INTERNATIONAL JOURNAL OF RESEARCH IN COMPUTER APPLICATIONS AND ROBOTICS
ISSN 2320-7345

AUTHENTICATION MECHANISM FOR FAST HANDOVER PMIPv6 NETWORKS

N.S.Nandhinee
PG Student
Department of Computer Science and Engineering,
Easwari Engineering College,
Chennai, India,
nandhineeshanmugam@gmail.com

S.Kayalvizhi
Professor
Department of Computer Science and Engineering,
Easwari Engineering College,
Chennai, India,
kayalnaag@yahoo.co.in

***Abstract*—The Internet Engineering Task Force (IETF) proposed a host-based mobility management protocol, called Mobile IPv6 (MIPv6) protocol for mobile nodes (MNs) to maintain continuous service when they move among different foreign networks. However, Mobile IPv6 does not provide good service for real-time applications because it causes longer disruptions when the handoff takes place. Recently, the IETF NETLMM working group developed a network-based localized mobility management protocol called Proxy Mobile IPv6 (PMIPv6) to reduce the handoff latency of MIPv6. PMIPv6 still suffers from packet loss problem and signaling overhead. This paper performs a Bicasting scheme to reduce packet loss, use the piggyback technique to reduce the signaling overhead, ticket based authentication scheme for supporting the global access techniques, also provides Authentication mechanism for protecting valid user from attacks in PMIPv6 networks.**

***Keywords*—Authentication, bicasting, handover, piggyback, Proxy Mobile IPv6 (PMIPv6)**

1. INTRODUCTION

As wireless technologies have grown, all the people want to use wireless networks while moving from one place to another. At the same time Mobile MIPv6 was developed by the internet Engineering Task Force (IETF) to support the Mobile Node. Even after introducing the Mobile IPv6 Mobile Nodes (MNs) did not receive any data packets when it performs the handover that involves , IP address configuration, movement detection and location update latencies. To reduce the handover latency, Fast Handover has been developed. Fast handover performs the movement detection and IP address whenever the Mobile Nodes move from one location to another. Therefore Fast handover protocol reduces the handover latency.

However , MIPv6 cannot satisfy all the requirements of real time applications such as video streaming service and voice over internet protocol (VoIP) service due to its high handover latency. To address this problem, the Internet Engineering Task Force (IETF) NETLMM working group developed a network based localized mobility management protocol called Proxy Mobile IPv6 (PMIPv6) to reduce the handoff latency of MIPv6.Moreover, PMIPv6 provides the IP with the mobility to support MNs without requiring its participation in any mobility-related signaling.

Although PMIPv6 reduces lots of handoff latency compared with MIPv6, it still suffers from packet loss, signaling overhead and inefficient authentication procedure problems during handoff. This is because PMIPv6 does not use any

buffer mechanism during the handoff procedure and performs the authentication and registration phases separately. Therefore this paper used a bicasting scheme for packet loss problem and piggybacking technique for signaling overhead and also we are going to propose a ticket based authentication scheme for supporting the global access techniques.

2. RELATED WORKS

Chaung and Lee [2] proposed handoff schemes for PMIPv6 networks perform the authentication and registration phases separately, resulting in longer handoff latency.

A. Pre-Handoff procedure

The movements of an MN is detected using the MAG and it performs mobility-related signaling with the LMA in place of the MN. The pre-handoff phase starts only when the MN is going to leave the range of the serving MAG (i.e., MAG1). First, MAG1 sends a handoff initial (HI) message to the target MAG(i.e., MN-ID) and the address of the target MAG. Then , MAG2 sends back a handoff acknowledgement (HACK) message to MAG1, and then a bi-directional tunnel is built between MAG1 and MAG2. After the bi-directional tunnel is built , the buffer of MAG2 prepares to buffer.

B. Fast Handoff procedure

When the MN moves out of the transmission range of the MAG1, the MAG1 immediately starts sending the MN'S packets to MAG2 at the same time it buffers the packets to prevent from packet loss. After that MAG2 can start the authentication phase immediately. Now, MAG2 sends the AAA request which includes the profile of Mobile Node (i.e., MN-ID) to authenticate the MN and simultaneously sends the PBU message which piggybacks DeReg PBU message to refresh the binding cache entry of LMA. That is , the target MAG (i.e., MAG2) performs the registration phase on behalf of the Deregistration phase of previous MAG (i.e., MAG1).MAG1 stops the service and MAG2 takes the position of MAG2. Moreover, the authentication and registration phases are simultaneously performed so the executing time of these phases are overlapped. On receipt of the PBU message, the LMA sends a PBA message, which includes the HNP of the MN, deletes the old binding cache entry, establishes a new binding cache entry, and sets up a bi-directional tunnel between the LMA and new MAG (i.e., MAG2). Afterward through the new path the LMA transmits the packet to MAG2 and MAG2 buffers these packets for the MN. At the same time, the AAA server starts to authenticate. The MN sends the AAA response to MAG2. MAG2 also immediately sends an RA message to the MN when it detects the MN's attachment. After receiving the RA message, the MN checks the RA message for finding where the MN locates in. The MN retains the original address if the MN moves in the same LMD. Otherwise, the MN configures the global IPv6 address on its interface from the HNP. Finally, the MN downloads the buffered packets from MAG2.

Kim et al [4] The ERP exchange is not necessarily a full EAP method between the EAP peer and the EAP authenticator. It uses MSK sent from EAP server. In this paper, the EAP peer is the MN, the EAP authenticator is a Access Pointer (AP), EAP server is a AAA server and the LMA includes the AAA server.

A. EAP authentication in PMIPv6

The MN sends the EAP-Request/Identity to previous AP (p-AP) and receives EAP Response/Identity from the EAP authentication. After the AP performs the EAP method exchange using AAA protocol, it performs the EAP method exchange with the MN. In the case of successful authentication, a MSK is sent by the AAA server to the AP. TSK is made using the MSK after when the MSK is received. TSK is shared with the MN and the TSK is used for per-packet access enforcement by the MN.

B. Fast Handover scheme with ERP exchange in PMIPv6

In Proxy MIPv6, whenever the MN moves from its attachment AP to a new attachment AP within the Access Router, it delivers the MSK and performs the re-authentication process. However, the MN performs the Full EAP Method when the MN moves from one attachment MAG network to another new MAG network. In Fast Handover of PMIPv6, the MN performs the Full EAP Method. During Fast Handover period the full EAP method is delayed. The ERP Exchange scheme is used in Fast Handover of PMIPv6 to reduce the full EAP delay. In PMIPv6, Fast Handover schemes are under the propounded phase. Therefore we select the best Scheme of the Fast Handover schemes after the MN performs the Full EAP Method, MSK is received from EAP server and uses the MSK. When the movement of the MN is detected by p-AP, it sends a HO initiate message which includes the MN Identifier (MN ID), new-AP ID and the MSK to the p-MAG. The p-MAG sends a Fast PBU message to the LMA which also receives the HO initiate message. Note that the Fast PBU message includes the information of the HO initiate message. Once the LMA sends back the Fast PBA to the p-MAG it establishes a binding between the HNP which is assigned to the MN and its new PCoA. A Reverse PBU message is sent to the n-MAG by the LMA. The Reverse PBU message

consists of the MN ID, HNP of the MN used in the p-MAG, n-AP ID, and the MSK sent from the EAP server. The RA message consists of the HNP, and the MSK which is sent by the n-MAG. MN does not perform a new EAP Method and AAA (EAP Method) scheme when it performs fast handover. Therefore the MSK used in the n-MAG network can also be used in the p-MAG network and the MN is not necessary to complete EAP Method and AAA (EAP Method) between the AAA server and AP.

Ryu et al [6] PFMIPv6 to reduce the handover latency occurred in PMIPv6 . PFMIPv6 has two mode: one is the predictive mode and the other is the reactive mode.

The solution for handover is described in the following steps :

First: The MN reports the identifications of its own (MN ID) and the access point (New AP ID) to which the Mobile Node is most likely to move and also detects that a handover is immediate. The NMAG receives the HI from PMAG which is sent by it. The HI message must include the MN ID and should include the MN-HNP, the MN-ID and the address of the LMA that is currently serving the MN

Second: A bi-directional tunnel is built between the PMAG and NMAG and the packets decided for the MN are forwarded from the PMAG to the NMAG over this tunnel. The packets may be buffered at the NMAG after the decapsulation process. If the connection between the N-AN and NMAG has already been established, then those packets may be forwarded towards the N-AN.

Third: The MN establishes a connection (e.g., radio channel) with the N-AN, which in turn initiates the establishment of the connection between the N-AN and NMAG if it has not been established already. The NMAG starts to forward packets destined for the MN via the N-AN. The uplink packets from the MN are sent to the NMAG and the NMAG forwards them to the PMAG. The PMAG then sends the packets to the LMA that is currently serving the MN.

Final: The NMAG sends the PBU message to the LMA, in which address is provided in HI message from the PMAG to NMAG.

Ryu et al [5] Mobile IPv6 needs client functionality in the IPv6 stack of a mobile node (MN). Exchange of signaling messages between the MN and a home agent (HA) enables the creation and maintenance of binding between the MN's home address and its care-of address. Mobility as specified in Mobile IPv6 requires the IP host to send IP mobility management signaling messages to the HA, which is located in the network. MIPv6 is a approach of host-based mobility to solve the IP mobility challenge. However, it takes a very long time to process handover and there is much packet loss during handover, since there are many signaling messages through wireless link which occurs longer delay during handover process. Network-based mobility is another approach to solve the IP mobility challenge. By extending Mobile IPv6 signaling messages and reusing the HA it is possible to support mobility for IPv6 nodes without host involvement. This approach to support mobility does not require the Mobile Node to be involved in the exchange of signaling messages between itself and the Home Agent (HA). A Mobile Access Gateway (MAG) does the mobility management on behalf of the MN attached to the network and also performs the signaling with the HA . This protocol is known as Proxy Mobile IPv6 (PMIPv6) in Network-based Localized Mobility Management (NETLMM) working group of Internet Engineering Task Force (IETF). Since the proxy mobility agent on behalf of the Mobile Node performs handover process,PMIPv6 can reduce handover latency. That is, there are some signaling message via wireless link. Heavy packet loss occurs during handover in PMIPv6, although PMIPv6 reduces handover latency.This paper propose a Packet- Lossless PMIPv6 (PL-PMIPv6) with authentication to reduce the packet loss problem in PMIPv6. The similar kind of scheme was studied to reduce packet loss and handover latency in Mobile IPv6, such as fast handovers for MIPv6 (FMIPv6) . In PL-PMIPv6, a previous MAG (pMAG) registers to a Local Mobility Anchor (LMA) on behalf of a new MAG (nMAG) during layer 2 handoff. Then, during handover after registration nMAG buffers.

Compared to MIPv6 and PMIPv6, PL-MIPv6 can reduce more packet loss. To receive the MN's profile securely we use Also, we use Authentication, Authorization and Accounting (AAA) infrastructure to authenticate the MN and to receive MN's profiles securely. We show the performance of PL-PMIPv6 through the comparison of packet loss during handover of MIPv6, PMIPv6 and PLPMIPv6.

Authentication with Packet-Lossless PMIPv6 (PL-PMIPv6), to reduce packet loss in PMIPv6. The order of signaling flow in PMIPv6 is followed by PL-PMIPv6 and reduces packet loss. Once the pMAG is aware of the MN's detachment, it sends the DeReg PBU message to the LMA in PMIPv6. When pMAG sends the DeReg PBU message, nMAG's PBU message is included in DeReg PBU message in PL-PMIPv6. That is, the pMAG registers on behalf of the nMAG in advance to reduce handover latency. As a result, the tunnel between the nMAG and the LMA is built in

advance. Also, the nMAG begins to buffer packets to the MN after it receives the PBA message. After layer 2 handoff, the MN sends the RS message and receives the RA message including the MN's home network prefix.

3. NETWORK ARCHITECTURE

LMA	:Local Mobility Anchor
MAG	:Mobile Access Gateway
AAA	:Authentication, Authorization, Accounting server
MN	:Mobile Node
CN	:Correspondent Node
LMD	:Localized Mobility Domain
TBA	:Ticket Based Authentication Mechanism

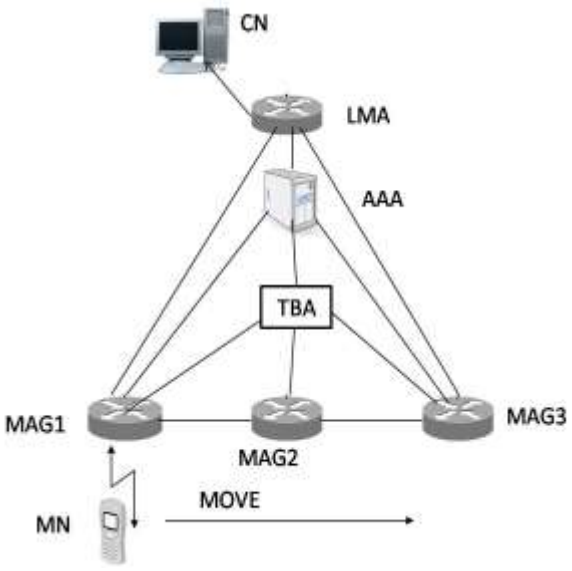

Fig. 1. Network Architecture for PMIPv6.

Fig. 1 clearly shows the network architecture of Proxy Mobile IPv6,this architecture consists of 3 network entities: the Local Mobility Anchor (LMA), the Mobile Access Gateway (MAG) and the Authentication, Authorization and Accounting server. The movement of the Mobile Node is detected by the MAG and also the MAG performs mobility related signaling in place of the MN with the LMA. LMA is nothing but the home agent in MIPv6 which maintains the binding cache entries for the registered MN's. The procedure of handover consists of three phases they are : deregistration , authentication and registration phases. In the deregistration phase the DeReg PBU message will be sent to the LMA by the previous MAG (i.e., MAG1) and then the overdue binding cache entry for MN is deleted by the LMA. In authentication phase, when the MN starts to move and gets attached to the new MAG that is MAG2 , the authentication process begins having the identity of the Mobile Node (i.e., MN-ID).In registration phase, once the authentication process is done, the new MAG will receive the profile of MN. To update the LMA, proxy binding update message (PBU) which contains the profile of MN is sent by the MAG. After receiving the PBU message the LMA will send back the proxy binding acknowledgement (PBA) message, creates the binding cache entry, which builds a bidirectional tunnel between the LMA and the new MAG.MN maintains the original address if it's movement is within the same LMD. Finally, packet is transmitted from correspondent node to the MN through the bidirectional tunnel between the LMA and the MAG.

4. PROPOSED MECHANISM

Although various researches proposed the fast handover schemes for reducing the handover latency, but they have not discussed about the security flaws in PMIPv6 networks. Our purpose is to intend an authentication mechanism. First we will see the authentication mechanism (AM) in detail then we incorporate authentication mechanism and bicasting scheme in the handover procedure for achieving the flawless handover. Also the previous paper did not discuss about the Ticket based authentication scheme.

A. Authentication Mechanism (AM)There are three procedures in proposed mechanism they are: service initialization, authentication procedure and the password change procedure.

1) Service Initialization: Before the MN enters the Localized Mobility Domain, it has to undergo registration process. The MN will send the public identification ID_{MN} and the password PW_{MN} to the AAA. AAA will store and send back these authentication parameters through the secure channel. In this the verification information need not be stored in the AAA and MAG and this process avoids the stolen verified attack.

2) Authentication Procedure: Whenever the MN attaches to a localized mobility domain or joins different nearby MAG's, the MAG starts the authentication procedure. The authentication procedure consists of two parts one is mutual authentication between MN and MAG another mutual authentication between MAG and LMA. Now the MN will enter the ID_{MN} and $PW_{MN.}$ It verifies and allows the MN to enter the LMD. Then the MN will send the authentication request to the MAG in the encrypted form and the MAG will decrypt it using the pre shared symmetric key. Then MAG will send back the authentication reply to the MN. Now the MN will send the encrypted message to the MAG. After this the mutual authentication between MAG and LMA takes place in the same way as it held between the MN and MAG.

3) Password change procedure: This procedure starts if the user wants to change the password. Only if the user gives the old or previous ID and password of the MN they can change it to new password.

B. Bicasting scheme and piggybacking technique: Bicasting scheme is used to reduce the packet loss problems. Packet loss occurs when the MN tends to leave the range and attaches to the new MAG. Whenever packet loss occurs the buffer will store all the sent packets and at the time of packet loss it can be re-transmitted. Piggybacking occurs when the MAG gets busy. If n number of requests sent from the MN and the MAG is busy serving other MN's means the packets will be shifted that is it piggybacks to the nearby MAG's.

C. Ticket based authentication technique: This is used when the server load gets increased. If suppose two MN's requesting the same MAG the MN which requested first will be given priority. Other MN's will be given ticket to arrange them in queue and get serviced by that particular MAG. The same credentials can be reused again in this technique. This will gradually decrease the load of the server.

5. ANALYSIS

A. Security Analysis

We now see the security features of Authentication Mechanism. This mechanism will satisfy the following security mechanisms.

1) Anonymity: The original ID of the MN is converted into alias which is based on nonce. Therefore an attacker cannot find the original identity of MN.

2) stolen verified attack: During authentication process the AAA and MAG's need not store or save the verification table. So that any type of an attacker cannot retrieve the authentication detail of MN's

3) Mutual authentication to prevent spoofing attack: First step here is the MAG verifies whether the MN is a valid user and at the same time the MN needs to verify that the MAG is not a forgery. Likewise LMA verifies whether the MAG is a valid MAG and at the same time LMA needs to verify that the MAG is not a forgery. In the procedure of handover, the LMA authenticates the MAG, MAG authenticates the LMA, MAG authenticates the MN, MN authenticates the MAG, respectively. Therefore this type of authentication procedure will prevent spoofing attack.

4) Modification attack resistance : Any attacker can try to modify the authentication message of the Mobile Node or MAG. But here in this paper we used a one way hash function so that information cannot be modified. Therefore this attack can be easily identified because the attacker cannot easily obtain the value of nonce.

B) Packet loss (PL)

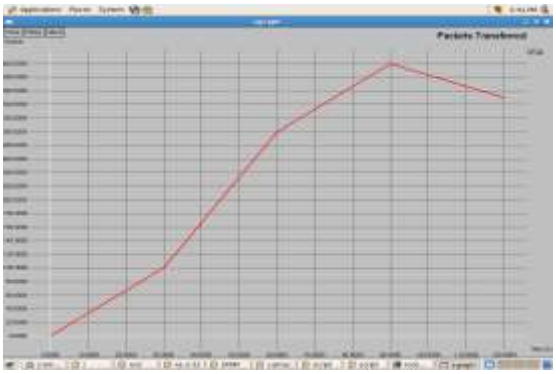

Fig. 2 . Performance of packet loss

Proxy Mobile IPv6 always loses many number of packets as it does not use a buffer mechanism in it. Eventhough building a bidirectional tunnel PL-PMIPv6 still loses some packets. Authentication mechanism uses buffer mechanisms and bicasting schemes to reduce the packet loss problem.

6. APPLICATION

1) Selective IP Traffic Offload Support with Proxy Mobile IPv6

2) Network-based Mobility Management in a local domain (Single Access Technology Domain)

3) Inter-technology handoffs across access technology domains (Ex: LTE to WLAN, eHRPD to LTE, WiMAX to LTE)

4) Access Aggregation replacing L2TP, Static GRE, CAPWAP based architectures, for 3G/4G integration and mobility

7. ABBREVIATIONS

MN	Mobile Node
MIPv6	Mobile Internet Protocol Version 6
PMIPv6	Proxy Mobile Internet Protocol Version 6
MAG	Mobile Access Gateway
LMA	Local Mobility Anchor
PBU	Proxy Binding Update
HO	Handover
HNP	Home Network Prefix
EAP	Extensible Authentication Protocol
ERP	Extensible Re-Authentication Protocol
nMAG	New MAG
pMAG	Previous MAG

8. CONCLUSION

Fast handovers are transferring of ongoing calls from one channel to another without interruption. Here , Fast Handover analysis reduces the latency in sending the packets from one node to another. In this paper techniques like piggybacking is used to reduce the signaling overhead , bicasting scheme reduces the packet loss by storing all the packets in a buffer and whenever the packet is lost ,the packets are retransmitted from the buffer. Previous papers used only ID for

authentication process, this paper used a password authentication mechanism. The result analysis showed that these schemes provide a better solution than existing schemes.

9. REFERENCES

[1] Chowdhury K., Koodli R and Yokota H., (2010) 'Fast Handovers for Proxy Mobile IPv6', IETF Draft, draft-yokota-mipshop-pfmipv6-13 (work in progress).

[2] Chuang M.-C. and Lee J.-F., (2011) 'FH-PMIPv6: A fast handoff scheme in proxy mobile IPv6 networks', in Proc. IEEE CECNET,
pp. 1297–1300.

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

[4] Chung T.-M., Kim S.-D., and Lee J.-H., (2009) 'Secure fast handover scheme of proxy mobile IPv6', in Proc. IEEE Int. Joint Conf. INC IMS IDC NCM, pp. 555–558.

[5] Kim B., Kim G-Y, Mun Y. and Ryu s., (2008) 'A scheme to reduce packet loss during PMIPv6 handover considering authentication', in Proc. IEEE Int.Conf. Comput. Sci. Its Applicat., pp. 47-51.

[6] Kim M., Mun Y. and Ryu S., (2009) 'Enhanced fast handovers for proxy mobile IPv6' , in Proc. IEEE Int. Conf. Comput. Sci. Its Applicat. (ICCSA), pp.39-43.

[7] Zhang H. and Zhou H., (2008) 'An authentication protocol for Proxy Mobile IPv6' ,in Proc. IEEE Int. Conf. Mobile Ad-Hoc Sensor Network, pp. 129-136.