A NOVEL SECURE HANDOVER MECHANISM IN PMIPV6 NETWORKS

K.Mayuri and K.S.Ranjith

Department of Computer Science and Engineering,
SreeVidyanikethan Engg.College, Tirupati, India

ABSTRACT

The Internet Engineering Task Force (IETF) proposed proxy mobile ipv6 (PMIPv6) is a very promising network based mobility management protocol. There are three entities LMA MAG and AAA server required for the proper functioning of PMIPv6.. In PMIPv6 Networks having many disadvantages like signaling overhead , handover latency ,packet loss problem and long authentication latency problems during handoff. So we propose a new mechanism called SPAM which performs efficient authentication procedure globally with low computational cost. It also supports global access technique using ticket based algorithm. Which allows user's mobile terminals to use only one ticket to communicate with their neighbor Access Points? This algorithm not only reduces the mobile terminal's computational cost but also provides user ID protection to protect user privacy. Through this technique, it can implement handover authentication protocol, which in turn results in less computation cost and communication delay when compared with other existing methods.

KEYWORDS

Authentication, handover, Proxy Mobile IPv6 (PMIPv6).

1. INTRODUCTION

In future Networks wants to allow seamless and secure roaming of mobile devices across wireless networks through heterogeneous access technologies. PMIPv6 network reduces the handover latency compared to MIPv6, but it still suffers from packet loss and out-of-sequence problems, inefficient authentication procedures. Most of the wireless networks use EAP-TLS protocol to provide mutual authentication mechanism, but PMIPv6 networks do not support this protocol. The reasons are

1) Mobile node and Authentication server needs to transfer more number of authenticated messages between them.
2) This protocol uses mostly in large distance between the MN and the CN , it produces the long handover latency.

So PMIPv6 protocol calls for an efficient handover mechanism such as secure password authentication mechanism (SPAM) for protecting the legal user from various attacks in PMIPv6 networks. This networks are having some feasible solutions for solving the flaws of the authentication and handover procedures of PMIPv6.

1) Our scheme performs a bi-casting scheme for avoiding the packet loss problem.
2) It proposes the global authentication mechanism for reducing the authentication latency.
3) It uses the piggyback technique to reduce the signaling overhead.

DOI:10.5121/ijitcs.2014.4401

These techniques are combined with SPAM which produces the global access technique, and it produces the low computational cost, low handover latency in proxy mobile IPv6 networks. In this paper, we propose a novel integrated mechanism in PMIPv6 Networks , It provides global accessibility for communicating the mobile devices in case of roaming situations.

2. NETWORK ARCHITECTURE

Fig. 1 shows the network architecture of PMIPv6, which contains three network entities: the mobile access gateway (MAG), the local mobility anchor (LMA), and the authentication, authorization and accounting (AAA) server.

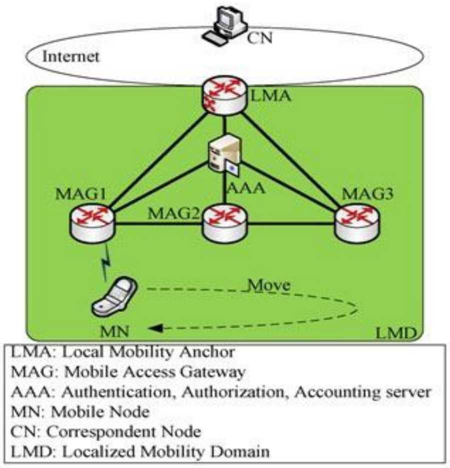
CN
Internet
LMA
AAA
MAG1
MAG2
MAG3
Move
MN
LMD
LMA: Local Mobility Anchor
MAG: Mobile Access Gateway
AAA: Authentication, Authorization, Accounting server
MN: Mobile Node
CN: Correspondent Node
LMD: Localized Mobility Domain

Fig 1: Network Architecture

The MAG is responsible for detecting the movements of an MN and performs mobility-related signaling with the LMA in place of the MN. The LMA acts in a similar way to the home agent in MIPv6, and it maintains the binding cache entries for currently registered MNs. The AAA server is responsible for authenticating the MN.

3. RELATED WORK

Several approaches have been proposed to focus signaling cost, packets loss, computation cost. In [3] and [4], the authors used AAA Server infrastructure for MN authentication in PMIPv6. The limitations in their approach are the packets loss and inefficient authentication. The approaches in [5]-[6] are tried to enhance the handover performance in Proxy Mobile IPv6 Networks , but the packet loss problem is still there because of the wrong prediction of MN's movement [7]. Packet lossless PMIPv6 (PL-PMIPv6) is proposed in [8], to prevent the issue of packet loss using buffer technique.

In wireless networks are assumed to fully integrate different wireless access technologies, in order to enable their users to exploit the advantages of the various technologies, depending on the momentary requirements and circumstances. Such access technologies are e.g., the 3GPP Long Term Evolution (LTE) for wide area coverage at moderate data rates and (future) members of the IEEE 802.11 family of Wireless Local Area Networks (WLANs)[9,10,11] for high data rates at hotspots. Our contribution extends PMIPv6 with ideas from Fast Handovers for Mobile IPv6 (FMIPv6) Networks . It will be referred to from now on as FPMIPv6 Networks. Our addition PMIPv6 aims to allow the network to manage handovers with support from the mobile, while at the same time considerably reducing handover delays, computational cost.

4. EXISTING SYSTEM

Previously the wireless technologies adopt on authentication protocol with the transport layers security service in order to attain a mutual authentication. There arise some drawbacks for the authentication protocol. Finally a lot of authentication message should be handled by both the mobile node and the AAA server. Secondly the AAA server validates in mobile node every time when it get attached to the different MAG. But the authentication latency should be considered very high, if the distance between becomes larger. Because of these Disadvantages, the extensible authentication protocol has a very high signaling overhead and haring a longer latency for authentation. SPAM performs local authentication procedure. It should not be able to handle the handover problem. More over the secure password authentication mechanism does not use any of the buffer mechanism which leads to packet loss problem , it does not supports the global access technique and do not provide any secure group communication.

5. PROPOSED MECHANISM:

In Proposed system, we have to introduce a bi-casting scheme to avoid the packet loss and out-of-sequence problems and piggyback technique is used to reduce the signaling overhead. PMIPv6 Networks suffer from more number of attacks that can be avoided from by using a secure password authentication mechanism (SPAM). SPAM provides high security properties, including anonymity, locality privacy, correlated authentication, faking attack resistance, speed error detection, no clock synchronization problem, scarf-verified attack resistance, alteration attack resistance, replay attack resistance, and session key agreements .

In this paper, we have to proposed a new algorithm called ticket based algorithm it performs fast re-authentication method for supporting the global access technique. This ticket based scheme integrates with the SPAM technique, which reduces the mobile node's computational cost. It allows mobile terminal to use single ticket for fast re-authentication to their neighbor Mobile Access Gateway (MAG). The mobile node (MN) receives the handover ticket as a proof of authorization in authentication server and gives this corresponding ticket while associating with new MAG.

The proposed algorithm also reduces the handover delay during the re-authentication phase to delay of 2-way handshake between an Mabile Access Gateway and Mobile Node. Comparing with other algorithms , this gives fewer burdens while satisfying PMIPv6 security requirements that results in the reduction of mobile terminal's computation cost and authentication steps. It also provides an efficient key management scheme for secure group communications in PMIPv6 networks. The System architecture can be shown in Fig 2.

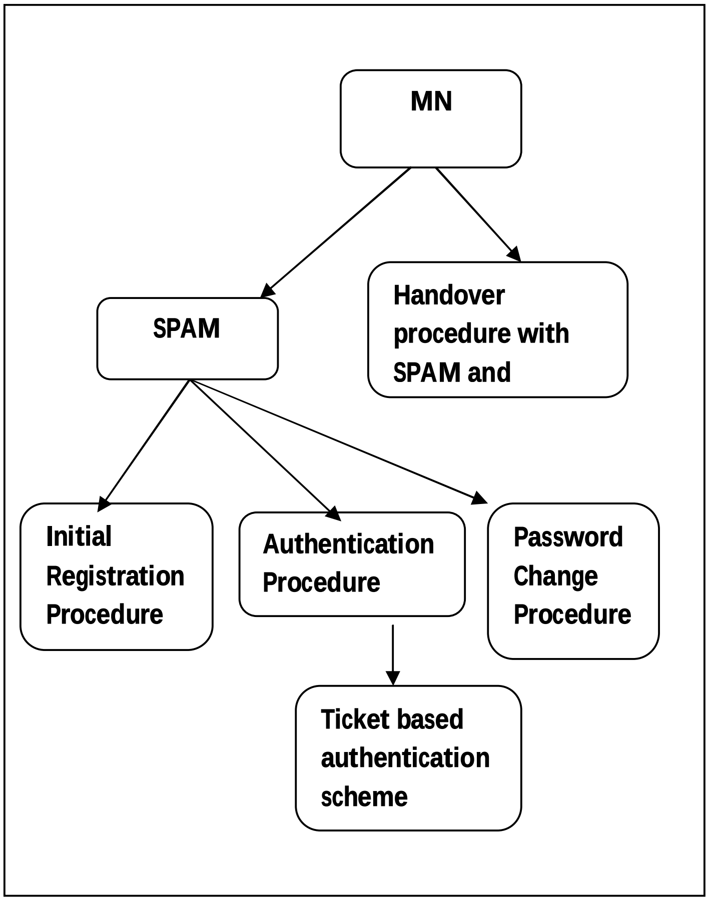
MN
SPAM
Handover procedure with SPAM and
Initial Registration Procedure
Authentication Procedure
Password Change Procedure
Ticket based authentication scheme

Fig 2: System Architecture

A. Assumptions

The main assumption of this paper is that the MAG, LMA and AAA have the protection links by using Internet Key Exchange Protocol version 2. Therefore, they can use pre-shared symmetric key to support the authentication procedure.

B. Bi-casting technique

The Bi-casting technique helps to avoid some problems such as packet loss and out-of-sequence problems. The authentication procedure performing at the AAA server results in increased handover latency and also the workload increased within many of the mobile node change to the efficient MAG location frequently. By the integration of secure password authentication mechanism in handover procedure. The handover latency would be reducing.

In addition to this bi-casting technique help to prevent the loss of packet during sending and receiving. The bi-casting procedure commences when the sever MAG sends an initial handover proxy message to the target MAG which was encrypted by a symmetric key. The target MAG decrypts the message and starts to buffer the packet to in order to avoid the packed loss. The target MAG sends an encrypted message to the LMA at that the verification process can be done. If it is success then the LMA replies with the encrypted message to the target MAG. If it is not success then the process can't be run further. The extra signaling message was not transmitted from the LMA to the target MAG because it piggybacks the data packets.

The LMA was verified by the target MAG for the mutual authentication and it replies with an acknowledgment message to the server MAG. The mobile node sends a message to the target MAG that piggybacks all the information that are authentication after which a global authentication was performed by the target MAG. The target MAG encrypted the message with the help of the session key and sends it to LMA which replay with the PBA message to the target MAG. The encrypted message was finally send the mobile node after verification.

C. Piggyback mechanism

The piggyback mechanism helps to reduce the signaling overhead. When the mobile node send the RS message to the target MAG. the piggyback mechanism piggyback the message that are authenticated. The target MAG after the successful verification of the encrypted PBA message send the RA message to the mobile node which piggybacks the authentication result.

D. Ticket based Algorithm:

The proposed algorithm is composed of two parts that are initial registration procedure and authentication procedure.

1. **Notations**: The notations used throughout this paper are listed in Table I.

Symbol	Description
PW_{MN}	Password of MN
ID_{MN}	Public Identification of MN
MN_{mac}	MN's MAC address
E_k	MAG's and AAA pre-shared group key
T	A Validity time for the handover ticket
HT_{MN}	A Handover ticket for MN to use for handover to their neighbor MAG's
r_{MN}	A random number generated by MN
MIC_{MN}	A Message Integrity Code for MN and MAG to authenticate each other
PTK	A Session key uses between MN and MAG
PRF	Pseudo Random Functions
ID_{MAG}	Public Identification of MAG
Sk_{i-j}	Session key between entity i and j
$E_{ski-j}(M)$	Message M is encrypted Using Session key Sk_{i-j} with symmetric Cryptography
h()	Collision free one way hash function
N_i	Nonce or random number i
PSK	Secure pre shared symmetric Key among legal MAGs and the LMA
$\oplus$	XOR operator
||	Combination of Strings
PMK	Pair wise Master Key

Table 1: Notations

2. Initial Registration Procedure

Before an MN joins in a localized mobility domain, it needs to perform the initial registration procedure with the AAA server via a secure channel. The steps of the procedure are described as follows:

1. First MN sends the ID and Password to the AAA server.
2. The AAA server stores this information and generates the handover ticket.
3. The AAA server sends both information includes ID_{MN} and ticket send to the MN and at the MN side it stores the information in the smartcard.

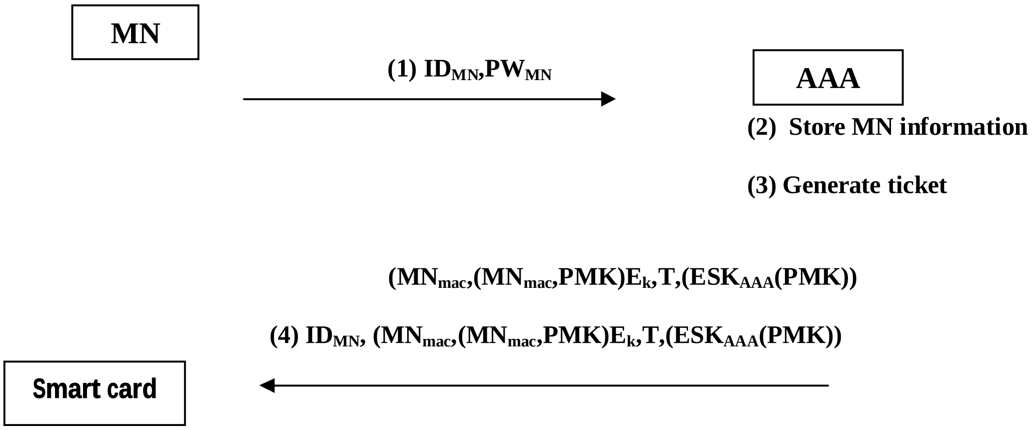
MN
(1) ID_{MN},PW_{MN}
AAA
(2) Store MN information
(3) Generate ticket
(MN_{mac},(MN_{mac},PMK)E_k,T,(ESK_{AAA}(PMK))
(4) ID_{MN}, (MN_{mac},(MN_{mac},PMK)E_k,T,(ESK_{AAA}(PMK))
Smart card

Fig 3: Initial registration procedure

3. Authentication Procedure

This section contains two parts. In Part 1, the mutual authentication between the MN and the MAG. This authentication process is executed between the MN and MAG by using the ticket. Fig 4.shows the authentication process of the Part I.

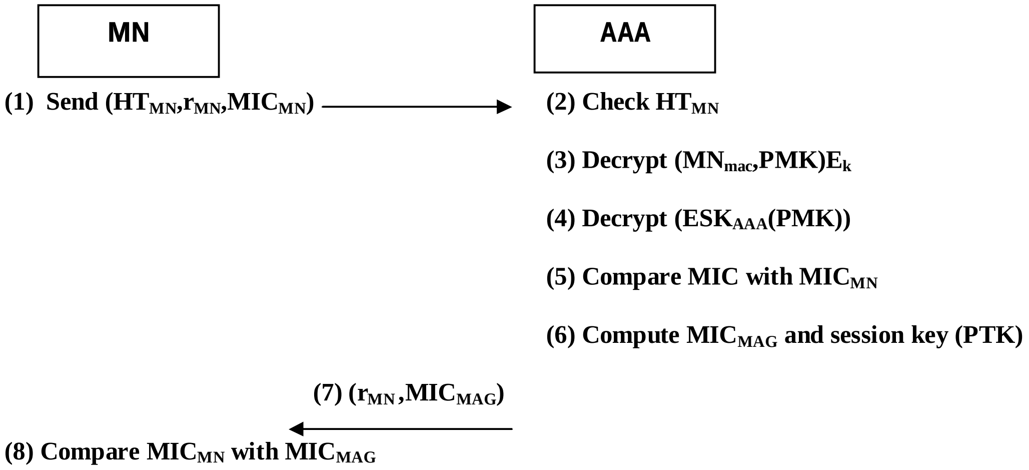
MN
AAA
(1) Send (HT_{MN},r_{MN},MIC_{MN})
(2) Check HT_{MN}
(3) Decrypt (MN_{mac},PMK)E_k
(4) Decrypt (ESK_{AAA}(PMK))
(5) Compare MIC with MIC_{MN}
(6) Compute MIC_{MAG} and session key (PTK)
(7) (r_{MN} ,MIC_{MAG})
(8) Compare MIC_{MN} with MIC_{MAG}

Fig 4: Part 1- Mutual Authentication between the MN and the MAG

Whenever the user wants to access the services, she or he inserts the smart card to the card reader and enters the ID and password of MN. The smart card checks whether it is valid or not if it is valid then MN sends re-authentication request to MAG include (HT_{MN},r_{MN},MIC_{MN}).

After receiving the authentication request by MAG then it first checks HT_{MN} ,T is in a validity time or not, if it is valid then uses the MAG and AAA pre-shared group key to decrypt(MN_{MAC}(PMK))to get PMK ,after that compare PMK is identical or not ,if it is identical its indicates handover ticket is issued from AAA server.

Afterwards compare MIC with MIC_{MN} ,if they are identical it indicates MN is a legitimate MN, then computes MIC_{MAG} and session key (PTK),after that sends re-authentication response(r_{MN} ,MIC_{MAG})to the mobile node. After MN receives (r_{MN},MIC_{MAG}) comparing MIC_{MAG} with MIC_{MN} , MAG, if they are identical it indicates that MAG is a legitimate MAG, MN computes PTK for communicating with MAG.

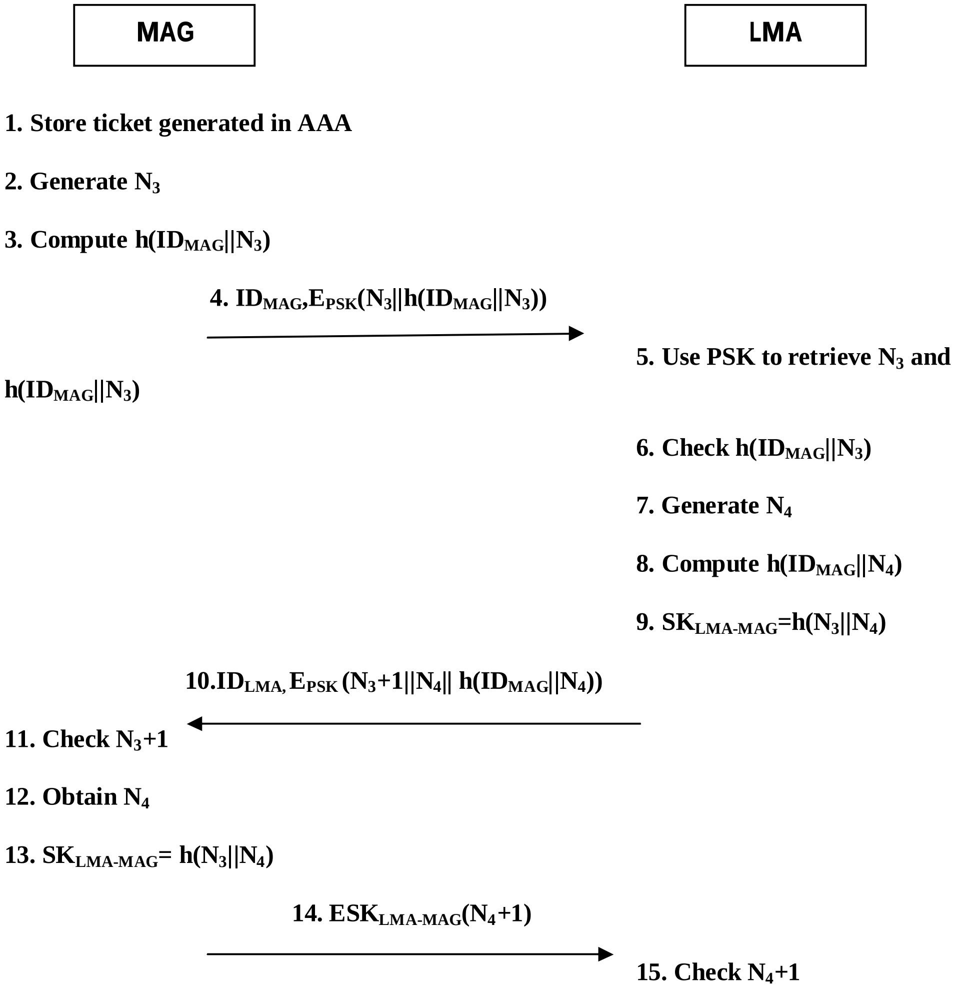
MAG
LMA
1. Store ticket generated in AAA
2. Generate N_3
3. Compute $h(ID_{MAG}||N_3)$
4. ID_{MAG},$E_{PSK}(N_3||h(ID_{MAG}||N_3))$
5. Use PSK to retrieve N_3 and
$h(ID_{MAG}||N_3)$
6. Check $h(ID_{MAG}||N_3)$
7. Generate N_4
8. Compute $h(ID_{MAG}||N_4)$
9. $SK_{LMA\text{-}MAG}=h(N_3||N_4)$
10.ID_{LMA}, E_{PSK} $(N_3+1||N_4||\ h(ID_{MAG}||N_4))$
11. Check N_3+1
12. Obtain N_4
13. $SK_{LMA\text{-}MAG}= h(N_3||N_4)$
14. $ESK_{LMA\text{-}MAG}(N_4+1)$
15. Check N_4+1

Fig 5: Part 2 – Mutual Authentication between the MAG and the LMA

In Part 2 the mutual authentication between the MAG and LMA it shows in Fig 5. The MAG generates the nonce and computes the hash function. This encrypted message send to the LMA, then the LMA is decrypted this message and compared it. This two messages are equal means it generates the nonce otherwise it drops the message. Again LMA replies to the MN it contains ID of LMA, and the encrypted message. After receives the message then MN decrypts the encrypted message send by the mobile node, if the result is same MN calculates the session key then the MN using that session key and generates the encrypted message to the LMA. The LMA uses the same symmetric key to decrypt the message and provides the nonce value to avoid unacceptable MAG executing replay attack.

4. Handover Procedure by using Ticket Based Algorithm and Bicasting Scheme

The following procedure explains the handover process by using the ticket based scheme in PMIPv6 networks. Here the purpose of this algorithm is to provide global access instead of using local authentication and the bi-casting scheme is used to avoid the packet loss and out-of-sequence problems.

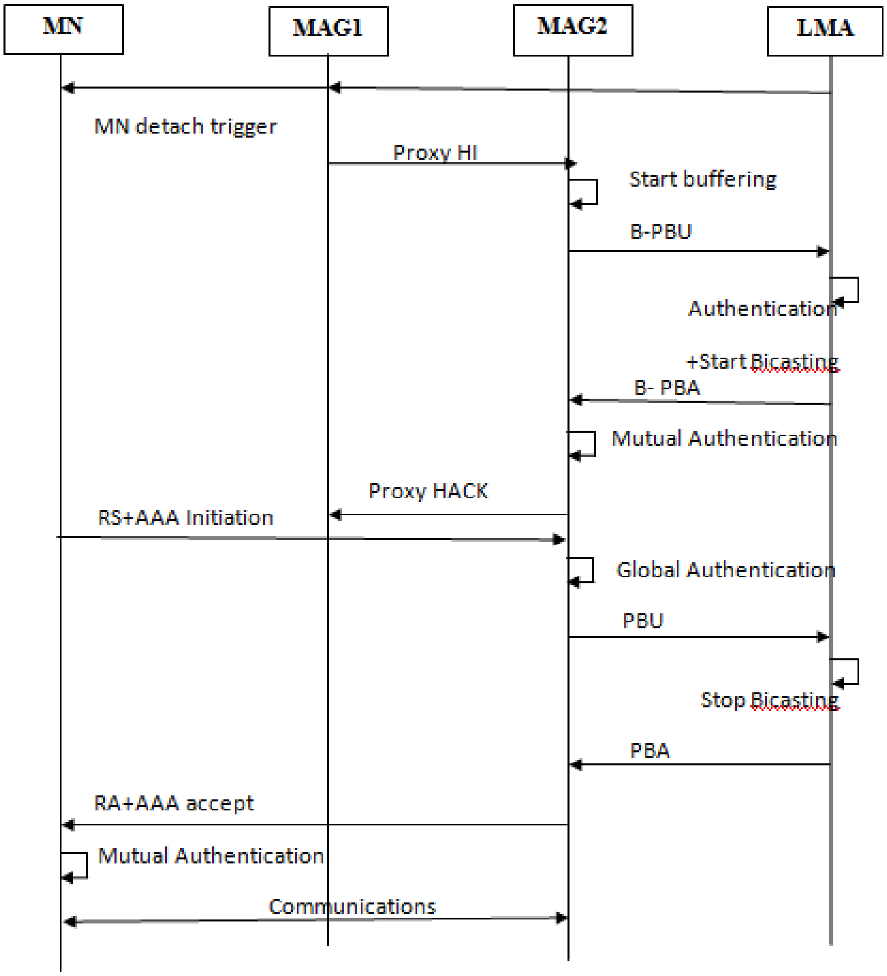

Fig 6: Handover process with Ticket based and Bicasting scheme

HI – Handover Initiation
PBU – Proxy Binding Update
PBA – Proxy Binding Acknowledgement
HACK – Handover Acknowledgement
RS – Router Solicitation
RA – Router Acknowledgement
Fig6. Describes the handover procedure is as follows:
Firstly MAG was detecting the MN range whenever the MN to leave the range of the serving MAG (i.e. MAG1).

Step 1: MAG1 (serving MAG) sends a proxy HI message to the MAG2(target MAG) , this message includes the ID of MN, and pre-shared symmetric key.
Step 2: MAG2 decrypts the message which can be received from the MAG1 and starts the buffering to avoid the packet loss.
Step 3: MAG2 sends the encrypted message i.e. (E_{PSK} (B-PBU||N_3||h (N_3||ID_{MAG}))) to the LMA.
Step 4: LMA verifies MAG2 (in part 2 of Fig 5) and generates the session key and also stores the binding table entry of the mobile node. Afterwards the LMA builds the bicasting tunnel between the LMA and the MAG2. The LMA starts to transmit the packet to both MAG1 and MAG2.
Step 5: LMA sends the encrypted message (E_{PSK} (B-PBA||N_3+1||N_4||h(N_4||ID_{LMA}))) to the MAG2. The B-PBA message is used to avoid the signaling overhead messages from LMA to MAG2.
Step 6: The MAG2 verifies the LMA (in part2 of fig 5) for the mutual authentication, and MAG2 Calculates the session key $SK_{LMA\text{-}MAG.}$
Step 7: MAG2 replies the MAG1 (Proxy HACK) encrypted message by the pre-symmetric key.
Step 8: MN sends the RS message which includes the (AID_{MN}, E_{C4} (R_S||$AUTH_{MN}$||N_1)to the MAG2 and it is attached to the MN.
Step 9: MAG2 performs the global authentication procedure and the detailed process explained in Part 1 of Fig 4.
Step 10: MAG2 sends the BPU encrypted message by using session key $SK_{LMA\text{-}MAG}$ to the LMA.
Step 11: LMA decrypts the BPU message and stops the bicasting also refreshes the binding entry of MN.
Step 12: Again the LMA replies an encrypted PBA message to the MAG2.
Step 13: The MAG2 verifies the PBA message and send the RA message to the MN.
Step 14: On receipt of RA message, the MN authenticates the MAG for achieving the mutual authentication. Detailed processes are described in part 1 of Fig 4. If the MN is same in Localized Mobility Domain (LMD) it retains the original address, otherwise MN configures the global IPv6 address from the Host Network Prefix (HNP) auto configuration procedures. Then MN generates the session key $SK_{MN\text{-}MAG}$ for secure communication.
Step 15: MN communicates with the MAG2 with low handover latency, low computational cot and avoids the packet loss problem.

E. key Management

Key management has set of techniques and other procedure support for establishing a strong and secure relationship between the authorized parties. The key management is provided with the security policy that defined the threats of the system either explicates or implicit.

The security policy may affect the cryptographic requirements of the system based on the environment of the susceptibility. The security policy specific some procedures to be carried out for the technical aspect of the key management which involves the security of each parity involved. The digital signature which provides the authentication of data is valid if and only if the private key of the user is maintained security.

6. ANALYSIS

The following results are obtained by using a tool called ns2 (Network Simulator Tool).

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:

$$\begin{aligned} HL_{SPAM} &= t_{L2} + t_P + t_R + t_{RS/RA} \\ &= t_{L2} + t_P + 2t_{MN\text{-}MAG} + \\ &\quad 2t_{LMA\text{-}MAG} + t_{MAG\text{-}AAA} \end{aligned}$$

In above equation, we supposed that

t_{L2}= handover latency of layer 2.
t_p=authentication procedure processing latency.
t_R= registration latency.
$t_{RS/RA}$ = latency for RS and RA messages.
$t_{MN\text{-}MAG}$ = wireless propagation delay between MN and MAG.
$t_{LMA\text{-}MAG}$ = propagation delay between LMA and MAG.
$t_{MAG\text{-}AAA}$ = propagation delay between MAG and AAA server.

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.

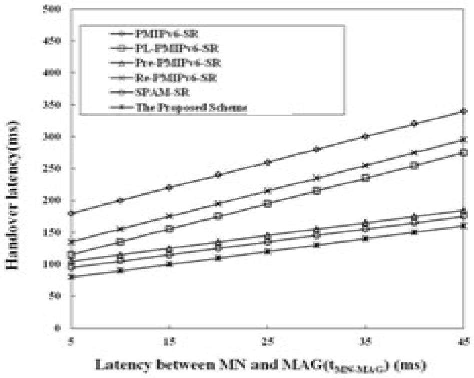

Fig 7. Handover latency versus $t_{MN\text{-}MAG}$ latency.

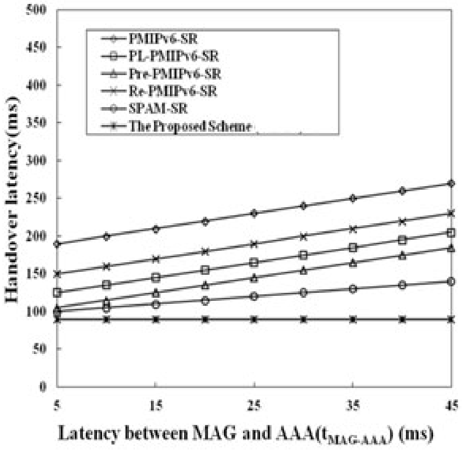

Fig 8. Handover latency versus $t_{MAG\text{-}AAA}$ latency

Fig.7 shows the handover latency versus latency between MN and MAG. The results demonstrate that if latency is increased between MN and MAG, the SPAM has lower handover latency than existing schemes. In Fig. 8 shows 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 SPAM. Thus, in terms of handover latency SPAM performance is more efficient than other schemes.

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. The FF mobility model is adopted to distribute the movement direction of MN uniformly in the range of (0, 2 π). The crossing rate for subnets (MAG and LMA) is computed as follows:

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

In the above equation, μ represents unit of transmission cost for wired link, λ represents unit of transmission cost for wireless link, n represents total number of MAGs in a domain, the other network parameters such as n, $D_{MAG-MAG}$, and etc.are considered as variables.

The values for different parameters are set as: d=.00314(MNs/m2), l =100m, $\mu = 1$, $\lambda = 2$, D_{MN-MAG} = 1 hop, $D_{MAG-MAG}$= 1 hop and $D_{MAG-LMA=}$ 1 hop.

Fig 9: shows 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 globally and AAA server is excluded.

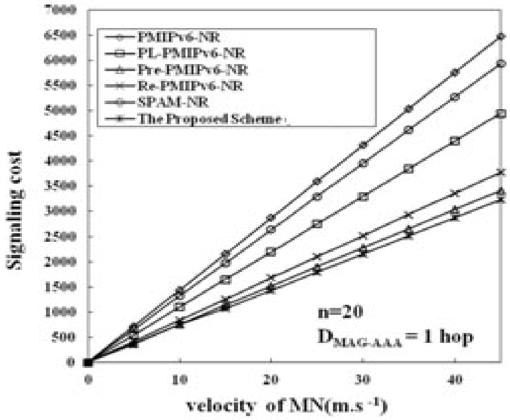

Fig 9. Signaling cost versus velocity of MN ($D_{MAG-AAA}$ = 1 hop).

3) Packet loss

In Fig. 10 and Fig. 11, 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. The SPAM uses buffer and local mutual authentication without the inclusion of AAA server, which helps in avoiding the issue of packets lost completely.

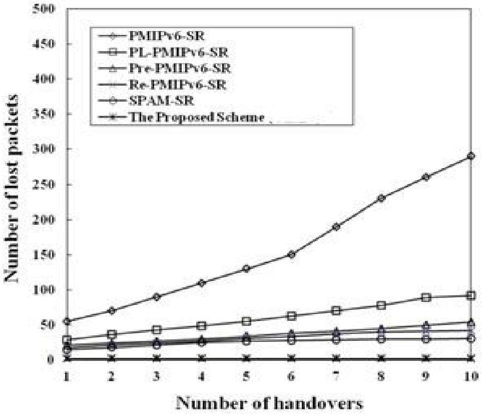

Fig 10. Packet loss versus number of handovers (# of target MAG =1).

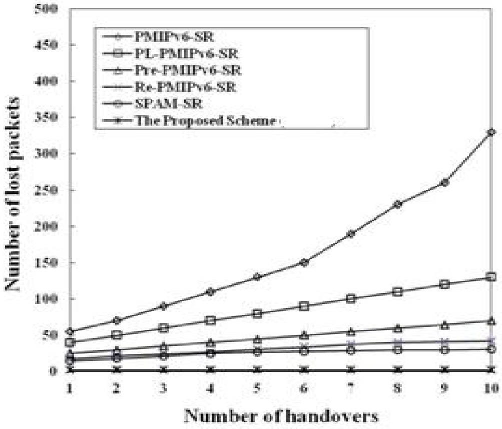

Fig 11. Packet loss versus number of handovers (# of target MAG =5).

4) Computational Cost

Earlier days we have to use some public key schemes to reduce the computational cost that can be araised as a part of communication between the mobile devices . But Now a days these schemes such as asymmetric cryptosystem and RSA algorithm are not suitable to be implemented in mobile devices. Because they cannot afford high computational load due to limited resources of energy and computing capabilities. So our proposed scheme uses symmetric cryptographic and hash operations to make it cost effective and simple for implementation in mobile devices. The existing schemes are 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.

7. CONCLUSION

This paper proposed a secure handover mechanism In PMIPv6 Networks that Combined with Group Key Ticket based fast re-authentication protocol which helps to reduce the mobile terminal computational cost and also authentication steps. It allows mobile terminal to use one ticket without storing lots of tickets that results in fast re-authentication to the neighbor MAG's and free from PMK different problem. Thus the proposed scheme makes MN and MAG authenticating each other that become more facilitate and flexible. SPAM should be able to meet the security requirements for the network. In addition to that the key management should be able to provide the secure data communication from the source to destination. The work should be further proceeded to handle the security issue of in mobility management over some complex environment and using of cryptanalysis technique for providing the robust security system in that network.

REFERENCES

1. Ming-Chin Chuang, Jeng-Farn Lee, Meng-Chang Chen SPAM: A Secure Password Authentication Mechanism for Proxy Mobile IPv6 networks, Vol.7, NO.1, MARCH 2013.
2. 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 its Applications, 2012, pp. 348-353.
3. 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.
4. 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.
5. F.Xia and B.Sarikaya, "Mobile node agnostic fast handovers for proxy mobile IPv6," IETF Draft, Nov 2007.
6. 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.
7. M.C. Chuang and J. F.Lee, "A lightweight mutual authentication mechanism for network mobility in IEEE 802.16e wireless networks," Compute. Net., vol.55, no.16, pp.3796–3809, Nov 2011.
8. 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. Compute. Sci. Its Applica. 2008, pp. 47– 51.
9. J.Lei and X.Fu, "Evaluating the benefits of introducing PMIPv6 for localized mobility management," in Proc., IEEE Int. Wireless Comm. Mobile Compute. Conf.,Aug.2008pp.74–80.

10 .J.Guan, H.Zhou, W. Xiao, Z.Yan, Y.Qin and H.Zhang, "Implementation and analysis of network-based mobility management protocol in WLAN environments," in Proc. ACM Mobility Conf. Mobile World Workshop, Sep. 2008,pp.1–9.

11. F.Xia and B.Surabaya, Mobile Node Agnostic Fast Handovers for Proxy Mobile IPv6, IETF Draft, Draft-xianetlmm- fmip-mnagno-02, Nov. 2007.

AUTHORS

K. Mayuri received the B.Tech degree in Computer Science and Engineering from the Department of CSE, Narayana Engineering College affiliated to JNTUA, Guduru , Andhra Pradesh, in 2012. She is currently doing M.Tech degree in Computer Science from the Department of Computer Science and Engineering, Sree Vidyanikethan Engineering College, Tirupati , Andhra Pradesh, during 2012-2014.Her current research interests include network security, mobility management and cloud computing.

K.S. Ranjith received the M.E degree in Computer Science from the Department of Computer Science and Engineering, Hindustan Institute of Technology and Science, Hindustan University, Chennai, 2012. He is currently Working as an Assistant Professor in CSE Department at Sree Vidyanikethan Engineering College, Tirupati , Andhra Pradesh. His current research interests include Software testing, network security and mobility management.