Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 46 (2015) 1064 – 1071

Procedia Computer Science

International Conference on Information and Communication Technologies (ICICT 2014)

Handover efficiency improvement in Proxy Mobile IPv6(PMIPv6) networks

Asiya Ahmad[a,*] , Deepthi Sasidharan[b]

[a,b]*Government Engineering College, Barton Hill, Trivandrum, 695035, India*

Abstract

The Internet Engineering Task Force proposed a Network based Local Mobility Management (NETLMM) scheme called Proxy Mobile IPv6(PMIPv6) to provide efficient mobility support for the IPv6 enabled nodes, without the involvement of the nodes themselves. Here the burden of maintaining the mobility is transferred from Mobile Nodes(MNs) to the networking architecture. But frequently moving MNs suffered from considerable latency and packet loss during handovers even within the PMIPv6 domain. The number of signalling messages required for handover was also high. A communication state dependent chaining scheme is used in this paper to meet these inherent drawbacks of PMIPv6 domain and is called the Chaining Based PMIPv6(CB-PMIPv6). Here the Mobility Access Gateways(MAGs) are chained to support movements within the PMIPv6 domain. Packet loss is mitigated by using a buffering scheme and handover latency is reduced with the help of a triggering scheme.

Peer-review under responsibility of organizing committee of the International Conference on Information and Communication Technologies (ICICT 2014)

*Keywords:*NETLMM; PMIPv6; AAA server; PBU; PBA

1. Introduction

The world is getting flooded with a large number of interconnected devices which demand seamless mobility. Not

* Asiya Ahmad: Tel +91 8089425245
Email aaasiyaa@gmail.com

Peer-review under responsibility of organizing committee of the International Conference on Information and Communication Technologies (ICICT 2014)
doi:10.1016/j.procs.2015.01.018

just the mobile phones, but each and every component in the day to day life including wrist watches, vehicles and body sensors are all showing the tendency to get connected to some or other networks[1]. IPv6 could meet the need

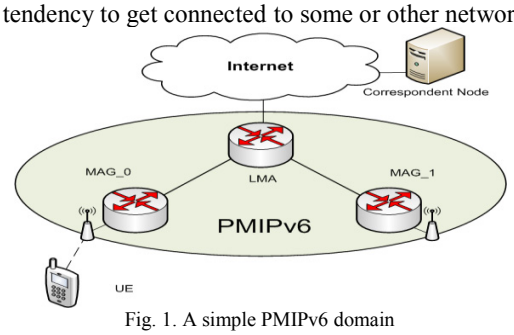

Fig. 1. A simple PMIPv6 domain

for assigning such a large number of IP addresses. Providing efficient mobility for such IPv6 nodes was the next challenge. Mobile IPv6(MIPv6) is a host based approach which could give a solution to this problem[2,3].

Though the introduction of MIPv6 was a milestone, it had a number of limitations. It suffered from great handover delay and packet loss. Moreover, heavy mobility signalling generated by the mobile nodes for each handover will consume the wireless access link to a great extend. The signal generation and processing will be an overhead for the mobile nodes and make them more complex. A mobility stack must be present in the MN and the MN needs to be upgraded for each updation in the mobility technology. Also the host based mobility management can not impose much control over the network since the MNs take the mobility decisions independently.

These limitations prompted the development of a Network based Local Mobility Management(NETLMM) approach. Proxy Mobile IPv6(PMIPv6) is the only NETLMM standardized by IETF[4]. PMIPv6 can be used for mobility support in campus networks, in telecommunication technology beyond 3G and also in 6LOWPAN(IPv6 over LOW power Personal Area Networks) technology. Local Mobility Agent (LMA) and Mobile Access Gateway (MAG) are the two integral parts of PMIPv6 domain. The functionality of LMA is similar to that of Home Agent(HA) of MIPv6[5]. But unlike HA, LMA can perform network-based mobility management. MAG acts on behalf of the MNs attached to its access link and performs the mobility related signalling. The structure of a single PMIPv6 domain is shown in fig.1.

MN needs to be authenticated by the AAA server each time it gets attached to a new MAG within the PMIPv6 domain. After successful authentication, MAG starts to act on behalf of the MN and performs the MN registration with the LMA. A Proxy Binding Update(PBU) message is used for this purpose. On receiving the PBU message, the LMA will update its Binding Cache Entry(BCE) table with the details of the MN. Then a Proxy Binding Acknowledgement(PBA) message which contains the Home Network Prefix(HNP) will be sent back to the MAG. The MAG will advertise the HNP to the MN and the MN can configure its IP address using Stateless Address Auto Configuration(SLAAC). Each time the MN makes a handover from one MAG to another, the same HNP will be advertised to the MN thus making a feel that the MN is still roaming within the same network.

If an MN is moving frequently from one MAG to another MAG, then a large number of signals will be required for the location updation, even if the MN is in idle state(not participating in any communication). In order to overcome this, a pointer forwarding methodology named Chaining Based Proxy Mobile IPv6(CB-PMIPv6)is proposed. In CB-PMIPv6, MAGs within the domain are chained to reduce the LMA access for location updation[6]. Chaining will be performed only if the MN is in idle state(not participating in any communication). The maximum length up to which the chain can be prolonged is set as the threshold value. If the MN is busy, chain will not be prolonged, instead buffering mechanism will be initiated.

2. System description

2.1. Chain forwarding decision making

When the MN moves from the current MAG(cMAG) to the next MAG(nMAG), we have two options. First option is the obvious one, that is the new MAG will perform location updation with the LMA. The second option is to form a forwarding chain between the cMAG and the nMAG such that the nMAG needs not perform a location updation with the LMA[7]. The decision depends on the current length of the forwarding chain and the communication state of the MN. If the current length of the forwarding chain, i.e., CCL(Current Chain Length), has reached a threshold value, T, then the chain can't be prolonged. In this case, the nMAG should perform location updation. This is to ensure that the overhead involved in following a very long chain to deliver the message is avoided. Also if the MN is currently participating in a communication, chain will not be prolonged and location updation takes place. In all other cases, we can prolong the forwarding chain from the cMAG to the nMAG..

2.2. Chain forwarding decision making

A number of approaches are available for identifying the next MAG and triggering it to prolong the forwarding chain. The prominent one is to run a Neighbor Discovery(ND) algorithm and trigger all the MAGs present at one hop in advance. So that, all the next hop MAGs will be ready to receive the MN. But the problem here is that, a number of extra messages are required for neighbor discovery and triggering. Signaling overhead is increased considerably. In order to overcome this limitation, partial involvement of the MN is used to identify the next MAG. MN scans the available access links and identifies the best access link. The MN sends an indication message to the cMAG as soon as the signal strength of the cMAG goes below a threshold value. The message informs the cMAG about the nMAG. The indication message is sent before the current connection is lost. The current communication state of the MN and the current length of the forwarding chain can be obtained from this message.

2.3. Performing the handover

Each MAG in the CB-PMIPv6 will maintain a Pointer Table(PT). The three fields of the table are HNP(MN's HNP), PREVIOUS (CoA of the MN's previous MAG area) and NEXT(CoA of MN's next MAG area). The procedure for handover execution is shown below:

- When the MN attaches for the first time(let it be at MAG1), both the PREVIOUS and the NEXT fields will be NULL(Shown in fig. 2).
- If a handover indication message with MAG2 as the target MAG comes from the MN, (i.e., the MN is about to perform a handover to MAG2),
  - If the MN is idle and the CCL < T, (Forwarding chain can be prolonged)
    - MAG1 sends a PBU message to MAG2 mainly containing the MN's ID and MN's HNP.
    - MAG2 adds a new entry in its PT containing the MN's HNP, PREVIOUS field set to MAG1's ID and NEXT field set to NULL(Shown in fig. 3).
    - MAG2 replies to MAG1 with a PBA message.
    - Now, MAG1 updates its PT by setting MN's NEXT field entry to MAG2's ID(Shown in fig. 4). (Thus one hop chain forwarding is finished).
  - Else if the MN is busy or CCL=T,
    - MAG1 sends a PBU message to MAG2 mainly containing the MN's ID and MN's HNP.
    - MAG2 sends another PBU message to LMA for location updation.
    - But since MN is still connected through MAG1, LMA will add the details of the MN to its Binding Cache Entry(BCE) but with the status as DORMANT(Shown in fig. 5)
    - LMA sends PBA message to MAG2.
    - MAG2 sends an acknowledgement message(PBA) to MAG1.
    - Now MAG1 updates its PT with the NEXT field having the address of MAG2.

- Once the MN detaches from MAG1, all the packets destined to the MN(if the MN is currently communicating) will be forwarded to MAG2 and MAG2 will buffer those packets.
- When the mobile node is detected by MAG2, MAG2 sends another PBA message to LMA requesting to activate the MN's binding.
- LMA will deregister MAG1 and will set the status of binding of MN to MAG2 as ACTIVE(shown in fig. 6).
- MAG2 will deliver the buffered packets to the MN and thus handover delay and packet loss are mitigated.

2.4 Downstream packet forwarding

The packets from a CN will reach the LMA and the LMA forwards the packets to the most recently registered MAG. The current MAG may not have registered with the LMA yet. If the NEXT field value of the most recently registered MAG is null, then the packets are delivered to this MAG. Otherwise the packets will be forwarded as per the forwarding chain and finally will be delivered to the MAG with the NEXT field value null. This MAG will perform location updation with the LMA and the following packets will be delivered directly from LMA to this MAG.

HNP	PREVIOUS	NEXT
HNP1	NULL	NULL

Fig 2. PT entry of MAG1 when MN attaches for the first time

HNP	PREVIOUS	NEXT
HNP1	MAG1	NULL

Fig. 3. MAG2's PT entry after receiving PBU message from MAG1.

HNP	PREVIOUS	NEXT
HNP1	NULL	MAG2

Fig. 4. MAG1's PT entry after establishing chain to MAG2

HNP	CoA	STATUS
HNP1	MAG1	ACTIVE
HNP1	MAG2	DORMANT

Fig. 5. BCE of LMA before MN is detected by MAG2

HNP	CoA	STATUS
HNP1	MAG2	ACTIVE

Fig. 6. BCE of LMA after MN is registered at MAG2

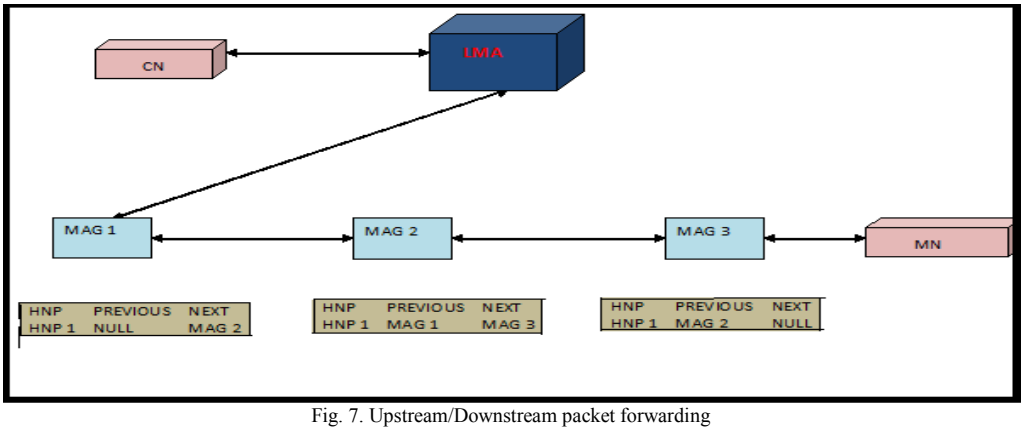

Fig. 7. Upstream/Downstream packet forwarding

2.5 Upstream packet forwarding

When an idle MN sends a packet to a CN, the packets will be routed in the reverse direction until the first registered MAG(i.e., the MAG with the PREVIOUS field set to null) is reached. Thus the packet will reach the LMA and thereby to the CN. At the same time this reverse routing is performed, the current MAG will contact the LMA, and will perform registration with the LMA. Once the registration is complete, the following packets from the MN will be delivered directly to the LMA from the current MAG. The upstream / downstream forwarding technique is shown in fig. 7.

2.6 Avoiding frequent AAA registrations using modified PBUs.

Each time the MN changes the MAG, AAA server needs to be contacted to identify and authenticate the MN. Even with pointer forwarding, authentication is required multiple times. If the decision is to prolong the chain from previous MAG(pMAG) to next MAG(nMAG), as soon as the MN is detected by nMAG, nMAG authenticates the MN before establishing the chain with pMAG. This is to ensure that the MN has already registered with the PMIPv6 domain and has the privilege to use the domain service. This gives rise to performance degradation, since AAA server access time can increase the total handover latency even if the decision is to prolong the chain. The problem becomes more severe if the PMIPv6 domain size is considerably large and the AAA server is located at a distance. Moreover, the load at AAA server goes up if the MN is frequently moving. The AAA server can become a bottleneck in chaining the MAGs. Incorporating certain authentication functionalities with the MAG can mitigate the problem. i.e., a light weight localized AAA server can be placed at each MAG. The authentication procedure can be classified in to two. When the MN attaches with the domain for the first time, it undergoes a lengthy authentication procedure and the MAG associated with the MN should contact the AAA server. But, if the MN is changing the point of attachment from one MAG to another MAG within the same domain, it needs to undergo only a simple re-authentication procedure. This light weight procedure doesn't demand the involvement of the AAA server. This can be achieved by using a token based encryption scheme[8]. Here a ticket will be issued to the MN at the time of initial authentication and this ticket can be presented to the subsequent MAGs for further authentications. Therefore the authentication procedure becomes very fast and signaling overhead and network traffic get mitigated. The load at AAA server is also reduced considerably.

2.6.1 Assumptions:

The various assumptions taken while performing the token based authentication are :

- The MN and the AAA server(AS) share a symmetric key and is called $K_{MN,AS}$
- The MAG and the AS share a symmetric key and is called $K_{MAG,AS}$
- Each MAG shares one symmetric key each with each of the neighbouring MAGs. Its denoted by Kp_{MAG},n_{MAG}
- A proper synchronization mechanism is used to make sure that the clock at each MAG is synchronized.

2.6.2 Initial Authentication:

The following steps are performed when the MN attaches with the PMIPv6 domain for the first time. The signal flow is given in fig. 8.

- AAA_Req1 : NAI_{MN} || NAI_{MAG} || Times || Nonce1
- AAA_Req2 : AAA_Req1 || Nonce2
- AAA_Reply1:NAI_{MN} || Ticket || $E(K_{MN,AS}[K_{MN,MAG}$ || NAI_{MAG} || Nonce1]) || $E(K_{MAG,AS}[K_{Auth}$ || Times || Nonce2])
- AAA_Reply2 : NAI_{MN} || Ticket || $E(K_{MN,AS}[K_{MN,MAG}$ || NAI_{MAG} || Nonce1])
- Challenge : Ticket || Authenticator

- Response : $E(K_{MN,MAG}[NAI_{MN} \| Times \| Nonce3+1])$
- Ticket : $E(K_{Auth}[K_{MN,MAG} \| NAI_{MN} \| Times])$
- Authenticator : $E(K_{MN,MAG}[NAI_{MN} \| Times \| Nonce3])$

2.6.3 *Handoff Authentication:*

The following steps are performed when the MN makes a handover within the same domain. The signal flow is given in fig 9.

- Auth Mat is an encrypted message encrypted using the symmetric key shared between neighbouring MAGs. i.e., E(KpMAG,nMAG[KAuth,NAIMN,Timestamp]).
- Challenge and response messages are the same as that of initial authentication with the exception that nonce value is changed.

2.6.4 *Modified PBU messages*

The PBU messages transferred between the MAGs for chaining and fast handover purposes can be modified to support the handoff authentication. As soon as the MN indicates the handover from one MAG to another, the Auth Mat message needs to be transferred from the current MAG to the next. This information can be included in the PBU messages exchanged between the MAGs for chaining. Thus the existing tunnel for chaining purpose can be exploited to support local authentication and thus can avoid additional messaging and tunneling overhead.

2.6.5 *Double buffer mechanism:*

Two buffers are kept at each MAG. A LMA Packet Buffer(LPB) and a MAG Packet Buffer(MPB). LPB will buffer the packets from the pMAG at the time of a busy MN handover. The packets arriving in the time between the MN detachment with pMAG and attachment with nMAG are buffered by nAMG. These packets are buffered in MPB. Once the registration with LMA is complete, packets will start arriving from the LMA. These packets will be buffered in LPB. The packets from MPB will be delivered to the MN first. Then the packets from the LPB will be delivered. Thus better packet delivery can be obtained.

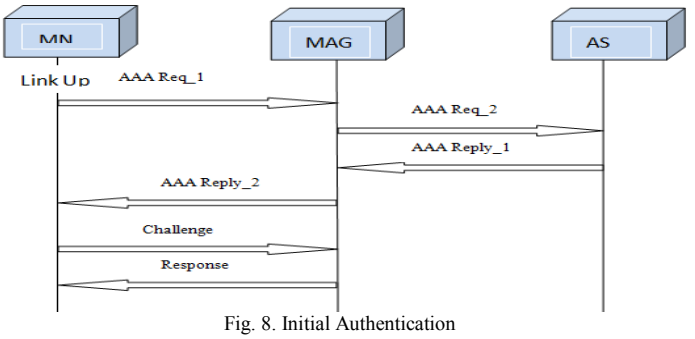

Fig. 8. Initial Authentication

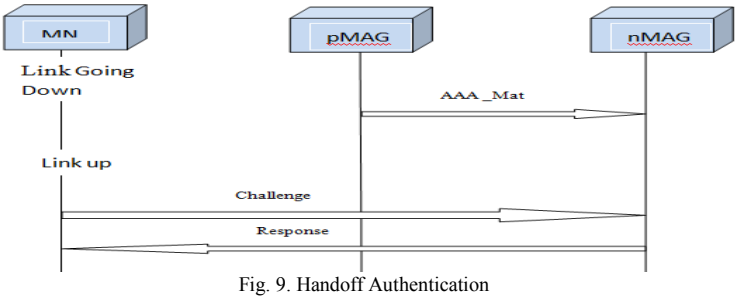

Fig. 9. Handoff Authentication

3. **Evaluation**

Performance of the proposed system is evaluated using the NS2 simulation tool. Handover latency is calculated using awk scripting and packet loss is calculated by writing code for calculation in .cc file itself. Number of additional messages required for authentication is calculated theoretically. The performance of 3 different systems are compared. First one is the basic PMIPv6 which is the base protocol. Second one is a simple chaining scheme in which MAGs are chained to minimize the number of LMA accesses. The third one is the CB-PMIPv6 which is our proposed system.

- Performance Metric 1 : Handover latency

The handover latency is calculated by considering the time difference between the detachment event from one MAG and the attachment event at the next MAG. The time at which detachment takes place is taken as the point of time when the pMAG's Binding Update List(BUL) is updated with MN detachment. Similarly, The time at which attachment takes place is taken as the point of time when the nMAG's Binding Update List(BUL) is updated with MN attachment. The delay is calculated for an idle MN handover as well as a busy MN handover and the average is taken. The comparison is shown in fig.10. Here the handover delay present in our proposed system is compared against basic PMIPv6 and existing simple chaining scheme.

- Performance Metric 2 : Number of additional messages required for authentication.

EAP-TLS is the authentication algorithm used in basic PMIPv6. Using EAP-TLS requires 8 messages in the wired link and 8 messages in the wireless link for each authentication, irrespective of if its initial authentication or handover authentication. In the proposed system, MIT's Kerberos version 5 is used for authentication. As can be inferred from Fig. 8, it requires only 4 messages in the wired link and 2 messages in the wireless link for initial authentication. For handoff authentications, 1 message and 2 messages are required in wired and wireless link respectively. This information can be obtained from Fig. 9. The only one message required in the wired link for handoff authentication can be avoided, by incorporating the information required for re-authentication in the PBU message itself. Thus the total number of additional messages required in the wired link for handoff authentication is zero. A comparison involving the number of additional messages required for authentication is given in Fig. 10.

Basic PMIPv6	Existing Chaining Scheme	Proposed System
0.355s	0.316s	0.264s

Fig. 10. Comparison of handover delay

	Initial Auth (Wired)	Initial Auth (Wireless)	Handoff Auth (Wired)	Handoff Auth (Wireless)
EAP TLS	8	8	8	8
Token Based	4	2	0	2

Fig. 11. Comparison of number of messages for authentication

- Performance Metric 3 : Packet drop.

Fig.12 shows a comparison of packet drop involved in basic PMIPv6, existing chaining method and the proposed system. The MN is performing a handover in busy mode between 1.2s and 1.6 s. Therefore the packet drop is higher during this interval when compared to rest of the time period. Basic PMIPv6 is having the maximum packet loss. Existing chaining algorithm could mitigate the packet drop to some extend. In the proposed system, the double buffering scheme and local authentication mechanism could help in further mitigating the packet drop.

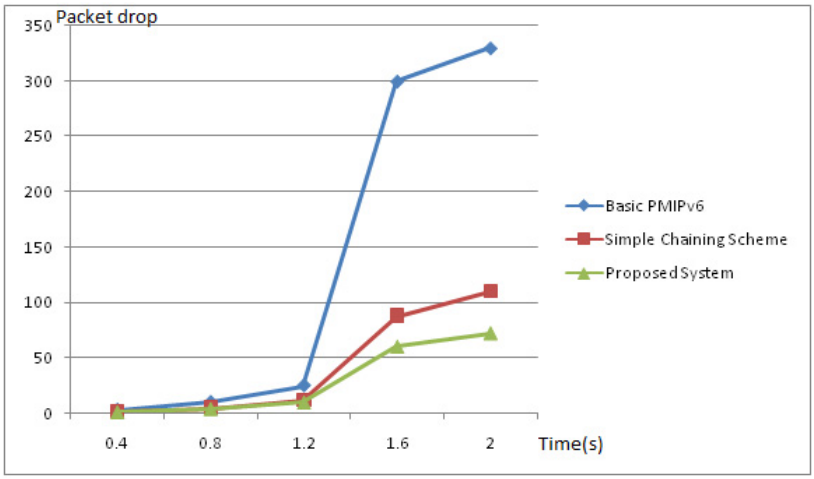

Fig. 12. Packet drop comparison

4. Conclusion

Incorporating a communication state aware chaining scheme and ticket based re-authentication mechanism in to basic PMIPv6 domain improved the handover performance to a good extend. Double buffering scheme could enhance the packet delivery. Simple and fast re-registration procedure during intra domain handovers reduced the number of AAA accesses and avoided the problem of AAA server bottleneck. This re-authentication procedure didn't require additional tunnel maintenance and message passing overheads since it can be incorporated in to the chaining mechanism itself.

References

1. Jinho Kim, Rim Haw, Choong Seon Hong, and Sungwon Lee. A 6LoWPAN Sensor Node Mobility Scheme Based on Proxy Mobile IPv6. *IEEE Transactions On Mobile Computing*; VOL. 11 December 2012.
2. Jong-Hyouk Lee, 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, NO. 3 March 2013.
3. Ki-Sik Kong, Wonjun Lee, Youn-Hee Han, Myung-Ki Shin, and Heungryeol Yu. Mobility Management FOR All-Ip Mobile Networks Mobile IPv6 vs. Proxy Mobile IPv6. *IEEE Wireless Communications*;April 2008
4. Sri Gundavelli, Kent Leung, Vijay Devarapalli, Kuntal Chowdhury. Proxy Mobile IPv6. *IETF Request for Comments 5213*;August 2008.
5. Ignacio Soto, Carlos J. Bernardos, and Mara Caldern, and Telemaco Melia. PMIPv6: A Network-Based Localized Mobility Management Solution. *The Internet Protocol Journal*; Volume 13, No.3
6. Myung-Kyu Yi, Jae-Young Choi, Jin-Woo Choi, Seok-Cheon Park, and Young-Kyu Yang. A Pointer Forwarding Scheme for Minimizing Signaling Costs in Proxy Mobile IPv6 Networks. *2013 IEEE Seventh International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing*.
7. Seung Yoon Park, Jae Young Choi, and Jong Pil Jeong . AMM-PF : Additional Mobility Management Scheme Based on Pointer Forwarding in PMIPv6 Networks. *Springer* 2013
8. Oong-Hee Lee, Jong-Hyouk Lee, and Tai-Myoung Chung. Ticket-based Authentication Mechanism for Proxy Mobile IPv6 Environment. *The Third IEEE International Conference on Systems and Networks Communications*.