EM^3A: Efficient Mutual Multi-hop Mobile Authentication Scheme for PMIP Networks

Sanaa Taha*, Sandra Céspedes*†, and Xuemin (Sherman) Shen*
*Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, Canada
†Department of Information and Communications Technology, Icesi University, Cali, Colombia
{staha,slcesped,xshen}@bbcr.uwaterloo.ca

***Abstract*—In this paper, we propose EM^3A, a novel scheme that guarantees the authenticity of a mobile node (MN) and a relay node (RN) in a multi-hop-enabled Proxy Mobile IP (PMIP) network. EM^3A works in conjunction with a proposed scheme for key establishment, based on symmetric polynomials, to generate a shared secret key between MN and RN. This scheme achieves lower revocation overhead than that achieved by existing symmetric polynomial-based schemes. For a PMIP domain with n points of attachment, EM^3A achieves $t \times 2^n-$secrecy, whereas the existing authentication schemes achieve only $t-$secrecy. Computation and communication overhead analysis, as well as simulation results, demonstrate that EM^3A achieves low authentication delay and is suitable for seamless multi-hop IP communications.**

I. Introduction

Mobile wireless networks are envisioned to support multi-hop communications, in which intermediate nodes help to relay packets between two peers in the network. Therefore, in infrastructure-connected multi-hop mobile networks, such as the one presented in Fig 1, the connection from the mobile node (MN) to the point of attachment may traverse multiple hops [1]. The reasons for relaying packets in infrastructure-connected mobile networks are twofold: 1) direct connection to the infrastructure may not always be available; and 2) relay nodes may obtain benefits, in the form of credits or rewards, from offering their services as temporary relays.

In order to support seamless communications, in our previous work, we have proposed an adaptation for Proxy Mobile IPv6 (PMIP) to provide IP mobility support in an infrastructure-connected multi-hop vehicular network [2]. In such multi-hop PMIP network, an MN uses a relay node (RN) for communicating with its Mobile Access Gateway (MAG) (i.e., the point of attachment to the infrastructure). The existing authentication schemes that can authenticate this MN to its MAG , use the RN to only forward the authentication credentials between MN and MAG. However, an extra mutual authentication, between MN and RN, is required to early prevent authentication attacks. Without that authentication, the mobile node may initiate a denial of service (DoS) attack toward the MAG, or the RN may initiate a fraud attack to mislead the MN. In mobile environments, DoS and fraud attacks can cause service disruptions and financial losses, due to resources exhaustion and high end-to-end delay [3]. However,

Accepted in IEEE ICC'12, to appear.

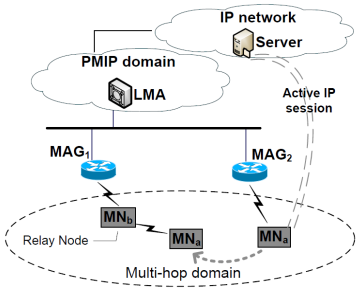


Fig. 1. Infrastructure-connected multi-hop mobile network. MN_a is roaming to a relayed communication through relay node MN_b

the difficulty of generating a security association between MN and RN, which are arbitrary nodes and have not met each other before, makes proposing a preserving authentication scheme a challenge. Moreover, if public-key authentication schemes are employed for this MN-RN authentication, they would require a large delay that can not be tolerated by seamless communications.

In this paper, we propose an efficient mutual authentication scheme for multi-hop-enabled PMIP networks, which thwarts different authentication attacks. In addition, we present a key establishment scheme based on symmetric polynomials [4],[5], which generates a shared secret key between MN and RN. Compared to existing authentication schemes, our proposed scheme achieves higher secrecy as well as lower computation and communication overheads. For a domain with n MAGs, our scheme achieves $t \times 2^n-$secrecy, whereas existing symmetric polynomial based authentication schemes achieve only $t-$secrecy. Extensive simulations are performed to demonstrate that our scheme can be applied for seamless communications since it results in low authentication delay. In addition, the proposed key establishment scheme achieves lower revocation overhead than that achieved by existing symmetric polynomial-based schemes.

The remainder of the paper is organized as follows. Section II reviews the related work. Section III describes our system model. The proposed scheme is introduced in Section IV. The security analysis and performance evaluation are presented in Sections V and VI, respectively. Finally, the conclusion and future work are presented in Section VII.

II. Related Work

Current authentication schemes employed in multi-hop networks have two different approaches: 1) to use an RN to only forward the authentication credentials between MN and the infrastructure; and 2) to apply hop-by-hop authentication. For

the first case, in [6], the MN uses its public key certificate to authenticate itself to the foreign gateway. On the other hand, the scheme in [7] uses both a symmetric key for authenticating an MN to its home network, and a public key schemes for mutual authentication between home network and foreign network. However, the expensive computation involved with public key operations tends to increases the end-to-end delay. A symmetric key-based authentication scheme for multi-hop Mobile IP is proposed in [8]. In that work, an MN authenticates itself to its home authentication server (HAAA), which derives a group of keys to be used by the MN. Despite its low computation and communication overheads, the symmetric key-based schemes cannot achieve strong levels of authentication.

For the second case, a mutual authentication scheme is proposed in [9], which depends on both secret splitting and self-certified schemes. However, they both are prone to DoS attack. Another scheme for hop-by-hop authentication called Alpha is presented in [10]. Alpha proposes that the MN signs its messages using a hash chain element as the key for signing, and then delays the key disclosure until receiving an acknowledgement from the intermediate node. Although it protects the network from insider attacks, Alpha suffers from a high end-to-end delay. A hybrid approach, the adaptive message authentication scheme (AMA), is proposed in [11]. It adapts the strength of the security checks depending on the security conditions of the network at the moment of packet forwarding.

III. System Model

A. Network and communication model

Consider an infrastructure-connected multi-hop mobile network such as that depicted in Fig. 1. The IP mobility support in MNs is provided by means of an adapted version of PMIP for multi-hop domains [2]. The only modification we introduce to [2] is the strict requirement for the MN to first connect directly to a MAG in order to obtain a valid IP prefix in the domain. After that, the MN may eventually divert to use an RN to reach the fixed network. We also assume that, after authenticating them, legitimate nodes in the PMIP domain faithfully follow the routing protocol when they are selected to provide their relay services for another MN in their surroundings.

The multi-hop communications that are studied in our system model are those occurring between MN and RN, when the MN intends to maintain a connection to the infrastructure.

B. Threat and Trust Models

We consider both internal and external adversaries. Internal adversaries are legitimate users who exploit their legitimacy to harm other users. Two types of internal adversaries are defined: impersonation and colluder. The former impersonates another MN's identity and sends neighbor discovery messages such as Router Solicitation through the RN. The latter colludes with other domain users in order to identify the shared secret key between two legitimate users.

External adversaries are unauthorized users who aim at identifying the secret key and breaking the authentication scheme. We consider replay, MITM, and DoS attacks as external adversaries. The goal of the MITM and replay attacks is to identify a shared key between two legitimate users, while the goal of DoS attack is to exhaust the system resources. In our model, we consider the PMIP entities (i.e., the local mobility anchor [LMA] and the MAGs) as trusted nodes.

C. Symmetric Polynomials

A symmetric polynomial is defined as any polynomial of two or more variables that achieves the interchangeability property, i.e., $f(x, y) = f(y, x)$. Symmetric polynomials are used by key establishment schemes to generate a shared secret key between two entities. A polynomial distributor (PD), such as the access router, securely generates a symmetric polynomial and evaluates this polynomial with each of its users' identities. For example, given two users identities 1 and 2, and the symmetric polynomial $f(x, y) = x^2y^2 + xy + 10$, the resultant evaluation functions are $f(1, y) = y^2+y+10$ and $f(2, y) = 4y^2 + 2y + 10$, respectively. The PD keeps the original polynomial secured and sends the evaluated polynomials to each user in a secure way. Afterwards, the two users can share a secret key between them by calculating the evaluation function for each other. Continuing with the previous example, user 1 evaluates its function, $f(1, y)$, for user 2 and obtains $f(1, 2) = 16$. In the same way, user 2 evaluates the function, $f(2, y)$, and obtains $f(2, 1) = 16$. Therefore, both users share a secret key, 16, without transmitting any additional messages to each other.

New decentralized key generation schemes are proposed in [4],[5] to generate a shared secret key between two arbitrary MNs that are located in two heterogeneous networks. These schemes achieve $t-$secrecy level, where t represents the degree of the generated polynomial. A scheme with $t-$secrecy property can be broken if $t + 1$ users collude to reveal the secret polynomial. Moreover, for only one MN's revocation, the decentralized schemes require to change the entire system's keys, which leads to a high communication overhead. Later in section VI, we show how EM^3A reduces the revocation overhead and increases the achieved secrecy level obtained by previous schemes.

IV. Efficient Mutual Multi-hop Mobile Authentication Scheme (EM^3A)

EM^3A consists of three main phases: key establishment phase for establishing and distributing keys, mobile node registration phase for MN's first attachment to the PMIP domain, and authentication phase for mutually authenticating the MN and RN.

A. Key Establishment Phase

Considering a unique identity for each MAG, the LMA maintains a list of those identities and distributes them to all legitimate users in the PMIP domain. The MAGs list's size depends on the number of MAGs in the domain. For n MAGs, each legitimate MN requires $(n \times \log n)$ bits to store this list. We argue that such storage space can be adequately found in mobile networks, such as vehicular networks. The LMA is also authorized to replace the identity of any MAG with another unique identity (this is specially useful for the management of MN's revocation, as it will be illustrated in section IV-D).

Each MAG in the domain generates a four-variables symmetric polynomial $f(w, x, y, z)$, which we call the network polynomial, and then sends this polynomial to the LMA in its domain. After collecting the network polynomials,

$f_i(w,x,y,z)$, from all MAGs, the LMA computes the domain polynomial, $F(w,x,y,z)$, as follows:

$$F(w,x,y,z) = \sum_{i=1}^{l} f_i(w,x,y,z), 2 \leq l \leq n \qquad (1)$$

where n is the number of MAGs in the domain. The LMA randomly chooses and sums l network-polynomials from the received n polynomials in order to construct the domain polynomial. The reason for not summing all the network polynomials is twofold: increasing the secrecy of the scheme from $t-$secrecy to $t \times 2^n-$secrecy, and decreasing the revocation overhead at the time of MN's revocation. After constructing the domain polynomial $F(w,x,y,z)$, the LMA evaluates it for each MAG's identity, ID_{MAG}, individually. The LMA then securely sends to each MAG its corresponding evaluated polynomial. Later on, those evaluated polynomials, $F(ID_{\text{MAG}_i},x,y,z)$, with $i = 1,2,....,n$, are used to generate shared secret keys among arbitrary nodes in the domain.

B. MN Registration Phase

When an MN firstly joins the PMIP domain, it authenticates itself to the MAG to which it is directly connected. This initial authentication may be done by any existing authentication schemes, such as RSA. After guaranteeing the MN's credentials, the MAG securely replies by evaluating its domain polynomial, $F(ID_{\text{MAG}},x,y,z)$, using the MN's identity, to obtain $F(ID_{\text{MAG}},ID_{\text{MN}},y,z)$. Afterwards, the LMA also sends the list of current MAGs's identities to the MN. The MN stores this list along with the identity of its first-attached MAG (ID_{FMAG}). As a result, a mobile node a can establish a shared secret key with another mobile node b in the same PMIP domain, by evaluating its received polynomial $F(ID_{\text{FMAG-}a},ID_a,y,z)$ to obtain $F(ID_{\text{FMAG-}a},ID_a,ID_{\text{FMAG-}b},ID_b)$. Similarly, b evaluates its received polynomial, $F(ID_{\text{FMAG-}b},ID_b,y,z)$, to obtain $F(ID_{\text{FMAG-}b},ID_b,ID_{\text{FMAG-}a},ID_a)$. Since the domain polynomial F is a symmetric polynomial, the two evaluated polynomials result in the same value and they represent the shared secret key between mobile nodes a and b, K_{a-b}.

C. Authentication Phase

When an MN roams to a relayed connection, the neighbor discovery messages for movement detection in the multi-hop-enabled PMIP scheme will go through an RN. The goal of the authentication phase is to support mutual authentication between the roaming MN and the RN. After a successful authentication phase, the RN ensures that the MN is a legitimate user, and the MN ensures that the RN is a legitimate relay. The following steps describe the MN-RN authentication phase (Fig. 2):

1) The MN broadcasts a Router Solicitation (RS) that includes its identity, ID_{MN} and its first attached MAG's identity, $ID_{\text{FMAG-MN}}$.

2) Upon receiving the RS, the RN checks its stored list of MAGs to see if $ID_{\text{FMAG-MN}}$ is currently a valid identity. If there is no identity equals to $ID_{\text{FMAG-MN}}$, the RN rejects the MN and assumes it is a revocated or malicious node. Otherwise, if $ID_{\text{FMAG-MN}}$ is a valid identity, the RN generates the shared key $K_{\text{MN-RN}}$ as described in the registration phase. The RN then constructs a challenge message, which includes its own identity, ID_{RN}, the MN's identity, a random number

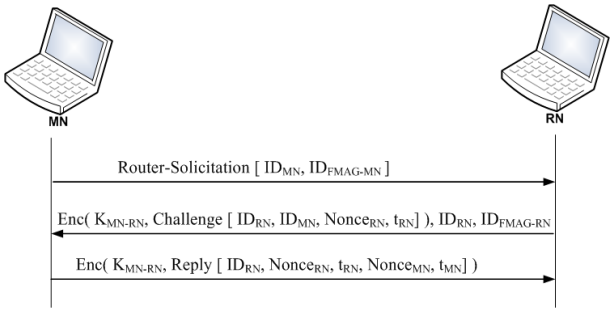


Fig. 2. EM^3A authentication phase.

$Nonce_{\text{RN}}$, and a time stamp t_{RN}. This information is encrypted in the challenge message using the shared key, $K_{\text{MN-RN}}$, and it is sent by the RN, along with ID_{RN} and its first attached MAG's identity, $ID_{\text{FMAG-RN}}$, to the MN.

3) After receiving the challenge message, the MN checks if $ID_{\text{FMAG-RN}}$ is a valid identity using its stored MAGs' identities list. The MN then reconstructs the shared key, by using the RN's identity and $ID_{\text{FMAG-RN}}$, and decrypts the received challenge message. The MN accepts the RN as a legitimate relay if the RN's decrypted identity is the same as the identity received with the challenge message, i.e., ID_{RN}.

4) The MN constructs a reply message, which includes RN's identity, $Nonce_{\text{RN}}$, t_{RN}, a new random number $Nonce_{\text{MN}}$, and a time stamp t_{MN}. The MN then encrypts the reply message using the shared key, and sends it to the RN, which accepts the MN as legitimate user if the decrypted $Nonce_{\text{RN}}$ equals to the original random number that the RN sent in the challenge message.

In Fig. 2, Enc(K, M) represents an encryption operation of a message M using a key K. In addition, the Router-Solicitation, Challenge, and Reply are the three messages transmitted between the MN and the RN.

D. Mobile Node Revocation

When an MN is revocated, the LMA replaces this MN's first-attached MAG's identity, $ID_{\text{FMAG-MN}}$, with another unique identity, ID_{NFMAG}, and sends the new one to all legitimate nodes in the domain. Subsequently, each legitimate node updates its stored list of MAGs. The LMA also sends a message to each MAG in the domain, which includes a list of the mobile nodes that have ID_{NFMAG} as their first-attached MAG's identity, along with an evaluated polynomial, $F(ID_{\text{NFMAG}},x,y,z)$ that uses the FMAG's new identity. Afterwards, the MAGs send the evaluated polynomial for those MNs that are in the received list and under MAGs' coverage areas. Eventually, each mobile node, in the MNs list, receives a new evaluated polynomial, $F(ID_{\text{NMAG}},ID_{\text{MN}},y,z)$, for both its identity and the new first-attached MAG's identity. Therefore, instead of changing the entire domain keys, only the MNs that share the same $ID_{\text{FMAG-MN}}$ need to change their evaluated polynomials and keys.

V. Security Analysis

A. Internal adversaries

Consider an impersonation attack, in which an adversary A aims at impersonating an MN, in order to join a new MAG throuhg an RN, an illegally benefit from the domain services. Then, for A to pass the authentication check, it

needs to decrypt the challenge message and identify the RN's random number, $Nonce_{\text{RN}}$, which is included in the encrypted challenge message. However, A cannot reconstruct the shared key by using only the identities of the MN and RN. In addition to the identities, the adversary needs to know one of the evaluated polynomials, $F(FMAG_{\text{MN}}, ID_{\text{MN}}, y, z)$ or $F(FMAG_{\text{RN}}, ID_{\text{RN}}, y, z)$. Since both polynomials are secret, it is impossible for an impersonation adversary to break EM^3A.

Moreover, EM^3A mitigates the collusion attacking impact by increasing the secrecy of the proposed key establishment scheme. Generally, a $t-$degree symmetric polynomial allows for a $t-$secrecy scheme, which means that $t+1$ colluders are needed to identify the secret polynomial and reconstruct the whole system's keys. However, in EM^3A, the domain polynomial is constructed as in (1), where the LMA randomly selects a group of the network polynomials to calculate the domain polynomial. Consider n MAGs in the domain and the secrecy of each network polynomial to be t, then the secrecy s of the domain polynomial is:

$$
\begin{aligned}
s &= \sum_{k=2}^{n} \binom{n}{k} \times t \\
s &= t \times \sum_{k=0}^{n} \binom{n}{k} - [\binom{n}{0} + \binom{n}{1}] \\
s &= t \times [2^n - (1+n)] \\
s &\simeq t \times 2^n
\end{aligned} \tag{2}
$$

Since the secrecy increases from t to $t \times 2^n$, the number of colluders that can break the scheme also increases from $t+1$ to $(t \times 2^n)+1$.

B. External Adversaries

A DoS attackers may trigger forged RS messages in order to exhaust the RN and MAG resources. However, using EM^3A, a DoS adversary A should know a valid shared key, $K_{\text{MN}_i\text{-RN}}$in order for the RN to forward the RS message. Since A is an external adversary, it cannot construct any key, even if it knows the identity of a legitimate MN. In addition, EM^3A thwarts replay attacks by adding both a time stamp and a random nonce for each transmitted message between the MN and the RN. Finally, A may trigger an MITM attack in order to impersonate an MN or an RN. However, given that both the challenge and replay messages are encrypted, A cannot replace the MN or RN identities. Once more, A should know the shared key first in order to perform such attack.

VI. Performance Evaluation

A. Computation and Communication Overheads

In this section, we evaluate the EM^3A scheme compared to previous multi-hop authentication schemes. Table I shows the comparisons in terms of computation and communication overheads. T represents the required time for an operation and B represents the transmitted bytes. Our scheme has the smallest computation overhead among other schemes, because EM^3A requires only two symmetric-key encryption operations ($2 \times T_c$). AMA [11] and GMSP [7] require time for signing and verifying signatures (T_s, T_v), hence their computation overheads are higher than that of EM^3A. The multi-hop MIP scheme [8], similar to EM^3A, requires small time computation; however, it requires high communication overhead to exchange a large number of keys. Moreover, ALPHA [10] requires an extra time ($T_{disclose}$) to delay the disclosure of the secret key.

TABLE I
Computation and Communication Overheads

Scheme	Comp. overhead	Comm. overhead
AMA [11]	$T_s + T_v \times Pr_{check}$	B_{cert}
GMSP [7]	$T_s + T_v + T_c$	B_{cert}
Multi-hop MIP [8]	$T_c + T_{EAP}$	$B_{EAP} + B_{key-exchange}$
ALPHA [10]	$T_c + T_{disclose}$	$B_{ACK} + B_{disclose}$
EM^3A	$2 \times T_c$	$B_{FMAGs-list}$

To illustrate and compare the cost of each scheme, in Fig. 3 we employ Crypto++ benchmark [1], and use AES and RSA 1024 (for symmetric and public key operations, respectively), in order to calculate the computation time required by the different schemes. The round trip time (RTT) considered between MN and RN is 5ms.

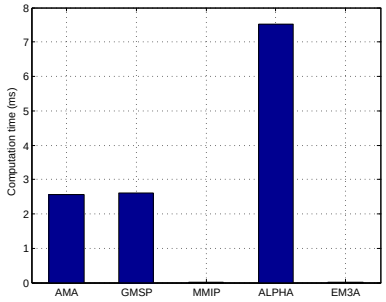


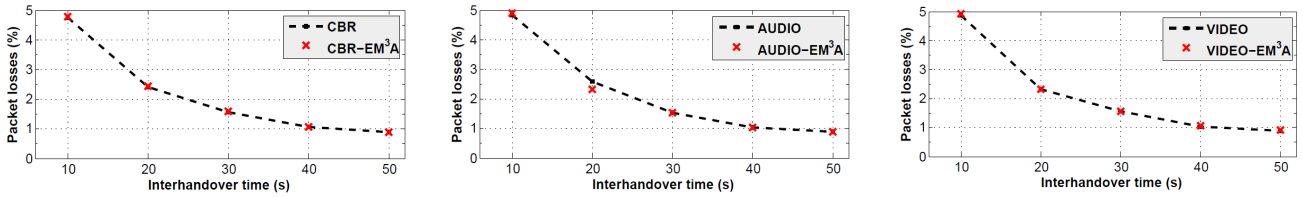
Fig. 3. Computation time for EM^3A and existing schemes.

B. Simulation results

We also evaluate the impact of EM^3A on the overall performance of the network when an MN experiences handovers that involve the use of RNs. Experiments were conducted through simulations using OMNET++ tool. The MN is moving at different speeds that cause the frequency of handovers to vary from one every 10s to one every 50s (i.e., highly dynamic and slow changing scenarios). In every handover, we consider the worst-case scenario in which every time the MN joins a new MAG, it first connects to an RN, so that EM^3A authentication is required before the exchange of neighbor discovery packets and PMIP signalling may happen. Other details of the simulation parameters are provided in Table II.

Fig. 5(a) shows the average throughput obtained, for the multi-hop-enabled PMIP, when the EM^3A scheme is deactivated and activated respectively. It can be seen that the achieved performance with activated EM^3A is almost equivalent to that achieved when no authentication has been activated. Thanks to the registration phase, which is executed when every node first joins the PMIP domain, at the moment of handover, EM^3A requires only one RTT between MN and RN before allowing for the continuation of normal handover signalling. The downside of such registration phase is the overhead and storage required for sending and maintaining the list of current identities for all the MAGs in the domain.

[1] http://www.cryptopp.com/benchmarks.html



(a) Packet losses for CBR traffic. (b) Packet losses for VBR audio traffic. (c) Packet losses for VBR video traffic.

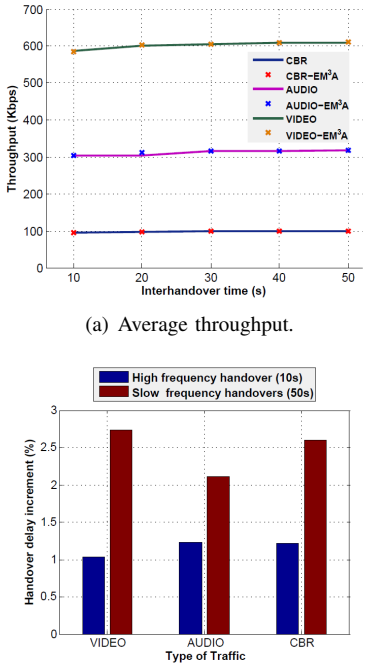
Fig. 4. Average packet losses obtained by EM^3A compared to non-secure multi-hop-enabled PMIP.

TABLE II
SIMULATION PARAMETERS

PHY Layer	2.4GHz, 5.5Mbps, 100mW Tx power, -110dBm sensitivity
MAC Layer	802.11 ad hoc mode, 150m radio range
Traffic type/rates	UDP / VBR video (mean 600Kbps), VBR audio (mean 320Kbps), CBR best effort 100Kbps
Session time	∼3min

To better illustrate the impact of EM^3A, we provide the details for the handover delay obtained during highly dynamic and slowly-changing scenarios, as shown in Fig. 5(b). When the EM^3A has been activated , the delay increases by $\sim$1.1% and $\sim$ 2.5% in each scenario. Consequently, the low computation overhead of the symmetric key encryption/decryption operations makes the authentication process a light-weight mechanism for securely using multi-hop communications in PMIP domains.

Fig. 4 shows the performance of the network in terms of packet losses for real time (audio and video) and best effort traffic. In general, the authentication scheme does not present a major impact compared with non-secure multi-hop PMIP. In the most demanding scenario, where handovers occur every 10s, a low 0.03% average increment among the three types of traffic results due to the delay caused by the processing of EM^3A traffic. In the case of medium-to-slow changing scenarios, packet losses remain as low as 1%, and EM^3A accounts only for a 0.01% increment.



(a) Average throughput.

(b) Handover delay increase.

Fig. 5. Comparison of performance between EM^3A and non-secure multi-hop-enabled PMIP.

VII. CONCLUSIONS AND FUTURE WORK

In this paper, an efficient mutual authentication scheme, EM^3A, has been proposed to be employed between a mobile node and a relay node in a multi-hop-enabled PMIP domain. EM^3A achieves higher secrecy level than that achieved by other symmetric polynomial authentication schemes, and lower computation and communication overheads than those achieved by multi-hop authentication schemes. Moreover, EM^3A thwarts internal and external authentication adversaries. We have demonstrated that EM^3A results in a low delay and allows for seamless communications even in highly mobile/highly traffic-demanding scenarios.

In the future, we will extend EM^3A to increase its secrecy level as well as adding anonymity and location privacy services to the mobile nodes.

REFERENCES

[1] S. Pack, X. Shen, J. Mark, and J. Pan, "Mobility management in mobile hotspots with heterogeneous multihop wireless links," *Communications Magazine, IEEE*, vol. 45, no. 9, pp. 106 –112, september 2007.

[2] M. Asefi, S. Cespedes, X. Shen, and J. W. Mark, "A Seamless Quality-Driven Multi-Hop Data Delivery Scheme for Video Streaming in Urban VANET Scenarios," in *Proc. of IEEE ICC 2011*, pp. 1–5.

[3] C. Guo, H. J. Wang, and W. Zhu, " Smart-Phone Attacks and Defenses," 2007.

[4] A. Gupta, A. Mukherjee, B. Xie, and D. P. Agrawal, "Decentralized Key Generation Scheme for Cellular-based Heterogeneous Wireless Ad hoc Networks," *J. Parallel Distrib. Comput.*, vol. 67, pp. 981–991, 2007.

[5] K. Pillai and M. Sebastain, "A Hierarchical and Decentralized Key Establishment Scheme for End-to-End Security in Heterogeneous Networks," in *Proc. of IEEE IMSAA 2009*, pp. 1 –6.

[6] C. Tang and D. Wu, "An Efficient Mobile Authentication Scheme for Wireless Networks," *IEEE Trans. Wireless Commun.*, vol. 7, no. 4, pp. 1408 –1416, 2008.

[7] B. Xie, A. Srinivasan, and D. Agrawal, "GMSP: A Generalized Multi-hop Security Protocol for Heterogeneous Multi-hop Wireless Network," in *Proc. of IEEE WCNC 2006*, vol. 2, pp. 634 –639.

[8] A. Al Shidhani and V. C. M. Leung, "Secure and Efficient Multi-Hop Mobile IP Registration Scheme for MANET-Internet Integrated Architecture," in *Proc. of IEEE WCNC 2010*, pp. 1 –6.

[9] Y. Jiang, C. Lin, X. Shen, and M. Shi, "Mutual Authentication and Key Exchange Protocols for Roaming Services in Wireless Mobile Networks," *IEEE Trans. Wireless Commun.*, vol. 5, no. 9, pp. 2569 – 2577, 2006.

[10] T. Heer, S. Götz, O. G. Morchon, and K. Wehrle, "Alpha: an adaptive and lightweight protocol for hop-by-hop authentication," in *Proc. of ACM CoNEXT '08*, pp. 23:1–23:12.

[11] N. Ristanovic, P. Papadimitratos, G. Theodorakopoulos, J.-P. Hubaux, and J.-Y. Le Boudec, "Adaptive Message Authentication for Multi-hop Networks," in *Proc. of Eighth International Conference on Wireless On-Demand Network Systems and Services (WONS) 2011*, pp. 96 –103.