

# PMIPv6 Handover in L3

Ms.Sridevi

Assistant Professor, Department of Computer Science, Karnatak University, Dharwad

## Abstract

*Mobile IP though allows mobility features to a node it suffers from signalling latencies which are mainly incurred due to the fact that the MN itself is involved in the handover process. To overcome this problem Proxy Mobile IPv6 (PMIPv6) was defined where the mobility signaling is taken care of by a proxy server while keeping track of the MN's movement. PMIPv6 has considerably reduced the handover latency but the demand for real time applications over the network has increased tremendously due to recent explosion of the cloud era. This research paper focuses on increasing the L3 handoff signaling efficiency by reducing the latency. This is achieved by both the AAA authentication as well as the LMA registration in PMIPv6 at the same time. The simulation results show that proposed approach perform better than the current PMIPv6 L3 handover signaling reducing the latency as well as packet loss.*

**Keywords:** IPv6, PMIPv6, handoff, LMA, VOIP, etc...

## 1. Introduction

In the past few years there has been a tremendous increase in the usage of mobile devices such as PDA's, smart phones etc. Due to this explosive growth the demand for Internet access while the devices are in motion also increased. Alongside there has been a huge increase in the demand of real-time applications on mobile devices such as VoIP, real-time streaming etc. Due to the mobility of the nodes there exists sudden changes in network connectivity and IP addresses which in turn effects the performance of real-time applications over the mobile wireless networks. Internet Engineering Task Force (IETF) proposed an IP mobility scheme where a mobile node can communicate with other nodes after changing its link-layer point of attachment, without changing its IP address. Mobile IP [1] overcomes the drawback of changing the IP address when the mobile changes its point of contact and supports location independent routing of IP datagrams. In this protocol each device or mobile node is identified by its home address, independent of the point of attachment. In context of supporting mobility Mobile IP defines two new entities as home agent(HA)and foreign agent. HA is a router in the mobile nodes home network that acts as a regular router when the mobile node is in the home network and tunnels the IP datagrams to the foreign agent when it is away from the home network. The HA also maintains the current location of the mobile node. Foreign agent is a router on the network that the mobile node visits during its mobility. The foreign agent detunnels the packets from the HA and forwards it to the mobile node.

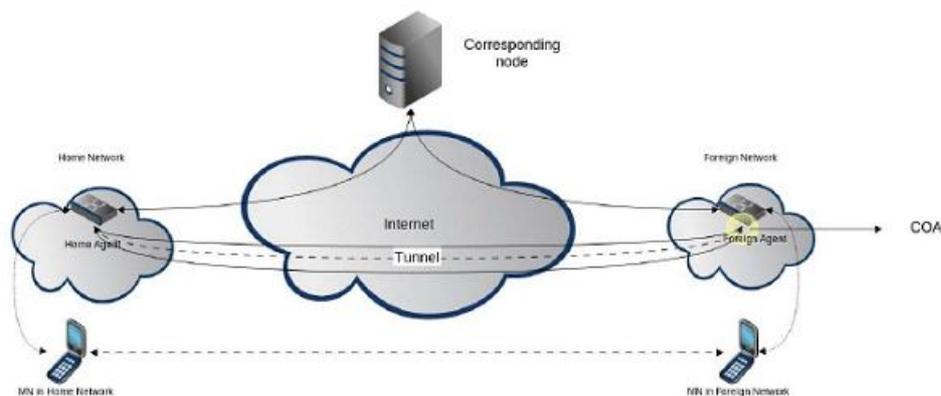
### 1.1 Mobile IP Working

When a mobile node initially registers in its home network the HA assigns an IP address to the mobile node and communication between the mobile node and the corresponding node happens through the HA. When the mobile node moves away from the home network, it registers its care-of-address which belongs to the foreign network with the HA directly if it has a collocated address(which is an address assigned directly to the mobile nodes interface) or through the foreign agent if it has the care-of-address acquired from a foreign agent (which has an interface on the foreign agent). The HA or the foreign agent can advertise their availability on each link to which they provide service. A mobile node can solicit an agent advertisement using the agent solicitation message, and can decide if it is on the home network or the foreign network. If a mobile node detects that it is on the home network, it functions without any mobility services. If the mobile node detects that it is in the foreign network then it register its care-of-address and a tunnel is established between the HA and the foreign agent. The care-of-address can be assigned by the foreign agent or can be directly acquired using Dynamic Host Configuration Protocol (DHCP). The corresponding node sends data packets to the home address of the mobile node. If the mobile node is the home network the packets are directly delivered to the mobile node. If the mobile node is in a foreign network then the packets are tunneled to the foreign agent using the care-of-address. The foreign agent is endpoint of the tunnel and the packets are forwarded to the mobile node on its access link. The reverse communication can happen in two ways. One method is the packets from the mobile to the corresponding node follow the same path as the packets form the corresponding node to the mobile node or the packets can be directly sent to the corresponding node from the foreign agent bypassing the HA.

Figure 1 shows the mobile IP architecture consisting of the HA(HA), Foreign Agent(FA), mobile Node(MN) and the Corresponding Node(CN). When the mobile node is in the home network all the packets from the CN are directly

delivered to the MN. When the mobile node moves from the home network and enters foreign network it detects that it has moved away from the home network and starts the registration process. It registers its care of address (CoA) with the HA. The care of address can be an address of one of the interfaces of the foreign agent or an address on the mobile node itself. After the registration is successful the HA and FA establish a tunnel through which the packets destined to the mobile node are tunneled from the HA to the FA. At the FA the packets are detunneled and sent to the MN.

The working of Mobile IP consists of mainly three phases, 1) Agent Discovery, 2) Registration, 3) Tunneling. The agent discovery phase is where the mobility agents advertise their services on the network. These advertisements sent by the mobility agents are ICMP route discovery messages with a mobility agent advertisement extension. Mobile nodes identify the current point of attachment using these service advertisements. The Mobile node rather than waiting for the agent advertisement, can send an agent solicitation message. This message is identical to the ICMP router solicitation message with a TTL field set to 1. When the agent receives this solicitation message it can send a agent advertisement on that link. When a mobile node receives a foreign agent advertisement and detects that it has moved out of its home network it starts the registration phase.



**Figure 1: Mobile IP Architecture**

### 1.2 Proxy Mobile IP

Though the Mobile IP is a revolutionary technology is supporting mobility for Internet Protocol it suffers from few drawbacks. First and the most difficult problem in deploying Mobile IP is not backward compatible. Mobile IP is not compatible with the traditional IP structure. Significant changes have to make to the TCP/IP stack of the mobile nodes. Also all the control signaling is performed by the mobile node on the wireless medium. The wireless medium is more prone to the error and packet loss and this increases the registration delay. This increases the power needs of the mobile node which runs on a limited power source. To overcome these drawbacks a network based mobility management protocol called PMIPv6 [2] was proposed by the IETF. In this approach the mobile node is not required to participate in the mobility session.

## 2. Related work

Though Mobile IP solved the issue of IP mobility, it suffers from some critical performance issues such as handoff latency, packet loss and signaling cost. Since all the handoff signaling is carried out by the mobile node itself, the handoff process suffers from the wireless delays increasing the handoff latency. As the handoff latency increases the packet loss also increases because the mobile has not yet registered with the foreign agent and there is no way the home agent can relay the packets to the mobile node. Apart from these drawbacks Mobile IP technology has to handle the packet loss incurred during the handoff signaling due to wireless media. All these factors motivated to develop extensions of this protocol for better performance.

### 2.1 Proxy Mobile IPv6 Signaling

Proxy Mobile IPv6 has considerably reduced the handoff latency by reducing the mobile nodes involvement during handoff signaling. The protocol however follows a sequential process during the handoff signaling. The figure 2 below shows the handoff process in the PMIPv6 domain. In Figure 2 NMAG after establishing an L2 connection with the MN sends a AAA authentication request to the AAA server. The AAA server verifies the identity of the MN and returns a reply to the MAG. If the AAA authentication was successful then the MAG sends a PBU to the LMA. The LMA then checks for all the required fields updates the binding cache entry for the MN and sends the acknowledgment.

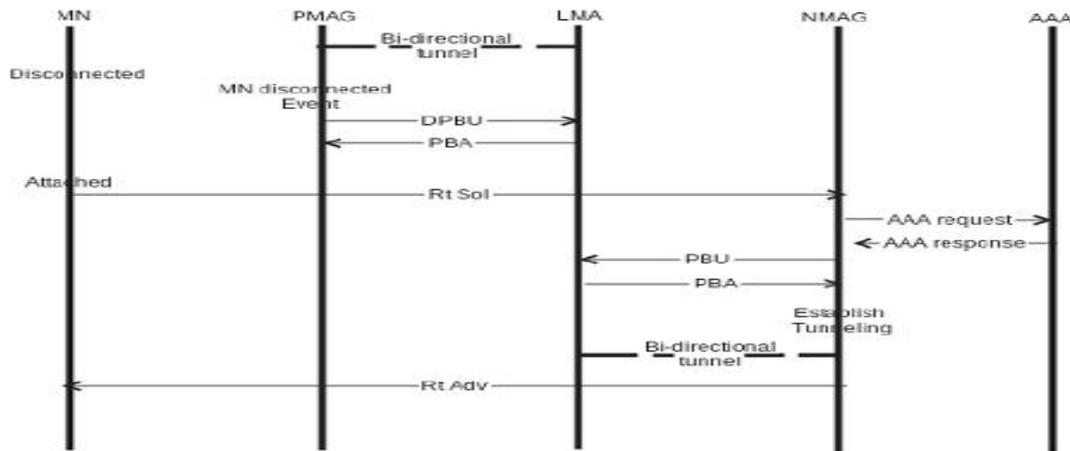


Figure 2: Proxy Mobile IPv6 Signaling

This sequential process can also be illustrated using a Pertinent (State transition system). Figure 3 shows the Petrinet of PMIPv6 signaling.

2.2 Petrinet Representation of PMIPv6 Signaling

Petrinet is one of many ways to describe a distributed system. A Petrinet consists of places (conditions or state of the system) represented by circles, transitions (events) represented by bars and tokens represented by dots indicating the current state of the system. Figure 3 shows the Petrinet for the current PMIP signaling approach. The figure consists of 4 subsystems (MN, MAG, AAA and LMA). The token in each subsystem indicate the current state.

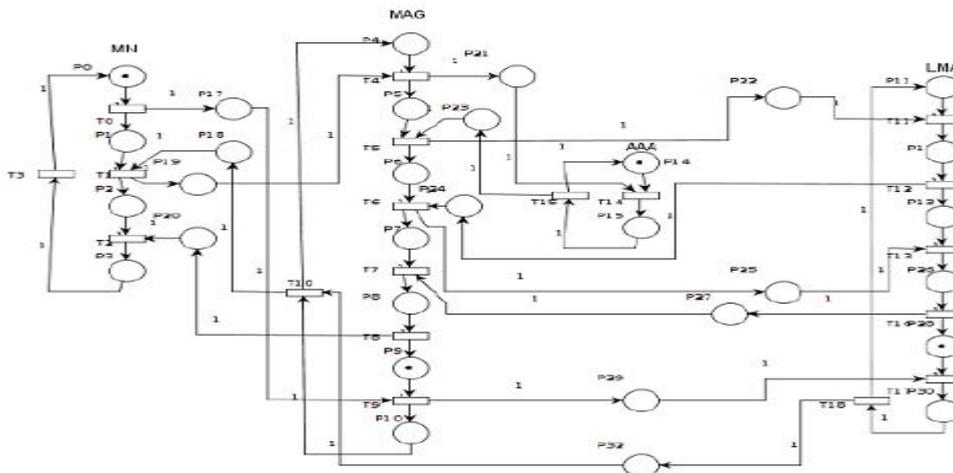


Figure 3: Petrinet of PMIPv6 Signaling

Table 1: Place definitions of Petrinet of PMIPv6 Signaling

P0 MN Connected	P1 Disconnected	P2L2 Connection Established	P3 Received Route adv	P4 MAG intial state
P5 Waiting for AAA authentication	P6 Waiting for LMA authentication	P7 Waiting for tunneling	P8 Preparing for route advertisements	P9 New node authentication done
P10 Node disconnected waiting for deregistration		P11 LMA Intial State	P12 Performing Registration	P13 Waiting for Tunnel Establishment
P14 AAA Server intial state	P15 Authentication Process	P26 waiting for Tunnel Request Ack	P28 New node Authentication done	P30 Deregistration

2.2.1 Deregistration

Initially the MN is connected to the MAG which is indicated by place P0. The MAG also is in the connected state with respect to that mobile node indicated by place P9. The AAA server is in its initial state(or authentication completed

state) indicated by place P14, while the LMA is in state(place) P28 where it has completed the registration of the MN. When an L2 detach happens then the T0 event is fired where the mobile node starts searching for a new AP. This in turn fires a series of event. The

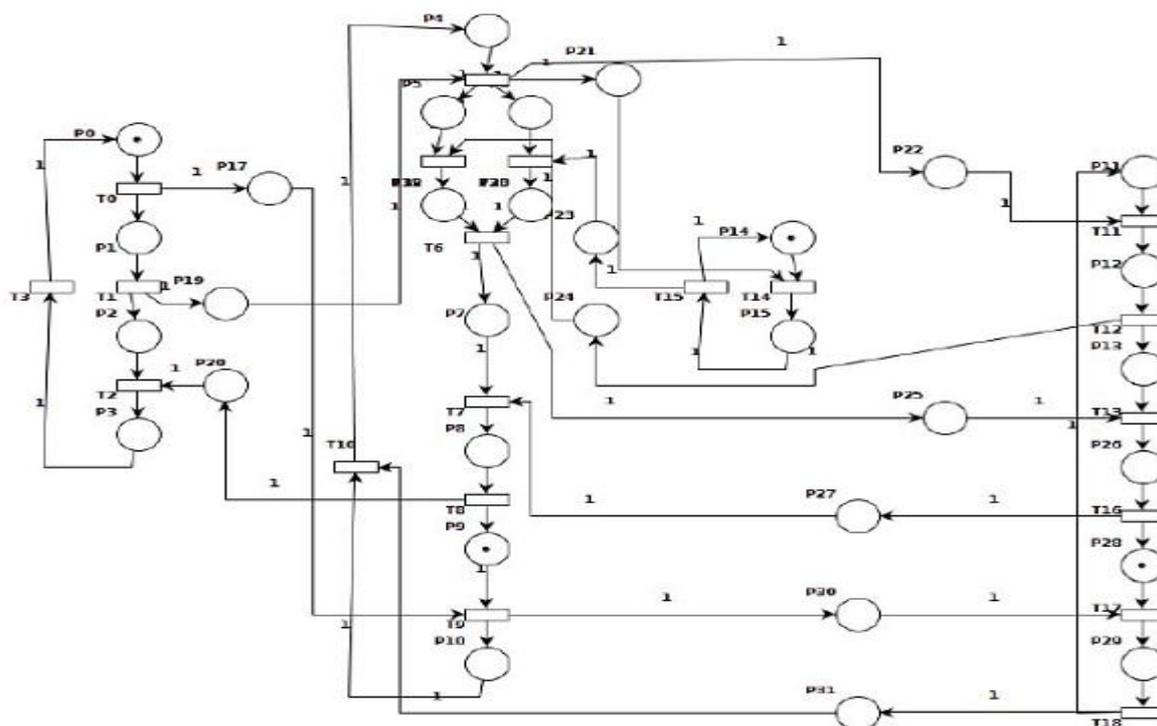
MAG moves to the deregistration state after sending the deregistration PBU (event T9). The LMA receives the PBU (event T17) and moves to the Deregistration state. After the deregistration is complete the event T18 is fired on the LMA subsystem moving it to the initial state. This triggers event T10 shifting the MAG to the initial state.

**2.2.2 Registration**

When the mobile node finds an AP and an L2 attach happens then event T1 is fired which fires event T4 in the MAG subsystem. The MAG sends the authentication request to the AAA server and waits for the response(P5). The AAA server receives the AAA authentication request firing event T14. Now the AAA server moves to the authentication state. After the authentication is done the AAA server returns to its original state by sending the AAA response (event T15). The MAG after receiving

the AAA response sends the PBU message firing the event T5 and waits for the LMA response (P6). The LMA after receiving the PBU (event T11) processes the PBU message and sends the reply back firing event T12. The MAG process this message and if the registration was successful sends a unidirectional tunnel establishing request (event T6) for the uplink. The LMA responds to this event by send a unidirectional tunnel establishment for the downlink (event T16) and completes the registration (P28). The MAG after establishing the bidirectional tunnel sends a route advertisement to the mobile node (event T8) and completes the registration phase with respect to the MAG(P9). The mobile node after receiving the route advertisement configures the IPv6 address, completes the registration and moves to the connected state (P0). Here the MAG is idle while waiting for the AAA response, which adds redundant time in the handoff latency. And also during the LMA registration the LMA checks for all the required fields even when the MN has a BCE in the LMA database. This adds extra processing time on the LMA when a lot of handovers are taking place, reducing the efficiency of the LMA and eventually affecting the performance of the protocol.

The Proposed approach is shown in Figure 4 where the MAG sends a AAA request and the PBU to the LMA at the same time without waiting for the AAA response. The MAG sends a AAA authentication request to the AAA server with the MN ID as one of the attributes. The MAG does not wait for the policy profile from the AAA server instead sends a PBU message with only the MN-ID field set and waits for both the AAA response and the LMA response. The AAA server inspects the MN-ID sent by the MAG and verifies if the mobile node is eligible for the mobility session and sends the response back. The LMA extracts only the MN ID and looks for an entry corresponding to the MN ID in the BCE. If the LMA finds an entry for the MN ID in the BCE then it sends the PBA message with the status as accepted. If the LMA doesn't find any entry corresponding to the MN ID then it checks for all the required parameters and works normally. After sending the AAA request and the PBU request, the MAG waits for the response from both the AAA server and the LMA server. There are two cases that can occur in this scenario.



**Figure 4:** Proposed Petrinet of PMIPv6 Signaling Approach

**Case 1: AAA response arrives before the PBA**

When the AAA response arrives before the PBA then the MAG checks if the MN is authenticated and just waits for the PBA message from the LMA. When it receives the PBA message as accepted and if the MN as authenticated then it establishes the tunnels and sends a route advertisement to the MN containing the same HNP. If the MN is not authenticated then the MAG sends a DPBU to the LMA.

**Case 2: PBA arrives before the AAA response**

When the PBA arrives before the AAA response then the MN establishes a conditional tunnel with the LMA. When it receives a AAA response and if the response is accepted then the MAG sends a route advertisement. If the AAA authentication of the MN fails then the MAG sends a DPBU and discards all the buffered packets.

In Both the cases the MAG has two additional fields in the BUL of the corresponding MN. One field indicates the successful authentication on the MN, while the other field indicates the successful registration of the MN with the LMA. In case 1 where the AAA response arrives before the LMA response the MAG sets the successful AAA registration variable to 1 and waits for the LMA response. When it receives the LMA response it sets the LMA registration response variable to 1 and moves forward with the tunnel setup and route advertisement. In case 2 when the MAG receives the LMA registration response before the AAA response the MAG goes ahead with the tunnel setup but wait for the AAA response before sending out a route advertisement. As soon as it receives a AAA response as accepted it sends out a route advertisement to the MN.

**3. Mathematical model**

The Mathematical representation of the delay of the handoff process is described in this section. The Abbreviations of each event is described below. The total handoff delay is given by

The total handoff delay is given by

$$T_{L3HO} = T_{AUTH} + T_{REG} + T_{TUN} \dots\dots\dots(1)$$

The AAA server authentication delay is given by

$$T_{AUTH} = T_{MAG-AAA} + T_{AAA-MAG} + P_{AAA} \dots\dots\dots (2)$$

And the LMA registration delay is given by

$$T_{REG} = T_{MAG-LMA} + T_{LMA-MAG} + P_{LMA} \dots\dots\dots(3)$$

Substituting (2) and (3) in (1)

$$T_{L3HO} = T_{MAG-AAA} + T_{AAA-MAG} + P_{AAA} + T_{MAG-LMA} + T_{LMA-MAG} + P_{LMA} + T_{TUN} \dots\dots\dots (4)$$

**Where**  $T_{HO}$  Total handoff delay,  $T_{AUTH}$  Total delay of AAA authentication,  $T_{REG}$  Total LMA registration delay,  $T_{TUN}$  Tunneling delay,  $T_{MAG-AAA}$  MAG to AAA server uplink delay,  $T_{AAA-MAG}$  MAG to AAA server downlink delay,  $P_{AAA}$  Processing time of AAA server  $T_{MAG-LMA}$  MAG to LMA uplink delay,  $T_{LMA-MAG}$  MAG to LMA downlink delay,  $P_{LMA}$  Processing time of AAA

This is the layer 3 handoff latency experienced when we use the general PMIPv6 approach. The layer 3 handoff latency using the proposed approach is has two cases

Case 1: When AAA response arrives before PBA.

$$T_{L3HO} = T_{REG} + T_{TUN} \dots\dots\dots (5)$$

Because the MAG waits for the PBA message from the LMA. (5) can also be written as

$$T_{L3HO} = T_{MAG-LMA} + T_{LMA-MAG} + P_{LMA} + T_{TUN} \dots\dots\dots (6)$$

Case 2: When PBA arrives before AAA response.

$$T_{L3HO} = T_{AUTH} + T_{TUN} \dots\dots\dots (7)$$

Which can also be written as  $T_{L3HO} = T_{MAG-AAA} + T_{AAA-MAG} + P_{AAA} + T_{TUN} \dots\dots\dots (8)$

$$T_{L3HO} = \text{Max} ((T_{MAG-AAA} + T_{AAA-MAG} + P_{AAA}), (T_{MAG-LMA} + T_{LMA-MAG} + P_{LMA})) + T_{TUN} \dots\dots\dots (9)$$

In the ideal case when both  $T_{AUTH}$  is equal to  $T_{REG}$  the Layer 3 handoff latency is reduced by 50%.

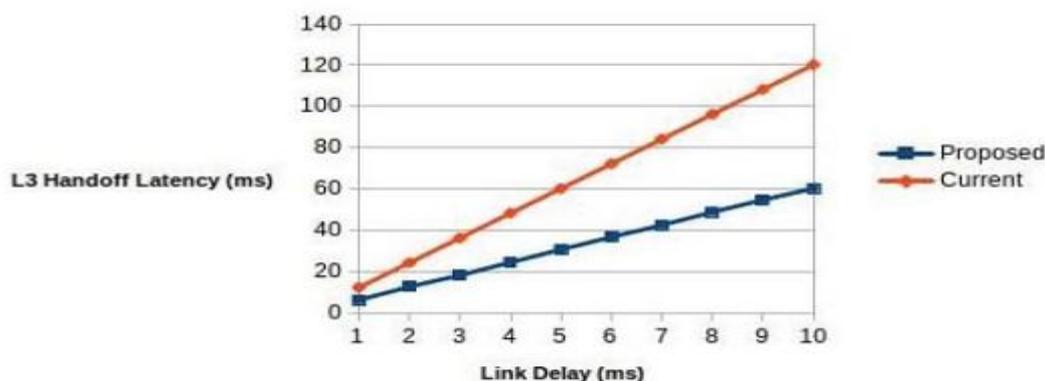
**4. Simulation Results**

**4.1 L3 Handoff Latency without Data Traffic**

Figure 5 shows the link delay vs L3 handoff latency comparison for both the current approach and the proposed approach when there is no data traffic present. We can see that the proposed approach performs better than the current approach and as the link delays increase the current PMIP standard has approximately double the L3 handoff latency compared to the proposed approach. Table 2 shows the values obtained for the simulation without data traffic.

**Table 2:** L3 Handoff Latency Readings (No data Traffic)

Link Delay(ms)	Proposed Approach(ms)	Current Approach(ms)
1	6.181	12.233
2	12.658	24.233
3	18.173	36.233
4	24.416	48.233
5	30.647	60.233
6	36.718	72.233
7	42.492	84.233
8	48.825	96.233
9	54.758	108.233
10	60.264	120.233



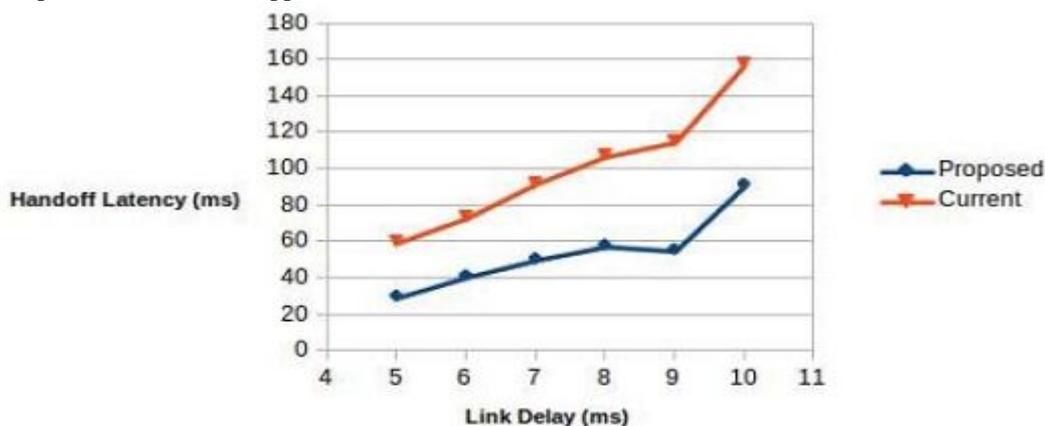
**Figure 5:** L3 Handoff Latency without Data traffic

**4.2 L3 Handoff Latency with Data Traffic**

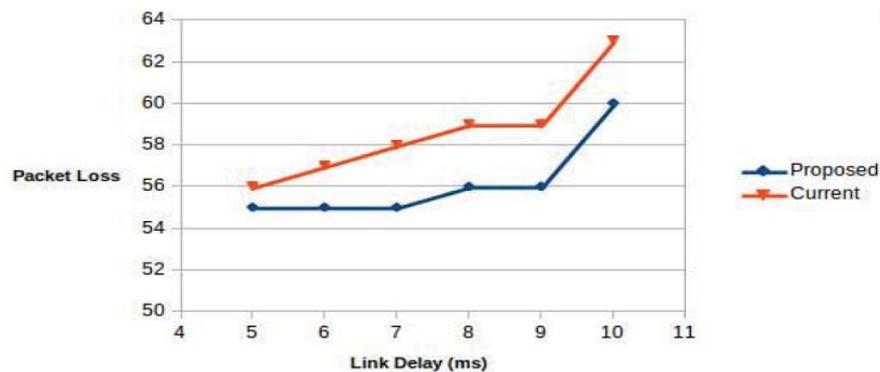
Figure 6 shows the link delay vs L3 handoff latency comparison for both the current approach and the proposed approach with VOIP traffic present. The VOIP traffic has a packet size of 160 Bytes and inter packet arrival time of 20ms [12]. Even though there is of extra delay during L3 handoff in both the scenarios we can see that the proposed approach still performs better than the current approach.

**3. Packet Loss with Data Traffic**

Figure 6 shows the link delay vs packet loss for both the approaches with VOIP traffic. Due to the decrease in L3 handoff latency in our proposed approach the packet loss is also less compared to the current approach. These results are for VOIP traffic which requires relatively low bandwidth and the inter-packet arrival time is significantly high compared to video streaming or services which require high bandwidth and the inter-packet arrival time is very less. In such cases the proposed approach perform has less packet loss compared to the current approach.



**Figure 6:** L3 Handoff Latency with Data traffic



**Figure 7:** Packet Loss with data traffic

#### 4. Conclusion

Studied the proxy mobile ipv6 protocol in detail and also different approaches proposed to reduce the handoff latency and packet loss. The sequential process of how a MAG handles the L3 handoff to a more time saving process where the MAG does not wait for the AAA response but initializes a conditional registration process. The registration is valid only if the MN is authenticated by the AAA server else the MAG deregisters the MN. This approach has shown significant reduction in L3 handoff latencies of upto 50%. Performed simulations in network simulator 3 with PMIPv6 module add-on. Made some modifications to the PMIP framework to simulate the current and the proposed version of PMIP. The results from the simulation are very close to theoretical calculations and that the proposed version always performs better than the current version.

##### 4.1 Future Scope

The packet loss has decreased due to the decrease in the L3 handoff latency we can still reduce the packet loss by allowing packet buffering at the MAGs and forwarding them to the new MAG using predictive handoff approach.

#### References

- [1] D. Johnson, C. Perkins, and J. Arkko, "Ip mobility support," Request For Comments 3775, June 2004.
- [2] S. Gundavelli, K. Leung, V. Devarapalli, K. Chowdhury, and B. Patil, "Proxy mobile ipv6," Request For Comments 5213, August 2008.
- [3] H. Soliman, C. Castelluccia, K. E. Malki, and L. Bellier, "Hierarchical mobile ipv6 mobility management," Request For Comments 4140, August 2005.
- [4] R. Koodli, "Fast handovers for mobile ipv6," Request For Comments 4068, July 2005.
- [5] R. Koodli, H. Yokota, K. Chowdhury, and B. Patil, "Fast handovers for proxy mobile ipv6," Request for Comments 5949, September 2010.
- [6] H. Choi, K. Kim, H. Lee, S. Min, and Y. H. Han, "Seamless handover scheme for proxy mobile ipv6 using smart buffering," IEEE International Conference on Wireless Mobile Computing, Networking Communication, 2008.
- [7] I. A. Surmi, M. Othman, N. A. W. A. Hamid, and B. M. Ali, "Latency low handover mechanism considering data traffic lost preventing for proxy mobile ipv6," Wireless Personal Communications, May 2013.
- [8] S. Ryu, G. Y. Kim, B. Kim, and Y. Mun, "A scheme to reduce packet loss during pmipv6 handover considering authentication," Computational Sciences and Its Applications, July 2008.
- [9] H. Y. Cho, S. G. Min, Y. H. Han, J. Park, and H. Kim, "Implementation and evaluation of proxy mobile ipv6 in ns 3 network simulator," Ubiquitous Information Technologies and Applications, December 2010.
- [11] C. Rigney, S. Willens, A. Rubens, and W. Simpson, "Remote authentication dial in user service (radius)," Request For Comments 2865, June 2000.
- [12] "Voice over ip per call bandwidth consumption." <http://www.cisco.com/>.