International Journal on New Computer Architectures and Their Applications (IJNCAA) 1(3): 624-639
The Society of Digital Information and Wireless Communications, 2011 (ISSN: 2220-9085)

One-time key and Diameter Message Authentication Protocol for Proxy Mobile IPv6

Md. Mahedi Hassan and Poo Kuan Hoong
Multimedia University
63100 Cyberjaya, Malaysia
md.mahedi.hassan08@mmu.edu.my, khpoo@mmu.edu.my

ABSTRACT

The working group of NetLMM has proposed a new approach, known as network-based mobility management protocol that is actively standardized by Internet Engineering Task Force called Proxy Mobile IPv6 where many mobility signaling messages are performed by a network entity on behalf of a mobile host. Proxy Mobile IPv6 is an effective mobility management protocol for next generation wireless networks that are expected to enable network access ubiquity. Proxy Mobile IPv6 has salient features that attract a lot of attention among the telecommunication and Internet communities. However, Proxy Mobile IPv6 stills suffer from lengthy handover latency and packet loss when Mobile Host moves away to a new network with high speed mobility during the handover process. In order to improve the performance of Proxy Mobile IPv6, we proposed a solution scheme with integration of Media Independent Handover and neighbor discovery message of IPv6 to reduce handover latency and packet loss. But, this proposed protocol does not have methods to prevent security threats such as replay attack and key exposure when mobile host first enters into Proxy Mobile IPv6 domain and also during the handover process. In order to protect this proposed protocol, an authentication method based on the authentication protocol is presented in this paper that can prevent security threats. Also, this authentication method reduces authentication latency.

KEYWORDS

Proxy Mobile IPv6, Authentication Latency, Performance Analysis, Security

1 INTRODUCTION

Most of the wireless networks and the mobile cellular networks are quickly evolving towards all-IP networks. With the rapid expansion of the number of mobile and laptop users that are using the internet in wireless environment, the issue of IP mobility management technology is on the rise.

The Proxy Mobile IPv6 (PMIPv6) is designed to provide an effective network-based mobility management protocol for next generation wireless networks that supports a MH in a topologically domain [1] [2]. Therefore, PMIPv6 extends MIPv6 signaling messages and reuses the functionality of Home Agent (HA) to support mobility for MH without host involvement. It is a solution in the system architecture evolution (SAE) [3]. In the network, mobility entities are introduced to track the movement of MH, initiate mobility signaling on behalf of MH and setup the required routing state. The core functional entities in PMIPv6 are the Mobile Access Gateway (MAG) and Local Mobility Anchor (LMA). Typically, MAG runs on the access router (AR). The main role of the MAG is to perform the detection of the MH

movement and initiate mobility-related signaling with the MH's LMA on behalf of the MH. In addition, the MAG establishes a tunnel with the LMA for forwarding the data packets destined to MH and emulates the MH's home network on the access network for each MH. On the other hand, LMA is similar to the Home Agent (HA) in MIPv6. It is also the HA of a MH in a PMIPv6 domain. The main role of the LMA is to manage the location of a MH while it moves around within a PMIPv6 domain and it also includes a binding cache entry for each currently registered MH and allocates a Home Network Prefix (HNP) to a MH.

When the MH first enters in the PMIPv6 domain, it sends Router Solicitation (RS) message to MAG. When MAG in the access network receives the request from the MH, the access authentication and authorization procedures are performed using the MH's identity before providing PMIPv6 services. While access is authenticated or network attachment events are notified, the MAG obtains the MH profile which contains MH-Identifier and uses it to access the MH's policy server (e.g. authentication, authorization and accounting [AAA] server), supports address configuration mode and retrieves the address of the LMA that serves as the MH's HA. After successful access authentication, MAG configures a proxy care-of-address (PCoA) for the MH and sends a proxy binding update (PBU) message including the MH-Identifier to the MH's LMA on behalf of the MH. In return, the LMA updates its binding cache entry (BCE) for that MH and checks policy store to ensure that the sender is authorized to send the PBU message. If the sender is a trusted MAG, the LMA accepts the PBU message and replies with a Proxy Binding Acknowledgment (PBA) that contains the MH's home network prefix assigned by the LMA. Upon receiving the PBA, the MAG establishes a bidirectional tunnel between its proxy CoA (PCoA) and the LMA address. Then, the MAG periodically sends Router Advertisement (RA) messages to the MH on the access link advertising the MH's home network prefix as the hosted on-link prefix. In order to reduce the handover latency and packet loss, our proposed integration solution architecture of PMIPv6-MIH is shown in fig. 1 [4].

The key functionality is provided by Media Independent Handover (MIH) which is communication among the various wireless layers and the IP layer. The working group of IEEE 802.21 introduces a Media Independent Handover Function (MIHF) that is located in the protocol stack between the lower layer wireless access technologies and IP at upper layer. It also provides the services to the layer 3 and layer 2 through well defined Service Access Points (SAPs) [5].

Neighbor Discovery (ND) [4] enables the network discovery and selection process by sending network information to the neighbor MAG or new MAG (n-MAG) before handover that can help to eliminate the need for MAG to acquire the MH-profile from the policy server/AAA whenever a MH performs handover between two networks in micro mobility domain. It avoids the packet loss of on-the-fly packet which is routed between the LMA and previous MAG (p-MAG). This network information could include information about route discovery, parameter discovery, MH-profile which contains the MH-Identifier, MH home network prefix, LMA address (LMAA), MIH

handover messages etc., of nearby network links.

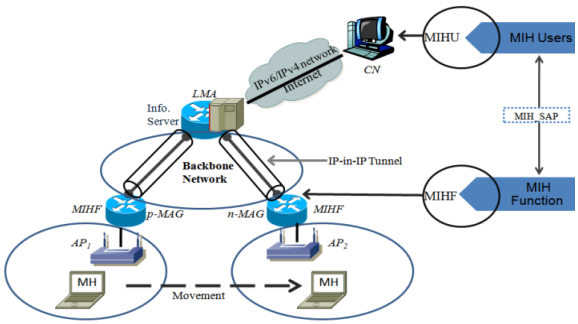

Fig. 1: Integration Solution Architecture of PMIPv6-MIH

The main objective of this paper is to propose a method to prevent security threats such as replay attack and key exposure, to authenticate the MH properly and also reduce the authentication latency. The rest of this paper is organized as follows: Section 2 presents some related works, while Section 3 introduces security threats to PMIPv6. Section 4 briefly explains proposed authentication method for PMIPv6-MIH. The analytical model and performance evaluation are described in Section 5 and Section 6 shows comparison and results of performance analysis of the proposed authentication method. Finally, Section 7 concludes the paper and provides future works.

2 RELATED WORKS

To establish, update and tear down routes for mobility signaling messages of a MH, PMIPv6 is executed on the interface between a MAG and an LMA. However, there are many security threats to PMIPv6 that includes man-in-the-middle attacks such as intercept, flaw, modify, or drop such traffic, or denial-of service attacks on high-profile web servers such as banks, credit card payment gateways, and even root name servers, or redirect it to destination in collusion with the attacker with compromise or impersonation of a legitimate MAG or a legitimate LMA [6]. A compromised MH can also attack the PMIPv6 system. Through inspection, attacker can access authentication data for MH and also spoofing attack can be done to MH's home network.

The current authentication problems on PMIPv6 can be summarized as follows:

• There is no way to authenticate the legality of a MH
• Compromise or impersonation of a legitimate MAG or a legitimate LMA
• Compromise or impersonation of a legitimate MH

In order to solve these problems, there are two commonly used authentication protocols implemented to secure authentication of MH such as One Time Password and One Time Key Generation. One Time Key Generation is one part of One Time Password (OTP) because it uses a time-synchronization type OTP function to generate a key. Using the key, MH can authenticate when MH first enters in a PMIPv6 domain. When MH moves from one network to the other within same domain, MH accesses the new network to use that key.

2.1 One Time Password

An attacker can easily capture or steal or attempt to crack traditional or static passwords. To overcome these problems the network working group developed One-Time Password (OTP) system that is valid for only one login session. Based on some specific values, OTP generates temporary password that can be used only once [7].

There are three approaches to generate password in OTP system. First approach: using a mathematical algorithm, OTP generates new password based on the previous password. Second approach: based on the time-synchronization, OTP also generates password between authentication server and the client. In this algorithm, password is valid for only short period of time. Third approach: the new password is based on a challenge chosen by authentication server or by client using a mathematical algorithm.
Capitalize the first letter of each word. Use a bold font.

2.2 One-time Key Generation

One-time key Generation protocol was proposed by Song et. al. [8][10]. The protocol introduced two terminologies local-LMA and home-LMA. This authentication protocol can generate One-time key with Timestamp, Device ID and Key and some special functions as shown in fig. 2.

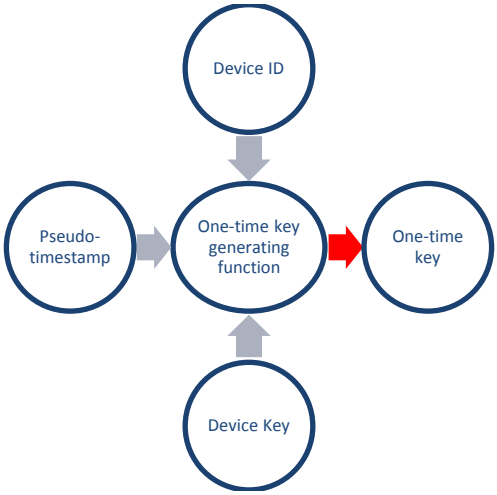

Fig.2: One-time Key Generation

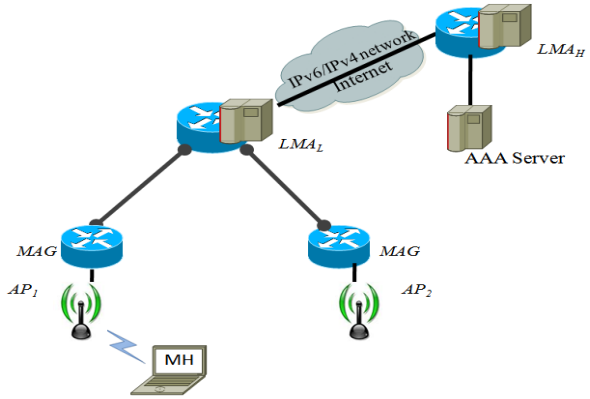

Fig.3: One-time Key Generation of PMIPv6

In fig. 3, delivering authentication message from MH to home-LMA (LMAH) will take an extra time because they used pseudo-Timestamp first and could not transmit Timestamp value with authentication request message for security reasons also there was a lack space for Timestamp in MH-Identifier. So, at the same time MH and home-LMA could not generate One-time Key. To overcome this problem, MH and home-LMA used pseudo-Timestamp that does not match the exact current timestamp. They could get pseudo-Timestamp from simple modulo operation.
Capitalize the first letter of each word. Use a bold font.

3 PROPOSED AUTHENTICATION METHOD for PMIPv6-MIH

The One-time Key authentication protocol does not have a method to prevent from replay attack and key exposure and it is also time consuming. In order to address the problems, we propose an alternative solution using One-time key Generation with Diameter message to prevent security threats like replay attack and key exposure [8]. The Diameter message was used to communicate with backend AAA/Policy server for applications such as network

access or IP mobility. Diameter message consists of a Diameter Header that is followed by a number of Diameter attribute value pairs (AVPs). This Diameter Header comprises binary data which is similar to an IP header [9]. AVPs contain AAA information elements and also routing, security and configuration information elements which are relevant to the particular Diameter request or answer message. Each AVP contains some AVP-specific data and an AVP header. Diameter message is also intended to work in both local and roaming AAA situations. We also introduced a terminology LMA/HA configuration of our proposed modified PMIPv6 to reduce the authentication time which is depicted in fig. 4.

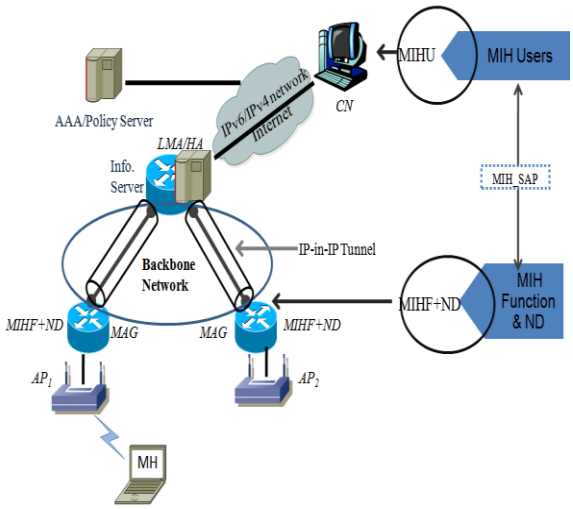

Fig.4: Proposed Authentication Protocol of PMIPv6-MIH

A MH is identified by its globally unique network access identifier (NAI). When a MH first enters into the PMIPv6 domain, the MH will initiate One-time key generation authentication procedure with the AAA server by sending Mobile Host-Identifier.

3.1 Mobile Host-Identifier (MH-Identifier)

According to the document of [8] [10], they specified definition of format for MH-Identifier using One-time key. In our proposed protocol, we introduce the same format for MH-Identifier using Diameter message. MH-Identifier with Diameter Message format is shown below in fig. 5:

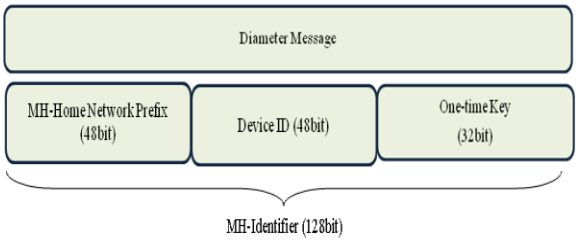

Fig. 5: MH-Identifier with Diameter Message

MH-HNP (48bit)
MH-HNP represents the home network prefix of MH. It also introduces a per-MH prefix model in which every MH is assigned a unique address. LMA/HA can find AAA/Policy server with this field. After finding the AAA/policy server, LMA/HA converts PBU message to Diameter Authentication Request message and sends it to AAA/Policy server.

Device ID (48bit)
This is typically a MAC address of interface or given special ID by service provider. This is used to distinguish each MH and for generating properly the next field named One-time Key field [10].

One-time Key (32bit)
One-time Key is the verification field for MH and generated code by the specific random function which installed both sides of MH and AAA/Policy server. They used a time-synchronized type OTP function. There are two approaches for generating this key. One of them is Device ID and the other is current timestamp. The OTP function must have

to regenerate One-time Key every few seconds, because sequence of setting up will be done in a few hundred milliseconds. This is one of the main features of this protocol. With this One-time Key, MH can authenticate in a simple one-way message from MH to AAA/Policy server and also prevent man-in-the-middle attack because of short time validity of the One-time key.

3.2 Interfacing between MH and MAG

MAG invokes the *MH_ATTACH* function on MAG when MH attaches to MAG that is mentioned in this document [3] and [11]. This function has sub-function that is called *MAG_GET_MH_ID*. With this sub-function, MAG can get MH- Identifier. During the MH attachment, MAG invokes *MIH_Link_up* function on MAG.

3.3 Interfacing MAG and LMA/HA

The authentication mechanism among the MAG, LMA/HA and AAA/policy server are based on shared-key security association for communicating securely each other because of some security threats that is described in [6]. As in theoretically, there are lots of MAG than LMAs and number of MAGs are expanding while deployment of PMIPv6 is ongoing. So, one PMIPv6 domain has one or several LMAs and one or several MAGs have one LMA. As mentioned earlier, One Time Key generation protocol has two terminologies that cannot prevent security threats like replay attack and key exposure and also it is time consuming. So, we introduced a terminology LMA/HA that means home-LMA and local-LMA are one LMA. On the other hand, LMA is also similar to the HA. LMA/HA are both under same operator's network with MAG that MH is attached and also under the home network of MH. The MAG and LMA/HA can have predefined shared key security association that both MAG and LMA/HA can communicate each other through the secure channel.

MAG builds up PBU message with the MH-Identifier mobility option for MH and sends it to LMA/HA when MH attaches to MAG. MAG sends RA message to MH with data from PBA if MAG receives positive reply from LMA/HA.

3.4 Interfacing LMA/HA and AAA/Policy Server

When LMA/HA receives PBU from MAG, LMA/HA extracts home network prefix (HNP) from the PBU message and sends Diameter Authentication Request Message to AAA/Policy Server. Using Public Key Infrastructure such as X.509 [12], LMA/HA can authenticate from AAA/Policy Server. The MH-AAA authentication mobility option is used to authenticate the PBU message between the MH and AAA/Policy Server. To verify the PMIPv6 protocol, the mobility message replay protection option is generated and these messages are not replayed by an attacker from some previous message. To compute a session key between MAG and LMA/HA, the key generation nonce request option in the PBU is constructed to request a nonce and that nonce can be stored into the key generation Nonce reply option of PBA. The IPv6 home address request option and the IPv6 assigned home address option are designed to request the HoA of MH.

3.5 Sequences of Authentication Protocol

The sequence of proposed PMIPv6 authentication protocol based on authentication method is shown in fig. 6:

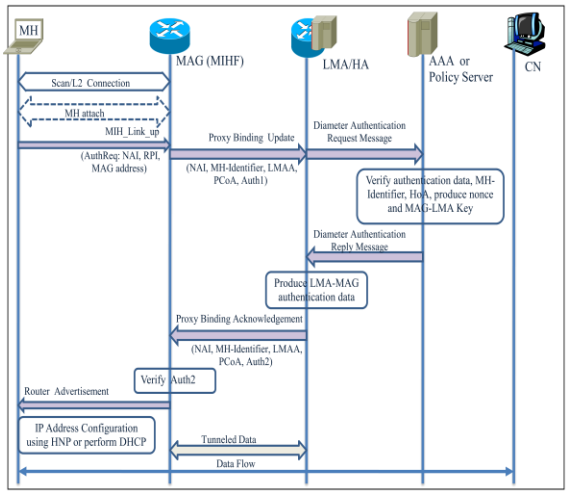

Fig. 6: PMIPv6-MIH Authentication Procedure

The sequences of proposed PMIPv6 authentication signaling are summarized as follows:

Step A:
MH_ATTACH has sub-function such as MAG_GET_MH_ID with that sub-function MAG can get MH-Identifier. When MAG receives MIH_Link_up trigger from link layer to IP layer in the MH, the MH sends an authentication request (AuthReq) message that contains NAI, identity of MAG and replay protection indicator (RPI) which are used for the AAA/Policy Server to identify the MH and to protect from replay attack. RPI is a timestamp or a random number. Then a key is computed between MAG and AAA/Policy server called MAG-AAA-KEY when MAG receives the AuthReq message. After authentication, the MAG-AAA-KEY is sent to the MAG. In addition, the MH sends RS message to the MAG to request its home of address (HoA). MAG acquires a PCoA in its PMIPv6 domain. The MAG builds up PBU message with the MH-Identifier mobility option for MH. An authentication data is computed using the MAG-AAA key and is put into the MH-Identifier mobility option of PBU.
Auth1 = (Hash-based Message Authentication Code-Secure Hash Algorithm1) HMAC-SHA1 (MAG-AAA-KEY, PCoA||LMAA|| PBU|| "MAG-AAA-PMIPv6") ..... (1), where HMAC-SHA1(K,m) [13] is a keyed hash function computed on message m with key K.
Therefore, the MAG sends this PBU to the LMA/HA;

Step B:
Upon receiving the PBU message to LMA/HA, it constructs a Diameter authentication Request message which includes many attribute value pairs (AVPs) as follows:
1. PMIPv6-Home-LMA-IPv6-Address
2. MH-Identifier
3. PMIPv6-MAG-Address
4. PMIPv6 Timestamp
5. PMIP Nonce=0
6. MIH Handover Indicator
7. Replay Protection Indicator
8. Access Technology Type

The LMA/HA transmits the Diameter PMIP authentication request message to the AAA server.

Step C:
Upon receiving the Diameter message to AAA/Policy server, it acquires the MH-Identifier and AVP also. It looks up the entire database which stored user identity to identify the requested MH. It also searches the database, if there is Device ID in the subscriber list or not. After that, the AAA generates MH-

ONE-TIME-KEY with Device ID and timestamp and verifies whether the timestamp is in the correct range to prevent replay attack. After checking the MH-Identifier data in AAA/Policy server, the AAA can authenticate the MH and verify that the PBU is correct. If all information is valid, then the AAA/Policy server generates a key generation nonce and computes a session key shared between LMA/HA and MAG.

PMIP-MAG-LMA-KEY=HMAC-SHA1 (MAG-AAA-KEY, PCOA||LMAA||MH-ONE-TIME-KEY||PMIP Nonce)…… (2)

The AAA will construct a Diameter authentication answer message which includes many AVPs as follows:

1. PMIPv6-Home-IPv6-HoA
2. PMIP-MAG-LMA-KEY
4. PMIP-MAG-LMA-KEY Lifetime
5. E (MAG-AAA-KEY, MH-ONE-TIME-KEY, PMIP Nonce)

The AAA replies the result to the LMA/HA with the diameter answer message. The key generation nonce is encrypted by the MAG-AAA-KEY.

Step D:

Upon receiving the diameter answer message to LMA/HA, LMA/HA computes the Mobility Message Authentication option of PBA.

Auth2=HMAC-SHA1 (PMIP-MAG-LMA-KEY, IPv6 HoA||PBA||"LMA-MAG-PMIPv6")….. (3)

The LMA sends this PBA message to MAG.

Step E:

The MAG receives this PBA message. The MAG extracts the PBA message and decrypts nonce and calculates PMIP-MAG-LMA-KEY. The MAG uses this key to verify the correctness of authentication data and avoid the possibility of exposure to other network entities. If it is valid, the MAG can authenticate the PBA.

The MAG sends Router advertisement message with encrypt MH-ONE-TIME-KEY including IPv6 HoA to the MH.

Step F:

The MH decrypts MH-ONE-TIME-KEY and authenticates and also configures IP address using received IPv6 HoA.

Handover Authentication Procedure

Fig. 7 & 8 illustrates the handover authentication architecture and procedure of proposed integration solution with PMIPv6-MIH.

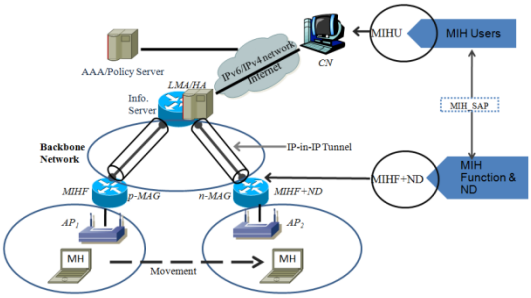

Fig. 7: Authentication Protocol of PMIPv6-MIH

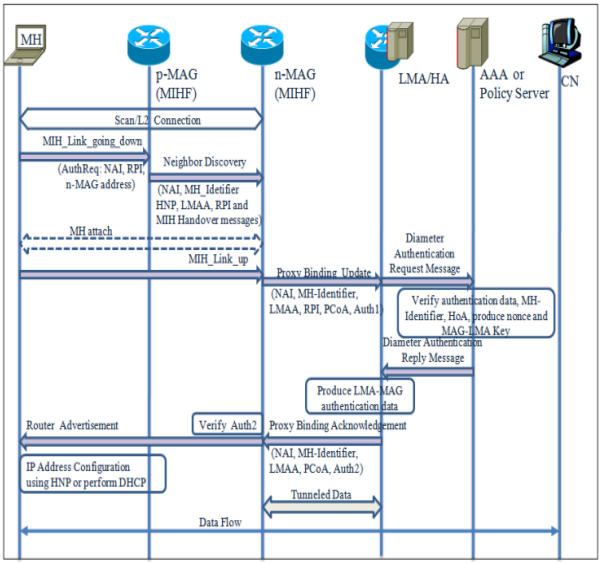

Fig. 8: Handover Authentication Procedure

From the above fig., when p-MAG receives MIH_Link_going_down (MIH_LGD) trigger from link layer to IP layer in the MH, the MH sends an AuthReq message that contains NAI, MH profile, RPI and n-MAG address. p-MAG sends this message to n-MAG using the Neighbor Discovery message of IPv6. This Neighbor Discovery message also contains MH -HNP, LMAA and MIH handover messages. This eliminates the need for the MAG to acquire the MH profile from AAA/Policy server whenever an MH performs a handover.

4 ANALYTICAL MODELS AND PERFORMANCE EVALUTION

The overall handover latency consists of the layer 2 (L_2) and layer 3 (L_3) operations. The handover latency is consequent on the processing time involved in each step of handover procedure on each layer. The handover latency ($L_{seamless}$) can be expressed as:

$$L_{seamless} = L_{L_3} + L_{L_2} \quad (1)$$

where L_{L_3} represents the network layer as example switching latency and L_{L_2} represents link layer as example switching time.
On L_3, the handover latency is affected by IP connectivity latency. The IP connectivity latency results from the time for movement detection (MD), configure new CoA (care-of-address), DAD (Duplicate Address Detection) and binding registration. Therefore, L_3 can be denoted as follows:

$$L_3 = T_{config} + T_{DAD} + T_{reg} + T_{move} \quad (2)$$

,where T_{move} represents the time required for the MH to receive beacons from the n-MAG, after disconnecting from the p-MAG. In order to estimate the movement detection delay, based on the assumptions of mobility management protocols that the time taken for MD are RS and RA messages as follows:

$$T_{move} = T_{RS} + T_{RA} \quad (3)$$

T_{config} represents the time taken for new CoA configuration. T_{reg} represents the time elapsed between the sending of the PBU from the MAG to the LMA/HA and the arrival/transmission of the first packet through the n-MAG. Binding registration is the sum of the round trip time between MAG and LMA/HA and the processing time as follows:

$$T_{reg} = T_{PBU} + T_{PBA} \quad (4)$$

T_{DAD} represents the time required to recognize the uniqueness of an IPv6 address. Once the MH discovers a new router and creates a new CoA it tries to find out if the particular address is unique. This process is called DAD and it is a significant part of the whole IPv6 process.

As simplification of (2), (3), (4) equations, it can be expressed as:

$$L_3 = T_{config} + T_{DAD} + T_{PBU} + T_{PBA} + T_{RS} + T_{RA} \quad (5)$$

On L_2, MH has to perform three operations during the IEEE 802.11 handover procedure such as scanning (T_{scan}), authentication (T_{AAA}) and re-association ($T_{re\text{-}ass}$). Handover latency at L_2 can be denoted as follows:

$$L_2 = T_{scan} + T_{AAA} + T_{re-ass} \quad (6)$$

T_{scan} represents the time taken by the MH to perform a channel scanning to find the potential APs (access point) to associate with. When MH detects link deterioration, it starts scanning on each channel finding the best channel based on the Received Signal Strength Indicator (RSSI) value.

T_{AAA} represents the time taken for authentication and depends on the type of authentication in use. The authentication time is round trip time between MH and AP.

$T_{re\text{-}ass}$ represents the time needed for re-association which consists of re-association request and reply message exchange between MH and AP if authentication operation is successful.

As a result, the equation (5) & (6) can be expressed as:

$$L_{seamless} = T_{config} + T_{DAD} + T_{BU} + T_{BA} + T_{RS} + T_{RA} + T_{scan} + T_{AAA} + T_{re-ass} \quad (7)$$

4.1 Analytical Model

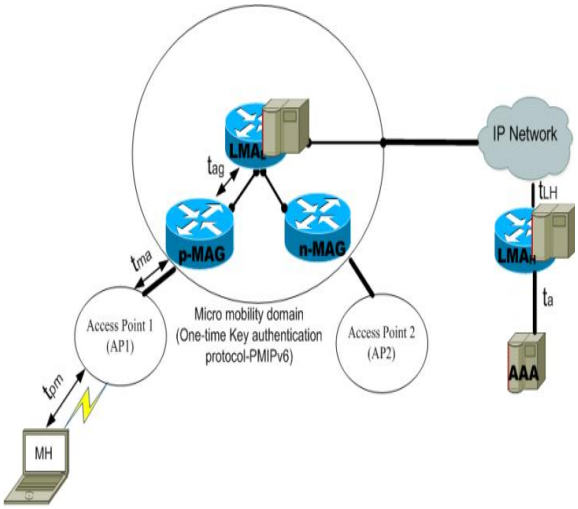

Fig. 9: An Analytical Model of One-time key Authentication Protocol for PMIPv6 (when MH first time enters into PMIPv6 domain)

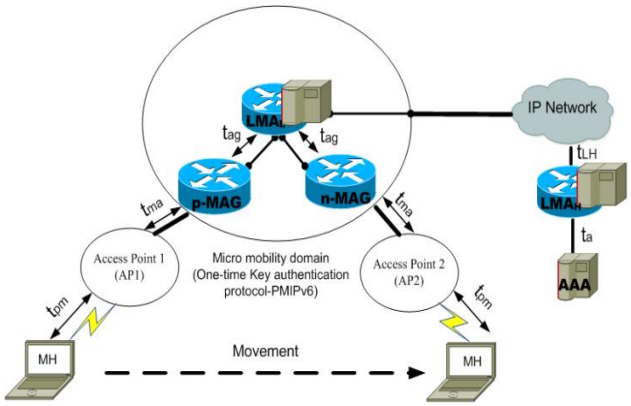

Fig. 10: An Analytical Model of One-time key Authentication Protocol for PMIPv6 (during the handover)

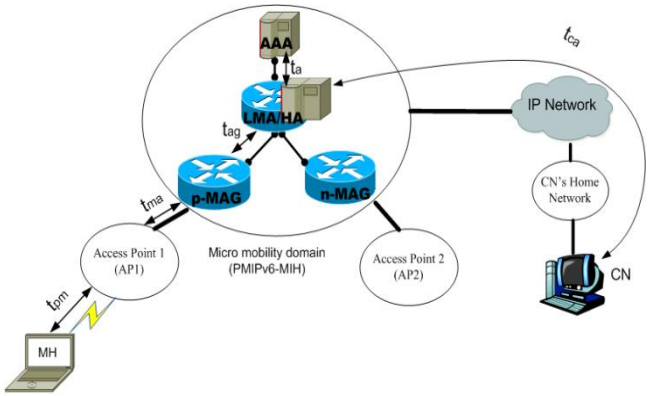

Fig. 11: An Analytical Model of Proposed Authentication Protocol for Integration solution of PMIPv6-MIH (when MH first time enters into PMIPv6-MIH domain)

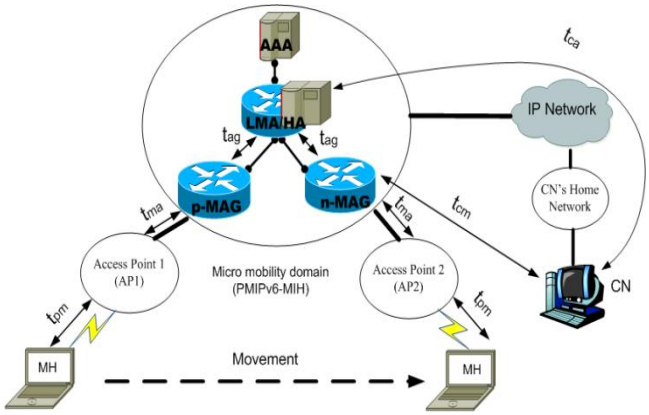

Fig. 12: An Analytical Model of Proposed Authentication Protocol for Integration solution of PMIPv6-MIH (during the handover)

The fig. 9, 10, 11 and 12 can be summarized as follows:

• The delay between the MH and AP is t_{pm}, which is the time required for a packet to be sent between the MH and AP through a wireless link.
• The delay between the AP and p-MAG or n-MAG is t_{ma}, which is the time between the AP and the n-MAG connected to the AP.
• The delay between the p-MAG or n-MAG and LMAL or LMA/HA is t_{ag}.
• The delay between the LMAL and LMAH is t_{LH}.
• The delay between the LMA/HA and CN is t_{ca}.
• The delay between the p-MAG or n-MAG and CN is t_{cm}, which is the time required for a packet to be sent between the p-MAG or n-MAG and the CN.
• The delay between the mobility agents and AAA is t_a.

Notably, from the fig. 9, 10, 11 and 12, the handover delay of PMIPv6 and integration solution of PMIPv6-MIH is due to many processes when MH first enters the specific domain. Therefore, it can be expressed that the handover delay of PMIPv6 and integration solution of PMIPv6-MIH in a micro mobility domain based on authentication protocol is as follows:

In PMIPv6 domain, registration delay can be expressed:

$$T_{PBU_L} = t_{ag}$$
$$T_{PBA_L} = t_{ag}$$
$$T_{PBU_H} = t_{LH}$$
$$T_{PBA_H} = t_{LH}$$

We can add the above equations,

$$T_{PBU} + T_{PBA} = 2t_{ag}$$
$$T_{PBU_H} + T_{PBA_H} = 2t_{LH}$$

In PMIPv6-MIH domain, registration delay can be expressed:

$$T_{PBU} = t_{ag}$$
$$T_{PBA} = t_{ag}$$

We can add the above equations,

$$T_{PBU} + T_{PBA} = 2t_{ag}$$

Movement Detection delay:

$$T_{RS} = t_{pm} + t_{ma}$$
$$T_{RA} = t_{ma} + t_{pm}$$
$$T_{RS} + T_{RA} = t_{pm} + t_{ma} + t_{ma} + t_{pm} = 2(t_{ma} + t_{pm})$$

One-time key Authentication delay:
When MH first enters into PMIPv6 domain, the authentication delay can be expressed as:

$$T_{AAA} = \text{query} + \text{reply} = t_a + t_a = 2t_a$$

But it can't prevent security threats from replay attack and key exposure and it is also time consuming.
Even, when MH moves inside the PMIPv6 domain, it stills need to acquire information from LMA_L and LMA_H that makes time-consuming.

Proposed Authentication delay:
When MH first enters into PMIPv6-MIH domain, the authentication delay with authentication method can be expressed as:
$T_{AAA} = \text{query} + \text{reply} = t_a + t_a = 2t_a$

When MH moves inside the PMIPv6-MIH domain, the authentication delay with authentication method can be expressed as:
$T_{AAA} = 0$, because n-MAG obtains all information about the MH-Identifier and network information through ND message before the actual handover process.

Attachment notification delay:
The attachment notification delay due to the packet from the AP that informs the

MAG of an MH's attachment denote T_{attach}

The handover Latency can be expressed when MH first enters into PMIPv6 and PMIPv6-MIH domain based on authentication protocol as:

$$L_{2_{PMIPv6}} = L_{2_{PMIPv6-MIH}} = T_{scan} + 2t_a + T_{re-ass} \quad (8)$$

$$L_{3_{PMIPv6}} = T_{attach} + T_{config} + T_{DAD} + T_{PBU_L} + T_{PBA_L} + T_{PBU_H} + T_{PBA_H} + T_{RS} + T_{RA} \quad (9)$$

$$L_{3_{PMIPv6}} = T_{attach} + T_{config} + T_{DAD} + 2t_{ag} + 2t_{LH} + 2(t_{ma} + t_{pm}) \quad (10)$$

$$L_{3_{PMIPv6-MIH}} = T_{attach} + T_{config} + T_{DAD} + T_{PBU} + T_{PBA} + T_{RS} + T_{RA} \quad (11)$$

$$L_{3_{PMIPv6-MIH}} = T_{attach} + T_{config} + T_{DAD} + 2t_{ag} + 2(t_{ma} + t_{pm}) \quad (12)$$

Seamless Handover Latency can be expressed as:

$$L_{seamless_{PMIPv6}} = T_{attach} + T_{config} + T_{DAD} + 2t_{ag} + 2t_{LH} + 2(t_{ma} + t_{pm}) + T_{scan} + 2t_a + T_{re-ass}$$

$$L_{seamless_{PMIPv6-MIH}} = T_{attach} + T_{config} + T_{DAD} + 2t_{ag} + 2(t_{ma} + t_{pm}) + T_{scan} + 2t_a + T_{re-ass}$$

Configuration and DAD delay:

PMIPv6 does not require T_{config} and T_{DAD} because MH is already in the PMIPv6 domain. Once the MH has entered and is roaming inside the PMIPv6 domain, T_{config} is not relevant since according to the PMIPv6 specification, the MH continues to use the same address configuration. A T_{DAD} is required for a link-local address since address collision is possible between MH, MAG and all MHs attached to the same MAG. The T_{DAD} may significantly increase handover delay and is a very time consuming procedure. Typically, T_{DAD} is around one second and sometimes can be much more than. Therefore, PMIPv6 introduces a per-MH prefix model in which every MH is assigned a unique HNP. This approach may guarantee address uniqueness. The new IP address configuration and the DAD operation for global address are appreciable only when the MH first enters in the PMIPv6 domain or move to new PMIPv6 domain.

Evidently, from the fig. 1, we proposed integration solution of PMIPv6-MIH to reduce handover latency as the time taken for scanning by informing the MH about the channel information of next APs and use Neighbor Discovery message of IPv6 to reduce handover delay and packet loss on network layer at n-MAG to avoid the on-the-fly packet loss during the handover process.

During the IEEE802.11 handover procedure the MH performs scanning on a certain number of channels to find the potential APs to associate with. By informing the MH about the channel information of next APs can significantly reduce the scanning time.

However, the scanning time also depends on the type of scanning that is used. There are two types of scanning defined: active and passive. In active scan mode, MH sends probe request and receives probe response if any AP is available on certain channel. In passive scan mode, each MH listens to the channel for possible beacon messages which are periodically generated by APs. The handover delay in active scan mode is usually less than in passive scan mode. The operation of passive scan mode depends on the period of beacon

generation interval. Therefore, this can provide better battery saving than active scan mode of operation.

As in L_2 trigger, the p-MAG has already authenticated the MH and sends the MH profile which contains MH-Identifier to the n-MAG through the Neighbor Discovery message since the MH is already in the PMIPv6 domain and receiving as well as sending information to CN before the handover. As in security issue, proposed integration solution of PMIPv6-MIH cannot prevent from replay attack and key exposure when MH first enters in the PMIPv6 domain and also during the handover process. Therefore, we proposed an alternative method using One-time key Generation with Diameter message that can prevent replay attack and key exposure when MH first enters a PMIPv6 domain and also moves to new network. During the handover, MH already authenticate from AAA/Policy server that information already send to n-MAG through Neighbor Discovery message since MH already is in PMIPv6 domain. But, n-MAG does not authenticate from AAA/Policy server that cannot prevent from replay attack and key exposure because of new MAG. That's why, to prevent the security threats from replay attack and key exposure, we introduced the One-time key generation with Diameter Message that can generate a key between n-MAG and AAA/Policy server when n-MAG receives the AuthReq message from p-MAG through the Neighbor Discovery Message based on fig. 5. With this proposed authentication method, lot of MAGs can authenticate and protect from replay attack and key exposure when MH moves. Hence, the authentication delay can be expressed as in L_2 handover:

Based on analytical model as in fig. 12,

$$L_{2_{PMIPv6-MIH}} = T_{scan} + T_{re-ass} \qquad (13)$$

Some parts of L_3 handover delay should be taken into consideration in PMIPv6. Since we proposed the integration solution of PMIPv6-MIH services, the number of handover operations should not be considered for overall handover latency. The time required to obtain MH profile information can be omitted since n-MAG performs this information retrieval prior to MH actual attachment. As the specification of PMIPv6, the time needed to obtain the DAD operation and configure new CoA can also be non-appreciable, since n-MAG performs a pre-DAD procedure like assigning a unique HNP during available resource negotiation with p-MAG and the MH continues to use the same address configuration. Eventually, RS message transmission time may not be appreciable because of the specification of PMIPv6. The time required to obtain mobility-related signaling message exchange during pre-registration may not be considered since this negotiation is established before MH attachment. Since the MH is already pre-registered and there is no need to confirm at the n-MAG, therefore the last PBA message sent from the LMA/HA may be considered as a RA message.

As a result, L_3 handover delay considers only two things in integration solution of PMIPv6-MIH in a micro mobility domain.

i. When MH attaches to the n-MAG and delivers event notification of MIH_Link_up indication, n-MAG sends a PBU message to the LMA/HA for updating the lifetime entry in the binding cache table of the

LMA/HA and triggering transmission of buffer data for the MH

ii. RA message

Therefore, the overall handover delay at L_3 can be expressed in PMIPv6 and PMIPv6-MIH domain during the MH handover as:

$$L_{3_{PMIPv6}} = T_{PBU_L} + T_{PBA_L} + T_{PBU_H} + T_{PBA_H} + T_{RA}$$

$$L_{3_{PMIPv6-MIH}} = T_{PBU} + T_{RA}$$

Based on Analytical model of PMIPv6 and PMIPv6-MIH:

$$L_{3_{PMIPv6}} = 2t_{ag} + 2t_{LH} + t_{pm} + t_{ma}$$

$$L_{3_{PMIPv6-MIH}} = t_{ag} + t_{pm} + t_{ma}$$

Based on authentication protocol, PMIPv6 and integration solution of PMIPv6-MIH can be expressed as in Seamless Handover Latency:

$$L_{seamless_{PMIPv6}} = L_{L_{3_{PMIPv6}}} + L_{L_{2_{PMIPv6}}}$$

$$L_{seamless_{PMIPv6}} = 2t_{ag} + 2t_{LH} + t_{pm} + t_{ma} + T_{scan} + T_{re-ass}$$

$$L_{seamless_{PMIPv6-MIH}} = L_{L_{3_{PMIPv6-MIH}}} + L_{L_{2_{PMIPv6-MIH}}}$$

$$L_{seamless_{PMIPv6-MIH}} = t_{ag} + t_{pm} + t_{ma} + T_{scan} + T_{re-ass}$$

5 SECURITY AND PERFORMANCE ANALYSIS

5.1 Key Exposure

MAG-AAA-KEY is a shared-key association between a MAG and an AAA/Policy server. AAA/Policy server generates a key generation nonce and computes a session key between LMA/HA and MAG called PMIP-LMA-MAG-KEY and also generates MH-ONE-TIME-KEY with Device ID and timestamp for authenticate MH legally. Thus, it is desirable not to leak these keys to the other network entities. The AAA/Policy server constructs a Diameter PMIP authentication replay message with encrypts (MAG-AAA-KEY, MH-ONE-TIME-KEY and PMIP nonce) and sends it to the LMA/HA and the MH respectively. The value of key generation nonce encrypted by MAG-AAA-KEY can be decrypted by the MAG and also calculates PMIP-MAG-LMA-KEY, while the other value encrypted by MH-ONE-TIME-KEY is decrypted by the MH. Therefore, MAG-AAA-KEY and MH-ONE-TIME-KEY are not exposed to other entities except the MAG and the MH.

5.2 Replay Attack

Replay attack involves the passive capture of data and its subsequent retransmission to produce an unauthorized effect. A malicious node keeps an AuthReq message to make a false report of normal node and then it can retransmit an old AuthReq message to trick the AAA/Policy server for false authentication. This replay attack can be prevented as follows: when MH scans or tries to connect to layer 2 connection, local challenge is created randomly that is a random number for authentication procedure and hence it always changes. Therefore, the malicious node cannot replay the old AuthReq message. When even the same local challenge can be selected by the MAG by chance, RPI can prevent the replaying attack.

5.3 Analysis

In PMIPv6 domain, One-time Key authentication protocol (OK-AP) can also be suitable for authenticating MH. But, this protocol cannot prevent from security threats and also increases authentication latency. In the figure below, Table I shows the comparative results between OK-AP and our proposed protocol OK-AP with Diameter message with some security factors. The Main purpose of our proposed protocol is to prevent security threats from replay attack and key exposure and reduce authentication latency.

	PMIPv6 Authentication Protocol	
	OK-AP	**OK-AP with Diameter Message**
Auth MH (at home)	YES	YES
Auth MH (at foreign)	YES	YES
Auth LMA/HA	YES	YES
Auth MAG	Possible	YES
One-way Auth	YES	YES
Combinable with BU	YES	YES
Replay Attack-proof	NO	YES
Key Exposure-proof	NO	YES

6 CONCLUSION

With the proposed authentication method, we can prevent security threats like replay attack and key exposure when MH first enters in the PMIPv6 domain and also during the handover process. We also conducted an analytical model and performance evaluation and performance analysis. For our future work, we will improve and implement our proposed authentication method in a network simulation environment and more detail security analysis and also better comparisons with other new authentication mechanisms in the PMIPv6 domain will be done.

6 REFERENCES

1. Kong, K., Lee, L., Han, Y., Shin, M., You, H.: Mobility Management for all-IP Mobile Networks: Mobile IPv6 vs. Proxy Mobile IPv6. In: Proc. the International Conference on Wireless Communications, pp. 36-45 (2008).
2. Lee, H., Han, Y., Min, S.: Network Mobility Support Scheme on PMIPv6 Networks. International Journal of Computer Networks & Communications (IJCNC), vol.2, no.5 (2010).
3. Gundavelli, Ed, S., Leung, K., Devarapalli, V., Chowdhury, K., Patil, B.: Proxy Mobile IPv6. RFC 5213, Cisco: IETF (2008).
4. Hassan, M. M., Hoong, P. K.: Handover Latency Reduction Using Integrated Solution Scheme for Proxy Mobile IPv6. In: Proc. The Third International Conference on Wireless & Mobile Networks, vol. 162, part 1, pp. 45 – 56 (2011).
5. Taniuchi, K., Ohba, Y., Fajardo, V.: IEEE 802.21: Media Independent Handover: Features, Applicability, and Realization. In: Proc. IEEE Communications Magazine, vol. 47, Issue: 1, pp. 112–120 (2009).
6. Vogt, C., Kempf, J.: Security Threats to Network-Based Localized Mobility Management (NETLMM). IETF RFC4832 (2007).
7. Haller, N., Mets, C., Nesser, P., Straw, M.: A One-Time Password System. IETF RFC2289 (1998).
8. Song, J., Han, S.: One-time Key Authentication Protocol for PMIPv6. In: Proc. International Conference on Convergence and hybrid Information Technology, vol. 2, pp. 1150-1153 (2008).
9. Korhonen, J., Bournelle, J., Muhanna, A., Chowdhury, K., Meyer, U.: Diameter Proxy Mobile IPv6: Mobile Access Gateway and Local Mobility Anchor to Diameter Server Interaction. draft-korhonendime-pmip6-03.txt, Siemens AG,Cisco Systems (2008).

10. Song, J., Han, S.: Mobile Node Authentication Protocol for Proxy Mobile. International Journal of Computer Science and Applications, vol.6, no.3, pp 10-19 (2009).
11. Laganier, J., Narayanan, S., McCann, P.: Interface between a Proxy MIPv6 Mobility Access Gateway and a Mobile Node. IETF netlmm WG Draft (2008).
12. Cooper, M., Dzambasow, Y., Hesse, P., Joseph, S., Nicholas, R.: Internet X.509 Public Key Infrastructure: Certification Path Building. IETF RFC4158 (2005)
13. Krawczyk, H., Bellare, M., Canetti, R.: HMAC: Keyed-Hashing for Message Authentication, RFC 2104 (1997).