I. J. Computer Network and Information Security, **2017, 10, 1-12**
Published Online October 2017 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijcnis.2017.10.01

Secure and Optimized Authentication Scheme in Proxy Mobile IPv6 (SOAS-PMIPv6) to reduce Handover Latency

Arun Kumar Tripathi
KIET Group of Institutions, Ghaziabad, India
E-mail: mailtoaruntripathi@gmail.com

J. S. Lather
National Institute of Technology, Kurukshetra, India
E-mail: jslather@gmail.com

R. Radhakrishnan
E-mail: ramaswamiradhakrishnan@gmail.com

Received: 07 August 2017; Accepted: 25 August 2017; Published: 08 October 2017

***Abstract*—**Advancement in wireless technologies allows mobile devices to access Internet from anywhere at any time.

Each network is identified by unique IP address. Mobile IP allows a mobile node to change its network without changing IP address. Internet Engineering Task Force (IETF) has suggested several mobility management protocols such MIPv6, HMIPv6, PMIPv6 etc. for perpetual mobility. MIPv6 is a Host-Based Mobility Management (HBMM) protocol and provides global mobility solution to the mobile node. MIPv6 suffers from basic mobility related problems such as handover latency, packet loss etc. Recently the IETF has suggested Network-Based Mobility Management (NBMM) protocol. The Proxy Mobile IPv6 (PMIPv6) is first NBMM protocol. PMIPv6 significantly decreases the signaling overhead, but still has some issues related to the security, handover latency and packet loss. This paper proposes Secure and an Optimized Authentication Scheme in PMIPv6 (SOAS-PMIPv6) to reduce signaling overhead. The proposed scheme provides higher security than the basic PMIPv6 protocol and moreover reduces the signaling cost with respect to contemporary protocols. This paper performs comprehensive analysis on handover latency, packet delivery cost, packet loss etc. and the performance of protocols is mathematically investigated. Numerical result shows that the proposed scheme has improved performance than the MIPv6 in terms of handover latency and provides optimized security than PMIPv6 based protocols.

***Index Terms*—**Mobility Management, Proxy Mobile IPv6, Hanover Latency, Packet Loss, Signaling Cost, Performance Analysis.

I. Introduction

Due to the rapid development in the electronics industry, mobile devices such as wearable devices, mobile phones, tablets, laptops, and PDA etc. are introduced. To offer ubiquitous high-speed Internet services, the IETF has introduced Mobile IP with two standards: version 4 and version 6 for the HBMM. These versions are known as Mobile IPv4 (MIPv4) [1] and Mobile IPv6 (MIPv6) [2] respectively.

In MIPv6, the Mobile Node (MN) is accountable for the identification of its present point of attachment and maintaining connectivity to the Internet while switching between access routers. MIPv6 suffers from the unnecessary signaling overhead and duplicate address detection. This results higher handover latency and substantial packet loss. The subsequent version of the HBMM protocols, e.g. Fast Mobile IPv6 (FMIPv6) [3] and Hieratical Mobile IPv6 (HMIPv6) [4] etc. are proposed to overcome from problems associated with standard MIPv6. Above protocols reduce the handover latency, but not up-to mark. Although MIPv6 and its subsequent protocols allow the MN to maintain ongoing communications while moving from one subnet to another. Still, these protocols are not implemented in real life till yet because of two basic reasons: (i) it requires installation of mobility stack on each mobile node and (ii) the MN has limited battery power and most of the power may get consumed in signaling overhead.

In 2008, to overcome from problems associated with the HBMM protocols, the IETF has proposed the Network-based Localized Mobility Management (NETLMM) protocol. The first known NETLMM protocol is the PMIPv6 [5] [6]. It reduces signaling overhead considerably. However, it is still suffering from security issues. In PMIPv6 the network entities are

responsible for mobility related signaling overhead. The network entities are connected through uninterrupted power supply and have faster processing capabilities. Therefore, PMIPv6 provides fast and efficient handover management. This paper proposes a modification in the PMIPv6 authentication procedure by reducing the signaling message exchanged among network entities, which further reduces the delay of MN registration. The proposed SOAS-PMIPv6 is an efficient scheme than PMIPv6 [7] and secure scheme than basic PMIPv6.

The researchers have proposed a number of techniques for evaluation of mobility management. The analytical models can be categorized as random-walk-through models, fluid-flow models, simple numerical calculation-based approaches, and Markov-based models etc.

In this paper, a simple numerical calculation based approach [8] is used for analyzing the results of the proposed model. Initially, the paper explores the existing HBMM and NBMM protocols. Afterward, SOAS-PMIPv6 is proposed to reduce signaling overhead and packet loss in PMIPv6.

The rest of the paper is structured as follows. Section II deals with basic host-based and network-based mobility management protocols. In the section III describes the proposed work. Section IV deals with quantitative analysis of based on handover latency, packet delivery cost, total cost and packet loss. The section V deals with result analysis among MIPv6, PMIPv6 and SOAS-PMIPv6. In section VI the paper is concluded.

II. Related Works

In this section, basic existing host-based mobility protocol, i.e. standard MIPv6 and network-based mobility protocol i.e. PMIPv6 are discussed.

A. Standard Mobile IPv6 (MIPv6)

In the HBMM protocols [2] [7] the mobile entities are responsible for all mobility related signal. To achieve this the MN must be capable of managing mobility by itself. In MIPv6, the MN is uniquely identified by an address, irrespective of its point-of-attachment to the Internet. Within Home Network (HN), this unique address is known as Home Network Address (HoA). On the other hand, when MN is crosses the boundary of home network and visits to another network, it is still addressable by one or more unique addresses known as Care-of-Address (CoA). A router with special capabilities in home link is known as Home Agent (HA) and while in foreign link this router is known as Foreign Access Router (AR). The HA maintains Binding Cache Entry (BCE) for all MN's participating in mobility. Packets from the Correspondent Node (CN) to the MN are intercepted by the HA. The HA searches for an entry of the MN in the BCE. If entry found in the BCE, all packets are forwarded to the HoA or the CoA based on MN's location. Fig. 1 shows packet delivery procedure from the CN to the MN, when the MN is in the HN.

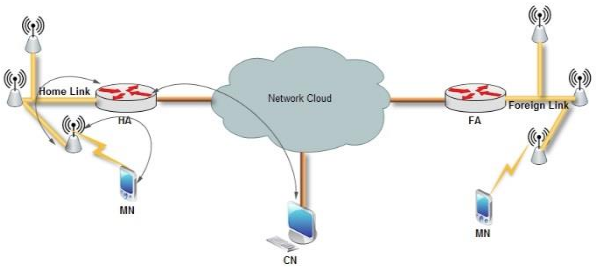

Fig.1. Delivery of packets from CN to MN in Home Network

Fig. 2 shows packet delivery procedure from the CN to the MN, when the MN is attached to a foreign link.

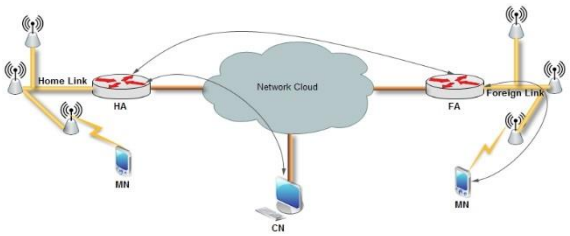

Fig.2. Delivery of packets from CN to MN in Foreign Network

In MIPv6, when the MN is attached to a foreign link after leaving the HN or to a new foreign link after leaving the previous foreign link, it suffers from handover latency and wastage of bandwidth because IP packets from the CN to the MN are firstly delivered to the HA. The HA encapsulates the packets and forwards the packets to the CoA associated with the MN via tunnel. This packet forwarding mechanism is known as triangular routing. To overcome this problem, the MIPv6 uses Return Routability Procedure (RRP). The RRP is responsible for secured route optimization. Fig. 3 shows direct delivery of IP packets between the MN and the CN without involving the HA in communication. In RRP, four messages Home-Test-Init (HoTI), Home-of-Test (HoT), Care-of-Test-Init (CoTI) and Care-of-Test (CoT) are exchanged between CN and MN. Once the route optimization is verified cryptographically, the CN can directly communicate to the MN. Due to route optimization, bottleneck problem at HA reduces significantly along with better bandwidth utilization.

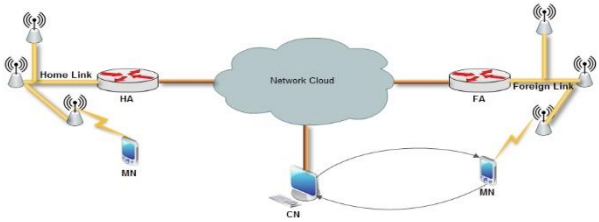

Fig.3. Direct delivery of data packets between MN and CN

- **Singling flow in MIPv6:** Fig. 4 shows the message or signaling flow in MIPv6. Each step is described as follows:

Step 1: As MN boots up (power on) or moves to a new network, after crossing the boundaries of the HN network. It sends multicast Router

Solicitation (RS) message to locate Access Routers (AR) on the link.

Step 2: On receiving the RS message, all AR in the range of the MN response back to the MN by sending Router Advertisements (RA) messages. The RA messages include information such as network prefixes, the link Maximum Transfer Unit (MTU), routes specification, etc.

Step 3: Based on the RA messages that the MN received from neighboring ARs, the MN selects a Candidate Access Router (CAR) for further communication and extract 64-bits of network prefix its RA message. The MN also generates one or more 64-bits suffix.

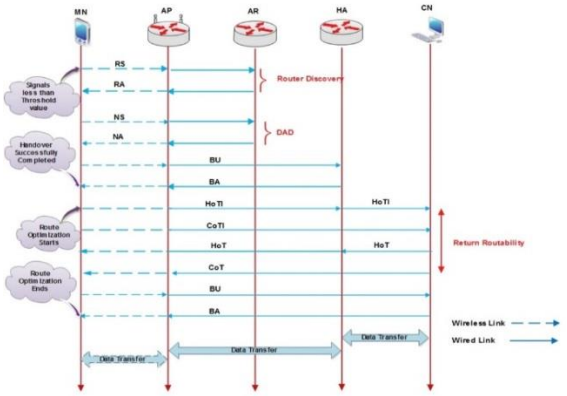

Fig.4. Signaling diagram in MIPv6

Step 4: One of the 64-bit suffix is appended to the 64-bit prefix, to generate 128-bit unique global address. This generated address is known as Tentative Care of Address (TCoA). To verify the uniqueness of TCoA, Duplicate Address Detection (DAD) process is performed.

Step 5: For the DAD, the MN broadcasts Neighbor Solicitation (NS) message containing TCoA to all MN on the local link. After receiving the TCoA, all neighboring nodes compare their own address with the received TCoA. If any neighboring node finds the TCoA is same as address that it has. It immediately responses to defend it's an address by sending Network Advertisement (NA) message to the MN. Now, the MN again performs step 4 and 5 to find unique TCoA on the local link.

Step 6: If MN doesn't receive the NA message within a reasonable time interval [2], it shows the success of the DAD. Now the TCoA is considered as unique on the link and this TCoA is immediately assigned as Care of Address (CoA) of MN.

Step 7: As the CoA is assigned to the MN, it immediately informs to the HA about its present location by sending the Binding Update (BU) message. On receiving the BU, the HA immediately updates or creates the BCE to update or create new point-of-attachment of MN.

Step 8: The HA also responses back to the MN about successful registration. For this, the HA sends the Binding Acknowledgement (BA) message to the MN.

Step 9: The triangular routing is responsible for the packet loss. To overcome from it, MN sends two messages HoTI via HA and CoTI directly to the CN. The HoTI message contains home-init cookie and requests for a home keygen token from the CN. Similarly, CoTI message contains care-of init cookie and requests for a care-of keygen token from CN.

Step 10: The CN send HoT and CoT messages in response HoTI and CoTI respectively. The HoT is sent via HA and CoT directly to the MN. The HoT contains home keygen token, home init cookie and home nonce index. Similarly, the CoT contains care-of keygen token, the care-of init cookie and care-of nonce index.

Step 11: After receiving the HoT and the CoT messages, the MN compares the received messages for verification and after successful verification, the MN sends the BU message to the CN. The purpose of this message to notify about present location i.e. present the CoA of the MN to the CN.

Step 12: After receiving the BU from the MN, the CN immediately updates its BCE with the present CoA as well as inform to the MN about the BCE update by sending the BA.

Step 13: The BA message works as an indication about successful route optimization. Now, the MN communicates directly to the CN without participating the HA in communication.

B. Proxy Mobile IPv6 (PMIPv6) Protocol

The network-based mobility management approach has numerous advantages over the host-based mobility management approach. In network-based mobility management protocols, the MN neither requires special security configurations nor special software update for providing IP-based mobility support. PMIPv6 [8], [9] reuses basic concept of the standard MIPv6. It works in Localized Mobility Domain (LMD) without involving the MN in mobility related signaling. All the mobility related signals are carried out by network entities. These entities are Mobile Access Gateway (MAG), Local Mobility Anchor (LMA) and Authentication, Authorization, Accounting (AAA) server. The MAG in PMIPv6 has the same responsibilities as the AR in standard MIPv6 with some additional capabilities. The MAG is positioned in between the MN and the LMA. The basic responsibility of the MAG is Movement Detection (MD) of the MN and

initiation of mobility signaling on behalf of the LMA. Fig. 5 shows the MN's movement in LMD.

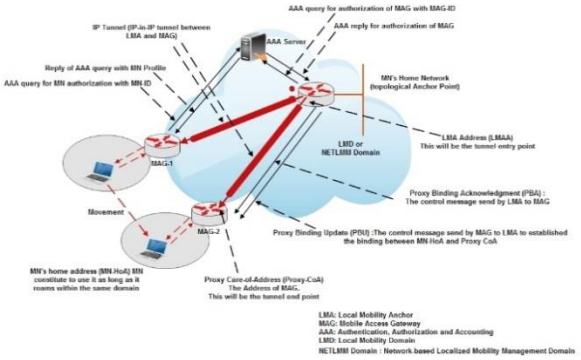

Fig.5. Architecture of PMIPv6

The MAG requests to the AAA server for necessary security checks in order to verify the MN's identity. After successful authentication from the AAA server and the MAG sends Proxy Binding Update (PBU) message to the LMA. The LMA responses to the MAG with Proxy Binding Acknowledgement (PBA) and then MAG setups a bidirectional tunnel for communication between the MAG and the LMA. All traffic from the LMA to the MN and from the MN to the LMA passes through the established tunnel. The MAG is also responsible for maintaining the Binding Update List (BUL). The BUL contains the information about all MNs to that are attached to individual MAG. Moreover, the LMA in a LMD is similar to the HA in standard MIPv6 with some supplementary capabilities required to support PMIPv6.

LMA works as a topological anchor point for LMD. LMA allocates Home Network prefix (HNP) to the MN and maintains the BCE. The BCE binds the IP address of the MN with the Proxy-Care-of Address (P-CoA). The P-CoA is the unique address, which is configured on the interface of the MAG at the bidirectional tunnel endpoint. The MN can communicate with the CN with the help of assigned P-CoA.

- **Signaling flow in PMIPv6:** Fig. 6 shows message or signaling flow in PMIPv6. Each step is described as follows:

Step 1: When a MN arrives into new LMD after leaving previous one or switch the power on in the existing LMD. The MAG immediately detects the presence of the MN.

Step 2: After detecting attachment, the MAG is responsible for verification of the MN's identity. For verification of MN's identity, the MAG requests to the AAA server by sending the MN-Identifier (MN-ID). The AAA server verifies the MN-ID from an existing database. If the MN is authenticated successfully, the AAA server responses to the MAG by sending MN's profile, the LMA Address (LMAA) and other information stored in the AAA server.

Step 3: At this step, the MAG requests to the LMA for registration of the MN by sending the PBU message. The PBU includes the MN-ID, the P-CoA, the MAG-ID, and the binding lifetime of MN's etc.

Step 4: After receiving the PBU the LMA sends AAA query message to the AAA server for verification of the authenticity of the PBU sender.

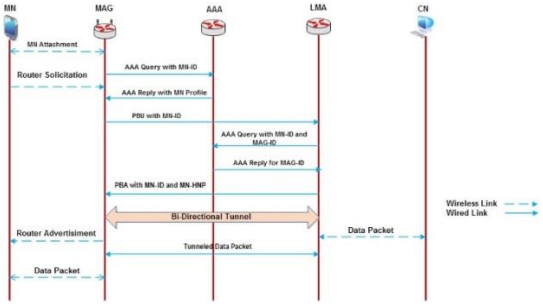

Fig.6. Signaling Diagram in PMIPv6

Step 5: The AAA server searches for MAG-ID in its database for verification and if MAG is successfully verified then it immediately responses to the LMA by the AAA response message.

Step 6: After successful verification from the AAA server, the LMA searches for MN's entry in the BCE, if MNs record is found in BCE, it immediately updates it by new MAG-ID or else the LMA immediately creates new record for the MN in the BCE. The LMA also informs back to the MAG about successful registration by sending the PBA message. The PBA message contains Home Network Prefix (HNP) of MN.

Step 7: After receiving PBA, the MAG establishes a bidirectional tunnel between the MAG and the LMA. This tunnel is responsible for transporting all the data traffic between the MAG and the LMA.

Step 8: The MAG informs about successful registration at LMA to MN by sending the Router Advertisement (RA) message.

PMIPv6 offers an efficient handover mechanism as compared to the MIPv6 for localized mobility. PMIPv6 reduces signaling overhead exponentially with respect to MIPv6. But still suffers from handover latency for real time applications due to signaling overhead.

III. Secure and Optimized Authentication Scheme for Proxy Mobile IPv6 (SOAS-PMIPv6) Scheme

The handover latency mainly depends on various factors such as layer-2 switching delay, Layer-3 movement delay, authentication delay, and registration delay etc. In this paper, we have proposed a novel scheme that reduces the authentication delay significantly with respect to the PMIPv6 proposed in [8]. In this scheme, we

have optimized the authentication process by removing redundant signaling messages.

In the existing PMIPv6 [8] the redundant authentication signal increases the singling overhead. As a result, the PMIPv6 has a higher handover latency and as a result higher packet loss. The authentication is a two-step process. In the first step, the MAG requests for verification of the MN to the AAA server by sending AAA query message containing the MN-ID and after successful verification, the AAA server response back by sending the MN profile to the MAG. In second step, the LMA request for verification of the MAG to the AAA server by sending AAA query message containing the MAG-ID and after successful verification, the AAA server response back by sending the MAG profile to LMA.

In case of SOAS-PMIPv6 scheme, the redundant signaling is reduced by multicast addressing and removes the dual authentication. This process decreases the authentication delay considerably.

- **Signaling flow in SOAS-PMIPv6:** Fig. 7 shows message or signaling flow in SOAS-PMIPv6. Each step is described as follows:

Step 1: As the MN migrates to new LMD from old LMD or boots up in same LMD. The MAG immediately detects the presence of the MN and establishes a point-to-point connection between the MN and the MAG.

Step 2: To verify the genuineness of the MN, the MAG sends MN-ID along with MAG-ID to the AAA server.

Step 3: In the meantime, the MN sends Router Solicitation (RS) message to a particular the MAG by selecting it for communication. The MN can send RS at any moment of time after entering in LMD.

Step 4: Once the AAA server verifies the MN's identity, it sends a multicast message to the MAG and the LMA. The message contains the MN's profile with the MN-ID, the MAG profile with MAG-ID, and reinforced address configuration mode etc. The LMA receives complete information required for MN's and MAG's registration at the LMA. Hence, the MAG has no need to send the PBU message to the LMA explicitly. The multicast message from the AAA server behaves same as the PBU message from the MAG.

Step 5: After receiving the response from the AAA server, the LMA immediately allocates the Home-Network-Prefix (MN-HNP) and create an entry with the address of the MAG in the BCE of the LMA. The BCE, encompasses information such as the MN-ID, the P-CoA and the prefix assigned to the MN by LMA. The LMA informs about successful creation of MN's entry in the BCE by sending the PBA message to the MAG.

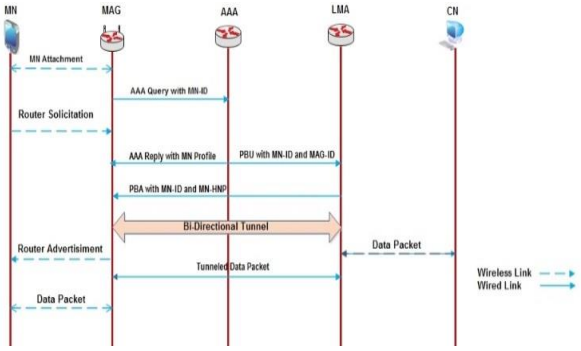

Fig.7. Signaling Flow in SOAS-PMIPv6

Step 6: The MAG construct a virtual bidirectional tunnel between the LMA and the MAG after receiving PBA for communication as well update or create an entry for the MN in the BUL.

Step 7: The MAG also informs to the MN about successful registration by sending the RA message. All the packets from the CN are redirected to the MN through established bidirectional tunnel.

IV. Quantitative Analysis of Handover Latency cost, Packet Delay cost and Total Cost in MIPv6, PMIPv6 and SOAS-PMIPv6 schemes

The root cause of handover latency in next-generation mobile-IP networks is the signaling overhead. The handover process is depends on the Layer-2 and the Layer-3 handover. The Layer-2 handover latency is the time between when the MN disconnects from Current Access Router (CAR) and get connected to the New Access Router (NAR) within same subnet. On the other hand, the Layer-3 handover includes agent discovery, authentication and registration process. The MN experience layer-3 handover as it crosses the boundaries of residing network. For analysis following assumptions are taken into considerations:

a. For analysis of MIPv6, PMIPv6 and SOAS-PMIPv6 protocols under the same network structure, the administrative domain can be applied as follows. In MIPv6, the administrative domain is considered as foreign network and for PMIPv6, it is considered as the home network domain because the MN is free to move in the LMD.

b. It is considered that the MNs can access a visiting network after successful completion of AAA procedure and access delays are same for MIPv6, PMIPv6, and SOAS-PMIPv6 protocols.

c. The elapsed combining MN-HNP with MN's suffix at interface is negligible.

d. All the delays considered are symmetric.

e. During return routability procedure, the time between the MN and the CN via HA is taken into consideration because it is larger than the required for direct communication between the HA and CN.

This section deals with numerical analysis based on simple numerical scheme among MIPv6 [1], PMIPv6 [8] and SOAS-PMIPv6. Fig. 8 shows network model considered for analysis. The proposed scheme incorporates basic assumptions taken into account in [8], [10], [11], [12], [13], [14]. In PMIPv6, the LMD is the localized mobility domain in which the LMA provides seamless mobility to the MN. There is no special sequence for sending the RS message by the MN to the MAG. After detecting the attachment by the MAG, the MN may send the RS message any instant of time. Therefore, its effect the RA message is not taken into consideration for the analysis.

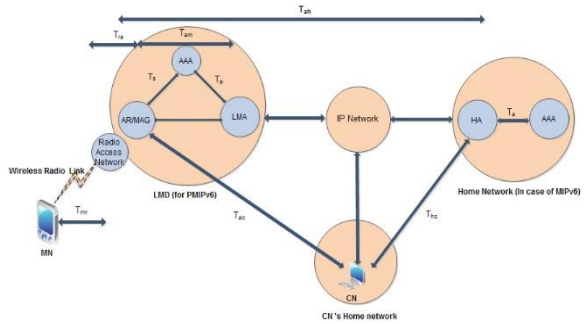

Fig.8. Analytical Model for Performance Analysis

The minimum amount of time before sending unsolicited multicast advertisements is Min_Rtr_Adv_Interval (MinInt) and the maximum amount of time before sending unsolicited multicast advertisements is Max_Rtr_Adv_Interval (MaxInt). Therefore, the mean time between two successive router advertisement messages can be calculated as (MinInt + MaxInt) / 2.

Movement Detection (MD) plays an important role and also very costlier. After establishing layer-2 connection, the layer-3 handover is identified by the MD. The MD is the time spent for the discovery of a new AR performed through the RS and the RA message exchanges between the MN. The mean value of MD delay is half of the mean time between unsolicited router advertisement messages and calculated as (MinInt + MaxInt) / 4.

A. Analysis of handover latency cost incurred in MIPv6, PMIPv6 and SOAS-PMIPv6

The basic objective of movement detection is to check that whether the MN has reached to a new network after crossing the previous network boundary or not. If movement detection is identified, then the previous CoA should be invalidated and a new CoA should be assigned to establish or maintain an upper layer connection. This process encompasses singling overhead.

- **Handover Latency Cost in MIPv6:** Handover latency in the MIPv6 depends on various factors such as movement detection delay, duplicate address detection delay, authentication delay and registration delay. The DAD process is very critical and has highest delay in MIPv6. The handover latency cost in MIPv6 is described as follows:

$$HLC_{MIPv6} = T_{MDD} + T_{DADD} + T_{AD} + T_{RD} \quad (1)$$

Where, T_{MDD} is the movement detection delay, T_{DADD} is the duplicate address detection delay, T_{AD} is the authentication delay / access delay and T_{RD} is the registration delay. These terms are described as follows:

The movement detection is described as follows:

$$T_{MDD} = (MinInt + MaxInt)/4 \quad (2)$$

The authentication delay between the AR and AAA server is same as delay between the HA and AAA server. The authentication delay is described as follows:

$$T_{AD} = 2 * (2T_{Authentication}) \quad (3)$$

The registration delay includes registration delay at the HA, route optimization delay and registration delay at CN.

$$T_{RD} = HA_{RD} + CN\_MN_{ROD} + CN_{RD} \quad (4)$$

Where, HA_{RD} is the home agent registration delay, CN_{RD} is the correspondent node registration delay and CN_MN_{ROD} is route optimization delay between MN and CN. Each of these delays are explored as follows:

$$HA_{RD} = 2(T_{MN-AP} + T_{AP-AR} + T_{AR-HA}) \quad (5)$$

$$CN_{RD} = 2(T_{MN-AP} + T_{AP-AR} + T_{AR-CN}) \quad (6)$$

$$CN_{MN_{ROD}} = 2(T_{MN-AR} + T_{AR-AP} + T_{AP-HA} + T_{HA-CN}) \quad (7)$$

We have considered that the delay between the AR to the CN through the HA rather than direct delay between MN and CN. Because, delay through the HA is always greater than delay in direct communication between the MN and CN. Therefore, the equation (1) becomes

$$HLC_{MIPv6} = T_{MD} + T_{DAD} + 4T_{AR-HA} + 6(T_{MN-AP} + T_{AP-AR}) + 2(T_{HA-CN} + T_{CN-AR}) \quad (8)$$

- **Handover Latency Cost in PMIPv6:** In PMIPv6, the authentication process is required only once for the MN either when the MN enters first time in the LMD boundary or boots-up first time in the boundary of LMD. The handover latency in PMIPv6 affected by the wireless signaling delay between the MAG to the MN, authentication process delay from the AAA server and, the registration process delay. In PMIPv6, for registration process two packets are transmitted one for the PBU and another one for the PBA. To authenticate the MN the MAG exchanges two messages with the AAA server and to authenticate the MAG the LMA exchanges two messages with the AAA server. Thus, total four messages are exchanged. Hence, the handover latency cost in PMIPv6 is described as follows:

$$HLC_{PMIPv6} = T_{RD} + T_{AD} + T_{MN-AP} + T_{AP-MAG} \quad (9)$$

The registration delay is described as follows:

$$T_{RD} = 2T_{MAG-LMA} \quad (10)$$

The authentication delay is described as follows:

$$T_{AD} = 2 * 2T_{Authentication} \quad (11)$$

Now the equation (9) is represented as

$$HLC_{PMIPv6} = 4T_{Authentication} + 2T_{MAG-LMA} + T_{MN-AP} + T_{AP-MAG} \quad (12)$$

- **Handover Latency Cost in SOAS-PMIPv6:** The proposed SOAS-PMIPv6 scheme optimizes significantly authentication delay process. In PMIPv6, for authentication total four messages are exchanges are exchanges among network entities.

While for authentication in SOAS-PMIPv6 only three packets are exchanged, one unicast packet for MN's authentication request containing MN-ID and MAG-ID from the MAG to the AAA server and two multicast authentication response packets are transmitted from the AAA server. One message to the MAG containing MN's successful authentication information and another one to the LMA for updating the BCE entry at LMA. The handover latency of SOAS-PMIPv6 can calculated as:

$$HLC_{SOAS-PMIPv6} = T_{RD} + T_{AD} + T_{MN-AP} + T_{AP-MAG} \quad (13)$$

The registration delay is described as follows:

$$T_{RD} = T_{MAG-LMA} \quad (14)$$

The authentication delay is described as follows:

$$T_{AD} = 3T_{Authentication} \quad (15)$$

Therefore, the equation (13) becomes

$$HLC_{SOAS-PMIPv6} = 3T_{Authentication} + T_{MAG-LMA} + T_{MN-AP} + T_{AP-MAG} \quad (16)$$

B. Analysis of packet delivery cost incurred in MIPv6, PMIPv6 and SOAS-PMIPv6

The packet delivery cost depends on various factors such as transmission delay, propagation delay, processing delay and queuing delay. Therefore the packet delay can be expressed as:

$$PD = T_{TD} + T_{ProcD} + T_{PropD} + T_{QD} \quad (17)$$

The T_{TD}, T_{ProcD}, T_{PropD} and T_{QD} are transmission delay, processing delay, propagation delay and queueing delay respectively. These delays are defined as follows:

a. Transmission Delay: It is defined as the amount of time required to transmit all of the packet's bits into the link. If L is the length of message and B is the bandwidth of link, then transmission delay is expressed as follows:

$$T_{transmission\_dealy} = \frac{L}{B} \quad (18)$$

b. Processing delay: It is the time elapsed in scrutinizing the header of packet. The processing time includes the time elapsed for analyzing bit level errors in the packet before sending the packet to the upstream node. The processing speed of sophisticated routers is normally in the order of microseconds or less.

c. Propagation Delay: It is the time that taken by a bit to propagate through the communication channel from a node to the next node. This delay depends of type of transmission media.

d. Queueing Delay: It is the time that a packet elapsed in a queue. The high-speed intermediate routers have incoming and outgoing queue both.

- **Packet Delivery Cost on wired and Wireless Links:** Total packet delivery cost includes, packet delivery cost on wired link as well as wireless link. These cost are defined as follows:

a. Packet delivery cost on wired link: The packet delivery cost for single hop on wired link expressed as follows:

$$PDC_{wired} = \frac{L}{B_{wd}} + T_{wd} + T_{QD} \quad (19)$$

Here, the bandwidth of wired link is represented by B_{wd}, the 'L' represents the length of the packet, T_{QD} represents the average queuing delay of each intermediate router on the Internet. Since, a wired link may have number of hops from sources to destination. Hence, Total delay on wired link can be expressed as:

$$DPC_{wired} = \left(\frac{L}{B_{wd}} + T_{wd} + T_{QD}\right) * N_{HOP} \quad (20)$$

b. Packet delivery cost on wireless link: Wireless links are less reliable than wired. Let n_f defines the number of wireless link failure [15] and P_{nf} describes probability that before successful transmission the message fails nf times. The mean number of nf is expressed as follows:

$$E_{nf} = \Sigma_{nf=0}^{\infty} n_f * P_{nf} = \frac{P_{wlf}}{1 - P_{wlf}} \quad (21)$$

Where, P_{wlf} defines the probability of wireless link failure. Thus, total wireless link delay to deliver packet $PDC_{wireless}$ is expressed as follows:

$$PDC_{wireless} = \left(\frac{L}{B_{wl}} + T_{wl} + T_p\right) + E_{nf} * \left(\frac{L}{B_{wl}} + T_{wl} + T_p + T_{wait}\right) \quad (22)$$

Where, B_{wl} represents the bandwidth of wireless link, T_{wl} represents propagation delay, T_p is the processing time of message and T_{wait} is waiting time to ensure that the message has been lost. The waiting time directly depends on Round Trip Time (RTT) and can be calculated as follows:

$$T_{wait} = \rho\left(\left(\frac{L}{B_{wl}}\right) + T_{wl} + T_p\right) \quad (23)$$

Where, ρ is the weight factor for waiting time. Hence, delay for single hop wireless link is expressed as:

$$PDC_{wireless} = \left(\frac{1+\rho*P_{wlf}}{1-P_{wlf}}\right) * \left(\frac{L}{B_{wl}} + T_{wl} + T_p\right) \quad (24)$$

- **Packet delivery Cost in MIPv6:** After successful route optimization, the MN can communicate to the CN directly. The communication process involves one wireless link and number of wired links depending on number of hops. Packet delivery cost in MIPv6 can be expressed as follows:

$$PDC_{MIPv6} = \left(\frac{1+\rho*P_{wlf}}{1-P_{wlf}}\right) * \left(\frac{L}{B_{wl}} + T_{wl} + T_p\right) + \left(\frac{L}{B_{wd}} + T_{wd} + T_{QD}\right) * N_{HOP} \quad (25)$$

- **Packet delivery Cost in PMIPv6:** The PMIPv6 is a localized Mobility management protocol. The communication process involves one wireless link and one wired link. Packet delivery cost in PMIPv6 can be expressed as follows:

$$PDC_{PMIPv6} = \left(\frac{1+\rho*P_{wlf}}{1-P_{wlf}}\right) * \left(\frac{L}{B_{wl}} + T_{wl} + T_p\right) + \left(\frac{L}{B_{wd}} + T_{wd} + T_{QD}\right) \quad (26)$$

- **Packet delivery Cost in SOAS-PMIPv6:** The SOAS-PMIPv6 is also network based localized mobility management protocol and communication process involves one wireless link and one wired link same as PMIPv6. Packet delivery cost in PMIPv6 can be expressed as follows:

$$PDC_{SOAA-PMIPv6} = \left(\frac{1+\rho*P_{wlf}}{1-P_{wlf}}\right) * \left(\frac{L}{B_{wl}} + T_{wl} + T_p\right) + \left(\frac{L}{B_{wd}} + T_{wd} + T_{QD}\right) \quad (27)$$

C. Analysis of total cost incurred in MIPv6, PMIPv6 and SOAS-PMIPv6

Total cost incurred in Mobile IP includes handover latency cost and packet delivery cost.

- **Total Cost in MIPv6:** The total cost in MIPv6 is the sum of handover latency cost and packet delivery cost. The communication process in MIPv6 involves one wireless link and number of wired links depending on number of hops. Total cost is expressed as

$$TC_{MIPv6} = T_{MD} + T_{DAD} + 6(T_{MN-AP} + T_{AP-AR}) + 4T_{AR-HA} + 2(T_{HA-CN} + T_{CN-AR}) + \left(\frac{1+\rho*P_{wlf}}{1-P_{wlf}}\right) * \left(\frac{L}{B_{wl}} + T_{wl} + T_p\right) + \left(\frac{L}{B_{wd}} + T_{wd} + T_{QD}\right) * N_{hop} \quad (28)$$

- **Total Cost in PMIPv6:** Similar to the MIPv6, the total cost in PMIPv6 represented as sum of handover latency cost and packet delivery cost. It is expressed as

$$TC_{PMIPv6} = (4T_{Authentication} + 2T_{MAG-LMA} + T_{MN-AP} + T_{AP-MAG}) + \left(\frac{1 + \rho * P_{wlf}}{1 - P_{wlf}}\right) * \left(\frac{L}{B_{wl}} + T_{wl} + T_p\right) + \left(\frac{L}{B_{wd}} + T_{wd} + T_{QD}\right) \quad (29)$$

- **Total Cost in SOAS-PMIPv6:** The total cost in SOAS-PMIPv6 is describe as summation of handover latency cost and packet delivery cost. The communication process involves one wireless link and one wired link. Total cost in SOAS-PMIPv6 is expressed as

$$TC_{SOAS-PMIPv6} = (3T_{Authentication} + T_{MAG-LMA} + T_{MN-AP} + T_{AP-MAG}) + \left(\frac{1+\rho*P_{wlf}}{1-P_{wlf}}\right) * \left(\frac{L}{B_{wl}} + T_{wl} + T_p\right) + \left(\frac{L}{B_{wd}} + T_{wd} + T_{QD}\right) \quad (30)$$

D. Analysis of packet loss incurred in MIPv6, PMIPv6 and SOAS-PMIPv6

Packet loss [16], [17] is one of critical issue in mobile-IP. During handover process the MN is unable to send or receive data packets and results packet loss. To overcome from packet loss an efficient buffering policy should be implemented at the HA in MIPv6, at MAP in HMIPv6 and at LMA in PMIPv6. Packet loss rate is expressed as product of Handover Latency (HL) and packet arrival rate (λ_p).

$$PL = HL * \lambda_P \quad (31)$$

Thus, we can say packet loss is directly proportional to handover latency and packet arrival rate. To reduce packet loss handover latency should less.

- **Packet Loss in MIPv6:** The packet loss in MIPv6 is expressed as follows:

$$PL_{MIPv6} = \lambda_P * (T_{MD} + T_{DAD} + 4T_{AR-HA} + 6(T_{MN-AP} + T_{AP-AR}) + 2(T_{HA-CN} + T_{CN-AR})) \quad (32)$$

- **Packet Loss in PMIPv6:** The packet loss in PMIPv6 is expressed as follows:

$$PL_{PMIPv6} = \lambda_P * (4T_{Authentication} + 2T_{MAG-LMA}$$

$$+ T_{MN-AP} + T_{AP-MAG}) \quad (33)$$

- **Packet Loss in SOAS-PMIPv6:** The packet loss in SOAS-PMIPv6 is expressed as follows:

$$PL_{SOAA-PMIPv6} = \lambda_P * (3T_{Authentication} + T_{MAG-LMA} + T_{MN-AP} + T_{AP-MAG}) \quad (34)$$

V. Resulsis

This section deals with mathematical analysis of the handover latency cost, packet delivery cost, total cost and packet loss among MIPv6, PMIPv6 and SOAS-PMIPv6 schemes based on considerations in section III and Table-1[8], [10], [12], [13].

Table 1. Symbolic Representation of Parameters and Their Default Values

Symbols	Meaning	Value
T_{MN-AP}	Signaling delay to between MN and AP over wireless links	10 msec.
T_{AP-AR} / T_{AP-MAG}	Signaling delay between AP and AR over wired link OR Signaling delay between AP and MAG over wired link	2 msec.
T_{AR-HA}/ $T_{MAG-LMA}$	Signaling delay between AR and FA over wired link OR Signaling delay MAG and LMA over wired link	10 msec.
T_{AR-HA}/ T_{MAG-HA}	Signaling delay between the AR and the FA OR Signaling delay between the MAG and the LMA	20 msec.
T_{CN-AR}/ T_{CN-MAG}	Signaling delay between the AR and the CN OR Signaling delay between the MAG and the CN (without including HA in communication)	20 msec.
T_{HA-CN}	Signaling delay between the HA and the CN	10 msec.
$T_{Authentication}$	Authentication Delay for the MN or the MAG at the MAG or the LMA respectively	3 msec.
T_{DAD}	Signaling delay during DAD process	1000 msec.
T_{MD}	Mean value of Movement-Detection Delay	25 msec.
MinInt	Minimum interval between unsolicited multicast Router Advertisement	30 msec.
MaxInt	Maximum interval between unsolicited multicast router advertisement	70 msec.
L	Length of the packet	512 bytes
B_{wd}	Bandwidth of wired link	1Gbps
B_{wl}	Bandwidth of wireless link	54 Mbps
T_{QD}	Average queuing delay of each router on the Internet	0.5 msec.
T_P	Processing Time	0.5msec.
T_{wl}	Propagation Delay	2msec.
T_{wd}	Propagation Delay	0.5 msec.
ρ	Weight factor for waiting time	1
P_{wlf}	Probability of wireless link failure	.1
N_{HOP}	Number of hops in wired link	3

A. *Impact of wireless link delay on handover latency*

The handover latency is a critical factor and depends on the signaling overhead. The communication signals are carried out by both wired as well as wireless links. The bandwidth of wireless is much lesser than the wired link and directly impacts on signaling delay. The chances of packet loss are more on wireless link than wired links. The retransmission of lost packets is a burden on network and network devices.

In MIPv6, the binding update process, the DAD process, and the route optimization process use wireless link to transmit the signals. The DAD process is extensively larger than any other delay and main cause of handover latency in MIPv6. The PMIPv6 and SOAS-PMIPv6 are least affected by wireless link delay because these protocols don't involves the MN in mobility related signaling. Fig. 9 shows the impact of wireless link delay on handover latency in MIPv6, PMIPv6 and SOAS-PMIPv6. The results shows that on increasing wireless link delay the handover latency also increases. The MIPv6 is most affected by wireless delay and SOAS-PMIPv6 is least affected.

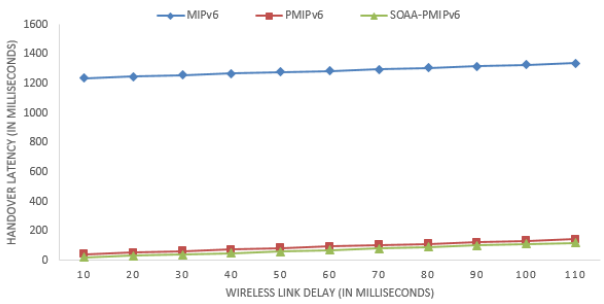

Fig.9. Impact of Wireless Link Delay on Handover Latency

B. Impact of delay on handover latency between MN and CN:

The wired and wireless mediums are responsible for overall delay between the MN and the CN. The delay depends on (T_{MN-AP}+ T_{AP-AR} + T_{AR-CN}) factors. Fig. 10 shows the impact of delay MN and CN on handover latency. The result shows that the proposed SOAS-PMIPv6 scheme has least handover latency among existing MIPv6 and secure PMIPv6 protocol.

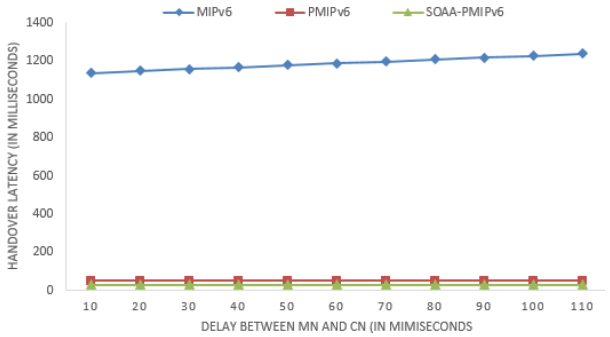

Fig.10. Impact of Wireless Link Delay on Handover Latency

In MIPv6, when a MN changes its subnet, it has to register itself with new CoA, to the HA and the CN. The PMIPv6 and the SOAS-PMIPv6 are based on localized mobility therefore no need to assign new IP address while the MN is roaming with in the LMD.

C. Impact of Movement Detection on handover latency

The PMPv6 and SOAS-PMIPv6 are localized mobility management protocols and these protocols don't required movement detection until the MN remains in the same LMD. On the other hand, the MIPv6 the handover latency is directly proportional to time taken in movement detection and care-of addresses assignment process. Fig. 11 shows the effect of movement detection on handover latency. The result shows that in MIPv6 the handover latency increases as the movement detection delay increases. On the other hand the PMIPv6 and SOAS-PMIPv6 protocols are not affected by movement detection.

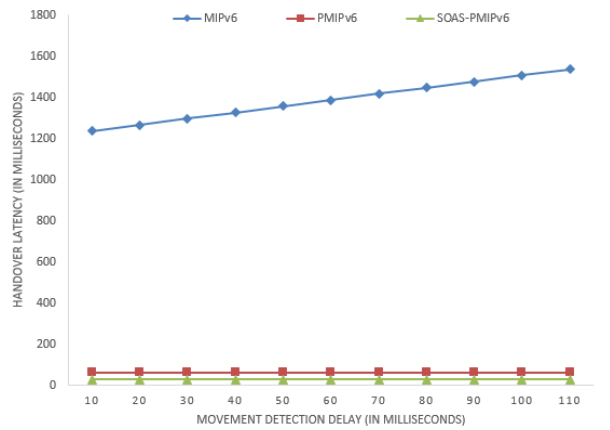

Fig.11. Impact of Movement Detection Delay on Handover Latency

D. Impact of increase in number of hops on wired link

On increasing the number hops on wired links, the packet delivery cost and total cost also increase. This is because, as the number of intermediate increases the processing time at each router and tunneling time between routers also increases. The packet are investigated at each intermediate router before forwarding to next router. This process increases the queueing time at router.

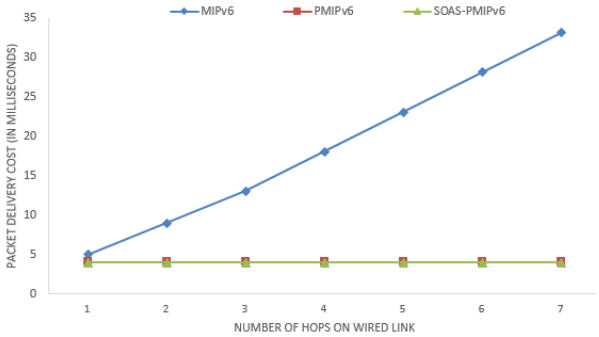

Fig.12. Impact of Number of Hops on Packet Delivery Cost

Fig. 12 shows the impact of the number of hops on packet delivery cost. The MIPv6 has highest packet delivery cost, while PMIPv6 and SOAS-PMIPv6 have same packet delivery cost.

Fig. 13 shows the impact on total cost due to change in number of hops on wired links. The result shows MIPv6 is highly affected by change in number of hops on wired link. On the other hand, PMIPv6 and SOAS-PMIPv6 have no effect on total cost due to change in number of hops. Because all MAGs are at only one hop distance from the LMA.

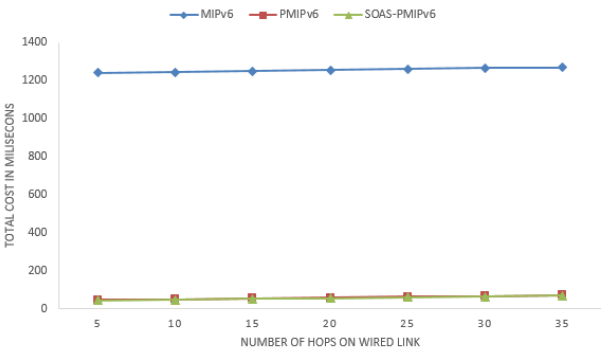

Fig.13. Impact on Total Cost Due to Change in Number Hops Wired Link

E. Impact of handover latency on packet loss

Packet loss depends on various factors such as link bandwidth, movement detection, authentication, registration, etc. The packet loss depends on handover delay and packet arrival rate. Here, we have considered that sufficient amount of bandwidth available and it does not affect packet loss. Fig. 14 shows the effect on packet loss due to delay in wireless on MIPv6, PMIPv6 and SOAS-PMIPv6.

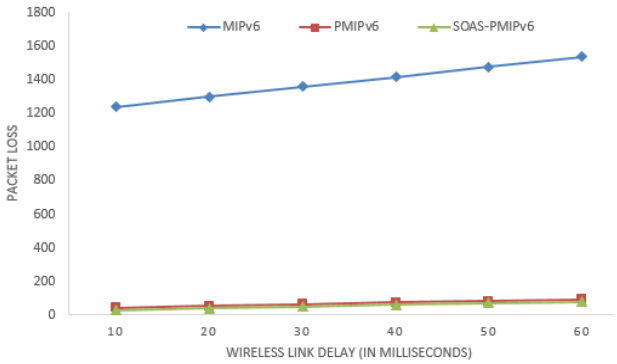

Fig.14. Impact of Wireless Link Delay on Packet Loss

Fig. 15 shows the effect on packet loss due to change in packet arrival rate on MIPv6, PMIPv6 and SOAS-PMIPv6.

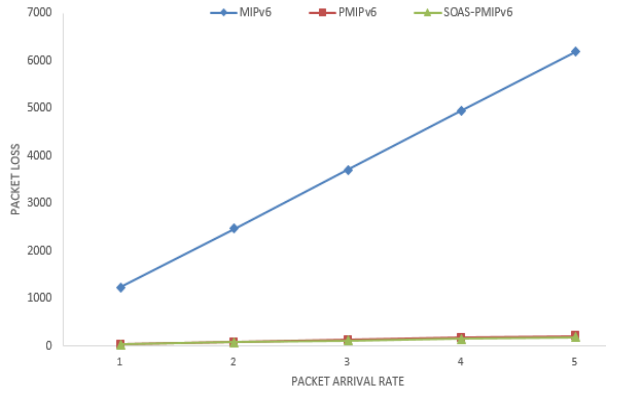

Fig.15. Impact of Packet Arrival Rate on Packet Loss

VI. Conclusions

The extensive growth of mobile users increases the data traffic on Internet. The mobile users are permitted to move from one location to another by crossing network boundaries. Handover management is a critical issue in All-IP mobile networks. Researchers have proposed numerous IPv6-based mobility management protocols for secure communication. The incorporation of security module in mobility management protocols increases the signaling overhead and as a result number of packet loss also increases.

This paper we have done the comprehensive analytical evaluation of existing mobility management protocols such as MIPv6 and PMIPv6. Later on, we have proposed a secure and optimized scheme for secure mobility management in PMIPv6. The performance of the proposed protocol is compared with existing protocols on various metrics such as handover latency, packet delivery cost, total cost, and packet loss. The result shows that the proposed protocol is completely secure has a less signaling overhead than existing protocols. Due to less signaling overhead, the handover latency decreases significantly and as a result total cost also decreases. The packet loss is a critical issue in mobile IP. The prosed protocol decreases packet loss considerably. This results improvement in the performance of SOAS-PMIPv6 than other existing protocols. We can improve the performance of the protocol by associating buffer at network entities.

References

[1] C. Perkins, IP Mobility Support for IPv4, IETF RFC-3775, August 2002.

[2] D. Johnson, C. Perkins, and J. Arkko, “Mobility Support in IPv6,” IETF RFC-3775, June 2004.

[3] R. Koodli, Mobile IPv6 Fast Handovers, IETF RFC-5568, July 2009.

[4] H.Soliman, C.Castelluccia, K.El.Malk, L.Bellier, “Hierarchical Mobile IPv6 (HMIPv6) Mobility Management”, IETF RFC-5380, October 2008.

[5] S. Gundavelli, K. Leung, V. Devarapalli, K. Chowdhury, B. Patil, “Proxy Mobile IPv6”, IETF RFC-5213, August 2008.

[6] Seil Jeon, Sergio Figueiredo, Rui L. Aguiar, and Hyunseung Choo, “Distributed Mobility Management for the Future Mobile Networks: A Comprehensive Analysis of Key Design Options”, IEEE Access, Vol. 5, pp: 11423 – 11436, June 2017.

[7] J. Lee., Kamal Deep Singh, Jean-Marie Bonnin, “Mobile Data Offloading: A Host-Based Distributed Mobility Management Approach,” IEEE Internet Computing, vol. 18, no. 1, pp: 20–29, February 2014.

[8] Ki-Sik Kong, Wonjun Lee, Youn-Hee Han, Myung-Ki Shin, Heung Ryeol You, “Mobility management for all-IP mobile networks: mobile IPv6 vs. proxy mobile IPv6”, IEEE Wireless Communications, Vol-15, Issue-2, pp: 36-45, 2008.

[9] Cho, Chulhee, Jae Young Choi, Jun Dong Cho, and Jongpil Jeong. "Design and performance analysis of a cost-effective proxy-LMA mobility management scheme in IP-based mobile networks with global mobility support", International Journal of Ad Hoc and Ubiquitous Computing, Vol. 21, Issue 4, 2016.

[10] Christian Makaya, and Samuel Pierre, “An Analytical Framework for Performance Evaluation of IPv6-Based Mobility Management Protocols”, IEEE Transactions on wireless communications, Vol. 7, No. 3, pp: 972-983, March 2008.

[11] Vasu, Kantubukta, Sudipta Mahapatra, and Cheruvu Siva Kumar. "A Comprehensive Framework for Evaluating IPv6 Based Mobility Management Protocols", Wireless Personal Communications, Vol. 78, Issue 2, pp 943–977, September 2014.

[12] Jong-Hyouk Lee and Thierry Ernst, “Lightweight Network Mobility within PMIPv6 for Transportation Systems”, IEEE systems journal, vol. 5, No. 3, pp: 352-362, September 2011

[13] Jong-Hyouk Lee, Member, Jean-Marie Bonnin, Ilsun You, and Tai-Myoung Chung, “Comparative Handover Performance Analysis of IPv6 Mobility Management Protocols”, IEEE Transactions on Industrial Electronics, Vol. 60, Issue 3, March 2013.

[14] Jong-Hyouk Lee, T Ernst, N Chilamkurti, Performance analysis of PMIPv6-based network mobility for intelligent transportation systems. IEEE Transactions on Vehicular Technology Vol. 61, Issue 1, pp: 74–85, 2012.

[15] Jyoti Madaan, Indu Kashyap,"Vertical Handoff with Predictive Received Signal Strength in Next Generation Wireless Network", International Journal of Computer

Network and Information Security (IJCNIS), Vol.8, No.8, pp.27-38, 2016.
[16] Jong-Hyouk Lee, Zhiwei Yan, Ilsun You, "Enhancing QoS of Mobile Devices by a New Handover Process in PMIPv6 Networks", Wireless Personal Communication, Vol. 61, pp: 591–602, November 2011.
[17] Riaz Ahmed Khan, Ajaz Hussain Mir, "Advanced Prediction Based Mobility Support for 6LoWPAN Wireless Sensor Networks", I. J. Information Technology and Computer Science, Vol.9, No.2, pp: 47-57, Feb. 2017.

Authors' Profiles

Arun Kumar Tripathi received the B.Sc. (Electronics) degree from Dr. Hari Gour University Sagar and M. Tech. Uttar Pradesh Technical University in Computer Science and Engineering. Presently, he is pursuing Ph.D. from National Institute of Technology, Kurukshetra. He joined the KIET group of Institution, Ghaziabad in 2003 and presently working as Associate Professor. His area of interest is Mobile and Wireless Communication. He has published more than 20 papers in various International National conferences and Journals.

Dr. J.S. Lather has received B.E, M. Tech from and Ph.D. REC Kurukshetra. He has more than 23 year experience and presently working as Professor in Electrical Engineering Department, NIT Kurukshetra. His area of interest Wireless Communication, Robust Control of Time Delay Systems, Networked Control Systems, Consensus in WSN, Coop Control in Multi Agent Sys, Control of FACTs incorporating renewable energy. He has published more than 50 papers in various International National conferences and Journals.

Dr. R. Radhakrishnana has received B.E. and M.E. from NIT Trichy and Ph.D. from Jamia Milia Islamia in Handover Management in MIPv6. He has more than 17 years Industry more than 10 years academic experience. His area of interest is Mobile and Wireless Communication. He has published more than 22 papers in various International National conferences and Journals.

How to cite this paper: Arun Kumar Tripathi, J. S. Lather, R. Radhakrishnan,"Secure and Optimized Authentication Scheme in Proxy Mobile IPv6 (SOAS-PMIPv6) to reduce Handover Latency", International Journal of Computer Network and Information Security(IJCNIS), Vol.9, No.10, pp.1-12, 2017.DOI: 10.5815/ijcnis.2017.10.01

