# CLAM: Cross-layer Localized Authentication Mechanism based on Proxy MIPv6 and SIP in Next Generation Networks

Muhammad Zubair[1], Xiangwei Kong[1], and Saeed Mahfooz[2]
[1]School of Information and Communication Engineering, Dalian University of Technology, China
[2]Department of Computer Science, University of Peshawar, Pakistan
Email: m.zubairpaf@gmail.com; kongxw@dlut.edu.cn; saeedmahfooz@upesh.edu.pk

***Abstract***—In this paper we propose a novel Cross-layer Localized Authentication Mechanism (CLAM) to secure mobility in Next Generation Networks. The proposed mechanism integrates Proxy MIPv6 and Session Initiation Protocol (SIP) to handle the authentication locally in real-time and non-real-time communications. The design objectives of CLAM are three fold: i) handover latency is minimized by the local management of authentication; ii) simple to implement in mobile devices because of symmetric cryptographic and one-way hash operations; iii) possesses important security properties such as resistance against various attacks, user anonymity, mutual authentication, user friendly, one-time session key agreement, backward secrecy, forward secrecy, and confidentiality. We analyze and compare the performance of CLAM with existing schemes in terms of handover latency, signaling cost, communication overhead, computational cost, and packet loss. The numerical and simulation results demonstrate that our proposed scheme outperforms the existing schemes.

***Index Terms***—Local authentication, mobility, next generation networks, Proxy Mobile IPv6 (PMIPv6), session initiation protocol

## I. Introduction

Next Generation Networks (NGNs) allow seamless and secure roaming of mobile devices or user equipments across wireless networks through heterogeneous access technologies such as Global System for Mobile Communications (GSM), Wireless Local Area Network (WLAN), Worldwide Interoperability for Microwave Access (WiMAX), Long-Term Evolution(LTE), Code Division Multiple Access (CDMA), and so on [1]. In order to offer continuous real-time and non-real-time IP services in mobile environment, Mobile Internet protocol (MIP) [2] and Session Initiation Protocol (SIP) [3] have been proposed by Internet Engineering Task Force (IETF). Particularly, MIP is considered as an efficient network layer mobility protocol, whereas SIP is more effective operating at the application layer for real-time applications and session mobility [4].

MIP has an update MIPv6 for NGNs, which has various primary extensions such as Fast MIPv6 [5], Hierarchical MIPv6 [6], and Proxy MIPv6 [7], [8]. These are used to handle seamless network layer mobility. In [9]-[12], the performance of these different enhancements of MIPv6 is compared. The results demonstrate that PMIPv6 is the most efficient one to manage network based mobility. Although PMIPv6 is effective at network layer mobility, but difficult to fill the mobility related functions in real-time communication operating at the application layer. Therefore, mobility and security support for real-time communication in NGNs, SIP is the leading candidate. Operating in application layer, SIP excels due to its flexible deployment, low-cost investment and lightweight processing. In addition, SIP has the providence of advanced mobility traits like renegotiation of session for real-time communication. Hence, considering the important visions of NGNs, mobility and security support for both real-time and non-real-time communications at network and application layers are desired in combined fashion.

In this paper, we propose a novel integrated solution based on PMIPv6 and SIP called Cross-layer Localized Authentication Mechanism (CLAM). Our solution combines the best features of both protocol, and incorporates a new authentication mechanism to secure both real-time and non-real-time communications. Notably, the redundancy problem due to separate registration with both protocols is also resolved in our proposed scheme. The main contributions of this paper are listed as follows:

- CLAM offers integrated local authentication to reduce the handover latency.
- CLAM proposes the solution for packet loss and handover latency problems associated with PMIPv6 and SIP during handover.
- CLAM possesses number of advantages: Firstly, it is simple to implement for all partakers because of simple symmetric cryptographic and one-way hash operations. Secondly, only one round is required for the messages exchange between mobile node (MN), mobile access gateway (MAG), local mobility anchor

Manuscript received October 3, 2013; revised February 5, 2014.
Corresponding author email: m.zubairpaf@gmail.com
doi: 10.12720 /jcm.9.2.144-156

(LMA), and home agent (HA). Thirdly, it has important security characteristics such as strong protection against different attacks, user anonymity, mutual authentication, user friendly, one-time session key agreement, confidentiality, forward secrecy, and backward secrecy.

The rest of the paper is organized as follows. The network architecture and the related work are described in section II and III respectively. Our proposed mechanism is presented in section IV. In section V, the analysis which includes security analysis and performance analysis are presented. And finally, we conclude the paper in section VI.

## II. Network Architecture

In this section the architecture for the proposed solution is presented as shown in Fig. 1. Proxy MIPv6 is integrated with Session Initiation protocol, to perform network based localized authentication. The authentication of both network layer mobility and session mobility is focused.

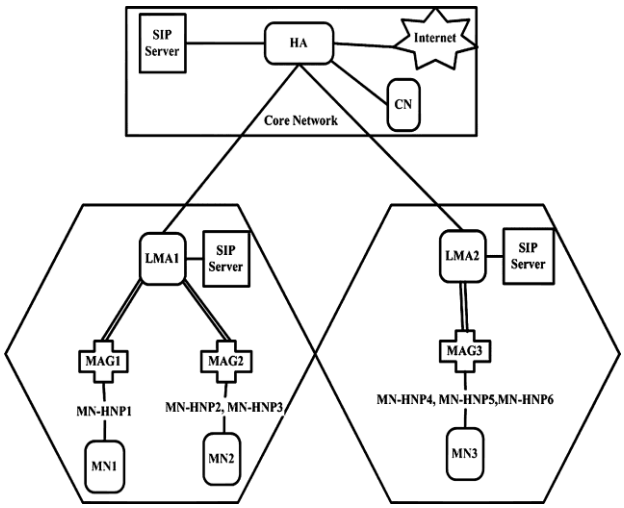


Fig. 1. Network architecture for CLAM.

PMIPv6 [7]-[8] is an extension of MIPv6 which has the support of network based localized mobility management that makes the MN not to participate in any mobility related signaling. The IP mobility is managed by network on behalf of MN. Two types of entities are introduced in PMIPv6 domain which is called local mobility anchor (LMA) and mobile access gateway (MAG). LMA acts as a local home agent (HA) and topological anchor point for MN's home network prefixes in PMIPv6 domain. The binding updates of MN are handled by LMA and facilitate the roaming of MN in its domain. A MAG runs as a function on default access router and acts on behalf of MN to manage mobility related signaling. It is responsible to authenticate and initiates MN's mobility signaling with LMA. Additionally, a bi-directional tunnel is established by MAG with LMA in order to capable the MN of using an address from its home network prefix. When MN enters into the PMIPv6 domain, a unique home network prefix is assigned by the serving network. The assigned prefix follows the MN throughout its roaming inside the PMIPv6 domain. A PMIPv6 domain consists of at least one LMA and MAGs giving look as a single link to the MN [7].

SIP is a text based protocol operating in application layer to set up and tear down the multimedia sessions [3], [13], [14]. In our proposed scheme, the SIP server is connected with HA, and LMAs at PMIPv6 domains. In PMIPv6, MAG performs registration with LMA on behalf of MN. The same registration request is forwarded to SIP server by LMA to make it register if the legality of the request is valid. Similarly, if the MN is in HA, the HA relay the registration request to SIP server. Therefore, there is no need of performing registration separately. Moreover, no extra time is required, because the registration with SIP is performed in parallel with the binding process between MAG and LMA, MN and HA.

The mobility in real-time applications is managed by SIP in two ways. At the start of multimedia session the mobility in SIP refers to pre-call mobility. Whereas, maintaining the seamless handover during an ongoing session, the mobility is termed as mid-call mobility [15]. In pre-call mobility, the MN registers itself with SIP server using REGISTER message. In our proposed scheme, the MN registration is performed with SIP server at the time of its registration with LMA. Once the MN address is registered with SIP server, then it is ready to maintain multimedia session with any Correspondent Node (CN). Suppose, CN in HA domain wants to connect with MN, it will send INVITE message to HA. The HA relay the message to MN's LMA in order to get the address of MN. As the SIP server is in connection with LMA, thus LMA sends the MN' address to HA. The HA forward the address to CN, and then CN starts communicating with MN directly using INVITE message. The MN checks the legality of INVITE message and sends 200 ok message to establish successful multimedia session. If the MN tries to initiate handover during ongoing session, then mid-call mobility needs to be performed. At the time of performing network layer mobility, the MN new address is also updated with SIP server. When the MN obtains new address, it sends re-INVITE message to CN. The CN replies with 200 ok message to ensure the seamless session continuity.

## III. Related Work

Since authentication management, especially reducing latency, signaling cost, packets loss, computation cost, and inefficient authentication during mobility are major challenges in NGNs. Several approaches have been proposed to focus these issues. In [9] and [11], the authors used authentication, authorization, and accounting (AAA) infrastructure for MN authentication in PMIPv6. The limitations in their approach are the packets loss and inefficient authentication. The approaches in [16]-[19] tried to enhance the handover performance in PMIPv6, but the packet loss problem is still there because of the wrong prediction of MN's movement [20]. Packet lossless PMIPv6 (PL-PMIPv6) is proposed in [21], to prevent the

issue of packet loss using buffer technique. But, long handover delay is resulted due to inefficient authentication of PL-PMIPv6. Further, the packet loss problem still exists before establishing the bi-directional tunnel between LMA and MAG. In [8], the concept of Re-PMIPv6 is proposed that also suffers from packet loss problem. The packet loss is occurred because the packets having time stamp may be discarded due to long handover and authentication latency of Re-PMIPv6. The Secure Password Authentication Mechanism **(**SPAM) in [22] used bicasting scheme to prevent the packet loss. This scheme puts a strain on limited resources such as buffer and bandwidth in network due to early start and late stop of bicasting process. Moreover, SPAM possesses low cost until and unless the number of hops is more between MAG and AAA server in other schemes such as MIPv6, PL-PMIPv6, Pre-PMIPv6 and Re-PMIPv6. But, if the number of hops is decreased between MAG and AAA server, the signaling cost is increased in SPAM as compared to these schemes.

In most wireless technologies including IEEE 802.11 and IEEE 802.16, extensible authentication protocol with transport layer security (EAP-TLS) [23] [24] scheme is adopted. The aim of this adoption is to achieve mutual authentication, and it can also applied to PMIPv6 in NGNs. But, due to the following serious drawbacks, EAP-TLS may not be feasible for NGNs.

- The messages exchange for authentication between MN and AAA server are too many.
- There is no providence of local authentication in EAP-TSL. Each time the MN attaches to new MAG needs to be validating with AAA server. If the AAA server and MN are located at much distance, then the authentication latency will be too long.

Due to these drawbacks, high signaling cost and long handover latency are resulted. In [25], the authors proposed secure authentication mechanism for PMIPv6 in NGNs. Their handover management is based on original PMIPv6, resulting in high handover delay. Moreover, the packet loss problem is there because they didn't use the buffer concept.

For the mobility regarding on-going real-time communication, SIP is the leading protocol in communication industry [26]. In order to maintain secure session mobility, two typical approaches such as IPSec and TLS/SRTP have been proposed. IPSec has the problem of complexity which makes it inefficient because the mobile devices have limited resources and battery life. In addition there is no such support of end-to-end security in its existing commercial products. The evidence in [26] showed that it is because of the termination of IPSec tunnel at IPSec server, instead of at the end point. In TLS/SRTP solution, Transport Layer Security (TLS) is used for the protection of SIP signaling, Whereas Secure Real Time Transport Protocol (SRTP) is adopted for authentication and encryption of real-time transport protocol packets. The issue with TLS/SRTP is that each time session is disconnected when IP address changes. In [26], the evidence about long delay is presented. It is because of several messages exchange to re-establish the session. Further, SRTP is able to protect RTP packets, but for the protection of non RTP packets, there is no such solution. Hence, the existing solution of TLS/SRTP is not enough to fulfill the security requirements for SIP in NGNs.

For optimization of network performance, cross layer is considered as an efficient technique because of its focus on the contributions of all relevant protocol stack layers. Several approaches [1], [4] [27]-[31] have been proposed in NGNs to resolve the mobility related issues. The schemes [1], [4], [27]-[30] incorporate enhancement to host-based mobility management, whereas [31] considered network-based mobility. But none of these schemes focused authentication management in their enhancements. Moreover, none of such integrated approach is adopted to handle authentication in both session and network layer mobility.

The next section introduces our proposed scheme to solve these issues.

## IV. Cross-Layer Localized Authentication Mechanism

In this section, we propose a novel Cross-layer Localized Authentication Mechanism (CLAM). The detailed explanation is divided into six phases; registration phase, login phase, MN's attachment and authentication phase, handoff phase, session key update phase, and password change phase. The different notations used throughout this paper are defined in Table I.

TABLE I: Notations

| Symbol | Description | Symbol | Description |
|---|---|---|---|
| $ID_{HA}$ | Identity of HA | $N_{MN}$, $N_{MAG}$, and $N_{LMA}$ | Random numbers selected by MN, MAG, and LMA |
| $ID_{LMA}$ | Identity of LMA | PK | Provisional key |
| $ID_{MAG}$ | Identity of MAG | SK | Session key |
| $ID_{MN}$ | Identity of MN | $K_{LMA}$ , $K_{MAG}$ and $K_{MN}$ | Common secret keys for LMA, MAG and MN |
| $PWD_{LMA}$ | Password of LMA | $r_0$ | Random number of m-bit |
| $PWD_{MAG}$ | Password of MAG | $H(\cdot)$ | A collision free one-way hash function |
| $PWD_{MN}$ | Password of MN | $\oplus$ | XOR operator |
| $TS_{MN}$, $TS_{MAG}$, and $TS_{LMA}$ | Timestamp generated by MN, LMA, and MAG | $\|\|$ | A concatenation operator |

An assumption of master secret keys is made such as $A_{HA}$, $B_{HA}$, $A_{LMA}$, $B_{LMA}$, $A_{MAG}$, and $B_{MAG}$ which are held by HA, LMA, and MAG. The keys $A_{HA}$, $A_{LMA}$, and $A_{MAG}$ are 256 in bit length, whereas the bit length of $B_{HA}$, $B_{LMA}$, and $B_{MAG}$ is 512. These values are composed of high-entropy random numbers. Before starting the authentication,

long-term common secret keys are assumed to be shared between each entity. These are: $K_{LMA} = h\ (ID_{LMA}||B_{HA})$ between LMA and HA, $K_{MAG} = h\ (ID_{MAG}||B_{LMA})$ between MAG and LMA, and $K_{MN} = h\ (ID_{MN}||B_{MAG})$ between MN and MAG. For sharing these keys, Diffie-Hellman key agreement protocol [32] is used as a key agreement technique. HA issues a key to each LMA, LMA issues a key to each MAG, and MAG issues a key to each MN. We use a collision free one-way hash function such as SHA-1 in our proposed mechanism. The bit length of an output of the hash function is 160, whereas the bit length of $K_{LMA}$, $K_{MAG}$, and $K_{MN}$ is 128.

### A. Registration

#### 1) MN registration with MAG

The MN chooses a random number $N_{MN}$ and 8 bytes password $PWD_{MN}$ in length consisting of both characters and digits. After computing $h\ (PWD_{MN} + N_{MN})$, the MN submits its $ID_{MN}$ of length 128 bits to MAG through secure channel. Following steps are performed upon receiving $ID_{MN}$ from MN.

Step 1) MAG calculates $SID_{MN} = (ID_{MAG} \oplus ID_{MN})\ A_{MAG}$ and $K_{MN} = h\ (ID_{MN} || A_{MAG} || M_{MN})$ where $M_{MN}$ is the secret random value of length $l$ for each MN by MAG. RC5 is used as a symmetric algorithm for encryption in the proposed scheme. Using RC5 algorithm, $L$ is assigned bit length of plain text. Therefore the bit length of cipher text must be:

$$\frac{L}{128} \times 128$$

Here the value 128 is assumed to be the bit length of $ID_{MAG}$.

Step 2) A smart card is issued to MN by MAG through secure channel which consists of $\{SID_{MN}, K_{MN}, h(.)\}$.

Step 3) The MN performs the following operations after getting smart card.

$$V_{MN} = K_{MN} \oplus h\ (ID_{MN} || h\ (PWD_{MN} \oplus N_{MN}))$$

$$H_{MN} = h(h(K_{MN}))$$

The $K_{MN}$ is replaced with $\{V_{MN}, H_{MN}\}$by MN and enters its random number $N_{MN}$ to the smart card. Finally the smart card includes $\{V_{MN}, H_{MN}, SID_{MN}, h(.), N_{MN}\}$.

#### 2) MAG registration with LMA

The MAG selects password $PWD_{MAG}$ of 8 bytes in length and a random number $N_{MAG}$. The selected password by MAG comprised both digits and characters. MAG submits its $ID_{MAG}$ of length 128 bits to LMA after the calculation of $h\ (PWD_{MAG} + N_{MAG})$. LMA performs the followings steps after receiving $ID_{MAG}$.

Step 1) LMA computes $SID_{MAG} = (ID_{LMA} \oplus ID_{MAG})\ A_{LMA}$ and $K_{MAG} = h\ (ID_{MAG} || A_{LMA} || M_{MAG})$ where $M_{MAG}$ represents secret random value of length $l$ for each MAG by LMA. The length of cipher and plain text is same as in registration of MN with MAG.

Step 2) The LMA issues smart card to MAG which includes $\{SID_{MAG}, K_{MAG}, h\ (.)\}$

Step 3) After getting smart card, LMA carries out the following operations.

$$V_{MAG} = K_{MAG} \oplus h\ (ID_{MAG} || h\ (PWD_{MAG} \oplus N_{MAG}))$$

$$H_{MAG} = h\ (h\ (K_{MAG}))$$

The MAG replaces $K_{MAG}$ with $\{V_{MAG}, H_{MAG}\}$ and inserts its random number $N_{MAG}$ to smart card. The smart card finally consist $\{V_{MAG}, H_{MAG}, SID_{MAG}, h\ (.), N_{MAG}\}$.

Similarly, LMA is registered with HA using its own password $PWD_{LMA}$ and random number $N_{LMA}$.

### B. Login Phase

The MAG registered with LMA has the responsibility to authenticate and gives the login access to legitimate MN upon its entrannce into the PMIPv6 domain. The MAG first authenticates the MN and then sends the Proxy Binding Updates(PBU) on behalf of MN to LMA. The LMA sends the REGISTER message and the information about MN to SIP server in its domain so that the redudancy factor is avoided. The redudancy is resulted due to separate registration and updation with LMA and SIP server. But in our proposed scheme, the SIP server is updated through LMA, so there is no need for separation registration and updation. In parallel with the updation process in SIP server, the LMA forward the BU to HA. The HA can use the BU, if MN is moving outside of the PMIPv6 domain.

In order to authenticate the MN with MAG, the MN inserts smard card into the device and enters its $ID_{MN}$ and password $PWD_{MN}$. Then, The smart card performs the following operations.

Step 1) Computation of $K_{MN} = V_{MN} \oplus h(ID_{MN} || h(PWD_{MN} \oplus N_{MN})$ and $H^*_{MN} = h(h(K_{MN}))$.

Step 2) The condition is checked whether the $H^*_{MN}$ and $H_{MN}$ is equal. If the answer is yes, then it is assured that the MN is legal and carried on to the next step. If the answer is no, the login request is rejected.

Step 3) The $E$ is comuputed as $E = (h\ (ID_{MN}) ||ID_{MAG}||r_0)\ PK_{MN}$ where $PK_{MN} = h\ (TS_{MN} \oplus K_{MN}))$ is the Provisional Key that is temporary in nature. $ID_{MAG}$ is the identity of MAG to which MN wants to login. The $r_0$ is the secret random number having length of m-bits which is supposed to be 256. MN selects $r_0$ to create session key between MN and MAG. $TS_{MN}$ is the time stamp having length 64 bits. MN uses the $TS_{MN}$ to resist against the replay attacks.

Step 4) MN sends the login message to MAG which consists of $M_1 = \{SID_{MN}, E, TS_{MN}\}$.

### C. MN's Attachment and Authentication Phase

After getting $M_1$, MAG checks the time stamp $TS_{MN}$. If the time stamp is found expire and invalid, the login request is rejected. Otherwise, the MAG uses $K_{MAP}$ to calculate keyed-Hashed Message Authetication Code [33],

and sends it to LMA for verification. In order to authenticate the MN locally by MAG before sending its BU to LMA, the following operations need to be performed.

Step 1) The acceptance window is checked, if the time stamp $TS_{MN}$ lies within it, then MAG uses $A_{MAG}$ to decrypt $SID_{MN}$ and can get $ID_{MN}$. If the format is found to be invalid, the authentication process is terminated. Otherwise, MAG uses $ID_{MN}$ to compute $K_{MN}= h\ (ID_{MN} \| A_{MAG} \| M_{MN})$ and generate provisional key $PK= h\ (TS_{MN} \oplus K_{MN}))$. Subsequently, MAG uses $PK_{MN}$ to decrypt message $E$ and obtains $\{h\ (ID^*_{MN}, ID^*_{MAG}, r_0\ )\}$. MAG computes $h\ (ID_{MN})$ and compare it with $h\ (ID^*_{MN})$ to check whether the MN is valid. If the MN is valid the session key $sk = h\ (h\ (K_{MN}) \| r_0\ )$ is generated and MAG believes that the $TS_{MN}$ is created by valid MN. Otherwise, the process of authentication is ended if the MN is found to be invalid.

Step 2) A message $M_2$ is sent to MN by MAG which includes $(PCert_{MN} \| h\ (r_0))_{sk}$ . Whereas, $PCert_{MN}$ is provisional certificate of length 256 bits which hold life time and other information. In parallel, the MAG sends $M_3$ and proxy binding updates (PBU) to LMA. After getting $M_3$ and PBU, LMA checks time stamp, HMAC and decrypt $E$. The $h\ (ID^*_{MAG})$ is compared with $h\ (ID_{MAG})$ to check whether the MAG is valid. If MAG is valid, LMA creates session key $sk = h(h(\ K_{MAG}\ ) \| r_0\ )$ and performs the registration in SIP server for MN. In addition, LMA relays the authentication and BU message to HA by inserting its own $SID$, $ID_{LMA}$, $TS_{LMA}$ and LMA address. Also, LMA saves information regarding MN so that it can be used in future. When the HA receives message, it checks the validity of LMA and generate session key if LMA is found to be valid. In response, binding update acknowledgment (BUA) is sent to LMA and information about MN is saved. HA uses this information if MN initiates handover from one PMIPv6 domain to another or going outside of the PMIPv6 domain.

Step 3) When MN recieves $M_2$ and router advertisment, it computes session key $sk$ and decrypt $M_2$ to obtain $PCert_{MN}$ and $r_0$. In order to check whether MAG is valid, $h(r_0)$ is compared with $h^*(r_0)$. As a result, MN guarantees that the communication is performed with its own MAG.

Step 4) The CN wants to connect with MN, it encrypts INVITE message $\{PCert_{CN}\| HA\text{-}Address \| CN\text{-}Address\| INVITE\}_{sk}$ using session key and sends it to HA because it is located in its domain. The HA relays the message to corresponding MN's LMA. As the SIP server is connected with LMA, it responds with *MN-HNP*. The CN directly communicates with MN by sending INVITE message $\{PCert_{CN}\| MN\text{-}HNP \| CN\text{-}Address\| INVITE\}_{sk}$. MN checks the $PCert_{CN}$, whether it is valid. If CN is valid, the MN replies with 200 ok message $\{PCert_{MN} \| CN\text{-}Address\| 200\ ok\ Message \| MN\text{-}HNP)\}_{sk}$ in order to perform pre-call mobility successfully. During the messages exchange, validity of each entity is checked using our proposed authentication mechanism.

In Fig. 2 , the complete signalling flow for login request, MN's attachement, and authentication procedure is demonstrated.

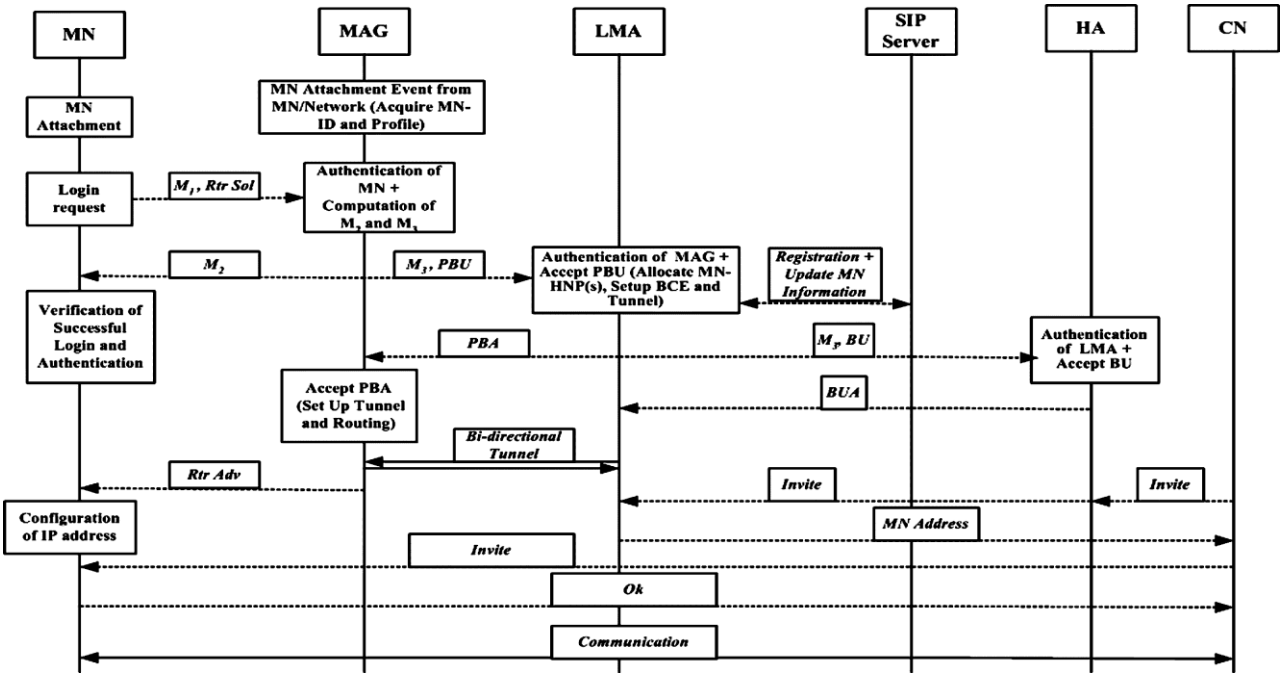


Fig. 2. Signaling flow of CLAM with authentication procedure.

 

### D. Handoff Phase

In this subsection, we demonstrate the handover process wih CLAM. Currently, the occurrence of long handover latency and packet loss are issues in all existing handover schemes for PMIPv6 networks. It is because the authetication is performed through AAA server that causes long delay due to which the packets with time stamp may be discarded. In addition, when the MN performs frequent hadover to different MAG, the heavy workload is resulted due to the presence of AAA server. In our proposed scheme, we perform local authentication during the handover process to minimize handover latency. Each entity authenticates the other entity without the involvement of AAA serevr. Further, the packet loss problem is completely avoided due to buffer and exclusion of AAA server. The complete flow of handover process for our proposed mechanism is presented in Fig. 3, and are explained as follows:

Step 1) As mentioned in subsection II-A, the MAG has the responsibility to detect movement and performs mobility-related signaling on behalf of MN. Thus, previous MAG (p-MAG) sends proxy handover initial(Proxy HI) message that holds the profile of MN to new-MAG(n-MAG).

Step 2) The n-MAG checks the validity of p-MAG upon receiving the proxy HI message. If the p-MAG is valid, the n-MAG replies with proxy handover acknowledgment(proxy HACK).

Step 3) The p-MAG upon receiving proxy HACK message, checks the legality of n-MAG. If it is found legal, the packets forwarding starts between p-MAG and n-MAG for buffering. In parallel, the p-MAG relays the detachment signal to LMA and removes the binding cache and the routing state. LMA identifies mobility session for which it receives detachment request. The request is accepted and waited for certain amount of time to get the binding updates from the n-MAG. During the waiting time, LMA updates the SIP server about the detachment event. If the LMA does not receive any binding update during the given time, it will delete the MN binding cache entry.

Step 4) The MN sends the router solicitation (RS) and login message to n-MAG. The n-MAG, upon detecting the MN attachement and login request, authenticates MN and sends the PBU to LMA. Authetication and MN's attachemnet steps are performed same as shown in Fig. 2. The LMA updates the SIP server about new link and response to MAG with proxy binding acknowledgment (PBA). The bi-directional tunnel is established between LMA and n-MAG. LMA sends router acknowledgment (RA) to MN to retains HoA/HNP(s), guarantees that no change in attachement regading layer-3 of MN interface is detected, and starts forwarding the buffered packets.

Step 5) The MN upon obtaining new HNP, sends re-INVITE message $\{\{PCertMN \| CN \| re\text{-}INVITE \| MN\text{-}HNP\}_{sk}$ to CN inorder to perform mid-call mobility. The message is encrypted with session key *sk*. In response, the CN checks the validity of MN, decrypt the message and sends 200 ok message $\{\{PCert_{MN} \| MN\text{-}HNP \| 200\ ok\ message \| CN\}_{sk}$. The successful mid-call mobility leads the MN to shift to the new link. The make before break concept is adopted to maintain the smooth network layer and session mobility.

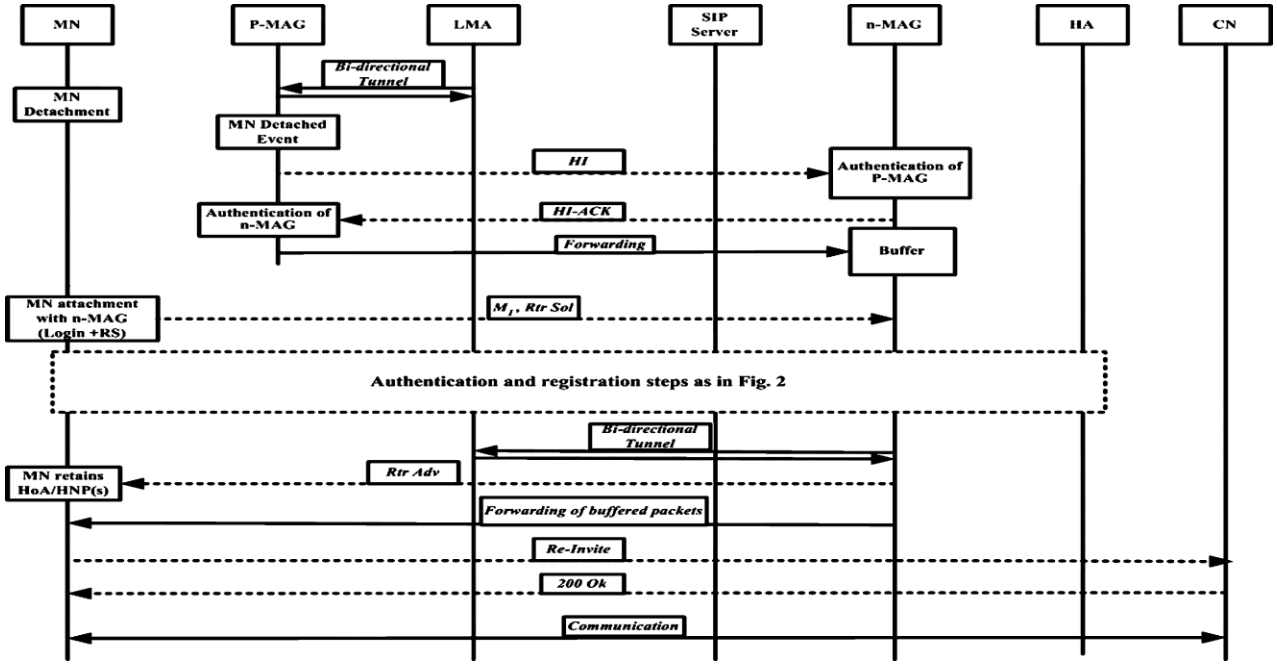


Fig. 3. Handover procedure with CLAM.

### E. Session Key Update Phase

The session key is updated periodically during the MN connection inorder to enhance efficiency and ensure the strong security. The session key updation is performed in the following way.

Suppose, an MN is in $i^{th}$ ongoing session, it sends a message to MAG that is $\{PCert_{MN}, (n_i \| PCert_{MN} \| Additional\ information)\ sk_i$. The message is encrypted with ith session key $sk_i = h\ (h\ (K_{MN} \| n_i\ -1)$, where i=1,2,…,N. The MAG, upon receiving the message, checks that whether the MN is valid. If it is valid, MAG decrypts the message and saves $n_i$ as a new session key for future use. Password Change Phase

The new password $PWD_{MNnew}$ is assigned to MN, if it wants to change password $PWD_{MN}$. The following steps are used to replace the old password with new one.

Step 1) MN inserts smart card into device, enters $\{ID_{MN}, PWD_{MN}\}$ and request to assign new password.

Step 2) The smart card in MN computes $K_{MN} = V_{MN} \oplus h\ (ID_{MN} \| h\ (PWD_{MN} \oplus N_{MN}))$ and $H^*_{MN} = h\ (h\ (K_{MN}))$. The password request is accepted and moved to next step if $H_{MN}=H^*_{MN}$. Otherwise, smart card rejects the password change request.

Step 3) $V_{MNnew}$ is computed by smart card, that is $V_{MNnew} = K_{MN} \oplus h\ (ID_{MN} \| h\ (PWD_{MNnew} \oplus N_{MNnew}))$. The $V_{MN}$ is replaced with $V_{MNnew}$ and it is saved for future use.

## V. Analysis

### A. Security Analysis

In this subsection, the security feautures of CLAM are considered. The proposed scheme satisfies the following security requirements and can resist against possible mentioned attacks.

*1) User anonymity*

In CLAM, the user anonymity is maintained by using symmetric cryptographics and hash operations. The real identity of the MN is managed locally by MAG. The MAG uses the key $A_{MAG}$ to decrpyt $SID_{MN} = (ID_{MAG} \oplus ID_{MN})\ A_{MAG}$. Therefore, only MAG knows about $A_{MAG}$.

*2) Mutual authentication*

The CLAM provides mutual authentication among all the entities such as MN, MAG, LMA and HA. If the message is sent by MN to MAG, the MAG can ensure that it is generated by valid MN. Similary other entities can guarantee the legality of one another.

*3) Backward secrecy*

Backward secrecy ensures that prior session keys cannot be discovered by a passive adversary who has information about subset of keys. In CLAM, the $h(K_{MN})$, $h(K_{MAG})$ and $h(K_{LMA})$ are fixed for each session between *MN-MAG*, *MAG-MAG*, *MAG-LMA*, and *LMA-HA*. In the case of *MN-MAG*, if an adversary has information about $sk_j$ and $sk_{j+1}$, he/she can get $Y_j$ by decrypting the message $(Y_j \| PCert_{MN} \| Additional\ information)sk_j$. Therefore, an adversary can make attempts to compute $h(K_{MN})$ from $sk_{j+1}=h(h(K_{MN})\|Y_j)$. But, hash function $h(.)$ gives output value $sk_j$, therefore to derive $h(K_{MN})$ is stubborn. Even, if an adversary has also information about $\{Y_j, Y_{j+1}\}$, still he/she cannot get $h\ (K_{MN})$. In addition, an adversary cannot compute $sk_j=h\ (h\ (K_{MN}) \| n_{j-1}))$, if he/she doesn't have information about $h\ (K_{MN})$. Thus, in terms of backward secrecy CLAM provides efficiency in real sense.

*4) Forward secrecy*

Forward secrecy ensures that without having information about subset of keys, the successive session keys cannot be discovered by a passive adversary. In CLAM, for each session the $h\ (K_{MN})$, $h\ (K_{MAG})$ and $h\ (K_{LMA})$ are fixed. The case MAG-LMA is considered here for better understanding. If an adversary has information about $sk_j$ and $sk_{j-1}$, he/she can get $Y_{j-1}$ by decrypting message $(Y_{j-1} \| PCert_{MAG} \| Additional\ information)sk_{j-1}$. Thus, attempts can be made by an adversary to compute $h\ (K_{MAG})$ from $sk_j=h\ (h\ (K_{MAG}) \|Y_j))$. But, $sk_j$ is obtained through $h\ (.)$, therefore to derive $h\ (K_{MAG})$ is stubborn. An adversary still cannot obtain $h\ (K_{MAG})$, even having the information about $Y_{j-1}$. Further, he/she cannot compute $sk_{j+1}(=h(h(K_{MAG}) \| n_j))$, if there is no information about $h(K_{MAG})$. Hence, CLAM provides forward secrecy in real sense.

*5) Confidentiality*

The CLAM keeps the messages $\{M_1, M_2\ and\ M_3\}$ confidential, and especially an adversary has no knowledge about $\{(h\ (ID_{MN} \| ID_{MAG} \| r_0), (h\ (K_{MN}) \| r_0))\}$. It is because these messages are kept secret from adversary in our proposed scheme.

*6) One-time session key agreement*

In CLAM, the session key between *MN - MAG*, *MAG-MAG*, *MAG-LMA* , and *LMA-HA* is generated in one round trip. The session key created through random number and hash function is then used to encrypt the succeeding packets in order to ensure the confidentiality in communciation.

*7) Fast error detection*

During the process of authentication or password change, if an adversary keys in the fake identification or password of the user, the errors can be immediately detected by smart card.

*8) Fraud avoidance*

In order to prevent fraud, each entities such as MN, MAG, LMA, and HA must authenticate each other. In CLAM, the mutual authentication between any two of these must ensure the avoidance of fraud. Each entity first check the validity of an other enitity, then session key is created and further communication is performed. If an adversary tries to impersonate any entity to cheat the other, it can be identified when validation is performed. For example, an adversray impersonate MN to cheat MAG by using fake $ID_{MN}$ and secret key $K_{MN}$. The MAG can identify this fraud $E^*$ by decrpting it. The reason is the MAG cannot obtain $\{h\ (ID^*_{MN}), ID^*_{MAG}\}$ and also an adversary has no information about the real identity of MN. Moreover the secret keys are protected by one- way hash

function *h(.)*, thus it is impossible for an adversary to perform impersonation attack.

*9) Known-key attack*

The known-key attack means: in the presence of an adversary who has information about other session keys, then a key agreement protocol can still achieve its objectives. In our proposed scheme, a random and independent nonce $r_i$ is used for each session which makes the session key $sk_i = h(h(K_{MN}) \| r_i - 1)$ independent. Thus, an adversary cannot derive new session key with the help of previous session keys knowledge, and vise versa. Due to this, CLAM has strong resistance against known-key attacks.

*10) Replay attack*

In replay attack, an adversary tries to save the messages and then replays it later on. Suppose, message $M_1$ is intercepted by an adversary, and replayed to login with MAG. This login request is failed during the verification process by MAG because of the interval $\{T^*_{MN} - T_{MN}\} > \Delta T$, where $T^*MN$ is the system time of MAG, when it received replayed message. Further, if an adversary tries to modify the time stamp $TS_{MN}$ and replay it, it cannot be verified by MAG because of $PK = h(TS_{MN} \oplus K_{MN})$. Similarly, if an adversary tries to intercept and replay the messages between MAG-MAG, MAG-LMA, and LMA-HA, it will be failed in verification due to the time interval.

*11) Insider attack*

The insider attack means when any one (e.g. manager) inside the system leaks the secret information; it can lead to serious security holes in authentication protocol. Suppose in our proposed system, a local administrator (LMA) obtains the password $PWD_{MN}$ of MN, and he/she tries to impersonate the user to access MAG. When registration is performed in our proposed scheme, the MN only sends $ID_{MN}$ to MAG and password is not revealed to MAG. Further, the MN must replace its default password $PWD_{MN}$ with the new one $PWD_{MNnew}$ in password change phase. Therefore, any insider cannot get the password of MN in our proposed scheme. It shows that CLAM has strong resistance against insider attacks.

*12) Offline password guessing attack*

The password makes its presence only once at the time when $V_{MN}$, $V_{MAG}$, and $V_{LMA}$ is generated. As in the case of *MN-MAG*, $V_{MN} = K_{MN} \oplus h(ID_{MN} \| h(PWD_{MN} \oplus N_{MN}))$ shows the presence of $PWD_{MN}$. Hence, an adversary is unable to guess the password if he/she does not have information about $ID_{MN}$. In addition, our proposed scheme also possesses the property of user anonymity, therefore it can strongly resists against offline password guessing attack with the security breach of smart card.

*13) Stolen-verifier attack*

In our proposed scheme, the verification table for MN does not save with MAG. Similarly, verification tables for MAG and LMA do not save with LMA and HA respectively. Hence, it is not possible for an adversary to get the information about any entity which shows the strong resistance of CLAM against stolen-verifier attacks.

*14) Modification attack*

An adversary can try to modify authentication messages. In order to resist against this kind of attack, the proposed scheme uses random number $r_0$. Thus, it is hard for an adversary to obtain $r_0$ and compute valid authentication messages.

## B. Performance Analysis

In this subsection we evaluated the performance analysis of the proposed scheme in terms of computational cost, handover latency, signaling cost and packet losses. The proposed network model as shown in Fig. 1 is considered for the comparison with other schemes such as PMIPv6 [7], Pre-PMIPv6 [10], PL-PMIPv6 [21], Re-PMIPv6 [10] and SPAM [22]. The results obtained through numerical analysis are denoted with "NR" in figures. Whereas, the results achieved through simulation are denoted with "SR". The simulation results are obtained using the OPNET simulation tool. An average of ten runs is performed to obtain each result. The simulation parameters are presented in Table II. In the simulation, various access networks such as WiMAX, WLAN, CDMA, IPv6 core network and simple voice network are considered to evaluate the performance of proposed network model in NGNs environment.

TABLE II: SIMULATION PARAMETERS

| | |
|---|---|
| Network size | 2000m*2000m |
| Wired bandwidth | 1Gb/s |
| Wireless link bandwidth | 100Mb/s |
| Packet size | I Kb |
| Moving speed | 5-45m/s |
| Packet rate | 150 packets/s |
| Processing time ($t_{Proc}$) | 5 ms |
| handover latency of layer 2 ($t_{L2}$) | 10 ms |
| Simulation time | 400s |

*1) Handover latency*

The handover latency refers to the time during which the MN is unable to transmit and receive packets when the handover is performed. The total handover latency is composed of delay that occurs while performing deregistration, authentication, registration, and RS/RA processes. The latency for these processes is represented as: $t_{DR}$ = deregistration latency, $t_A$ = authentication latency, $t_R$= registration latency, $t_{RS/RA}$ = latency for RS and RA messages, and $t_p$ = authentication procedure processing latency. The handover latency of the comparison between our proposed scheme and existing schemes can be represented as follows:

$$HL_{PMIPv6} = t_{L2} + t_{DR} + t_A + t_P + t_R + t_{RS/RA} \quad (1)$$
$$= t_{L2} + tp + 4t_{MN\text{-}MAG} + 4t_{LMA\text{-}MAG} + 2t_{LMA/MAG\text{-}AAA}$$

$$HL_{PL\text{-}PMIPv6} = t_{L2} + t_{DR} + t_A + t_P + t_{RS/RA} = t_{L2} + t_P + 4t_{MN\text{-}MAG} + 2t_{LMA\text{-}MAG} + 2t_{LMA/MAG\text{-}AAA} \quad (2)$$

$$HL_{Pre\text{-}PMIPv6} = t_{L2} + t_P + t_R + t_{RS/RA} = t_{L2} + t_P + 2t_{MN\text{-}MAG} + 2t_{LMA\text{-}MAG} + 2t_{MAG\text{-}AAA} \quad (3)$$

$$HL_{Re\text{-}PMIPv6} = t_{L2} + t_A + t_P + t_R + t_{RS/RA} = t_{L2} + t_P + 4t_{MN\text{-}MAG} + 2t_{LMA\text{-}MAG} + 2t_{MAG\text{-}MAG} + 2t_{MAG\text{-}AAA} \quad (4)$$

$$HL_{SPAM} = t_{L2} + t_P + t_R + t_{RS/RA} = t_{L2} + t_P + 2t_{MN\text{-}MAG} + 2t_{LMA\text{-}MAG} + t_{MAG\text{-}AAA} \quad (5)$$

$$HL_{CLAM} = t_{L2} + t_P + t_R + t_{RS/RA} = t_{L2} + t_P + 2t_{MN\text{-}MAG} + 2t_{LMA\text{-}MAG} \quad (6)$$

In above equations, we supposed that $t_{L2}$ is handover latency of layer 2, $t_{MN\text{-}MAG}$ is the wireless propagation delay between MN and MAG, $t_{MAG\text{-}MAG}$ is the propagation delay between MAGs, $t_{LMA\text{-}MAG}$ is the propagation delay between LMA and MAG, and $t_{MAG\text{-}AAA}$ is the propagation delay between MAG and AAA servers. The values of $t_P$, $t_{MAG\text{-}MAG}$ and $t_{LMA\text{-}MAG}$ are set as 10, 5 and 30ms respectively. The parameters $t_{MN\text{-}MAG}$ and $t_{MAG\text{-}AAA}$ are variables.

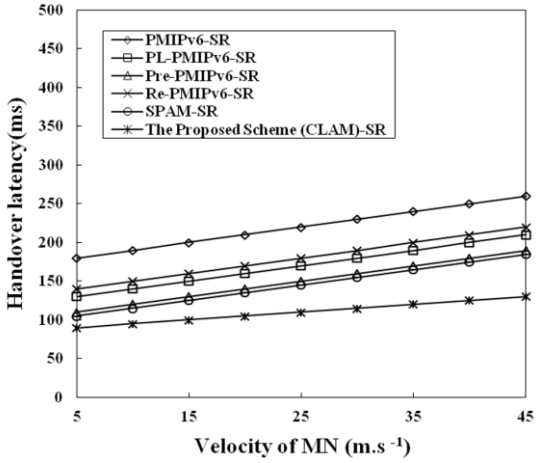


Fig. 4. Handover latency versus velocity of MN.

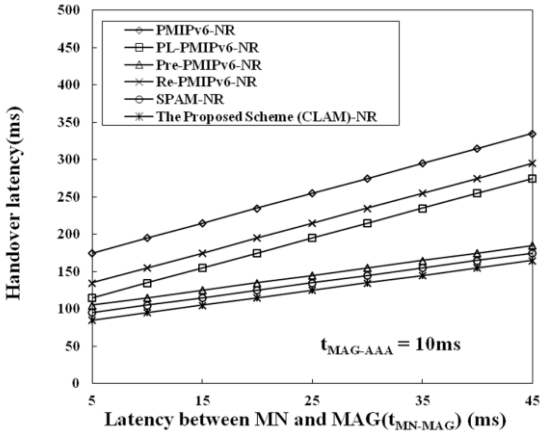


Fig. 5. Handover latency versus tMN-MAG latency (numerical results).

Fig. 4 depicts the average handover latency of the existing schemes and our proposed scheme in different velocities of the MN. The CLAM has significantly reduced the handover latency in terms of MN's velocity as compared to existing schemes. Fig. 5 and Fig. 6 show the handover latency versus latency between MN and MAG. The results demonstrate that if latency is increased between MN and MAG, the CLAM has lower handover latency than existing schemes. In Fig. 7 and Fig. 8, the variation of velocity between MAG and AAA servers has greatly affected the handover latency of existing schemes. Whereas, due to exclusion of AAA server, the velocity increases between MAG and AAA servers has no affect on CLAM. Thus, in terms of handover latency CLAM performance is more efficient than other schemes.

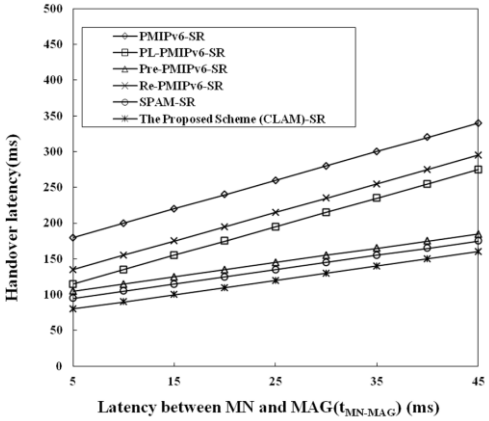


Fig. 6. Handover latency versus $t_{MN\text{-}MAG}$ latency (simulation results).

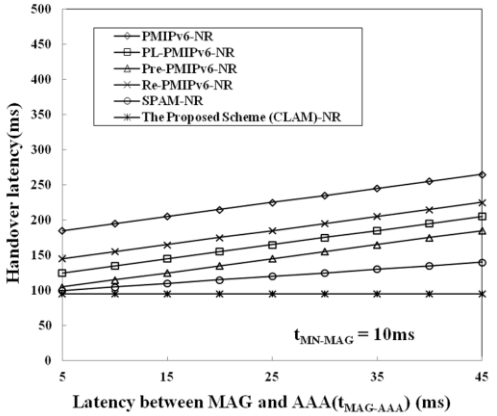


Fig. 7. Handover latency versus $t_{MAG\text{-}AAA}$ latency (numerical results).

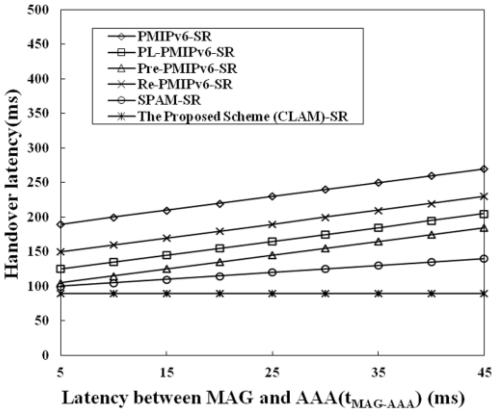


Fig. 8. Handover latency versus tMAG-AAA latency (simulation results).

*2) Signaling cost*

The signaling costs mean the total amount of cost for authentication and handover signaling when the MN performs handover. The handover process includes different phases such as deregistration, authentication and registration. Here, the performance of signaling costs regarding user mobility is evaluated through fluid flow (FF) mobility model [22]. The FF mobility model is adopted to distribute the movement direction of MN uniformly in the range of (0, 2 $\pi$).

The crossing rate for subnets (MAG and LMA) is computed as follows [34]:

$$C_r = \frac{d \times v \times l}{\pi} \quad (7)$$

where $d$ represents MN's density, $v$ represents average velocity, and $l$ is perimeters for MAG and LMA. In the following equations, the signaling cost is expressed for each scheme.

$$SC_{PMIPv6} = 2 \times C_r \times n \times \{[\mu \times D_{MAG-LMAJ} + [(\lambda \times D_{MN-MAG}) + (\mu \times D_{MAG-AAA})] + [(\lambda \times D_{MN-MAG}) + (\mu \times D_{MAG-LMA})]\} \quad (8)$$

$$SC_{PL\text{-}PMIPv6} = 2 \times C_r \times n \times \{[\mu \times D_{MAG-LMA}] + [(\lambda \times D_{MN-MAG}) + (\mu \times D_{MAG-AAA})] + [(\lambda \times D_{MN-MAG})]\} + Cr \times n \times (\mu \times D_{MAG-LMA}) \quad (9)$$

$$SC_{Pre-PFMIPv6} = 2 \times C_r \times n \times \{[(\mu \times D_{MAG-MAG}) + (\mu \times D_{MAG-AAA})] + [(\lambda \times D_{MN-MAG}) + (\mu \times D_{MAG-LMA})]\} \quad (10)$$

$$SC_{Re-PFMIPv6} = 2 \times C_r \times n \times \{[\mu \times D_{MAG-MAG}] + [(\lambda \times D_{MN-MAG}) + (\mu \times D_{MAG-AAA})] + [(\lambda \times D_{MN-MAG}) + (\mu \times D_{MAG-LMA})]\} \quad (11)$$

$$SC_{SPAM} = 2 \times C_r \times n \times \{[(\mu \times D_{MAG-MAG}) + (\mu \times D_{MAG-LMA})] + [(\lambda \times D_{MN-MAG}) + (\mu \times D_{MAG-LMA})]\} \quad (12)$$

$$SC_{CLAM} = 2 \times C_r \times n \times \{[(\mu \times D_{MAG-MAG})] + [(\lambda \times D_{MN-MAG}) + (\mu \times D_{MAG-LMA})]\} \quad (13)$$

In the above equations, $\mu$ represents unit of transmission cost for wired link, $\lambda$ represents unit of transmission cost for wireless link, $n$ represents total number of MAGs in a domain, and $D_{A-B}$ represents counting of hops between A and B.

The values for different parameters are set as: $d$=.00314(MNs/m$^2$), $l$ =100m, $\mu$ = 1, $\lambda$ = 2, $D_{MN-MAG}$ = 1 hop, $D_{MAG-MAG}$= 1 hop and $D_{MAG-LMA}$= 15 hops. The other network parameters such as $n$, $D_{MAG-MAG}$, and $v$ are considered as variables.

Fig. 9, Fig. 10 and Fig. 11 demonstrate the signaling cost of existing schemes and our proposed scheme in terms of MN's velocity.

In Fig. 9, the number of hops is kept 15 between MAG and AAA server. The results show that CLAM has the lowest signaling cost than other schemes. The number of hops is decreased to 10 and 1 in Fig. 10 and Fig. 11 respectively .The efficiency of SPAM has greatly affected because the signaling cost of other scheme such as pre-PMIPv6 and re-PMIPv6 is reduced by decreasing number of hops. We can observe that our proposed scheme performed efficiently in all the three situations in terms of signaling cost because the authentication and mobility is handled locally and AAA server is excluded.

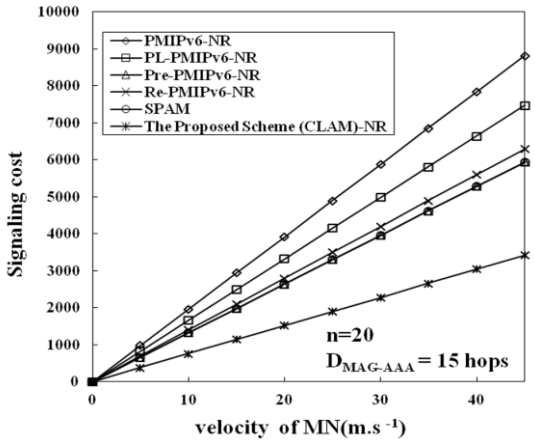


Fig. 9. Signaling cost versus velocity of MN ($D_{MAG-AAA}$ = 15 hops).

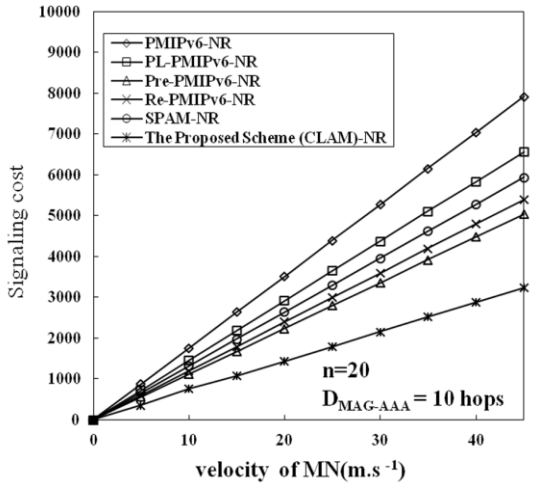


Fig. 10. Signaling cost versus velocity of MN ($D_{MAG-AAA}$ = 10 hops).

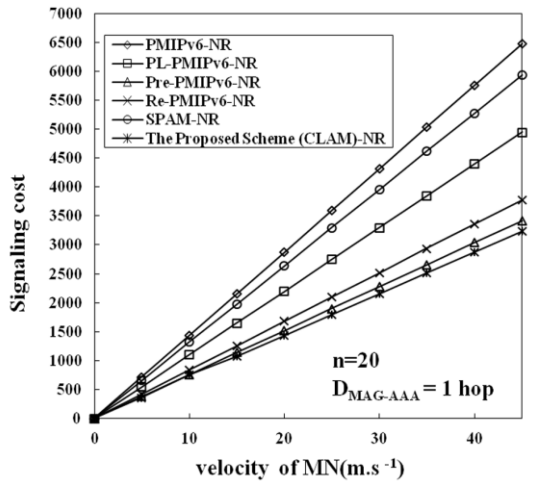


Fig. 11. Signaling cost versus velocity of MN ($D_{MAG-AAA}$ = 1 hop).

*3) Communication overhead*

In mobile communication, the computational and communication processes give birth to an important issue that is power consumption. These processes may include

wait time, parameters creation, comparison, etc. In terms of power consumption, no one can deny the fact of higher communication overhead than computation cost in mobile communication. In order to consider this issue, our proposed scheme reduced communication overhead by using only 3 messages exchange to perform successful authentication. Whereas, the existing schemes [7], [10], [21], [22] have the requirements of more messages than CLAM which results an extra communication overhead. Therefore, our scheme provides strong security over mobile communication in simple way.

*4) Computational cost*

The mobile devices cannot afford high computational load due to limited resources of energy and computing capabilities. Hence, the public key schemes such as RSA and asymmetric cryptosystem are not suitable to be implemented in mobile devices. Our proposed scheme uses symmetric cryptographic and hash operations to make it cost effective and simple for implementation in mobile devices. The existing schemes [7], [10], [21], and [22] used AAA server to authenticate the entities such as MN, MAG and LMA, which brings an extra computation cost and communication overhead over the network. We presented a simple and strong procedure in our scheme to mutually authenticate the entities without the inclusion of any extra computational and communication cost through any entity.

Moreover, the proposed scheme is very efficient regarding bandwidth saving because it can detect the validity very quickly. Suppose, an invalid message $\{ID^*_{MN}, PWD^*_{MN}\}$ is input by MN in login phase. The smart card calculates $H^*_{MN} = h(h(V_{MN} \oplus h(ID^*_{MN} || h(PWD^*_{MN}))))$ and then checks $H^*_{MN} = H_{MN}$ . If the $PWD_{MN} \neq PWD^*_{MN}$ *or* $ID^*_{MN} \neq ID_{MN}$, the login session is immediately terminated by MN.

*5) Packet loss*

In Fig. 12 and Fig. 13, our proposed scheme outperforms the existing schemes regarding packet losses. The packets loss rate in PMIPv6 is high because of having no buffer system during handover. In PL-PMIPv6, the packets loss occurred before the bi-directional tunnel process between LMA and new MAG. The rate of packets loss in Re-PMIPv6 is increased due to wrong handover action by increasing the number of target MAGs. In SPAM, at the time of bicasting some packets loss occurred whereas Re-PMIPv6 loses some packets due to the long handover and authentication latency. It is because the buffered packets are discarded due to expiration of time-stamp. The CLAM uses buffer and local mutual authentication without the inclusion of AAA server, which helps in avoiding the issue of packets lost completely.

In addition, the functionality of the proposed scheme is compared and analyzed with the existing schemes in Table III.

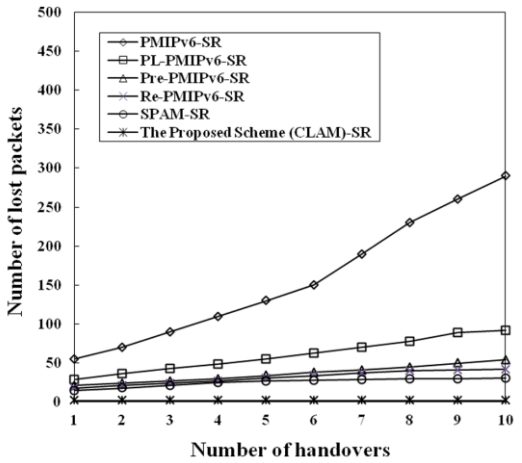


Fig. 12. Packet loss versus number of handovers (# of target MAG =1).

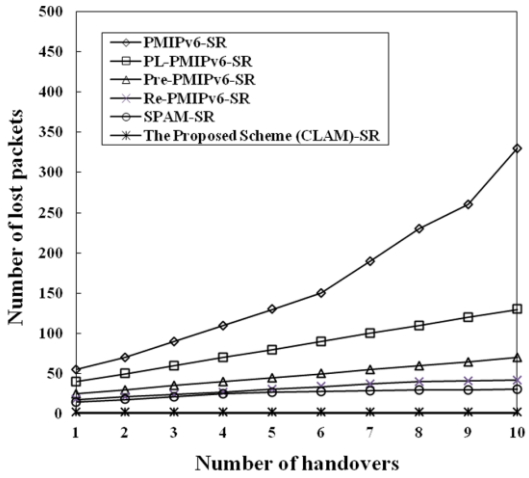


Fig. 13. Packet loss versus number of handovers (# of target MAG =5).

TABLE III: FUNCTIONALITY COMPARISON

| Functionality/Scheme | PMIPv6 | PL-PMIPv6 | Pre-PMIPv6 | Re-PMIPv6 | SPAM | Our Proposed Scheme (CLAM) |
|---|---|---|---|---|---|---|
| Buffer | No | Yes | Yes | Yes | Yes | Yes |
| Use of AAA server | Yes | Yes | Yes | Yes | Yes | No |
| Packet Loss | Yes | Yes | Possibly occur | Possibly Occur | Possibly Occur | No |
| Handover Latency | Long | Long | Moderate | Long | Moderate | Short |
| Signaling cost | High | High | Moderate | Moderate | High( if number of hops decrease between MAG and AAA server in other schemes) | Low |
| Network layer mobility | Yes | Yes | Yes | Yes | Yes | Yes |
| Session mobility operating at application layer | No | No | No | No | No | Yes |
| Local management of authentication | No | No | No | No | Yes | Yes |

## VI. Conclusion

We proposed a novel local authentication scheme called Cross-layer Localized Authentication Mechanism (CLAM) in NGNs. Network based mobility protocol that is Proxy MIPv6 and Session Initiation Protocol (SIP) are combined to secure both real-time and non-real-time communications. The local handling of authentication significantly reduced the handover latency in CLAM. Moreover, the use of buffer and exclusion of AAA server in CLAM avoided the packet loss completely. As the authentication with AAA server resulted an extra latency in existing schemes due to which the packets having timestamp may be discarded. Our proposed mechanism resolved this issue by mutual authentication among the entities without the inclusion of AAA server. In terms of implementation in mobile devices, CLAM is simple and an efficient because of symmetric cryptographic and one-way hash operations. Additionally, CLAM satisfied the following security requirements: resistance against various kinds of attacks, user anonymity, mutual authentication, user friendly, one-time session key agreement, confidentiality, forward secrecy, and backward secrecy. The conducted analysis results showed that CLAM provided a better solution than existing schemes.

## References


[1] W. K. Chiang, H. J. Dai, and C. Luo, "Cross-layer handover for SIP applications based on media-independent pre-authentication with redirect tunneling," in *Proc. Second International Conference on Digital Information and Communication Technology and it's Applications*, 2012, pp. 348-353.

[2] C. Perkins, D. Johnson, and J. Arkko, *Mobility Support in IPv6*, RFC 6275, C. Perkins, Ed., July 2011.

[3] J. Rosenberg, H. Shulzrinne, G. Camarillo, A. Johnston, *et al.*, "SIP: Session initiation protocol," RFC 3261, June 2002.

[4] Q. Wang and M. A. Abu-Rgheff, "Mobility management architectures based on joint mobile IP and SIP protocols," *IEEE Wireless Communications*, vol. 13, no. 6, pp. 68-76, Dec 2006.

[5] R. Koodli, *Mobile IPv6 Fast Handovers*, RFC 5568, July 2009.

[6] H. Soliman, C. Castelluccia, K. ElMalki, and L. Bellier, "Hierarchical mobile IPv6 (HMIPv6) mobility management," RFC 5380, Oct 2008.

[7] S. Gundavelli, K. Leung, V. Devarapalli, K. Chowdhury, and B. Patil, "Proxy mobile IPv6," RFC 5213, Aug. 2008.

[8] H. Yokota, K. Chowdhury, R. Koodli, B. Patil, and F. Xia, "Fast handovers for proxy mobile IPv6," RFC 5949, Sep. 2010.

[9] K.-S. Kong, W. Lee, Y.-H. Han, M.-K. Shin, and H. You, "Mobility management for all-IP mobile networks: Mobile IPv6 versus proxy mobile IPv6," *IEEE Wireless Communications.* vol. 15, no. 2, pp. 36–45, April 2008.

[10] J. Lei and X. Fu, "Evaluating the benefits of introducing PMIPv6 for localized mobility management," in *Proc. IEEE Int. Wireless Commun. Mobile Comput. Conf.*, 2008, pp. 74–80.

[11] K. S. Kong, W. Lee, Y. H. Han, and M. K. Shin, "Handover latency analysis of a network-based localized mobility management protocol," in *Proc. IEEE Int. Conf. Commun.*, 2008, pp. 5838–5843.

[12] L. Jong-Hyouk, *et al.*, "Comparative handover performance analysis of IPv6 mobility management protocols," *IEEE Transactions on Industrial Electronics*, vol. 60, no. 3, pp. 1077-1088, Mar 2013.

[13] J. Zhang, H. C. B. Chan, and V. C. M. Leung, "A SIP-based seamless-handoff (S-SIP) scheme for heterogeneous mobile networks," in *Proc. IEEE Wireless Communications and Networking Conference*, 2007, pp. 3946 – 3950.

[14] O. A. El-Mohsen, H. A. M. Saleh, and S. Elramly, "SIP-based handoff scheme in next generation wireless networks," in *Proc. 2012 6th International Conference on Next Generation Mobile Applications, Services and Technologies*, 2012, pp. 131-136.

[15] W. Wu, N. Bnaerjee, K. Basu, and S. K. Das, "SIP Based vertical handoff between WWAN and WLAN," *IEEE Wireless communication*, vol. 12, no. 3, pp. 66 – 72, June 2006.

[16] F. Xia and B. Sarikaya, "Mobile node agnostic fast handovers for proxy mobile IPv6," IETF Draft, Nov 2007.

[17] S. Ryu, M. Kim, and Y. Mun, "Enhanced fast handovers for proxy mobile IPv6," in *Proc. IEEE Int. Conf. Comput. Sci. Its Applicat.*, 2009, pp. 39–43.

[18] S. D. Kim, J. H. Lee, and T. M. Chung, "Secure fast handover scheme of proxy mobile IPv6," in *Proc. IEEE Int. Joint Conf. INC IMS IDC*, 2009, pp. 555–558.

[19] H. Zhou, H. Zhang, and Y. Qin, "An authentication method for proxy mobile IPv6 and performance analysis," *Security and Communication Networks*, vol. 2, no. 5, pp. 445–454, Sep 2009.

[20] M. C. Chuang and J. F. Lee, "A lightweight mutual authentication mechanism for network mobility in IEEE 802.16e wireless networks," *Comput. Netw.*, vol. 55, no. 16, pp. 3796–3809, Nov 2011.

[21] S. Ryu, G. Y. Kim, B. Kim, and Y. Mun, "A scheme to reduce packet loss during PMIPv6 handover considering authentication," in *Proc. IEEE Int. Conf. Comput. Sci. Its Applicat.*, 2008, pp. 47–51.

[22] M. C. Chuang, J. F. Lee, and M. C. Chen, "SPAM: A Secure password authentication mechanism for seamless handover in proxy mobile IPv6 networks," *Systems Journal, IEEE*, pp. 1-12, July 2012.

[23] D. Simon, B. Aboba, and R. Hurst, "The EAP-TLS Authentication Protocol," RFC 5216, Mar. 2008.

[24] T. N. Nguyen and M. D. Ma, "Enhanced EAP-based pre-authentication for fast and secure inter-ASN handovers in mobile WiMAX networks," *IEEE Transactions on Wirelessm Communications*, vol. 11, no. 6, pp. 2173-2181, June 2012.

[25] J. H. Lee and T. M. Chung, "Secure handover for proxy mobile IPv6 in next-generation communications: Scenarios and performance," *Wireless Commun. Mobile Comput.*, vol. 11, no. 2, pp. 176–186, Feb. 2011.

[26] L. Zhang, H. Miyajima, and H. Hayashi, "An effective SIP security solution for heterogeneous mobile networks," in *Proc. IEEE International Conference on Communications*, 2009, pp. 1 – 5.

[27] D. S. Nursimloo and H. A. Chan, "Integrating fast mobile IPv6 and SIP in 4G network for real-time mobility," in *Proc. 13th IEEE International Conference on Jointly held with the 2 IEEE 7th Malaysia International Conference on Communication*, vol. 2, 2005, pp. 16-18.

[28] L. F. Le and G. Li, "Cross-layer mobility management based on mobile IP and SIP in IMS," in *Proc. International Conference on Wireless Communications, Networking and Mobile Computing*, 2007, pp. 803-806.

[29] M. Zubair, S. Mahfooz, A. Khan, and W. ur Rehman, "Providing end to end QoS in NGNs using combined SIP HMIPv6 (CSH)," in *Proc. IEEE International Conference on Computer Networks and Information Technology*, 2011, pp. 113 – 118.

[30] S. Faisal, "Performance analysis of 4G networks," *Department of Electrical Engineering School of Engineering Bleking Institute of Technology*, SE-37 79 Karlskrona, Sweden, 2010.

[31] L. A. Magagula and H. A. Chan, "IEEE 802.21-assisted cross-layer design and PMIPv6 mobility management framework for next generation wireless networks," in *Proc. IEEE International Conference on Wireless and Mobile Computing Networking and Communications*, 2008, pp. 159-164.
[32] W. Diffie and M. E. Hellman, "New directions in cryptography," *IEEE Transaction on Information Theory*, vol. 22, no. 6, pp. 644–654, Nov 1976.
[33] M. Bellare, R. Canetti, and H. Krawczyk, "Message authentication using hash functions: The HMAC construction," *CryptoBytes Spring*, vol. 2, no. 1, pp. 12–15, 1996.
[34] S. Pack and Y. Choi, "A study on performance of hierarchical mobile IPv6 in IP-based cellular networks," *IEICE Trans. Commun.*, vol. E87-B, no. 3, pp. 462–469, 2004.

**Muhammad Zubair** has done his Bachelor and Master Degree in Computer Science from University of Peshawar, Pakistan in 2005 and 2007 respectively. Currently, he is a PhD student at Dalian University of Technology (DUT), Dalian, China. In Feb 2006, he joined Pakistan Air Force (Fazaia) Degree College, Peshawar as an instructor in computer science. He was promoted as a lecturer in 2007. In 2009, he was assigned with the responsibilities of Head of Computer Science Department in the college. He was also working as a visiting lecturer in Department of Computer Science, University of Peshawar, teaching to undergraduates and post graduates.
He was awarded as a master trainer in Pakistan by Intel. He is reviewer of IEEE Symposium on Wireless Technology & Applications (ISWTA). He is also member of Doctor Association in School of Information and Communication Engineering, DUT. His research interest lies in wireless communication system; particularly focusing on topics related to all aspects of mobility, QoS and security in Next Generation Networks.

**Kong Xiangwei** is currently a professor and director of Research Center of Multimedia Information Processing and Security of Dalian University of Technology, China. During 2006–2007, she was a visiting scholar of Purdue University, USA. Prof. Kong is a member of signal processing society of IEEE. From 2004–2009, she is a vice director of multimedia information security branch of Chinese Institute of Electronics, China. She is also the member of academic committee of China Image and Graphic Association, China. Now, she is a referee of IEEE Trans. Systems, Man and Cybernetics, Pattern Recognition, Fuzzy and System, Journal of Information and Computational Science and Acta Electronica Sinica etc. Her research contributions encompass aspects of multimedia information security, digital watermarking, digital image forensics, image and signal processing, and wireless networks.

**Saeed Mahfooz** has done his Ph.D. from Liverpool John Moore University, Liverpool, UK in Distributed Multimedia Systems in 2001. Before that he has done MS from WIU Arizona State, USA in 1990. He started his teaching career in 1990 which spans around 22 years. His research interest includes QoS Architectures, QoS Routing, Network Protocols, IPv6, Cloud Computing, Wireless Networks, MANETs, future Internet architecture and Next Generation Networks. He is also heading the Computer Networks Research Group at Department of Computer Science, University of Peshawar. In this group he has around 15 MS/PhD students that are pursuing research in different areas. He is also program chair and principal organizer of ICCNIT'11 IEEE conference. In '2012' he organized International Symposium on emerging technologies on IT. He was also part of program committee of PGNET conference for two years. He is also member of IEEE and currently he is Head of the Computer Science Department, University of Peshawar.