A PMIPv6-based Secured Mobility Scheme for 6LoWPAN

Yue Qiu and Maode Ma, *Senior Member, IEEE*
School of Electrical and Electronic Engineering, Nanyang Technological University, 639798, Singapore
{qiuy0005, EMDMA}@ ntu.edu.sg

***Abstract*— In order to promote the development of the IoT, the Internet Engineering Task Force (IETF) has been developing a standard named Internet Protocol Version 6 (IPv6) over Low Power Wireless Personal Area Networks (6LoWPAN) to enable IP-based devices to connect to the Internet. Besides, to support mobility management, a network-based localized mobility management (NETLMM) protocol named Proxy Mobile IPv6 (PMIPv6) is proposed. Although the 6LoWPAN standard has specified the important issues, some security and mobility issues have not been addressed. In this paper, a secure PMIPv6-based mobility scheme is designed. The proposed scheme enables a 6LoWPAN device to efficiently and securely roam in the 6LoWPAN networks. The formal verification by the Automated Validation of Internet Security Protocols and Applications (AVISPA) and the simulation by JAVA show that the proposed scheme in 6LoWPAN could efficiently enhance the security functionalities to prevent various malicious attacks with less computational cost.**

Keywords— 6LoWPAN; authentication; handover; PMIPv6

I. INTRODUCTION

With the growing demand for a more convenient life, wireless and mobile communication technologies have been developed in the past two decades to enable people to access all kinds of network services over mobile devices, anytime, anywhere. The mobility of the users needs efficient mobility management to prevent the disconnection of the network. A host-based Mobile IPv6 (MIPv6) protocol has been proposed by the IETF for mobile nodes (MNs) to continuously access the network services while moving among foreign networks. As specified in [1], it is required that the MN needs to send signaling messages to its home agent to maintain the binding state between the MN's home address and the care-of address. However, MIPv6 cannot provide an efficient service for real-time applications. Subsequent work in [2-3] has introduced new host-based schemes to improve the performance of MIPv6.

To seamlessly connect heterogeneous wireless networks with each other and to the open Internet has become a hot research issue. In order to allow larger number of devices to interoperate with the Internet, the standard of 6LoWPAN has been developed by the IETF to connect low power personal area networks to the Internet. However, the signaling overhead of MIPv6 is quite high to the 6LoWPAN devices. Thus, a network-based localized mobility management protocol, called PMIPv6 [4], has been further proposed to support the mobility management without the involvement of the MN. Instead, the mobile access gateway (MAG), which the MNs are attached to, is responsible for performing signaling with the local mobility anchor (LMA) on behalf of the MNs so that PMIPv6 can significantly reduce the signaling overhead of the MNs and lower the handoff latency.

To enhance the handover performance, the fast handovers for PMIPv6 (FPMIPv6) protocol has been proposed in [5]. FPMIPv6 performs better in term of packet loss compared to PMIPv6. However, more resources and larger buffer size of MAGs are required. To reduce the handover latency, a fast and localized PMIPv6 (FLPMIPv6) has been proposed in [6]. Although FLPMIPv6 ensures that the packet loss can be minimized, a MN with Media Independent Handover Function is required. Moreover, the signaling overhead is much higher than that of the PMIPv6 and FPMIPv6. A last packet marker based fast handover scheme [7] has been proposed to deal with the out of order packets problem. Due to frequent movement of the MNs, a large number of signal exchanges between the MAGs and the LMA are required to update the binding entry. To overcome this, a chaining based PMIPv6 (CB-PMIPv6) scheme [8] has been proposed. However, it requires powerful MAGs to store the chained information of each MN when many MNs attached to the network. Although the above mentioned schemes have improved the efficiency during the handover, the security issues have not been addressed by these schemes. Thus, MNs may suffer from various malicious attacks when roaming in the network.

To address the security with the mobility management, several PMIPv6-based authentication schemes [9-11] have been proposed for vehicular networks. However, very few of the proposals target at the security functions of the resource constrained PMIPv6-based devices in 6LoWPAN networks. A secure fast handover mechanism for PMIPv6 networks has been proposed in [12] to lower the authentication delay and provide security functionality in the handover process. It suffers from replay attacks and impersonation attacks. A secure password authentication mechanism (SPAM) for secured seamless handover in PMIPv6 has been proposed in [13]. Though its computational overhead is low, SPAM has some security weaknesses. The nonce sent in the first message during the authentication procedure cannot be verified whether it is fresh or not. Besides, one group key has been shared by all the MAGs and some of the secret parameters assigned to each MN are the same. Thus, some confidential information could be easily extracted to disguise a lot of legal MNs.

In this paper, as our major contribution, a PMIPv6-based secured mobility scheme (PBSMS) is designed to enhance the security for 6LoWPAN networks. A hybrid cryptography

978-1-5090-1328-9/16/$31.00 ©2016 IEEE

method is employed to provide security supports for MNs roaming in the 6LoWPAN networks with the consideration of the resource constrained 6LoWPAN devices. In order to improve the security and efficiency of the handover process, a key chain is generated for secure communication between 6MNs and 6MAGs to avoid the authentication on MNs each time when they are roaming among 6MAGs while still keeping security. Formal verification and the simulation results prove that the proposed scheme could not only prevent many malicious attacks but also incur less computational overhead and handover latency.

The remainder of this paper is organized as follows. In section II, the system model is introduced. In section III, the proposed scheme is described in details. The security analysis of the proposed scheme by using AVISPA is presented in section IV. The evaluation of performance of the proposed scheme is demonstrated in section V. Finally, the paper is concluded in section VI.

II. System Background

A. System Architecture

The architecture of the 6LoWPAN networks under the study is shown in Fig. 1. The system consists of a number of 6LoWPAN MNs (6MNs), some 6LoWPAN MAGs (6MAGs), a LMA and a remote authentication, authorization, and accounting (AAA) server. The 6MNs can be treated as the hosts, which are mobile devices for gathering sensory information. The 6MNs can move among different domains in the networks. The 6MAGs, which work as proxies, are responsible for detecting the movements of the 6MNs attached to it and sending binding updates to the LMA on behalf of the 6MNs. The LMA, which acts as a home agent in PMIPv6, maintains the binding cache entries for the registered 6MNs and forwards data packets for the 6MN and the correspondent node. The LMA assigns the 6MN's home network prefix to the link between the 6MN and the 6MAG, from which the 6MN can configure its IP addresses. The AAA server is responsible for authenticating the 6MNs and storing the policy files which are sets of configuration information of the 6MNs.

It is assumed that the LMA and the AAA server are the backbone entities trustworthy. The 6MAGs are connected with the LMA through wired links with high bandwidth and low bit error rates. Thus, the 6MAGs and the LMA are mandatory to implement the Internet Protocol Security (IPsec) to protect the signaling messages. By the IPsec, the LMA can effectively authenticate the 6MAGs within its scope. The IPsec is a security protocol to provide secure end-to-end communications at the IP layer. Besides, the Internet Key Exchange Protocol version 2 (IKEv2) is implemented to help the 6MAGs, the LMA and the AAA server to establish security associations for pre-sharing the symmetric keys among them. Although the IPsec and IKEv2 are mandatory with IPv6, they may not be suitable for the 6MNs because these devices do not have enough capability to perform all of the functions.

B. Attack Model

The 6LoWPAN devices are usually deployed in unattended and accessible locations and more vulnerable to malicious attacks compare to traditional equipment which has enough

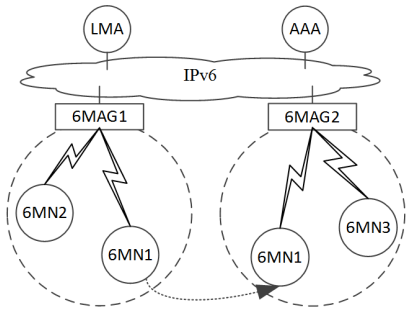

Fig. 1. System Architecture

resources. The threat model to PBSMS is based on the Dolev-Yao intruder model [14]. The attacker can eavesdrop on messages transmitted through the channel. Messages can be decrypted or encrypted if the attacker obtains the corresponding secret key. Besides, messages can be altered, constructed, decomposed, forged, injected or replayed and sent to any legitimate entity. Moreover, the attacker can impersonate a principal to communicate with the legal devices. However, it is assumed that an adversary is unable to guess a nonce which is chosen from a sufficiently large space. The attacker also cannot retrieve the information from a given ciphertext or generate a valid ciphertext from a given plaintext without a complete and correct key. A private key that matches a given public key cannot be calculated.

III. Proposed Scheme

A. Motivation

As pointed out in [15], though the SPAM scheme has some advantages to prevent packet loss, it has several fatal drawbacks. If an adversary eavesdrops on the link and obtains the authentication request message sent to a previous MAG (PMAG), the new MAG (NMAG) cannot distinguish whether the nonce is fresh or not. Since a group key is pre-shared among the MAGs and the LMA, the group key can be obtained by the adversary if any MAG is compromised. Therefore, a compromised MAG can assign the security parameters to a large number of MNs which may not exist. As a result, a lot of legal proxy binding update (PBU) messages are sent to the LMA resulting in a denial-of-service attack.

In order to overcome the shortcomings of the SPAM scheme, the PBSMS scheme is designed to provide a more secure and efficient handover procedure for 6LoWPAN networks. The 6MN and the LMA will generate a shared keychain for secure communication. Thus, the AAA server only needs to authenticate the 6MN in a certain period when the 6MN roams in the network to significantly reduce the handover delay. Besides, considering the resource constraints on 6MNs, only simple cryptographic operations are used to protect the transmitted messages. As for the 6MAGs, the LMA and the AAA server, since they are linked through wired links and have enough resources and capabilities, more complicated security schemes are used to support a more secure protection.

B. Details of the Proposed Scheme

The PBSMS is designed for secure mobility in 6LoWPAN networks, which consists of three phases: 1) pre-deployment phase, 2) authentication and key establishment phase and 3)

TABLE I. NOTATIONS

Notation	Description
ID_x	Identity of x
PW_x	Password of x
r	Nonce
Ti	Timestamp
s_x	Private key of x
Pub_x	Public key of x
SK_{x_y}	Session key established between x and y
kr	Registration key
H_1, H_2	One-way hash function.
$HMAC$	Hash-based message authentication code

handover phase. The notations used in the scheme are listed in Table 1. It is assumed that all of the 6LoWPAN devices have a unique 64-bit interface identifier or 16-bit short address and the links among the 6MAGs, the LMA and the AAA are connected using wired cable protected by the existing IPsec and IKEv2. Each legitimate device cannot leak the information to the third party. Besides, the backbone LMA and the authentication server are trustworthy.

1) Pre-deployment Phase: Before the deployment of a new 6LoWPAN node, a system parameter list *{p, q, a, b, P, n, h, G1, G2, e, H1, H2}* is published through the following steps:

- Choose two coefficients a and b specifying an elliptic curve E/F_p defined by the equation $y^2 = x^3 + ax + b \bmod p$ where p is a k-bit prime number.
- Choose a base point $P = (x,y)$ on $E(F_p)$ that generates the subgroup whose prime order is n and cofactor is h.
- Let G_1 is an addictive group and G_2 is a multiplicative group of order p, and choose an efficient and computable bilinear mapping algorithm [16] e: $G_1 \times G_1 \rightarrow G_2$.
- Let hash functions $H_1:\{0,1\}^* \rightarrow Z_q$ *and* $H_2:\{0,1\}^* \rightarrow G_1$ where q is a prime number.

After publishing the parameter list, a public/private key pair can be generated based on these parameters. For example, a secret number $s_i \in_R Z_q^*$ is selected to be the private key of a node i and Pub_i ($=s_iP$) is its public key.

By the PBSMS, prior to accessing the network services, each 6MN needs to perform the registration procedure with the AAA server through a secure channel. A unique identification ID and a password PW are chosen to be inputted to the tamper-resistant smart card of the 6MN for registration. The smart card calculates a pseudo ID, PID by using the equation $PID = H_1(ID||r)$ where r is a newly generated nonce. The 6MN first sends a registration request to the server with the real ID, PW, PID and the nonce r. After checking that the ID and PID have not been registered before, the server will send a signature $\sigma=s_{AAA}H_2(PID||ID_{AAA})$ and a key kr for registration in response to the request and store $<ID, PID, H_1(ID||PW||r), r, \sigma>$ in the database. Upon receiving the registration key and the signature, the 6MN stores $<ID, PW, PID, r, kr, \sigma>$ in its smart card. The registration steps are depicted in Fig. 2.

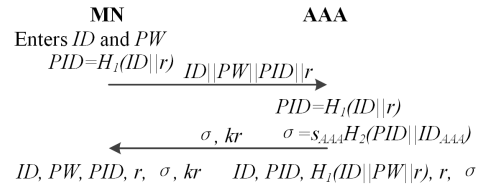

Fig. 2. Registration Phase

2) Authentication and Key Establishment Phase: In this phase, the 6MN, the 6MAG, the LMA and the AAA will exchange eight messages to achieve a mutual authentication as shown in Fig. 3. The details of the PBSMS process are described as follows.

When a 6MN first joins in a 6LoWPAN, it needs to enter the ID and the password for verification. After checking the legitimacy of the 6MN, it will send a router solicitation (RS) message to request a 6MAG to assign a network prefix for configuring the IPv6 address. The RS message includes the following information. Two random numbers x_0 and y_0 are chosen for the computation of the key chain. The key SK_{MN_AAA} is calculated by the function $SK_{MN\_AAA} = H_1(ID \oplus r||PID||T1)$. A message authentication code (MAC) will be calculated by the equation $MAC1 = HMAC(kr, NEW\ NODE||PID||T1||Msg)$. The 6MN sends $<NEW\ NODE||PID||T1||Msg||\ \sigma \oplus HMAC(kr, NEW\ NODE||PID||T1||\ Msg)>$ as message 1 to the nearest 6MAG where $Msg = E_{SKMN\_AAA}(x_0||y_0||PW||H_1(x_0||y_0))$. In order to reduce the time used in the authentication and key establishment phase, the key chain that will be used in handover process, is calculated in advance. The root values rt_1 and rt_2 are computed by the equation $rt_1 = H_1(PID||x_0)$ and $rt_2 = H_1(PID||y_0)$ respectively. A hash chain $rt_i, H_1(rt_i), \ldots, H_1^{\,m}(rt_i)$ is generated based on the root value rt_i, where $i = 1, 2$. Thus, the 6MN can produce the session key chain $key_n = H_1(H_1^{\,n}(rt_1)||H_1^{\,m-n+1}(rt_2))$ where $1 \le n \le m$.

The 6MAG, which receives the RS message from the 6MN, will check the validity of the timestamp by $|T1\text{-}T| < \Delta T$. If it is valid, the MAC value will be calculated using the received information by $HMAC(kr, NEW\ NODE||PID'||T1'||Msg')$ and the signature can be obtained by $\sigma' = \sigma \oplus HMAC(kr, NEW\ NODE||PID||T1||Msg) \oplus HMAC(kr, NEW\ NODE'||PID'||T1'||\ Msg')$ which can be further verified using bilinear pairing $e(\sigma', P) = e(H_2(PID'||ID_{AAA}), Pub_{AAA})$. If the equation is satisfied, the identity of the 6MAG and a new timestamp will be included in the message transmitted to the LMA. A new MAC will be calculated by the function $MAC2 = HMAC(SK_{MAG\_LMA}, PID||\ ID_{MAG}||\ T1||\ T2||\ Msg)$. The message $<PID, ID_{MAG}, T1, T2, Msg, \sigma \oplus MAC2>$ will be sent to the LMA as message 2.

After receiving the message 2, the LMA will verify it in the same way as the 6MAG. A new message $<PID, ID_{MAG}, ID_{LMA}, T1, T3, Msg, \sigma \oplus MAC3>$ will be sent to the AAA as message 3 where $MAC3 = HMAC(SK_{LMA\_AAA}, PID||\ ID_{MAG}||\ ID_{LMA}||\ T1||T3||\ Msg)$. Upon receiving message 3, the AAA will first check the validity of the message and verify the signature. If the 6MN has been registered before, the symmetric key is calculated by $SK_{MN\_AAA} = H_1(ID \oplus r||PID||T1)$ according to the stored data corresponding to the PID. The encrypted information Msg can be derived if the symmetric key is correct. The received PW can be verified using $H_1(ID||PW||r)$.

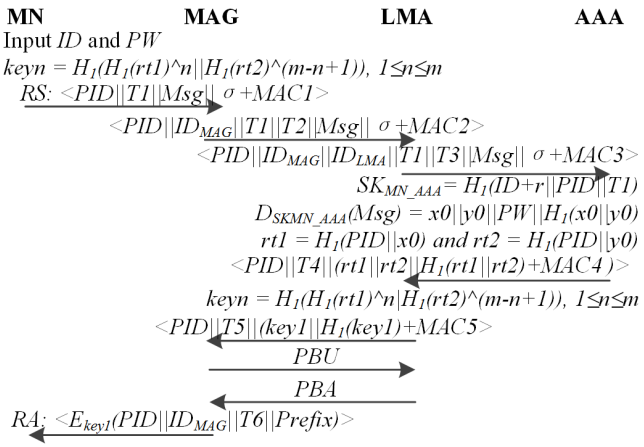

Fig. 4. Authentication Phase

Two root value rt_1 and rt_2 are calculated by the function $rt_1 = H_1(PID||x_0)$ and $rt_2 = H_1(PID||y_0)$ then sent to the LMA for session key establishment. The AAA sends message 4 as $<PID, T4, (rt_1||rt_2||H_1(rt_1||rt_2))\oplus MAC4>$ to inform the LMA that the 6MN is legitimate where $MAC4 = HMAC(SK_{LMA\_AAA}, PID||T4)$. If the 6MN has not been registered, a warning message will be sent to the LMA and the 6MAG to inform that the 6MN is an illegitimate device.

The LMA, which receives the message 4 from the AAA, will first check the validity of the timestamp (e.g. $|T4\text{-}T|<\Delta T$). Then, it will use the received information to compute the MAC value to extract the root key. The two root keys rt_1' and rt_2' can be derived by $(rt_1'||rt_2'||\ H_1(rt_1||rt_2))\oplus HMAC(SK_{LMA\_AAA}, PID||\ T4) \oplus HMAC(SK_{LMA\_AAA},\ PID'||T4')$. They are successfully obtained if $H_1(rt_1'||rt_2')=H_1(rt_1||rt_2)$. Then, the key chain is calculated $key_n = H_1(H_1{}^n(rt_1)||\ H_1{}^{m-n+1}(rt_2))$ with $1 \le n \le m$. After knowing the corresponding 6MN is legal, a new message $<PID||T5||(key_1||H_1(key_1))\oplus MAC5>$, where $MAC5$ is equal to $HMAC(SK_{MAG\_LMA}, PID||T5)$, will be sent as message 5 to the 6MAG to which the 6MN is attached.

When receiving the message 5, the 6MAG recovers key_1 from the received the data. After verifying key_1, the 6MAG will send a PBU request as message 6 to the LMA for binding. A proxy binding acknowledgement (PBA) will be sent back to this 6MAG as message 7 in which a unique network prefix is assigned to the 6MN by the LMA. The 6MAG will send a router advertisement (RA) in response to the RS. The encrypted message $<E_{key1}(PID||ID_{MAG}||T6|||Prefix|)>$ is included with the RA message sent to the 6MN.

The 6MN, which finally receives the RA message from the 6MAG, will derive the network prefix from the encrypted information by using the calculated session key. If the corresponding key is valid, the message can be obtained correctly. Thereafter, the 6MN and the 6MAG can communicate using the key key_1 in a valid session.

3) Handover Phase: Most existing schemes require that the authentication procedure is performed when each 6MN attaches to a new 6MAG resulting in a longer handover latency and heavy workload. The handover phase of the PBSMS scheme is depicted in Fig. 4.

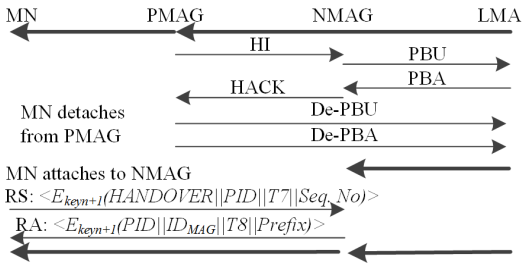

Fig. 3. Handover Phase

If a 6MN is going to leave the domain of the previous 6MAG (P6MAG), a handover initiate (HI) message is sent to a new 6MAG (N6MAG) predicted based on the direction of 6MN's movement. In addition, the PBU message is sent from the N6MAG to inform the LMA that the 6MN is going to roam in the domain of N6MAG. After checking the request, the LMA updates the binding cache entry for recording the N6MAG and sends the session $key_{(n+1)}$ in advance in response to the handover request. A bidirectional tunnel is built between the N6MAG and the LMA if the PBA message is valid. A handover acknowledgement (HACK) is sent to the P6MAG when N6MAG receives the PBA message and the session key from the LMA. Thus, a bidirectional tunnel is established between these two 6MAGs before the detachment of the 6MN.

When the 6MN detaches from the PMAG, a deregistration PBU message is sent to the LMA to inform that the MN has already left from its domain. Therefore, a marker message is added after the last data packet is sent to the PMAG. The undelivered messages are transmitted to the N6MAG and the N6MAG starts to buffer the data packets. A RS message, which includes the handover information $E_{keyn+1}(HANDOVER||PID||T7||Seq.\ No)$, is sent to the N6MAG if the 6MN enters its domain. If the handover information can be successfully decrypted from the RS message, the correct sequence number is retrieved. Then, a RA message is sent to the 6MN in which the same network prefix is included. Thus, the 6MN can communicate with the N6MAG using the key key_{n+1} to downloads the buffered data packets and successfully attaches to the N6MAG without changing its IP address.

IV. Security Analysis

In this section, the security of the PBSMS scheme is analyzed from two aspects. A formal verification is provided using AVISPA to verify the security functionalities. Moreover, a further analysis and explanation on the ability against various malicious attacks are provided.

A. Formal Verification

AVISPA is a formal verification tool which can automatically validate the network security protocols and applications. High Level Protocol Specification Language (HLPSL) is used to specify protocols and their security properties. Two back-ends, on-the-fly model checker (OFMC) and constraint logic based attack searcher (CL-Atse) are employed in the security analysis of the PBSMS scheme. The PBSMS scheme is modeled by HLPSL and is analyzed by the two above mentioned back-ends. It is assumed that the intruder of the PBSMS scheme initially has the identities and public keys of all the participants, its own private key, symmetric

```
SUMMARY
  SAFE
DETAILS
  BOUNDED_NUMBER_OF_SESSIONS
  TYPED_MODEL
PROTOCOL
  C:\progra~1\SPAN\testsuite\results\PBSMS.if
GOAL
  As Specified
BACKEND
  CL-AtSe
STATISTICS
  Analysed   : 5464 states
  Reachable  : 324 states
  Translation: 0.65 seconds
  Computation: 136.47 seconds
```

(a) Output Results using CL-Atse

```
% OFMC
% Version of 2006/02/13
SUMMARY
  SAFE
DETAILS
  BOUNDED_NUMBER_OF_SESSIONS
PROTOCOL
  C:\progra~1\SPAN\testsuite\results\PBSMS.if
GOAL
  as_specified
BACKEND
  OFMC
COMMENTS
STATISTICS
  parseTime: 0.00s
  searchTime: 30.15s
  visitedNodes: 5768 nodes
  depth: 9 plies
```

(b) Output Results using OFMC

Fig. 5. Output Results of AVISPA

keys shared with other entities, and other public functions. The outputs of the verification, as shown in Fig. 5, demonstrate that the PBSMS scheme is safe under various threat models. Therefore, the PBSMS scheme is proved to achieve a mutual authentication and goals as specified.

B. Ability against Malicious Attacks

1) Replay Attack: A reply attack is an action to send the previously obtained messages to a receiver to pretend a valid message sent from a legitimate device. By SPAM, although nonce can be used to prevent the replay attacks, the receiver cannot distinguish whether the nonce contained in the first authentication message is fresh or not. By the PBSMS scheme, if one of the transmitted messages is obtained by the attacker and resent to the receiver, such as $<PID||T5||(key_1||H_1(key_1)) \oplus MAC5>$. The receiver can compare the timestamp in the message with the receiving time. If the time difference is greater than a predefined threshold, the message will be considered as invalid to be ignored. Even if the attacker can alter or delete the timestamp in the message, the attack cannot success since the message is protected with a MAC value.

2) Man-in-the-middle (MITM) Attack: By a MITM attack, an adversary can eavesdrop, alter or delete the transmitted messages between two parties to make them believe that they directly communicate with each other. By SPAM, since a group key *PSK* is shared among the MAGs and the LMA, any MAG can derive the message encrypted by the PSK and re-encrypt. By the PBSMS scheme, since the MAC and signature have been employed for the protection, the MITM attacks can be prevented as well. For example, although a transmitted message $<PID, ID_{MAG}, T2, Msg, \sigma \oplus MAC2>$ can be obtained by the attacker, the signature value cannot be successfully obtained because the attacker does not have the session key. Besides, the attacker is unable to decrypt *Msg* to retrieve the secret value x_0 and y_0 without the session key SK_{6MN_AAA}.

TABLE II. COMPARISONS OF SECURITY PROPERTIES BETWEEN PBSMS AND SPAM

Properties	PBSMS	SPAM
Type of cryptosystem	Hybrid	Symmetric
Support for mobility	Yes	Yes
Against replay attack	Yes	No
Against MITM attack	Yes	No
Against impersonation attack	Yes	No
Against Sybil attack	Yes	No
Output result of AVISPA	SAFE	UNSAFE

3) Impersonation Attack: An impersonation attack can be launched by an adversary disguising as a legitimate party in the system. By SPAM, although the MN is registered with the AAA server beforehand, the AAA server is not involved in the authentication and handover phase. Thus, a dishonest MAG can impersonate a lot of MNs which may not exist. By the PBSMS scheme, since all of the devices have registered with the AAA server before the deployment, if an adversary impersonates a 6MN, the server will check its legitimacy by comparing the secret values included in the messages with the ones stored in its database. When a legitimate 6MN sleeps, an attacker may take its legal IP address to launch malicious attacks. However, it cannot succeed without knowing the session key key_n. Thus, the attacker cannot successfully impersonate a legal device without having the corresponding shared secrets such as the signature or the registration key.

4) Privileged Insider Attack: An insider attack is launched by a legal and authorized entity, who has a right to access the confidential information of its organization, to steal the security data or inject fraudulent data to the system. By SPAM, a dishonest MAG can retrieve the real ID of a MN and obtain every message sent from the MN. By the PBSMS scheme, since the real ID and the password is only known to the 6MN and the trusted server without leaking to other devices, the insider is not able to retrieve the information. Moreover, the root values used for generating the session key are protected by the symmetric key between the 6MN and the server. Therefore, the 6MN's information cannot be extracted by the insider of the network.

5) Sybil Attack: By a Sybil attack, an attacker can forge multiple identities to cheat the 6MAGs or the LMA that many legal devices are communicating with them leading to too much network resources consumed. SPAM is vulnerable to this kind of attacks. If the MAG is compromised or there is a dishonest MAG, the adversary can disguise as many MNs using secret parameters. Other devices cannot distinguish whether the MN is legal or not because the AAA server is not involved in the authentication and handover phase. The Sybil attacks can be prevented by the PBSMS scheme because a 6MN must be registered with the server before the deployment. Thus, the 6MNs with fake identities and security

TABLE III. COMPUTATIONAL TIME

Operations	Time (ms)
SHA-256	0.13
HMAC-SHA1	0.23
AES-CTR-256	1.04
Bilinear Pairing (ECC-160)	20

parameters cannot pass the authentication phase with the AAA server. Table 2 lists the comparison of security properties between PBSMS scheme and the SPAM scheme.

V. PERFORMANCE EVALUATION

In this section, the performance of the proposed PBSMS is compared with the SPAM scheme in term of computational overhead. The applied cryptographic algorithms employed in the comparison are SHA-256, HMAC-SHA1, AES-CTR-256, ECC-160 and bilinear pairing. Suppose that the length of the message is 256 bits, the time consumption of each cryptographic operation listed in Table 3 is analyzed by JAVA and conducted on Intel(R) Core(TM) i5-3317U CPU @ 1.70 GHz, 8 GB Ram, Windows 7.

Although SPAM uses simple hash functions and symmetric encryption which causes less time consumption, it has some security problems that need to be solved. To provide more secure functionalities to the 6LoWPAN network, the PBSMS employs more complicated algorithms for devices which have more capability to perform bilinear pairing. Thus, the total computational overhead in the authentication by the PBSMS is higher than that of the SPAM. When generating a key chain with *50* keys, the time consumption of authentication phase of SPAM and PBSMS are *13.69* ms and *138.32* ms, respectively. Although the time consumption is higher than SPAM due to employing the pairing method, the computational overhead of 6MNs by the SPAM and by the PBSMS are *3.65* ms and *2.57* ms, respectively. The more complicated calculations have been migrated to the components with more resources such as the 6MAGs, the LMA and the AAA server. Therefore, the resource constrained 6LoWPAN devices can achieve a better performance by the PBSMS scheme. A comparison of average computational overhead in the authentication and handover phase between PBSMS and SPAM is given in Fig. 6. With the increasing number of MAGs to which the MN has attached, the computational overhead of PBSMS is less than that of SPAM after 14 handovers.

VI. CONCLUSION

In this paper, the PBSMS scheme has been proposed to enhance the security functionality of the 6LoWPAN networks. A hybrid cryptographic method has been used to provide secure information exchanges among the 6MNs, the 6MAGs, the LMA and the AAA server. The proposed scheme enables a 6MN to efficiently and securely roam in the 6LoWPAN networks. The formal verification and security analysis have shown that the PBSMS scheme is safe with abilities to successfully prevent various malicious attacks. The performance evaluation of the PBSMS scheme demonstrates that the average overall overhead incurred in a handover can be reduced when the number of handovers supported by one

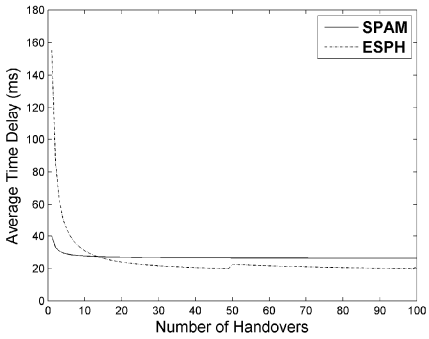

Fig. 6. Time Consumption of Authentication and Handover Phase

authentication gets larger, which can support more efficient handovers by the PBSMS scheme.

REFERENCES

[1] D. Johnson, C. Perkins, and J. Arkko, "Mobility Support in IPv6," IETF RFC 3775, 2004.

[2] R. Koodli, "Mobile IPv6 Fast Handovers," IETF RFC 5268, 2009.

[3] H. Soliman, C. Castelluccia, K. ElMalki, and L. Bellier, "Hierarchical Mobile IPv6 (HMIPv6) Mobility Management," IETF RFC 5380, 2008.

[4] S. Gundavelli, K. Leung, V. Devarapalli, K. Chowdhury, and B. Patil, "Proxy Mobile IPv6," IETF RFC 5213, 2008.

[5] H. Yokota, K. Chowdhury, R. Koodli, B. Patil, and F. Xia, "Fast Handovers for Proxy Mobile IPv6," IETF RFC 5949, 2010.

[6] S. Park, J. E. Lee, J. Choi, and Y. Kim, "Fast Localized Proxy Mobile IPv6 (FLPMIPv6)," IETF draft-park-netlmm-fastpmip-00, 2007.

[7] A. K. Quoc, D. S. Kim, and H. Choo, "A novel scheme for preventing Out-Of-Order Packets in fast handover for Proxy Mobile IPv6," Proceedings of 2014 International Conference on Information Networking (ICOIN), pp.422-427, Feb. 2014.

[8] A. Ahmad and D. Sasidharan, "Handover Efficiency Improvement in Proxy Mobile IPv6(PMIPv6) Networks," Proceedings of 2014 International Conference on Information and Communication Technologies (ICICT), vol. 46, pp.1064-1071, 2015.

[9] L. Y. Yeh, J. G. Chang, W. Huang and Y. L. Tsai, "A localized authentication and billing scheme for proxy mobile IPv6 in VANETs," Proceedings of 2012 IEEE International Conference on Communications (ICC), pp. 993-998, 2012.

[10] S. Céspedes, S. Taha and X. Shen, "A Multihop-Authenticated Proxy Mobile IP Scheme for Asymmetric VANETs," IEEE Transactions on Vehicular Technology, vol. 62, no. 7, pp. 3271-3286, Sept. 2013.

[11] L. Y. Yeh and Y. C. Lin, "A Proxy-Based Authentication and Billing Scheme With Incentive-Aware Multihop Forwarding for Vehicular Networks," IEEE Transactions on Intelligent Transportation Systems, vol. 15, no. 4, pp. 1607-1621, Aug. 2014.

[12] M. C. Chuang and J. F. Lee, "SF-PMIPv6: A secure fast handover mechanism for Proxy Mobile IPv6 networks," Journal of Systems and Software, Vol.86, Issue 2, pp.437-448, Feb. 2013.

[13] M. C. Chuang, J. F. Lee, M. C. Chen, "SPAM: A Secure Password Authentication Mechanism for Seamless Handover in Proxy Mobile IPv6 Networks," IEEE Systems Journal, vol.7, no.1, pp.102-113, Mar. 2013.

[14] D. Danny, and A. C. Yao. "On the security of public key protocols." IEEE Transactions on Information Theory, vol.29(2), pp.198-208, 1983.

[15] I. You, F. Leu, "Comments on "SPAM: A Secure Password Authentication Mechanism for Seamless Handover in Proxy Mobile IPv6 Networks," IEEE Systems Journal, vol.PP, no.99, pp.1-4.

[16] Q. Liu, G. Wang, J. Wu, "Secure and privacy preserving keyword searching for cloud storage services," Journal of Network and Computer Applications, vol 35, Issue 3, pp.927-933, May 2012.