transmit data packets. At this level, data packets are being transmitted to both p-MAG and n-MAG. Eventually, the LMA stops packet transmission to the p-MAG by releasing the old PMIP upon receiving the request from the n-MAG.

However, in PMIPv6 with partial bicasting [29], a different set of functions can be observed. By moving to the new MAG, the n-MAG will receive the HI message, whereas the PBAck and PBU messages will be exchanged among the n-MAG and the LMA.

The "partial" network region between the n-MAG and LMA is where the bicasting is performed, and not between the MN and LMA. Once the PBAck message is received from the LMA, a bidirectional tunnel will be established, and data packets from the LMA will be buffered by the n-MAG. Additionally, the p-MAG will receive a HI ACK message from the n-MAG requesting to stop bicasting data flows, after which the p-MAG will send the PBU message to the LMA and release the old PMIP tunnel (see Fig. 10).

The n-MAG begins forwarding the buffered data packets to the MN immediately after this new link is established. This is to reduce the loss of packets during the HO process. After this, all normal data transfer operations can now be done between the LMA and MN.

Multicast HO agent (MHA) is used to reduce the unnecessary data transmission and to support the fast neighbor attachment while performing a HO procedure [30]. The proposed scheme is called PMIP-MHA in which, when the link-detected (LD) signal is detected, the proxy multicast link detection (MLD) message will be sent from the MN to the p-MAG requesting preregistration before link local detachment. Upon receiving the MLD message, the MHA running on p-MAG updates its cache and initiates the fast join process with the correspondent MHA running on the n-MAG.
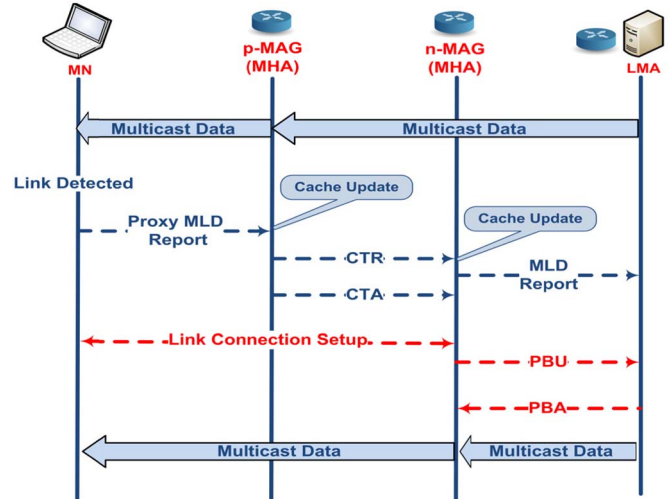
It is noted that the required information of n-MAG is included in LD trigger [31]. Thereafter, the p-MHA and n-MHA exchange context transfer request message and its acknowledgement, which contains the information of MN and the group address that enables the n-MAG to setup the connection with LMA and eventually establish a tunnel without the need of exchanging the route discovery message. However, in the PMIP-MHA scheme, it is assumed that the LD trigger is modified to contain certain MN information that violates the integrity of MN information transmission along with modification of MAGs to handle the MHA operations. Fig. 11 illustrates the PMIP-MHA HO procedure in steps.

In [32], a smart buffering scheme was proposed as a method to avoid data traffic loss. In the proposed scheme, the p-MAG buffers all data traffic without considering the target point of attachment and MN detachment time. In the smart buffering scheme, packet loss is prevented due to running a proactively buffering data packet mechanism on p-MAG by restraining network-side information only. Performing a redundant packet elimination procedure along with a packet-reordering function provides the possibility of the minimization of duplicate packet delivery and discovery mechanism without having an MN involved. Although, by utilizing the smart buffering scheme, the packet loss ratio has reached its minimum level, the high transmission cost of buffered data can be considered the main shortcoming of the proposed scheme. Since an additional signaling message is introduced to identify the target MAG as well as performing the buffering and forwarding procedures between the n-MAG and p-MAG, this scheme will cause some signal traffic overhead.

The literature [33] proposed deployment of a Head MAG scheme to maintain the information of the MN's mobility to the MAGs in the same LMA domain. This new MAG entity, which is called Head MAG, enables a fast HO process and reduced traffic loss by using buffering technique MAGs. The MAG that is located at the optimal location in an LMA domain is granted the Head MAG. Deployment of the Head MAG entity to maintain all the MAGs addresses accompanied with MN's information compels other MAGs to update this information

TABLE I
COMPRESSION OF PREVIOUS WORKS

	Handover Latency	Packet loss rate	Time spent on performing DAD procedure	Signaling Cost
Proxy Mobile IPv6 (PMIPv6) [7]	5	5	5	4
Fast Handover in PMIPv6 [8]	3	3	4	4
Hybrid-mode Fast Handover for PMIPv6 (HF-PMIPv6) [24]	3	3-4	3	3-4
Fast Localized Proxy Mobile IPv6 (FLPMIPv6)[10]	2	2-3	2-3	3-4
Packet Lossless PMIPv6 (PL-PMIPv6) [26]	2	4	3	3-4
Mobile Node's Home Network Prefix (MN-HNP) [27]	3	3	3	4
Proxy Mobile IPv6 -Multicast Handover Agent (PMIP-MHA) [30]	3	2-3	3	5
Smart Buffering scheme [31]	2	2	3	4
Head MAG [33]	2	2	3	5
EBR-PMIPv6	1	1-2	1	5

according to the new location of MNs. As a result, additional infrastructure cost and processing overhead are incurred. An extra mobility-related signaling cost is also incurred due to the introduction of additional messages (e.g., HI, Hack, and request forwarding). Furthermore, due to increasing transfer buffering traffic from the p-MAG to the n-MAG, there will be an additional traffic transmission cost from the uplink and downlink of traffic.

In [34], HO latency, packet loss, and signaling overhead have been analyzed in PMIPv6 in comparison with fast HO for PMIPv6 (PFMIPv6), which is standardized by IETF [35] to evaluate the performance of both protocols in various scenarios. PFMIPv6 is a predictive HO procedure in which the HO procedure will be started by performing the HI process in order to forward data packets from the p-MAG to the n-MAG, in addition to transferring the network-resident context before the MN detaches the current associated network. This is done by measuring the RSS value and by comparing that with the predefined threshold value in order to either trigger or not certain operations. Scanning the neighboring access networks in order to receive the strongest signal, reporting the scanned values to the p-MAG in order to establish the IP-in-IP tunnel with n-MAG, transferring some specific MN's information to the n-MAG and eventually forwarding the data packets from the p-MAG, and utilizing the buffering mechanism in n-MAG are considered the fundamental steps performed in PFMIPv6 HO procedure, respectively. However, the HI can be false due to measuring the RSS value, which may be calculated based on false information in the presence of obstacles or even when the MN changes its movement direction.

According to [36] relatively seamless HO could be approached by using the location information of MNs. Results have shown that utilization of GPS information of each and every single MN while traveling from one PoA to another could provide better opportunities for MAGs to manage the HO procedure in advance. Generally, delivering location information, attained from GPS satellites, to higher level entities in routing hierarchy (e.g., APs, MAGs, etc.) could not only provide sufficient amount of time for them to exchange vital signaling in time but also the exact neighboring destination could be determined [37]. Hence, ping-pong effect on the HO procedure could be alleviated significantly. However, there will be considerable amount of signaling, message exchange, and energy consumption due to retrieving the location information periodically. This could also be decreased by increasing the interarrival time of location information retrieval, which leads

to sacrificing the precision of determination of the exact neighboring destination, along with experiencing a lesser seamless HO procedure.

Table I indicates the effectiveness of the aforementioned schemes in terms of HO latency and packet loss, along with the amount of time spent on performing duplicate address detection procedure, with a rating system from 1 to 5, where 1 indicates the trivial impact of performing particular scheme on either of HO latency and packet loss, and 5 indicates the other end of extreme.

IV. CONCLUSION

In a network-based mobility management scheme such as PMIPv6, the serving network handles the mobility management in a topologically localized domain on behalf of an MN. Although deployment of PMIPv6 protocol has reduced the total amount of HO latency, which consequently alleviates the packet loss amount, it still encounters some connection disruption when performing the HO procedure. Several PMIPv6-enhanced approaches and schemes have been proposed in order to eliminate the HO latency and, eventually, packet loss amount by using a buffering mechanism, altering additional messages, deployment of new entities, and changing the message signaling sequence. However, the proposed schemes and approaches could not be fully adopted by network administration societies due to either being cost effective, having a large amount of bandwidth consumption, or incurring a large amount of burden on network entities. Several proposed schemes have been surveyed in detail in this paper accompanied with their shortcomings. Considering the HO procedure in PMIPv6, utilization of GPS technology could be significantly beneficial in the reduction of packet loss as it provides the preconfiguration information needed by the MN in order to have a seamless HO in advance. Therefore, proposing a novel scheme in which the MN is equipped with a GPS device and performs the HO procedure but with the ability of consuming less energy and message signaling cost could be offered as a future investigation on PMIPv6 HO performance.

REFERENCES

[1] D. Johnson, C. Perkins, and J. Arkko, Mobility Support in IPv6, 2004, IETF RFC 3775. [Online]. Available: http://www.ietf.org/rfc/rfc3775.txt
[2] N. Banerjee, W. Wu, and S. K. Das, "Mobility support in wireless internet," *IEEE Wireless Commun.*, vol. 10, no. 5, pp. 54–61, Oct. 2003.

[3] J. Kempf, Problem Statement For Network-Based Localized Mobility Management (NETLMM), Apr. 2007, RFC 4830. [Online]. Available: http://www.ietf.org/rfc/rfc4830.txt

[4] H. N. AL-Hashimi, K. A. Bakar, and K. Z. Ghafoor, "Inter-domain proxy mobile IPv6 based vehicular network," *Netw. Protocols Algorithms*, vol. 2, no. 4, pp. 1–15, 2011.

[5] J. Guan, I. You, C. Xu, H. Zhou, and H. Zhang, "Survey on route optimization schemes for proxy mobile IPv6," in *Proc. 6th Int. Conf. IMIS*, Palermo, Italy, Jul. 4–6, 2012, pp. 541–546.

[6] G. Iapichino and C. Bonnet, "Host identity protocol and proxy mobile IPv6: A secure global and localized mobility management scheme for multihomed mobile nodes," in *Procl Global Telecommun. Conf.*, Honolulu, HI, USA, Nov. 30/Dec., 4, 2009, pp. 1–6.

[7] S. Gundavelli, K. Chowdhury, V. Devarapalli, B. Patil, and K. Leung, Proxy Mobile IPv6, 2008, IETF RFC 5213. [Online]. Available: http://tools.ietf.org/html/rfc5213

[8] J. C. Lee and D. Kaspar, "PMIPv6 fast handover for PMIPv6 based on 802.11 networks," Network Working Group 2007. [Online]. Available: http://tools.ietf.org/html/draft-lee-netlmm-fmip-00

[9] F. Xia and B. Sarikaya, Mobile Node Agnostic Fast Handovers for Proxy Mobile IPv6, 2007, Network Working Group. [Online]. Available: http://tools.ietf.org/html/draft-xia-netlmm-fmip-mnagno-02

[10] S. Park, Fast Localized Proxy Mobile IPv6 (FLPMIPv6), 2007, Network Working Group. [Online]. Available: http://tools.ietf.org/html/draft-park-netlmm-fastpmip-00

[11] A. Rossi, S. Pierre, and S. Krishnan, "Secure route optimization for MIPv6 using enhanced CGA and DNSSEC," *IEEE Syst. J.*, vol. 7, no. 3, pp. 351–362, Sep. 2013.

[12] M.-C. Chuang, J.-F. Lee, and M.-C. Chen, "SPAM: A secure password authentication mechanism for seamless handover in proxy mobile IPv6 networks," *IEEE Syst. J.*, vol. 7, no. 1, pp. 102–113, Mar. 2013.

[13] J.-H. Lee and T. Ernst, "Lightweight network mobility within PMIPv6 for transportation systems," *IEEE Syst. J.*, vol. 5, no. 3, pp. 352–361, Sep. 2011.

[14] M. Gohar, S. J. Koh, T. W. Um, and H. W. Lee, "Seamless multicast handover in PMIPv6-based wireless networks," in *Proc. 12th ICACT*, Phoenix Park, Ireland, Feb. 7–10, 2010, vol. 1, pp. 502–507.

[15] A. J. Jabir, S. K. Subramaniam, Z. Z. Ahmad, and N. A. W. A. Hamid, "A cluster based proxy mobile IPv6 for IP-WSNs," *EURASIP J.*, vol. 2012, p. 173, May 2012.

[16] J. Lee, "PMIPv6-based distributed mobility management," Dongguk University, DMM Working Group, Seoul, Koera, 2013.

[17] T. C. Schmidt, M. Waehlisch, and S. Krishnan, Base Deployment for Multicast Listener Support in Proxy Mobile IPv6 (PMIPv6) Domains, 2011, IETF RFC 6224. [Online]. Available: http://tools.ietf.org/html/rfc6224

[18] J. Tang, C. Pei, and B. Su, "Research on the localized routing mechanism for the PMIPv6," *J. Xidian Univ.*, vol. 39, no. 1, pp. 98–104, 2012.

[19] M. Waehlisch, Mobile Multicast Sender Support in PMIPv6 Domains draft-schmidt-multimob-pmipv6-source-00, 2011.

[20] H. B. Lee, Y. H. Han, and S. G. Min, "Network mobility support scheme on PMIPv6 networks," in *Int. J. Comput. Netw. Commun. (IJCNC)*, Sep. 2010, vol. 2, no. 5, pp. 206–213.

[21] Z. Jia, G. Wang, and R. Zhao, "A literature survey on handoff for mobile IPv6," *J. Netw.*, vol. 6, no. 8, pp. 1137–1144, Aug. 2011.

[22] R. Li, J. Li, K. Wu, Y. Xiao, and J. Xie, "An enhanced fast handover with low latency for mobile IPv6," *IEEE Trans. Wireless Commun.*, vol. 7, no. 1, pp. 334–342, Jan. 2008.

[23] I. Zhang, L. J. Zhang, and S. Pierre, "Performance analysis of seamless handover in mobile IPv6-based cellular networks," *Intech*, vol. 7, no. 1, pp. 1–26, 2011.

[24] M. H. Lin, W. E. Chen, and C. H. Huang, "HF-PMIPv6: An enhanced fast handovers for network-based mobility management," in *Proc. ICAIT*, Wuhan, China, Jul. 11–14, 2011, pp. 1–7.

[25] I. Al-Surmi, M. Othman, N. A. W. A. Hamid, and B. M. Ali, "Latency low handover mechanism considering data traffic lost preventing for proxy mobile IPv6 over WLAN," *Wireless Pers. Commun.*, vol. 70, no. 1, pp. 459–499, May 2012.

[26] S. Ryu and Y. Mun, "Scheme to prevent packet loss during PMIPv6 handover," *Proc. Trans. Comput. Sci. VI*, vol. 5730, p. 131, 2009.

[27] S. Lee, H. A. Latchman, and B. Park, "Efficient handover scheme of proxy mobile IPv6 in wireless local area networks," *Int. J. Multimedia Ubiquitous Eng.*, vol. 5, no. 2, pp. 1–18, 2010.

[28] M. S. Bargh, B. Hulsebosch, H. Eertink, G. Heijenk, J. Idserda, J. Laganier, A. R. Prasad, and A. Zugenmaier, "Reducing handover latency in future IP-based wireless networks: proxy mobile IPv6 with simultaneous bindings," in *Proc. Int. Symp. World Wireless, Mobile Multimedia Netw.*, Newport Beach, CA, USA, 2008, pp. 1–10.

[29] J. I. Kim and S. J. Koh, "Proxy Mobile IPv6 with partial bicasting for seamless handover in wireless networks," in *Proc. ICOIN*, Barcelona, Spain, Jan. 26–28, 2011, pp. 352–356.

[30] M. Gohar, S. I. Choi, and S. J. Koh, "Fast handover using multicast handover agents in PMIPv6-based wireless networks," in *Proc. ICOIN*, Barcelona, Spain, Jan. 26–28, 2011, pp. 367–372.

[31] *IEEE Standard for Local and Metropolitan Area Networks- Part 21: Media Independent Handover*, IEEE Std 802.21-2008, 2009, pp. c1-301.

[32] H. Y. Choi, K. R. Kim, H. B. Lee, S. G. Min, and Y. H. Han, "Smart buffering for seamless handover in proxy mobile IPv6," *Wireless Commun. Mobile Comput.*, vol. 11, no. 4, pp. 491–499, Apr. 2011.

[33] N. Y. Kwon, H. Kim, S. T. Oh, and H. Choo, "Fast handover scheme based on mobility management of head MAG in PMIPv6," in *Proc. ICCSA*, Santander, Spain, Jun. 20–23, 2011, pp. 181–192.

[34] M. S. Kim, S. K. Lee, D. Cypher, and N. Golmie, "Performance analysis of fast handover for proxy mobile IPv6," *Inf. Sci.*, vol. 219, pp. 208–224, Jan. 2012.

[35] H. Yokota, K. Chowdhury, R. Koodli, B. Patil, and F. Xia, Fast handovers for proxy mobile IPv6, 2010, IETF RFC 5949. [Online]. Available: http://tools.ietf.org/html/rfc5949

[36] A. Moravejosharieh and H. Modares, "A proxy mipv6 handover scheme for vehicular ad-hoc networks," *Wireless Pers. Commun.*, Springer U.S., pp. 1–181, Aug. 2013. [Online]. Available: http://link.springer.com/article/10.1007%2Fs11277-013-1381-8

[37] A. Moravejosharieh, R. Salleh, and H. Modares, "A novel approach for efficient resource consumption in GPS- Based mobile IPv6 wireless LAN," in *Proc. 3rd Int. Conf. Comput. Intell., Modell. Simul.*, Langkawi, Malaysia, Sep. 20–22, 2011, pp. 303–307, DOI: 10.1109/CIMSim.2011.61.

Hero Modares received the Master's degree from the University of Malaya, Kuala Lumpur, Malaysia. She is currently working toward the Ph.D. degree in Mobile IPv6 (MIPv6) security with the Faculty of Computer Science and Information Technology, University of Malaya.

During her Master's degree, she was a Research Assistant. She is currently an Assistant Researcher with the Department of Computer System and Technology, University of Malaya. Her research interests include computer and network security, cryptographic protocol, digital signature and nonrepudiation, mobile communications security (MIPv6), and public-key infrastructure.

Amirhosein Moravejosharieh received the Master's degree in computer science from the University of Malaya, Kuala Lumpur, Malaysia. He is currently working toward the Ph.D. degree in wireless networks from the University of Canterbury, Christchurch, New Zealand.

His research interests include analysis of wireless networks in terms of handover procedures, quality-of-service during handover procedures, and security issues related to handover procedures in Mobile IPv6 wireless networks.

Jaime Lloret (M'07–SM'10) received the M.Sc. degree in physics in 1997, the M.Sc. degree in electronic engineering in 2003, and the Ph.D. (Dr. Ing.) degree in telecommunication engineering in 2006, all from University of Valencia, Spain.

He worked as a Network Designer and an Administrator in several enterprises. He is currently an Associate Professor with the Polytechnic University of Valencia, Valencia, Spain. He is the Head of the Communications and Remote Sensing Group of the Integrated Management Coastal Research Institute, and of the "Active and collaborative techniques and use of technologic resources in the education (EITACURTE)" Innovation Group. He is the Director of the University Master "Digital Post Production." He led many national and international projects. He is currently the Chair of the Working Group for the Standard IEEE 1907.1. He is a Cisco-certified Network Professional Instructor. He is the author of 12 books and more than 220 research papers published in national and international conferences and international journals (more than 50 with ISI Thomson Impact Factor).

Dr. Lloret is a Fellow of the International Academy, Research, and Industry Association (IARIA). He is currently the Vice Chair of the Internet Technical Committee of the IEEE Communications Society and the Internet Society. He has been the General Chair (or Cochair) of 18 international conferences. He has been involved in more than 160 program committees of international conferences and in many organization and steering committees. He has been the Coeditor of 15 conference proceedings and a Guest Editor of several international books and journals. He is the Editor-in-Chief of *Networks Protocols and Algorithms*, the IARIA Journals Board Chair (for eight journals), and an Associate Editor of several international journals.

Rosli Bin Salleh received the B.Sc. degree in computer science from the University of Malaya, Kuala Lumpur, Malaysia, in 1994 and the M.Sc. and Ph.D. degrees from the University of Salford, Salford, U.K., in 1997 and 2001, respectively.

In 2001, he joined the Department of Computer System and Technology, Faculty of Computer Science and Information Technology, University of Malaya, as a Lecturer, and since 2007, he has been appointed as a Senior Lecturer. His research interests include handoff techniques and security in wireless networking.

A Survey on Proxy Mobile IPv6 Handover

Hero Modares, Amirhosein Moravejosharieh, Jaime Lloret, *Senior Member, IEEE*, and Rosli Bin Salleh

Abstract—As wireless technologies have been improving in recent years, a mobility management mechanism is required to provide seamless and ubiquitous mobility for end users who are roaming among points of attachment in wireless networks. Thus, Mobile IPv6 was developed by the Internet Engineering Task Force (IETF) to support the mobility service. However, Mobile IPv6 is unable to fulfill the requirements of real-time applications, such as video streaming service and voice over IP service, due to its high handover (HO) latency. To address this problem, Proxy Mobile IPv6 (PMIPv6) has been introduced by the IETF. In PMIPv6, which is a network-based approach, the serving network controls mobility management on behalf of the mobile node (MN). Thus, the MN is not required to participate in any mobility-related signaling. However, the PMIPv6 still suffers from lengthy HO latency and packet loss during a HO. This paper explores an elaborated survey on the HO procedure of PMIPv6 protocols and proposed approaches accompanied by a discussion about their points of weakness.

Index Terms—Fast localized Proxy Mobile IPv6 (PMIPv6) handover (HO) procedure, HO in PMIPv6, PMIPv6, PMIPv6 with partial bicasting, predictive mode, reactive mode.

I. Introduction

THE future broadband wireless networks are quickly evolving toward all-IP networks. With an explosive growth in the number of users that are using the Internet in a wireless environment, the issue of IP mobility management technology is on the rise. Mobile IPv6 (MIPv6) [1], which is a host-based mobility management protocol, is one of the most representative efforts and proposed by the Internet Engineering Task Force (IETF) as the main protocol for mobility management at the IP layer. However, although MIPv6 is a well-known mature standard for IPv6 mobility, it has some well-known problems, such as handover (HO) latency, packet loss, and signaling overhead. Moreover, the MIPv6 requires protocol stack modification of the mobile node (MN) to support IP mobility [2]–[6]. Recently, Proxy MIPv6 (PMIPv6), which is one of the network-based mobility management protocols, has been standardized by the IETF Network-Based Localized Mobility Management Working Group [7]. Unlike the MIPv6, PMIP6 allows the serving network to control the mobility management on behalf of an MN, thereby eliminating the MN from any mobility-related signaling.

PMIPv6 is essentially based on MIPv6 in the sense that it extends MIPv6 signaling and reuses many concepts such as the functionality of the home agent (HA). However, PMIPv6 is also designed to provide network-based mobility management support to an MN in a topologically localized domain. Therefore, an MN is exempted from participation in any mobility-related signaling, and a proxy mobility agent in the serving network performs mobility-related signaling on behalf of the MN. However, a network-based mobility management protocol, such as PMIPv6, still suffers from HO latency and packet loss during a HO, such as in MIPv6. Although several fast HO schemes based on PMIPv6 have been already introduced to reduce the HO latency and packet loss [8]–[13], these schemes still experience some packet loss and packet-ordering problems during a HO [14]–[23]. In order to eventually come up with a robust and seamless HO procedure in PMIPv6 and its derived improved approaches, it is imperative to run as much comprehensive investigation as possible on previous related state of the arts. Here, we try to roughly examine various approaches in detail in the field of HO procedure improvement. Of course, it is obvious that the provided list of investigated approaches is not exhaustive.

This paper is organized as follows. Section II represents the background of PMIPv6 and the fundamental steps performed in the HO procedure. Section III discusses some of the schemes and approaches proposed in order to enhance the HO latency in the PMIPv6 network domain. The survey is concluded in Section IV, along with a discussion on future research opportunities in the PMIPv6 HO area.

II. Background

PMIPv6 is designed to provide network-based IP mobility management support to an MN in a topologically localized domain, without requiring the participation of the MN in any IP-mobility-related signaling. The core functional components used to support mobility in PMIPv6 are the policy store (PS), the local mobility anchor (LMA), and the mobile access gateway (MAG). The PS is the entity that manages the MN's authentication and maintains the MN's profile, which is a set of parameters configured for a given MN. The LMA is similar to the HA in MIPv6. However, it has additional capabilities required to support PMIPv6. The main role of the LMA is to maintain reachability to the MN's address, whereas the MN moves around within a PMIPv6 domain. The LMA includes a binding cache entry (BCE) for each currently registered MN. The main role of the MAG, which is typically the access router
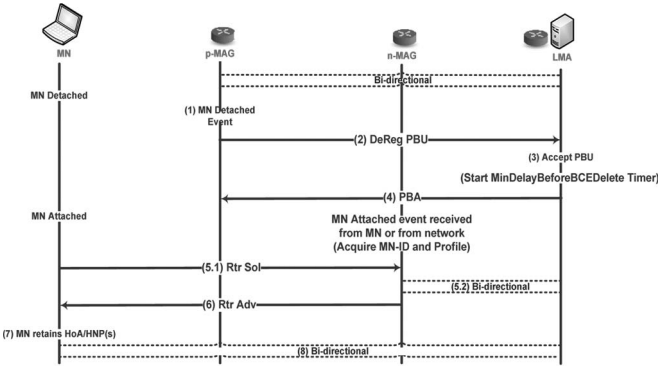
Fig. 1.   Signaling flow of PMIPv6.

Fig. 2.   Message flow of fast HO in PMIPv6.

(AR), is to detect the MN's movement and to send mobility-related signaling to the MN's LMA on behalf of the MN. Additionally, the MAG establishes a tunnel with the LMA for packet transmission. The MAG ensures that an MN can obtain an address from its home network prefix (HNP) and move anywhere within the PMIPv6 domain. Fig. 1 shows the signaling flow of the overall operations in PMIPv6 from the previously attached MAG (p-MAG) to the newly attached MAG (n-MAG). The HO procedure is described as follows [7].

Step 1: The HO procedure in PMIPv6 starts with MN's movement detection performed by the p-MAG along with the signaling LAM to report the MN's movement in order to update the BCE table inside the LMA.

Step 2: Upon receiving the update request sent from the p-MAG, the LMA identifies the sender of the request and waits for a certain amount of time to allow the n-MAG to request the binding update. However, the BCE will be deleted if the binding update request is not received within a certain amount of time.

Step 3: Upon detecting the MN on its access link, the n-MAG sends the PBU message to the MN's associated LMA.

Step 4: Upon receiving the PBU message, the LMA updates the related field in the BCE table and binds the MN-HNP to a Proxy Care-Of Address (proxy-CoA), which is the n-MAG address. Thereafter, a Proxy Binding Acknowledgement (PBAck) message containing the MN-HNP will be sent to the n-MAG.

Step 5: Upon (step 5.1) detecting the MN Router Solicitation (RS), (step 5.2) a bidirectional tunnel will be established between the LMA and the n-MAG.

Step 6: Upon receiving the PBAck sent from LMA, the n-MAG sets up the tunnel along by sending the Router Advertisement (RA) to the MN that contains updated MN-HNP and is sent from the LMA.

Step 7: When the MN receives the RA sent from the n-MAG, it starts to configure the new CoA address by utilizing either stateful or stateless address autoconfiguration procedures.

Step 8: By the completion of the address autoconfiguration procedure, data flows will be forwarded to the MN.

III. RELATED WORK

When an MN moves to a new access network in a PMIPv6 domain, it inevitably experiences packet loss or HO latency
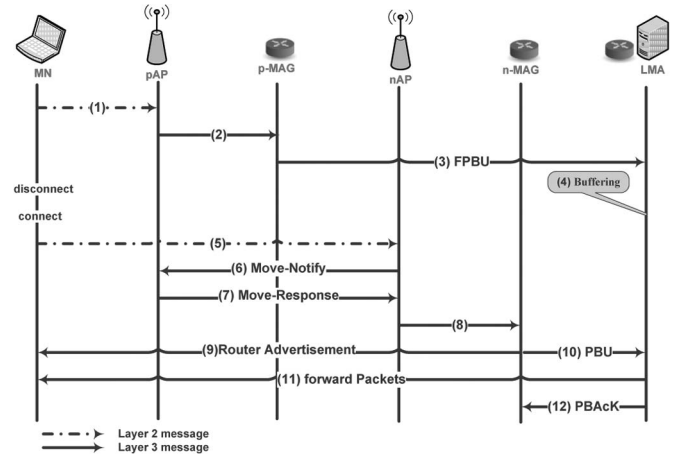
until it receives its MN-HNP advertisement from the n-MAG. Therefore, several fast HO mechanisms have recently been introduced to reduce the HO latency and packet loss with PMIPv6 [8]–[10].

A fast HO method was proposed [8] based on the 802.11 networks for the PMIPv6. Context information, such as the MN's authentication information and HNP, is transferred using the Inter-Access Point Protocol (IAPP) scheme.

Fig. 2 shows the sequence of message signaling related to the fast HO scheme for PMIPv6.

Step 1: *Sending the disassociation message (DM)*. The MN detects its movement by measuring the received signal strength (RSS) value, and it sends the DM that contains the MN's medium access control (MAC) address to its current connected AP when the RSS value exceeds the preconfigured threshold.

Step 2: *Forwarding the MN's ID*. Upon receiving the DM sent from MN, the associated AP [previous AP (pAP)] forwards the MN's ID (MAC address) to the current connected MAG (p-MAG).

Step 3: *Sending the fast PBU* (FPBU) *message*. The p-MAG then sends a FPBU message containing the MN's network access identifier (NAI) option to the LMA upon receiving the MN's ID.

Step 4: *Buffering*. Upon receiving the FPBU message, the LMA starts to buffer data flows destined to the MN.

Step 5: *Sending the reassociation (RA) message*. Once the MN attaches to the new point of attachment [new AP (nAP)], the RA message will be sent to the AP indicating the MN's MAC address and previous basic service set identification of the pAP.

Steps 6 and 7: *Exchanging MOVE-notify and MOVE response message*. Upon receiving the RA message, the MOVE-notify message will be transmitted from the nAP to the pAP via the distribution system (DS). Thereafter, context information that includes the HNP and authentication information, encapsulated in the MOVE-response message, will be replied from the pAP to the nAP.

Step 8: *Forwarding context information*. The nAP then forwards the context information of the MN to the n-MAG after the MOVE-response message is received.
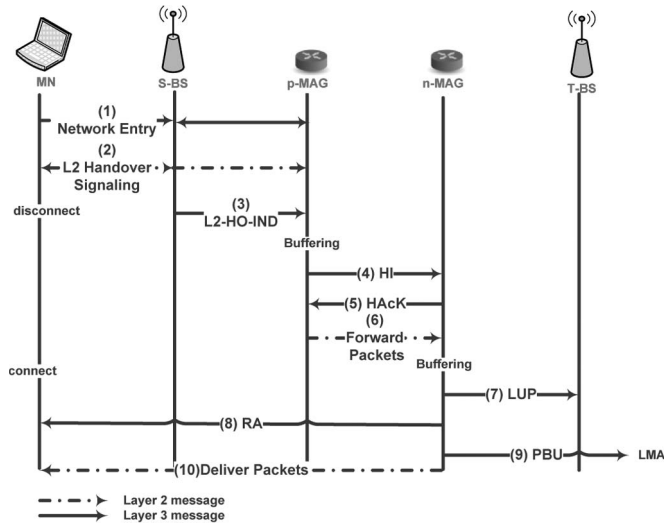
Fig. 3. Predictive mode.

Step 9: *Reconfiguring the default router for the MN*. When the MN's context information is delivered to the n-MAG, the RA message will be sent to the MN through the nAP in order to reconfigure the default router of the MN.

Step 10: *Configuring forwarding information*. Upon receiving the context information, the PBU message will be constructed by utilizing MN's context information and will be sent to LMA.

Step 11: *Forwarding buffered packets*. When the PBU message is received by the LMA, it then creates a route for the MN and begins to send the buffered data flows.

In a fast HO method [8], Lee *et al.* suggested adapting IAPP to reduce the "access authentication/obtaining MN's profile" time of the total HO delay. Nonetheless, the on-the-fly packets will be still lost during a HO.

An enhancement to the PMIPv6 protocol has been proposed in [9] to have the Layer 3 HO (L3 HO) performance and context transfer improved. This enhancement borrows a similar concept from fast HOs for FMIPv6. There are two modes of operation depending on whether the signaling of Layer 2 HO (L2 HO) is finished on the previous link or not: the predictive mode or reactive mode. During predictive mode, the HO initiation (HI) message is used by the p-MAG in order to transfer context to the n-MAG. While in reactive mode, an FBU message is used by the n-MAG instead of requesting MN's context information from the p-MAG. Eventually, a bidirectional tunnel will be established in order to transfer the packets buffered while performing the HO procedure.

A. Predictive Mode

In predictive mode, the L2 HO signaling finishes in the previous link. In this section, the MAG and the base station (BS) can be colocated using physical entities that are different (see Fig. 3). The procedure is described as follows.

Step 1: The network entry procedure is performed by the MN where access authentication and the configuration of the IPv6 are completed. After the IP connectivity is successful,

the mobility-related signaling of the MN will be done by the p-MAG on its behalf.

Step 2: When the MN is about to leave its associated BS coverage area, the MN and the associated BS negotiate through L2 HO signaling.

Step 3: The L2 HO-IND message, which includes the target BS ID (t-BS-ID), is sent by the serving BS (s-BS) to p-MAG once the L2 HO decision is made.

Step 4: The MAGs contain the [BS-ID, Proxy-CoA] tuples. Once the L2-HO-IND message is delivered, the p-MAG will then proceed to the following.

  Step 4.1: Collect the related context of the MN with the following information: MN Identifier, MN Home Address (MN-HoA), MN-HNP, and MN's Proxy-CoA in the p-MAG and the MN's MAC.

  Step 4.2: Determine the n-MAG's proxy CoA that will be retrieved by the p-MAG in order to send the HI message by utilizing the BS-ID field included in the L2-HO-IND message.

  Step 4.3: Send the HI message to the n-MAG.

Step 5: Start the creation of the Binding Update List in the n-MAG side based on information retrieved from the HI message. Thereafter, the HAck message will be sent to the p-MAG, and once the HAck message is delivered to p-MAG, a bidirectional tunnel will be established between n-MAG's proxy-CoA and p-MAG proxy-CoA as the two ends of the tunnel.

Step 6: Packets from the p-MAG meant for the MN are tunneled to the n-MAG according to the MN-HoA. The packets received by the LMA are decapsulated by the p-MAG, encapsulate back into the p-MAG/n-MAG tunnel, and then sent to the n-MAG. The packets should be buffered by the n-MAG until the n-MAG and MN link is ready.

Step 7: Once the MN attaches to the t-BS, the network reentry is performed. To expedite the procedure, the context transfer from the p-MAG is used. The Link UP (LUP) message is sent to the n-MAG by the t-BS indicating that L2 link is established.

Step 8: The RA message containing the n-MAG's information is sent by the n-MAG to the MN that helps data transmission between the MN and the n-MAG feasible.

Step 9: The binding in LMA is updated when the n-MAG sends the PBU.

Step 10: Eventually, The MN receives the buffered packets from the n-MAG.

B. Reactive Mode

The reactive mode is shown in Fig. 4. The following steps are performed to process the HO procedure.

Step 1: The link layer is established after the network reentry process is performed by the MN. In order to expedite the link process, the context from the original session is needed.

Step 2: In order to reduce the loss of packets during HO, packets should be automatically buffered by the p-MAG for the MNs that are no longer in the link. Two cases need to be covered here. In the first case, the p-MAG did
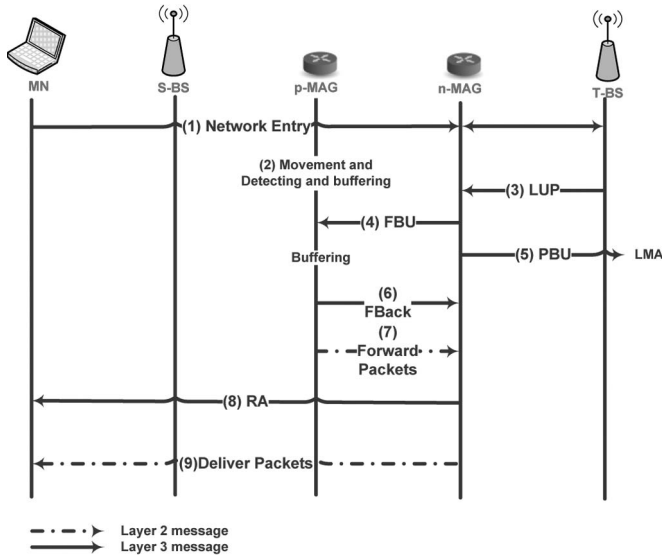
Fig. 4.   Reactive mode.

not know that the MN was handing over after it had just moved. In the second case, the MN knows that it is moving and that the procedure has not been completed yet, but the MN has already started exchanging L2 messages with the p-MAG. The packets will be automatically buffered (probably following a default period of time) by the p-MAG for every MN that is not within its link. The p-MAG could just buffer the packets because the chances of errors or denial-of-service attacks are very slim.

Step 3: Once the process of network reentry is completed, the n-MAG will receive the LUP message from the t-BS.

Step 4: The n-MAG immediately sends the FBU to the p-MAG once the previous BS-ID and MN's MAC becomes available after the network reentry process. The FBU contains the n-MAG's Proxy-CoA and the MAC of the MNs. By referring the [BS-ID, Proxy-COA] tuples in the n-MAG, the p-MAG's address can be determined. It is safe to assume that the previous BS-ID is exchanged during network reentry for this step, e.g., WiMAX links.

Step 5: The PBU is sent by the n-MAG to update the binding in LMA.

Step 6: The p-MAG identifies the MN's Binding Update List using the MN's MAC and retrieves the related context. The related context contains information such as the MN identifier, the MN-HoA, the MN-HNP, the MN's Proxy-CoA in the p-MAG, and the MN's MAC. The FBack message is used to transfer the context from p-MAG to n-MAG. The bidirectional tunnel will be established as soon as the n-MAG receives the FBack message. The tunnel will have the p-MAG's Proxy-CoA at one end and the n-MAG's Proxy-CoA at the other end.

Step 7: The p-MAG forwards the buffered packets to the n-MAG once the bidirectional tunnel is established.

Step 8: The RA and the n-MAG's information will be sent by the n-MAG to help MN send its packets.

Step 9: The MN receives the packets from the n-MAG.

The literature [9] utilizes the FMIPv6 signaling mechanism to improve the performance of the L3 HO. Before an MN moves from the s-BS to the t-BS, the MN provides the t-BS information (t-BS ID) during the L2 HO signaling procedure. The MN then acquires the IP address of the n-MAG from a tuple incorporated in all the MAGs and performs the L3 HO based on this information. However, this scheme also has some limitations.

1) Each MAG needs to have a tuple that contains the BS-IDs and IP addresses for all the MAGs in the PMIPv6 domain.
2) After a HO, a packet-ordering problem occurs between the packets buffered at the p-MAG and the packets from the LMA after registration.
3) The MN should provide information about the target network to the p-MAG through L2 signaling.

The literature [24] proposed a hybrid mechanism to reduce the HO latency along with a reduction in signaling cost and packet delivery cost in PMIPv6 called hybrid-mode fast HO for PMIPv6 (HF-PMIPv6). In HF-PMIPv6, a decision table is utilized to determine the mode of mobility (i.e., predictive or reactive). If the mobility mode is determined to be in predictive mode, then the HF-PMIPv6 will be performed as the same as F-MIPv6 in which a tunnel will be established between p-MAG and n-MAG to alleviate packet loss. Otherwise, the mobility mode will be considered in reactive mode; therefore, the HF-PMIPv6 directly performs the HO procedure without setting up the tunnel in order to reduce the HO latency, tunnel transmission cost, and eventually, signaling cost.

Park *et al.* [10] proposed fast and local PMIPv6 (FLPMIPv6) to reduce the HO latency and packet loss. This scheme is based on FMIPv6 and uses the messages defined in IEEE 802.21. The MN provides information on the n-MAG using a media independent HO (MIH) message before the HO. The current connected MAG (p-MAG) then sends a HO-related message to the n-MAG. However, since this scheme is derived from host-based mobility and initiated by MNs, the network access devices need to perform L2 intelligently. In addition, since the p-MAG sends a BU message to the LMA before the L2 HO occurs, this means the L3 HO is performed before the L2 HO. Therefore, significant packet losses occur from the time the L3 HO is completed until the end of the L2 HO. In order to perform the HO procedure, predictive mode has been utilized in FLPMIPv6, and its related HO procedure is shown in Fig. 5.

Step 2: An MIH HI message will be transmitted to previous proxy mobile agent (PMA) (p-MAG) to inform of its movement. The new PMA (n-MAG)'s [AR-ID, AR-Info] tuples are included in this command message.

Step 3: Once the MIH HI message is received by the p-MAG, the HI message is sent to the n-MAG by that p-MAG. The HI message will have the MN's IP address (PCoA) and the MN's Identifier. The n-MAG will examine the existence of a tunnel to the LMA for PCoA after receiving the HI message. If such a tunnel is already present, there are two possibilities for this. One, the p-MAG's HI message is spurious, and the tunnel has been set up by the n-MAG when it saw the L2 being triggered earlier. The second possibility is that another node is already present and already using the PCoA address on the link. The MN's
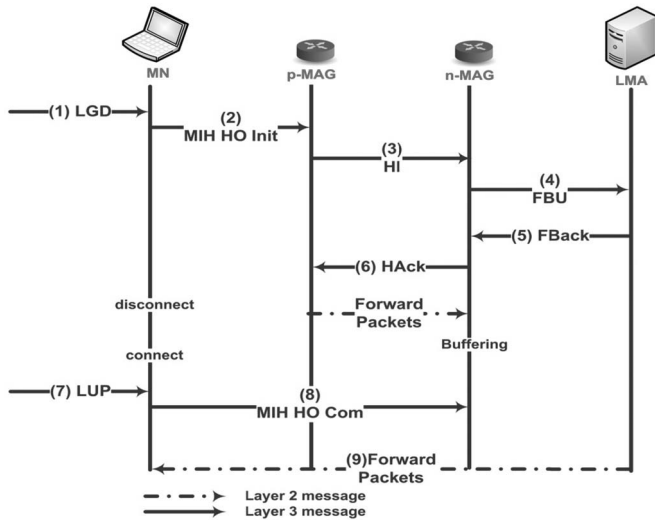
Fig. 5.   FLPMIPv6 HO procedure.

identifier is verified by the n-MAG to ensure if it is the same node. It will return a failure reply if the node is the same one, thus getting a Duplicate Address. However, if the HI message is accepted and processed by the n-MAG, the LMA will get the FBU message from the n-MAG. The tunnel from the p-MAG will then be redirected. The FBU message may contain the MN's unique identifier, which can be optionally included along with the PCoA as the HoA.

Step 4: The FBU message will be examined by the LMA to ensure whether there is a binding for the Regional Care-of Address (RCoA). A new binding entry will be created if such does not exist. If there is a binding, then the MN's identifier is verified with the one in the FBU to ensure it is similar. The binding information is updated if it matches and fails it if it does not. The tunnel is set (or updated) to the n-MAG after the FBU is successfully processed by the LMA. This tunnel is used to send and receive packets from the PCoA. Normally, the host route is added and points to the tunnel for the PCoA. The LMA will send an FBack message to the n-MAG if the MN's RCoA is updated successfully.

Step 5: The n-MAG will examine the FBU to ensure whether it has been processed successfully upon receiving the FBack message, and the HAck message will indicate a failure if it has not. Otherwise, a tunnel to the LMA is created. The forwarding is set up such that packets containing the PCoA's source address will be the one forwarded into the tunnel. States such as binding state is also maintained. This can be use as a verification method for any duplication or spurious indications of the MN or p-MAG. The host route is created to enable packets to be forwarded to the MN. A HAck message indicating a successful HO procedure will be sent back by the n-MAG to the p-MAG.

Step 6: Packets are forwarded to the n-MAG once the p-MAG receives the HAck message.

Step 7: The MN's MIHF will receive the LUP indicator from the MIHF when the MN connects to a new link. The n-MAG then receives the MIH HO Com message from the MN.
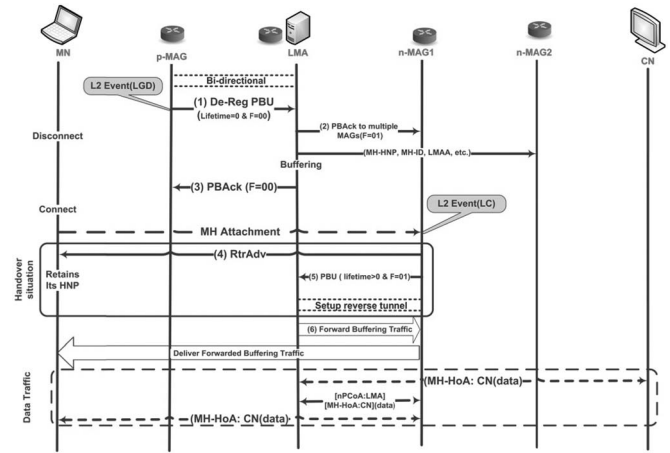

Fig. 6.   Latency low HO mechanism.

Step 8: Upon receiving the MIH HO Com message, the n-MAG will use this as an indication to begin packet forward to the MN. After which the buffered packets is forwarded.

In order to eliminate the connection failure and boost the HO performance up while the MN is roaming among PoAs, LMA plays a pivotal role as a context transfer node [25].

Whenever the LMA receives the link going down (LGD) message sent from p-MAG, it will multicast the MN's context information profile such as MN's ID and MN-HNP included in a modified PBAck message toward multiple neighboring MAGs. This is done based on a new MAG_Cache_Entry list configured at the LMA in order to perform the preregistration and preauthentication process closely together in advance before losing the connectivity with the associated MAG. The proposed mechanism enables the MN to quickly reconfigure its network interface immediately after receiving the RA message disseminated by n-MAG and resume its communication as quickly along with less connection failure as possible. Additionally, the buffering mechanism is offered to buffer outgoing data packets during the MN handing over procedure in order to be forwarded after the HO procedure completion. Fig. 6 illustrates the message signaling sequence of the proposed mechanism and the latency low HO mechanism.

Step 1: The p-MAG sends the deregistration request included in a PBU message to the LMA alerting the HO condition by LGD trigger. This notifies the LMA to update the BCE field related to MN and be ready for the proactive HO procedure.

Step 2: The LMA starts to multicast the PBAck message, which includes the MN's context information profile to multiple neighboring MAGs in order to enable the MN to perform the preregistration followed by the preauthentication process before a detachment event. Afterward, the LMA establishes a one-way tunnel to neighboring MAGs and starts to buffer the outgoing data packets.

Step 3: The PBAck message will be sent to the p-MAG in response to a PBU message.

Step 4: The MN's context information profile must be kept in neighboring MAGs for a certain amount of time. Therefore, upon detection of the Link Connect trigger, the new associated MAG sends the RA message with the same MN-HNP to the exact MN in order to enable the MN
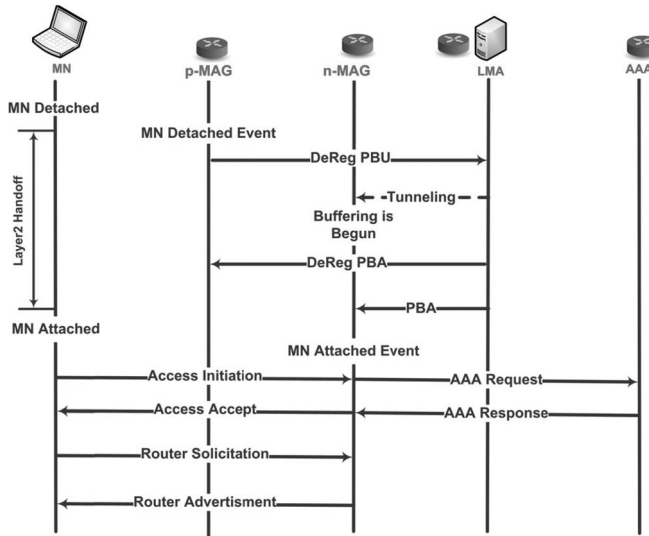
Fig. 7.   Signaling flow of PL-PMIPv6.

to reconfigure its network interface quickly. The prereg-istration followed by preauthentication process enable the n-MAG to bypass the registration and authentication pro-cess by simply comparing the MNID and MN-HNP with the received ones sent from the LMA.

- Step 5: The n-MAG sends the PBU message to the LMA requesting to update the current new location of the MN and sets up the reverse endpoint of the bidirectional tunnel in order to be able to retrieve the data packets destined for the MN.

- Step 6: Eventually, the LMA updates the BCE field related to MN upon receiving the PBU sent from n-MAG and forwards the buffered data packets toward the MN through n-MAG.

However, multicating MN's context information profile to all neighboring MAG and establishing the tunnels with all of them not only violates the integrity of information forwarding but also causes a huge amount of bandwidth consumption and resource usage.

The literature [26] reported a reduction in data traffic loss for PMIPv6 with authentication consideration. This is done using Packet Lossless PMIPv6 (PL-PMIPv6), which is an analytical model for lossless data traffic. In this model, the n-MAG registration with LMA is performed by the p-MAG on behalf of the n-MAG in advance in order to alleviate the L2 HO latency. Thereafter, the buffering mechanism will be utilized by the n-MAG to prevent the data packet loss. However, the success of the whole HO procedure is based on the correct prediction of the neighboring MAG that the MN is traveling to. More-over, a large amount of the data packet will be lost since the n-MAG buffers the data packets only after it receives the PBAck message. Fig. 7 illustrates the HO procedure performed in PL-PMIPv6.

The literature [27] proposed another scheme in which the MN information, such as MN-identifier (MN-HNP), is stored in an AAA server, enabling the n-MAG to request that information upon receiving the reassociation request message sent from the MN to the n-MAG via the n-AP (see Fig. 8).
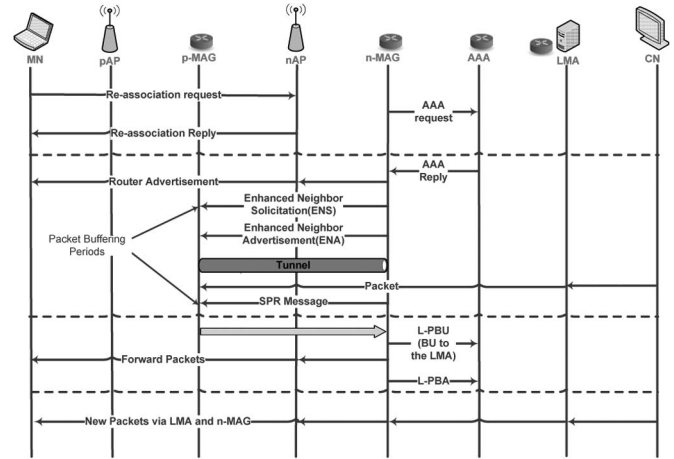

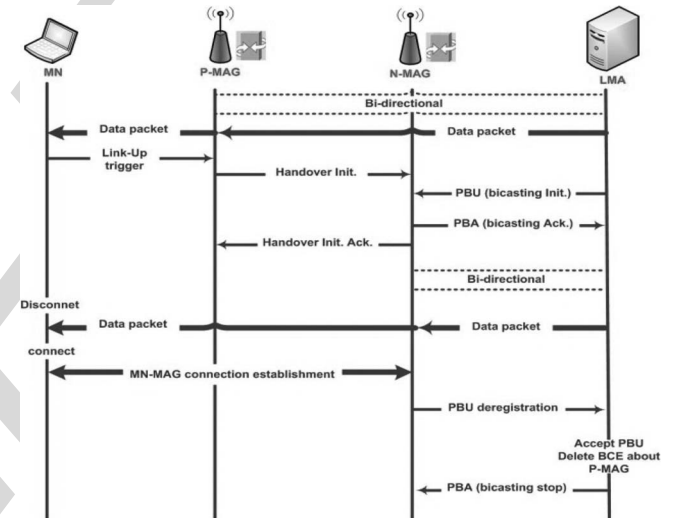Fig. 8.   Proposed fast HO scheme in the IEEE 802.11 network.

Fig. 9.   PMIPv6 with bicasting-enabled feature.

The RA reply message from n-MAG will be sent to the n-AP that contains the MN-HNP. Based on the retrieved infor-mation from the AAA server, the n-MAG informs the p-MAG that the MN is about to leave the current connected network (p-MAG network domain) by sending the Enhanced Neighbor Solicitation message that contains the MN-HNP requesting the performance of the HO procedure. Afterward, a bidirec-tional tunnel will be established between the n-MAG and the p-MAG upon stored packet request message transmission. At this point, the MN is able to receive data packets forwarded from the LMA to the n-MAG through a bidirectional tunnel established between the p-MAG and the n-MAG. Eventually, the LMA forwards data packets via the n-MAG upon receiving the PBU message sent from the n-MAG. Analytical results have shown that, although the proposed scheme reduced the packet loss, utilization of a new entity accompanied with new message signaling and large buffer capacity have made the proposed scheme cost effective and inappropriate to be applied on PMIPv6-based networks.

In PMIPv6 with bicasting [28] (see Fig. 9), upon receiving the Link-Up trigger message, an HI message will be sent from the p-MAG to the n-MAG requesting to establish a new PMIP
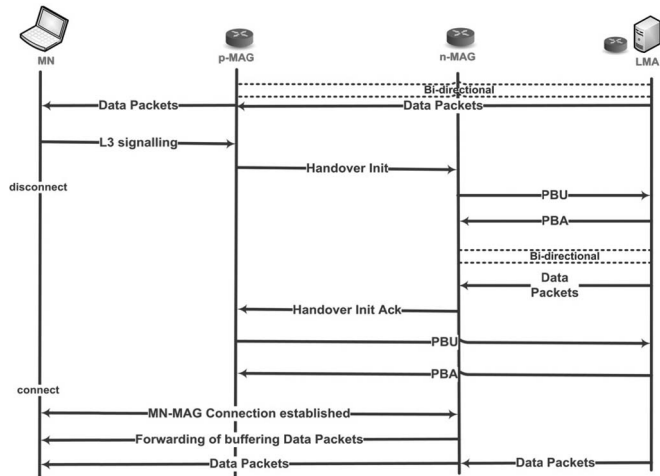
Fig. 10. PMIPv6 with partial bicasting.

Fig. 11. Proposed PMIP-MHA operations.

tunnel with LMA. The HI message contains the MN's proxy-CoA and HoA (MN-HoA). Thereafter, the n-MAG establishes the tunnel with LMA by sending the MN-HoA and MN-identifier encapsulated in a PBU message. Upon receiving the PBU message, the LMA updates the binding cache entry and sets the tunnel with the n-MAG in order to transmit data packets. At this level, data packets are being transmitted to both p-MAG and n-MAG. Eventually, the LMA stops packet transmission to the p-MAG by releasing the old PMIP upon receiving the request from the n-MAG.

However, in PMIPv6 with partial bicasting [29], a different set of functions can be observed. By moving to the new MAG, the n-MAG will receive the HI message, whereas the PBAck and PBU messages will be exchanged among the n-MAG and the LMA.

The "partial" network region between the n-MAG and LMA is where the bicasting is performed, and not between the MN and LMA. Once the PBAck message is received from the LMA, a bidirectional tunnel will be established, and data packets from the LMA will be buffered by the n-MAG. Additionally, the p-MAG will receive a HI ACK message from the n-MAG requesting to stop bicasting data flows, after which the p-MAG will send the PBU message to the LMA and release the old PMIP tunnel (see Fig. 10).

The n-MAG begins forwarding the buffered data packets to the MN immediately after this new link is established. This is to reduce the loss of packets during the HO process. After this, all normal data transfer operations can now be done between the LMA and MN.

Multicast HO agent (MHA) is used to reduce the unnecessary data transmission and to support the fast neighbor attachment while performing a HO procedure [30]. The proposed scheme is called PMIP-MHA in which, when the link-detected (LD) signal is detected, the proxy multicast link detection (MLD) message will be sent from the MN to the p-MAG requesting preregistration before link local detachment. Upon receiving the MLD message, the MHA running on p-MAG updates its cache and initiates the fast join process with the correspondent MHA running on the n-MAG.
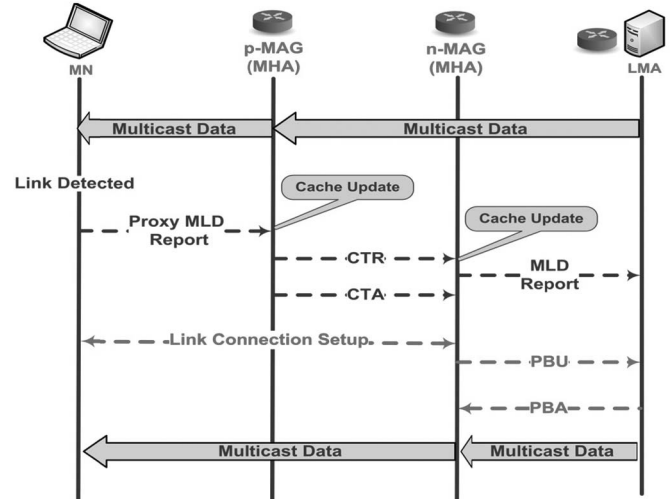
It is noted that the required information of n-MAG is included in LD trigger [31]. Thereafter, the p-MHA and n-MHA exchange context transfer request message and its acknowledgement, which contains the information of MN and the group address that enables the n-MAG to setup the connection with LMA and eventually establish a tunnel without the need of exchanging the route discovery message. However, in the PMIP-MHA scheme, it is assumed that the LD trigger is modified to contain certain MN information that violates the integrity of MN information transmission along with modification of MAGs to handle the MHA operations. Fig. 11 illustrates the PMIP-MHA HO procedure in steps.

In [32], a smart buffering scheme was proposed as a method to avoid data traffic loss. In the proposed scheme, the p-MAG buffers all data traffic without considering the target point of attachment and MN detachment time. In the smart buffering scheme, packet loss is prevented due to running a proactively buffering data packet mechanism on p-MAG by restraining network-side information only. Performing a redundant packet elimination procedure along with a packet-reordering function provides the possibility of the minimization of duplicate packet delivery and discovery mechanism without having an MN involved. Although, by utilizing the smart buffering scheme, the packet loss ratio has reached its minimum level, the high transmission cost of buffered data can be considered the main shortcoming of the proposed scheme. Since an additional signaling message is introduced to identify the target MAG as well as performing the buffering and forwarding procedures between the n-MAG and p-MAG, this scheme will cause some signal traffic overhead.

The literature [33] proposed deployment of a Head MAG scheme to maintain the information of the MN's mobility to the MAGs in the same LMA domain. This new MAG entity, which is called Head MAG, enables a fast HO process and reduced traffic loss by using buffering technique MAGs. The MAG that is located at the optimal location in an LMA domain is granted the Head MAG. Deployment of the Head MAG entity to maintain all the MAGs addresses accompanied with MN's information compels other MAGs to update this information

TABLE I
COMPRESSION OF PREVIOUS WORKS

	Handover Latency	Packet loss rate	Time spent on performing DAD procedure	Signaling Cost
Proxy Mobile IPv6 (PMIPv6) [7]	5	5	5	4
Fast Handover in PMIPv6 [8]	3	3	4	4
Hybrid-mode Fast Handover for PMIPv6 (HF-PMIPv6) [24]	3	3-4	3	3-4
Fast Localized Proxy Mobile IPv6 (FLPMIPv6)[10]	2	2-3	2-3	3-4
Packet Lossless PMIPv6 (PL-PMIPv6) [26]	2	4	3	3-4
Mobile Node's Home Network Prefix (MN-HNP) [27]	3	3	3	4
Proxy Mobile IPv6 -Multicast Handover Agent (PMIP-MHA) [30]	3	2-3	3	5
Smart Buffering scheme [31]	2	2	3	4
Head MAG [33]	2	2	3	5
EBR-PMIPv6	1	1-2	1	5

according to the new location of MNs. As a result, additional infrastructure cost and processing overhead are incurred. An extra mobility-related signaling cost is also incurred due to the introduction of additional messages (e.g., HI, Hack, and request forwarding). Furthermore, due to increasing transfer buffering traffic from the p-MAG to the n-MAG, there will be an additional traffic transmission cost from the uplink and downlink of traffic.

In [34], HO latency, packet loss, and signaling overhead have been analyzed in PMIPv6 in comparison with fast HO for PMIPv6 (PFMIPv6), which is standardized by IETF [35] to evaluate the performance of both protocols in various scenarios. PFMIPv6 is a predictive HO procedure in which the HO procedure will be started by performing the HI process in order to forward data packets from the p-MAG to the n-MAG, in addition to transferring the network-resident context before the MN detaches the current associated network. This is done by measuring the RSS value and by comparing that with the predefined threshold value in order to either trigger or not certain operations. Scanning the neighboring access networks in order to receive the strongest signal, reporting the scanned values to the p-MAG in order to establish the IP-in-IP tunnel with n-MAG, transferring some specific MN's information to the n-MAG and eventually forwarding the data packets from the p-MAG, and utilizing the buffering mechanism in n-MAG are considered the fundamental steps performed in PFMIPv6 HO procedure, respectively. However, the HI can be false due to measuring the RSS value, which may be calculated based on false information in the presence of obstacles or even when the MN changes its movement direction.

According to [36] relatively seamless HO could be approached by using the location information of MNs. Results have shown that utilization of GPS information of each and every single MN while traveling from one PoA to another could provide better opportunities for MAGs to manage the HO procedure in advance. Generally, delivering location information, attained from GPS satellites, to higher level entities in routing hierarchy (e.g., APs, MAGs, etc.) could not only provide sufficient amount of time for them to exchange vital signaling in time but also the exact neighboring destination could be determined [37]. Hence, ping-pong effect on the HO procedure could be alleviated significantly. However, there will be considerable amount of signaling, message exchange, and energy consumption due to retrieving the location information periodically. This could also be decreased by increasing the interarrival time of location information retrieval, which leads

to sacrificing the precision of determination of the exact neighboring destination, along with experiencing a lesser seamless HO procedure.

Table I indicates the effectiveness of the aforementioned schemes in terms of HO latency and packet loss, along with the amount of time spent on performing duplicate address detection procedure, with a rating system from 1 to 5, where 1 indicates the trivial impact of performing particular scheme on either of HO latency and packet loss, and 5 indicates the other end of extreme.

IV. CONCLUSION

In a network-based mobility management scheme such as PMIPv6, the serving network handles the mobility management in a topologically localized domain on behalf of an MN. Although deployment of PMIPv6 protocol has reduced the total amount of HO latency, which consequently alleviates the packet loss amount, it still encounters some connection disruption when performing the HO procedure. Several PMIPv6-enhanced approaches and schemes have been proposed in order to eliminate the HO latency and, eventually, packet loss amount by using a buffering mechanism, altering additional messages, deployment of new entities, and changing the message signaling sequence. However, the proposed schemes and approaches could not be fully adopted by network administration societies due to either being cost effective, having a large amount of bandwidth consumption, or incurring a large amount of burden on network entities. Several proposed schemes have been surveyed in detail in this paper accompanied with their shortcomings. Considering the HO procedure in PMIPv6, utilization of GPS technology could be significantly beneficial in the reduction of packet loss as it provides the preconfiguration information needed by the MN in order to have a seamless HO in advance. Therefore, proposing a novel scheme in which the MN is equipped with a GPS device and performs the HO procedure but with the ability of consuming less energy and message signaling cost could be offered as a future investigation on PMIPv6 HO performance.

REFERENCES

[1] D. Johnson, C. Perkins, and J. Arkko, Mobility Support in IPv6, 2004, IETF RFC 3775. [Online]. Available: http://www.ietf.org/rfc/rfc3775.txt

[2] N. Banerjee, W. Wu, and S. K. Das, "Mobility support in wireless internet," *IEEE Wireless Commun.*, vol. 10, no. 5, pp. 54–61, Oct. 2003.

[3] J. Kempf, Problem Statement For Network-Based Localized Mobility Management (NETLMM), Apr. 2007, RFC 4830. [Online]. Available: http://www.ietf.org/rfc/rfc4830.txt

[4] H. N. AL-Hashimi, K. A. Bakar, and K. Z. Ghafoor, "Inter-domain proxy mobile IPv6 based vehicular network," *Netw. Protocols Algorithms*, vol. 2, no. 4, pp. 1–15, 2011.

[5] J. Guan, I. You, C. Xu, H. Zhou, and H. Zhang, "Survey on route optimization schemes for proxy mobile IPv6," in *Proc. 6th Int. Conf. IMIS*, Palermo, Italy, Jul. 4–6, 2012, pp. 541–546.

[6] G. Iapichino and C. Bonnet, "Host identity protocol and proxy mobile IPv6: A secure global and localized mobility management scheme for multihomed mobile nodes," in *Procl Global Telecommun. Conf.*, Honolulu, HI, USA, Nov. 30/Dec., 4, 2009, pp. 1–6.

[7] S. Gundavelli, K. Chowdhury, V. Devarapalli, B. Patil, and K. Leung, Proxy Mobile IPv6, 2008, IETF RFC 5213. [Online]. Available: http://tools.ietf.org/html/rfc5213

[8] J. C. Lee and D. Kaspar, "PMIPv6 fast handover for PMIPv6 based on 802.11 networks," Network Working Group 2007. [Online]. Available: http://tools.ietf.org/html/draft-lee-netlmm-fmip-00

[9] F. Xia and B. Sarikaya, Mobile Node Agnostic Fast Handovers for Proxy Mobile IPv6, 2007, Network Working Group. [Online]. Available: http://tools.ietf.org/html/draft-xia-netlmm-fmip-mnagno-02

[10] S. Park, Fast Localized Proxy Mobile IPv6 (FLPMIPv6), 2007, Network Working Group. [Online]. Available: http://tools.ietf.org/html/draft-park-netlmm-fastpmip-00

[11] A. Rossi, S. Pierre, and S. Krishnan, "Secure route optimization for MIPv6 using enhanced CGA and DNSSEC," *IEEE Syst. J.*, vol. 7, no. 3, pp. 351–362, Sep. 2013.

[12] M.-C. Chuang, J.-F. Lee, and M.-C. Chen, "SPAM: A secure password authentication mechanism for seamless handover in proxy mobile IPv6 networks," *IEEE Syst. J.*, vol. 7, no. 1, pp. 102–113, Mar. 2013.

[13] J.-H. Lee and T. Ernst, "Lightweight network mobility within PMIPv6 for transportation systems," *IEEE Syst. J.*, vol. 5, no. 3, pp. 352–361, Sep. 2011.

[14] M. Gohar, S. J. Koh, T. W. Um, and H. W. Lee, "Seamless multicast handover in PMIPv6-based wireless networks," in *Proc. 12th ICACT*, Phoenix Park, Ireland, Feb. 7–10, 2010, vol. 1, pp. 502–507.

[15] A. J. Jabir, S. K. Subramaniam, Z. Z. Ahmad, and N. A. W. A. Hamid, "A cluster based proxy mobile IPv6 for IP-WSNs," *EURASIP J.*, vol. 2012, p. 173, May 2012.

[16] J. Lee, "PMIPv6-based distributed mobility management," Dongguk University, DMM Working Group, Seoul, Koera, 2013.

[17] T. C. Schmidt, M. Waehlisch, and S. Krishnan, Base Deployment for Multicast Listener Support in Proxy Mobile IPv6 (PMIPv6) Domains, 2011, IETF RFC 6224. [Online]. Available: http://tools.ietf.org/html/rfc6224

[18] J. Tang, C. Pei, and B. Su, "Research on the localized routing mechanism for the PMIPv6," *J. Xidian Univ.*, vol. 39, no. 1, pp. 98–104, 2012.

[19] M. Waehlisch, Mobile Multicast Sender Support in PMIPv6 Domains draft-schmidt-multimob-pmipv6-source-00, 2011.

[20] H. B. Lee, Y. H. Han, and S. G. Min, "Network mobility support scheme on PMIPv6 networks," in *Int. J. Comput. Netw. Commun. (IJCNC)*, Sep. 2010, vol. 2, no. 5, pp. 206–213.

[21] Z. Jia, G. Wang, and R. Zhao, "A literature survey on handoff for mobile IPv6," *J. Netw.*, vol. 6, no. 8, pp. 1137–1144, Aug. 2011.

[22] R. Li, J. Li, K. Wu, Y. Xiao, and J. Xie, "An enhanced fast handover with low latency for mobile IPv6," *IEEE Trans. Wireless Commun.*, vol. 7, no. 1, pp. 334–342, Jan. 2008.

[23] I. Zhang, L. J. Zhang, and S. Pierre, "Performance analysis of seamless handover in mobile IPv6-based cellular networks," *Intech*, vol. 7, no. 1, pp. 1–26, 2011.

[24] M. H. Lin, W. E. Chen, and C. H. Huang, "HF-PMIPv6: An enhanced fast handovers for network-based mobility management," in *Proc. ICAIT*, Wuhan, China, Jul. 11–14, 2011, pp. 1–7.

[25] I. Al-Surmi, M. Othman, N. A. W. A. Hamid, and B. M. Ali, "Latency low handover mechanism considering data traffic lost preventing for proxy mobile IPv6 over WLAN," *Wireless Pers. Commun.*, vol. 70, no. 1, pp. 459–499, May 2012.

[26] S. Ryu and Y. Mun, "Scheme to prevent packet loss during PMIPv6 handover," *Proc. Trans. Comput. Sci. VI*, vol. 5730, p. 131, 2009.

[27] S. Lee, H. A. Latchman, and B. Park, "Efficient handover scheme of proxy mobile IPv6 in wireless local area networks," *Int. J. Multimedia Ubiquitous Eng.*, vol. 5, no. 2, pp. 1–18, 2010.

[28] M. S. Bargh, B. Hulsebosch, H. Eertink, G. Heijenk, J. Idserda, J. Laganier, A. R. Prasad, and A. Zugenmaier, "Reducing handover latency in future IP-based wireless networks: proxy mobile IPv6 with simultaneous bindings," in *Proc. Int. Symp. World Wireless, Mobile Multimedia Netw.*, Newport Beach, CA, USA, 2008, pp. 1–10.

[29] J. I. Kim and S. J. Koh, "Proxy Mobile IPv6 with partial bicasting for seamless handover in wireless networks," in *Proc. ICOIN*, Barcelona, Spain, Jan. 26–28, 2011, pp. 352–356.

[30] M. Gohar, S. I. Choi, and S. J. Koh, "Fast handover using multicast handover agents in PMIPv6-based wireless networks," in *Proc. ICOIN*, Barcelona, Spain, Jan. 26–28, 2011, pp. 367–372.

[31] *IEEE Standard for Local and Metropolitan Area Networks- Part 21: Media Independent Handover*, IEEE Std 802.21-2008, 2009, pp. c1-301.

[32] H. Y. Choi, K. R. Kim, H. B. Lee, S. G. Min, and Y. H. Han, "Smart buffering for seamless handover in proxy mobile IPv6," *Wireless Commun. Mobile Comput.*, vol. 11, no. 4, pp. 491–499, Apr. 2011.

[33] N. Y. Kwon, H. Kim, S. T. Oh, and H. Choo, "Fast handover scheme based on mobility management of head MAG in PMIPv6," in *Proc. ICCSA*, Santander, Spain, Jun. 20–23, 2011, pp. 181–192.

[34] M. S. Kim, S. K. Lee, D. Cypher, and N. Golmie, "Performance analysis of fast handover for proxy mobile IPv6," *Inf. Sci.*, vol. 219, pp. 208–224, Jan. 2012.

[35] H. Yokota, K. Chowdhury, R. Koodli, B. Patil, and F. Xia, Fast handovers for proxy mobile IPv6, 2010, IETF RFC 5949. [Online]. Available: http://tools.ietf.org/html/rfc5949

[36] A. Moravejosharieh and H. Modares, "A proxy mipv6 handover scheme for vehicular ad-hoc networks," *Wireless Pers. Commun.,* Springer U.S., pp. 1–181, Aug. 2013. [Online]. Available: http://link.springer.com/article/10.1007%2Fs11277-013-1381-8

[37] A. Moravejosharieh, R. Salleh, and H. Modares, "A novel approach for efficient resource consumption in GPS- Based mobile IPv6 wireless LAN," in *Proc. 3rd Int. Conf. Comput. Intell., Modell. Simul.*, Langkawi, Malaysia, Sep. 20–22, 2011, pp. 303–307, DOI: 10.1109/CIMSim.2011.61.

Hero Modares received the Master's degree from the University of Malaya, Kuala Lumpur, Malaysia. She is currently working toward the Ph.D. degree in Mobile IPv6 (MIPv6) security with the Faculty of Computer Science and Information Technology, University of Malaya.

During her Master's degree, she was a Research Assistant. She is currently an Assistant Researcher with the Department of Computer System and Technology, University of Malaya. Her research interests include computer and network security, cryptographic protocol, digital signature and nonrepudiation, mobile communications security (MIPv6), and public-key infrastructure.

Amirhosein Moravejosharieh received the Master's degree in computer science from the University of Malaya, Kuala Lumpur, Malaysia. He is currently working toward the Ph.D. degree in wireless networks from the University of Canterbury, Christchurch, New Zealand.

His research interests include analysis of wireless networks in terms of handover procedures, quality-of-service during handover procedures, and security issues related to handover procedures in Mobile IPv6 wireless networks.

Jaime Lloret (M'07–SM'10) received the M.Sc. degree in physics in 1997, the M.Sc. degree in electronic engineering in 2003, and the Ph.D. (Dr. Ing.) degree in telecommunication engineering in 2006, all from University of Valencia, Spain.

He worked as a Network Designer and an Administrator in several enterprises. He is currently an Associate Professor with the Polytechnic University of Valencia, Valencia, Spain. He is the Head of the Communications and Remote Sensing Group of the Integrated Management Coastal Research Institute, and of the "Active and collaborative techniques and use of technologic resources in the education (EITACURTE)" Innovation Group. He is the Director of the University Master "Digital Post Production." He led many national and international projects. He is currently the Chair of the Working Group for the Standard IEEE 1907.1. He is a Cisco-certified Network Professional Instructor. He is the author of 12 books and more than 220 research papers published in national and international conferences and international journals (more than 50 with ISI Thomson Impact Factor).

Dr. Lloret is a Fellow of the International Academy, Research, and Industry Association (IARIA). He is currently the Vice Chair of the Internet Technical Committee of the IEEE Communications Society and the Internet Society. He has been the General Chair (or Cochair) of 18 international conferences. He has been involved in more than 160 program committees of international conferences and in many organization and steering committees. He has been the Coeditor of 15 conference proceedings and a Guest Editor of several international books and journals. He is the Editor-in-Chief of *Networks Protocols and Algorithms*, the IARIA Journals Board Chair (for eight journals), and an Associate Editor of several international journals.

Rosli Bin Salleh received the B.Sc. degree in computer science from the University of Malaya, Kuala Lumpur, Malaysia, in 1994 and the M.Sc. and Ph.D. degrees from the University of Salford, Salford, U.K., in 1997 and 2001, respectively.

In 2001, he joined the Department of Computer System and Technology, Faculty of Computer Science and Information Technology, University of Malaya, as a Lecturer, and since 2007, he has been appointed as a Senior Lecturer. His research interests include handoff techniques and security in wireless networking.