Graduate School ETD Form 9
(Revised 12/07)

PURDUE UNIVERSITY
GRADUATE SCHOOL
Thesis/Dissertation Acceptance

This is to certify that the thesis/dissertation prepared

By Sumith Dev Vojini

Entitled

Reducing Handoff Latency in Proxy Mobile IPv6

For the degree of Master of Science in Electrical and Computer Engineering

Is approved by the final examining committee:

Dr. Dongsoo Stephen Kim
Chair

Dr. Brian King

Dr. Paul Salama

To the best of my knowledge and as understood by the student in the *Research Integrity and Copyright Disclaimer (Graduate School Form 20)*, this thesis/dissertation adheres to the provisions of Purdue University's "Policy on Integrity in Research" and the use of copyrighted material.

Approved by Major Professor(s): Dr. Dongsoo Stephen Kim

Approved by: Dr. Brian King 11/19/2013
Head of the Graduate Program Date

REDUCING HANDOFF LATENCY IN PROXY MOBILE IPV6

A Thesis

Submitted to the Faculty

of

Purdue University

by

Sumith Dev Vojini

In Partial Fulfillment of the

Requirements for the Degree

of

Master of Science in Electrical and Computer Engineering

December 2013

Purdue University

Indianapolis, Indiana

ACKNOWLEDGMENTS

First and foremost, I would like to express the deepest appreciation to my thesis advisor Dr. Dongsoo Stephen Kim, for his immense guidance and support. Without his supervision and constant help this thesis would not have been possible. In addition, I would like to thank Sherrie Tucker and Summer Layton who assisted me while writing my thesis. I would like to thank all my friends and colleagues for their encouragement, support and assistance throughout my masters degree. Finally I would like to thank my family for believing in me and supporting me throughout my life.

TABLE OF CONTENTS

Page

LIST OF TABLES v

LIST OF FIGURES vi

ABBREVIATIONS vii

ABSTRACT viii

1 INTRODUCTION 1

1.1 Mobile IP 1

1.1.1 Mobile IP Working 2

1.2 Proxy Mobile IP 6

1.2.1 PMIP Working 6

2 RELATED WORK 9

2.1 Hierarchical Mobile IPv6 9

2.1.1 Working of HMIPv6 10

2.2 Fast Mobile IPv6 12

2.2.1 FMIPv6 Working 12

2.3 Fast Proxy Mobile IPv6 14

2.3.1 FPMIPv6 Working 15

3 HYPOTHESIS 19

3.1 Petrinet Representation of PMIPv6 Signaling 20

3.1.1 Deregistration 21

3.1.2 Registration 22

3.2 Mathematical model 25

4 SIMULATION 28

4.1 Extensions and Modifications in NS3 28

4.1.1 RADIUS 30

Page

5 RESULTS 38

5.1 Setup 38

5.2 Simulation Results 39

6 CONCLUSION AND FUTURE 44

6.1 Conclusion 44

6.2 Future Scope 44

LIST OF REFERENCES 45

LIST OF TABLES

Table Page

3.1 Place Definitions 21

3.2 Parameter Descriptions 26

4.1 Radius Header code 33

5.1 L3 Handoff Latency Readings(No data Traffic) 40

5.2 L3 Handoff Latency Readings(Voip data Traffic) 41

5.3 Packet loss Readings 42

LIST OF FIGURES

Figure Page

1.1 Mobile IP Architecture 3

1.2 Proxy mobile IPv6 Architecture 7

2.1 Hierarchical Mobile IP Architecture 11

2.2 Fast Mobile IP Architecture(Proactive Mode) 13

2.3 Fast Mobile IPv6 Architecture(Reactive Mode) 14

2.4 Fast Proxy Mobile IPv6 Architecture(Predictive Mode) 15

2.5 Fast Proxy Mobile IPv6 Architecture(Reactive Mode) 17

3.1 Proxy Mobile IPv6 Signaling 19

3.2 Petrinet of PMIPv6 Signaling 20

3.3 Petrinet of PMIPv6 Signaling(Proposed Approach) 23

4.1 PMIPv6 Topology without any modifications 29

4.2 Pcap trace of mobile access gateway 29

4.3 Radius AAA Transact Phase I 31

4.4 Radius AAA Transact Phase II 32

4.5 Radius Packet Structure 32

4.6 Radius Attribute Value Pair Structure 34

4.7 PMIPv6 Topology with the Radius Server 35

4.8 Pcap Trace of MAG2 (Current Approach) 35

4.9 Pcap Trace of MAG2 (proposed Approach) 36

5.1 Simulated Topology with current and proposed approach 38

5.2 L3 Handoff Latency without Data traffic 40

5.3 L3 Handoff Latency with Data traffic 42

5.4 Packet Loss with Data traffic 43

ABBREVIATIONS

AAA	Authentication Authorization and Accounting
CN	Corresponding Node
CoA	Care of Address
FA	Foriegn Agent
FBU	Fast Binding Update
HA	Home Agent
LMA	Local Mobility Anchor
MAG	Mobile Access Gateway
MAP	Mobility Anchor Point
NAR	New Access Router
PBU	Proxy Binding Update
PBA	Proxy Binding Acknowledgement
PAR	Previous Access Router
RCoA	Regional Care of Address
UNA	Unsolicitated Neighbor Advertisement

ABSTRACT

Vojini, Sumith Dev. M.S.E.C.E, Purdue University, December 2013. Reducing Hand-off Latency in Proxy Mobile IPV6. Major Professor: Dongsoo Stephen Kim.

Mobile IP though allows mobility features to a node it suffers from signaling 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. My thesis focuses on increasing the L3 handoff signaling efficiency by reducing the latency. This is achieved by our idea to do both the AAA authentication as well as the LMA registration in PMIPv6 at the same time. The simulation results show that our proposed approach perform better than the current PMIPv6 L3 handover signaling reducing the latency as well as packet loss.

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. Along side 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.

A traditional IP routing mechanism relies on the assumption that each node is connected to the network through a link identified by an IP address. IP routers look at the IP address prefix to identify the device's network. When the packet reaches this network, the routers in this network look for the next few bits to identify the sub-net and finally at the sub-net the routers look for the bits identifying the device. In this network scenario if the mobile node gets disconnected and tries to reconnect from a different sub-net we need to configure the device with a new IP address, appropriate sub-net mask and default gateway. Otherwise it would be difficult for the routers to deliver the packets because the device IP address does not belong to the current network location.

1.1 Mobile IP

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.

1.1.1 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 with out 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. This leads to the triangular routing problem. Triangular routing is a mechanism where the path taken by the data packets is different in both the directions that leads to low efficiency(when the delay is different in different directions) and also loss of data packets due to different security policies on different paths. Therefore this should be avoided.

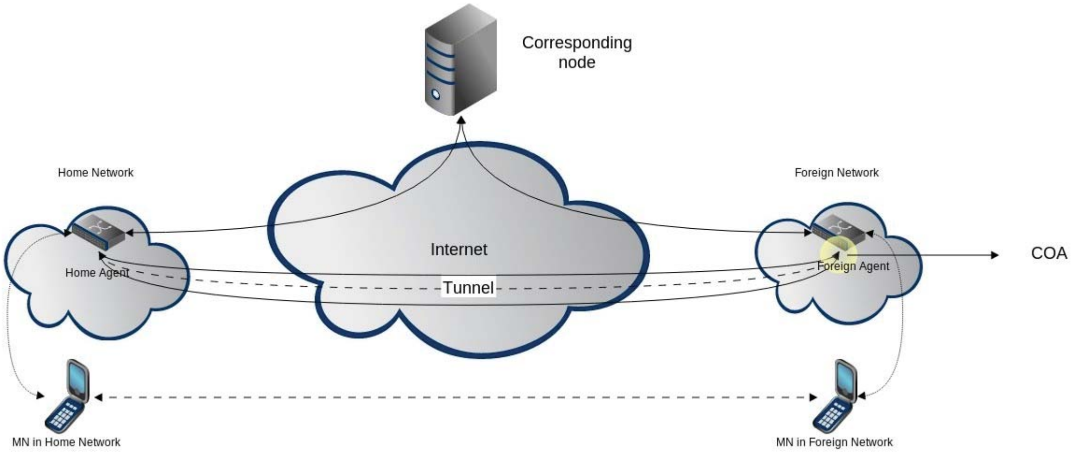


Fig. 1.1. Mobile IP Architecture

Figure 1.1 shows the 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.

Mobile IP registration allows the mobile nodes to request forwarding service from the HA when it is in a foreign network, inform the home-agent about the current location and reachability state, renew the registration if it is expiring and deregister when returned to the home network. The mobile is configured with an IP address of its home network and user identification such as a user-name of network access identifier. The Mobile Node uses this information along with the information that it learns from the Foreign Agent advertisements to form a Mobile IP registration request. It sends the registration request to its HA either through the Foreign Agent or directly if it is using a co-located care-of address and is not required to register through the Foreign Agent. A co-located care-of address is an IP address temporarily assigned to the interface of the Mobile Node itself. If the registration request is sent through the Foreign Agent, the Foreign Agent checks the validity of the registration request, which includes checking that the requested lifetime does not exceed its limitations, the requested tunnel encapsulation is available, and that reverse tunnel is supported. If the registration request is valid, the Foreign Agent adds the visiting Mobile Node to its pending list before relaying the request to the HA. If the registration request is not valid, the Foreign Agent sends a registration reply with appropriate error code to the Mobile Node.

The HA also checks the validity of the of the registration and also authentication of the mobile node. If the registration message is valid and the mobile node is authenticated then the HA creates a mobility binding which is the association of the mobile node's Home address with the care-of-address or else it sends a registration reply with appropriate error code. It also creates a tunnel to the foreign agent interface which is associated with the mobile node and also a forwarding rule to forward packets to the foreign agent. It sends a registration reply to the mobile node through the foreign agent if the request was sent through the foreign agent else directly. If the registration reply is sent through the foreign agent then the foreign agent also validates the reply, adds the mobile node to the visitors list and forwards that reply to the mobile node. The mobile node validates this reply and if the message is invalid it discards the reply else the reply is accepted. If the mobile node has a co-located address then it establishes a tunnel with HA.

The mobile node always has the source address set to the home IP address while communicating with the corresponding node irrespective of the location of the mobile node. This implies that the packet destined to the mobile node have a destination address set to the home IP address and are routed through the HA. The home network encapsulates these packets and forwards them through the tunnel to the foreign agent. At the other end of the tunnel the foreign agent decapsulates these packets and forwards them to the mobile node. As mentioned earlier this type of communication can lead to triangular routing problem. This can be avoided by using reverse tunneling scheme where the packets from the mobile node are to the HA and from the HA the packets are forwarded to the corresponding node.

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 made 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.

1.2.1 PMIP Working

In the context of supporting network based mobility, PMIPv6 defines two new entities Local mobility anchor(LMA) and Media access gateway(MAG). The LMA acts as a HA to the mobile node in the proxy mobile IPv6 domain. It is the topological anchor point and also maintains a binding cache which binds the MN's IP address with the proxy CoA. The function of LMA is similar to the functioning of a HA in mobile IP with additional capabilities to support proxy registration. The mobile access gateway runs on an access router which can manage mobility related signaling on behalf of the MN. MAG keeps track of the mobile nodes location and maintains a binding update list for all the mobile nodes currently connected to it. The LMA and the MAG establish bidirectional tunnels to forward packets destined to the mobile node.

When a mobile node enter the proxy Mobile IPv6 domain the MAG detects it on one of its link and acquires the MN's identification parameters. After receiving this information the MAG initializes the mobility signaling with the LMA on behalf of the mobile node. The network as a whole after determining that the mobile node is authorized to use the service, will make sure that the mobile node using any of the address configuration mechanisms permitted by the network will be able to to obtain the address configuration on the access link it was connected and move through out the local domain. From a mobile nodes point of view the entire PMIP domain appears as a single Link and the network ensures that the mobile node see the same link even when it changes the point of access. Figure 1.2 explains the working of PMIPv6.

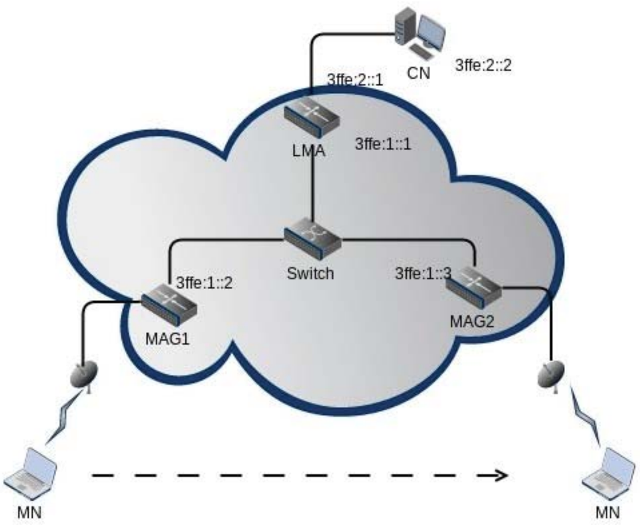


Fig. 1.2. Proxy mobile IPv6 Architecture

When a Mobile node enters the PMIP domain the mag acquires the MN identification and verifies whether the MN is a valid node or not using one of the AAA mechanisms and also receives a policy profile from the AAA server if validated. After validating the MN the MAG starts the registration process. It sends a Proxy Binding Update(PBU) message to the corresponding LMA with the MN identifications and also the policy profile for registration. The MAG also creates the binding update list entry for the mobile node after sending the PBU. This message is similar to the binding registration message sent by the mobile node but with an extra flag 'P' indicating a proxy registration. The LMA after receiving the Update message checks for all the information it need to perform the registration. If any of the fields are missing the LMA sends an acknowledgment with a message informing the MAG about the missing fields. If the update message is accepted the LMA sends a Proxy Binding Acknowledgment(PBA) with the home network prefix. The LMA also creates the binding cache entry for the MN. The LMA and the MAG establish a bi-directional tunnel to forward the data packets from the corresponding node to the mobile node and vice-versa. When the MAG receives a PBA with registration accepted message, it advertises the home network prefixes on the access link the mobile node is attached. Using these home network prefixes(HNP) the MN can configure the IP address for its interfaces. When a mobile node changes its point of attachment in the local domain then the network makes sure the MN see the same link by advertising the same HNP on the access link emulating a constant link in the local domain from the MN perspective.

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 researchers to develop extensions of this protocol for better performance.

2.1 Hierarchical Mobile IPv6

Hierarchical Mobile IP or HMIPv6 [3] is an extension to the existing Mobile IP which has localized mobility management. The basic idea in this approach is that the binding updates sent are locally handled which is not the case in MIPv6. The HMIPv6 protocol divides the network into independent regions with each region being managed by a unique device called the Mobility Anchor Point(MAP). A normal access router can also act as a MAP. MAP acts as the anchor point for any MN in that region.

When a Mobile Node enters the MAP domain or region it receives router advertisements containing information about the MAP. The MN can bind its current location i.e the on link CoA with the address on the MAP subnet i.e Regional CoA(RCoA). The MAP acts as a local Home Agent and will receive all the packets destined to the MN, encapsulate them and forward them to the MN. The RCoA does not change as long as the mobile node is in the same MAP region making the mobility transparent to the corresponding nodes. Access Routers define the MAP boundaries by advertising the MAP information to the MN.

2.1.1 Working of HMIPv6

In Figure 2.1 below the MAP will provide seamless mobility for the MN's as they move from one Access Router to another. When a MN enters a foreign network the mobile node will discover the global address of the MAP which is the RCoA. This information is stored in the Access Router and communicated to the MN using route advertisements(RA). The discovery phase continues as long as the mobile node moves from one subnet to another and the MN always detects whether the it is still in the same MAP domain. This is achieved by using information sent in RA's. If the MN detects a change in the MAP domain it must send a binding update(BU) to its home agent and corresponding node.

The mobile node now sends a local BU message to the MAP. The local BU message contains the RCoA as the Home address option and no other CoA is needed. The Local CoA(LCoA) is the source address of the BU message. the MAP has no knowledge of the MN's home address. The BU from the MN tell MAP that the MN has created a RCoA and if that is successful the MAP sends a Binding Acknowledgment(BA). As soon as the MN receives the BA, it informs its home agent and corresponding nodes about the RCoA and the home address. This completes the handoff of the MN into a new domain.The MAP accepts packets from the mobile node through a tunnel with the MN being the tunnel entry point and MAP being the exit point of the tunnel. It also acts as a HA for the RCoA and all the packets destined to the RCOA are intercepted by the MAP. When a mobile node moves from one access router to another in the same MAP domain, it needs to change only the LCoA and the changes

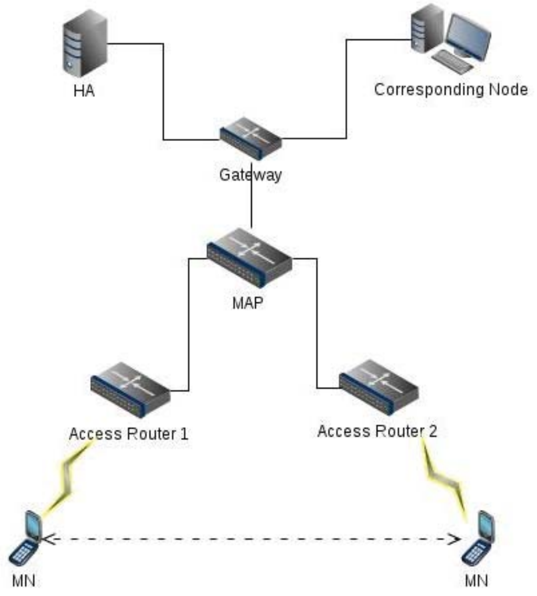


Fig. 2.1. Hierarchical Mobile IP Architecture

are local to only MAP. The HA and the CN need not know about the change. But if the mobile node is moving from one MAP domain to another then the LCoA and the RCoA configured from the new MAP have to be registered. This increases the signaling and processing overhead.

If the mobile node is not aware of the HMIPv6, then MAP discovery will not be used, and the general MIPv6 will be used for mobility management. If the MN is aware of HMIPv6 it should use the HMIPv6 implementation. The MN needs to register its home address and on-link address with the MAP where home address is the RCoA which is stored in the binding cache of the MAP so that it can forward packets destined to the MN. The MN always keeps information of the sender of the received packets to determine if route optimization is needed. The MN can register with multiple MAPs at the same time for bandwidth optimization.

2.2 Fast Mobile IPv6

FMIPv6 [4] is an extension of MIPv6 designed to reduce handoff latency. The time taken for a MN to receive packets from a new subnet depends on how long it takes for the IP connectivity to be established which in turn depends upon the time taken for the movement detection and configuring the CoA. This protocol allows the MN to quickly detect the movement away from the current serving access router by relaying the new access routers information including the subnet prefix information while the MN is connected to the current access router. This protocol specifies a binding between the Previous-CoA(PCoA) and New-CoA(NCoA) to reduce the binding update latency. Here the mobile node sends an unsolicited Neighbor Advertisement(UNA) message to the NAR as soon as it connects to NAR to reduce the latency incurred by the NAR to identify the MN's attachment. The AR's are also allowed to exchange control messages to verify if the proposed NCoA is acceptable.

2.2.1 FMIPv6 Working

When a MN detects that the link is degrading(a trigger) it will send a RtSolPr message to the current access router to get the subnet specific information from the Access point identifiers. The access router after receiving the RtSolPr message will send PrRtAdv message to the MN containing one or more tuple with information about the access point identifiers. Here it is assumed that the mobile node will discover the adjacent AR's through link-specific methods before sending the RtSolPr message. Using the information in the PrRtAdv the MN will generate a NCoA and send the Fast Binding Update(FBU) message to the PAR. The FBU allows the PAR to bind the PCoA with the NCoA so that the packets arriving can be sent through the tunnel to the new MN location. The FBU can be sent from the PAR's link or a new link. There are two modes in FMIPv6, they are explained below.

The MN node should try to send the FBU from the PAR's link when ever feasible. Figure 2.2 shows the proactive mode of PMIP,where if the FBU is sent from

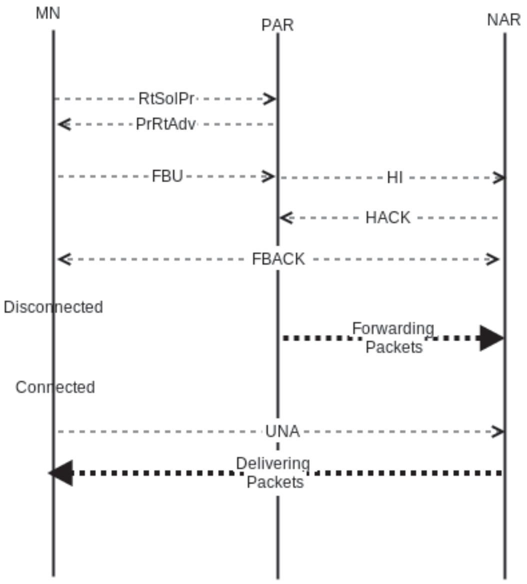


Fig. 2.2. Fast Mobile IP Architecture(Proactive Mode)

the PAR's link, then the Fast Binding Acknowledgment(FBACK) is also received on the previous link which indicates that the packet tunneling is already in progress. The MN should send a UNA immediately after it attached to the NAR so that the NAR can forward the packets being tunneled. The PAR can determine if the NCoA is acceptable before sending the FBACK to the MN. If assigned addressing is used then the PAR should send the proposed NCoA received in the FBU in the Handoff Initiation(HI) message. The NAR can assign the proposed NCoA or assign a new one and send that information in the Handoff Acknowledgment(HACK). The MN should use the NCoA present in the HACK irrespective of whether it is the proposed NCoA or not.

Figure 2.3 shows the reactive mode of FMIPv6, where if the MN does not receive the FBACK on the previous link either because it was not sent on that link or the MN has disconnected from that link, then the Mobile node has no means to determine if the FBU was successfully processed by the PAR. In this case the MN will send the FBU immediately after it sends the UNA message to the NAR. If the NAR decides

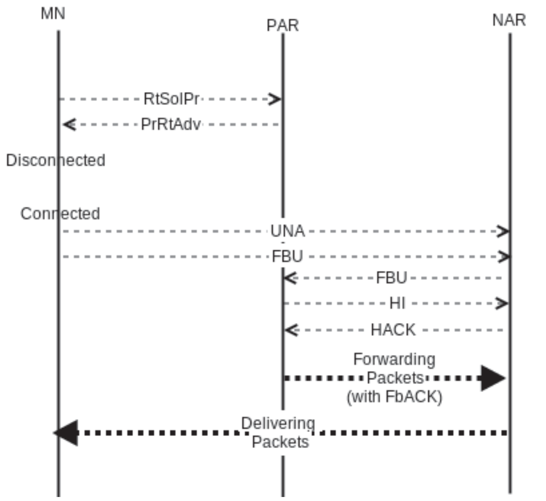


Fig. 2.3. Fast Mobile IPv6 Architecture(Reactive Mode)

to use a different address as the NCoA it has to send a router advertisement with a Neighbor Advertisement Acknowledgment(NAACK) option which includes the NCoA to be used for the mobile node.

2.3 Fast Proxy Mobile IPv6

Fast Proxy Mobile IPv6 or FPMIPv6 [5] is an extension on PMIPv6, which performs an efficient handoff by reducing delay during handoff and reducing packet loss. In order to improve the performance during the handoff this protocol establishes a bidirectional tunnel between the Previous MAG(PMAG) and New MAG(NMAG), so that the packets corresponding to the MN arriving at the PMAG can be tunnel to the NMAG. The HI message and the HACK message are extended for transfer of information such as network access identifier, home network prefix etc in order to allow the NMAG to send a PBU before the MN is attached to the link layer of the NMAG. Here the PAR and NAR would be replaced by PMAG and NMAG. Since the MN does not take part in the mobility session in PMIP the message formats such as the RtSolPr, PrRtAdv, NAACK, UNA are not applicable.

2.3.1 FPMIPv6 Working

Similar to the FMIPv6 FPMIPv6 also has two modes of operation, the Predictive mode and the Reactive mode. In the predictive mode a bidirectional tunnel is established between the PMAG and the NMAG before the MN is attached to the NMAG. In the reactive mode the Bidirectional tunnel is established after the MN is attached to the NMAG. To reduce packet loss during the handoff process the MAG's should be equipped with buffering mechanisms and enough capacity to buffer packets. The protocol operation is transparent to the local mobility anchor (LMA) therefore requiring no changes to the LMA.

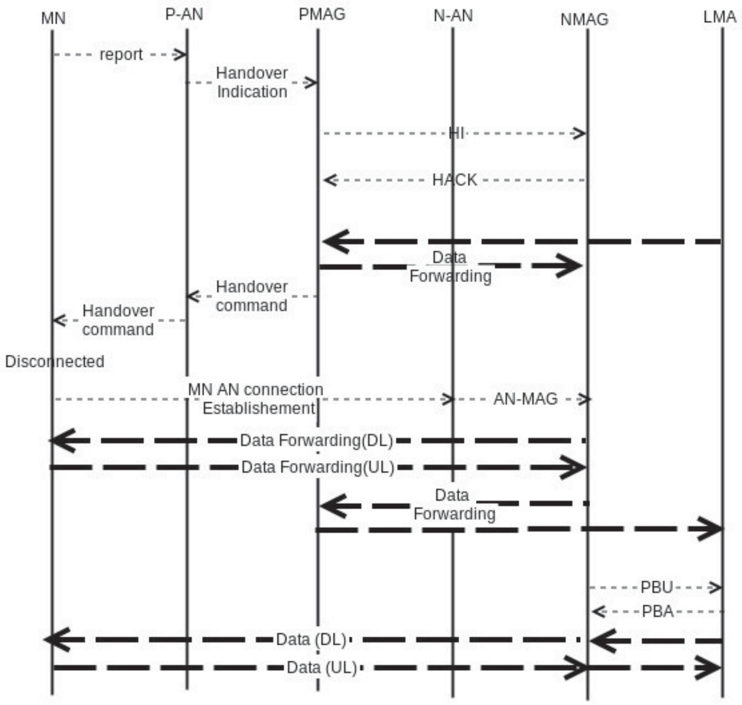


Fig. 2.4. Fast Proxy Mobile IPv6 Architecture(Predictive Mode)

In the predictive mode it is essential that the MN is capable of reporting the lower layer information to the access network(AN) as early as possible and the AN is capable of sending the handoff indication message to the PMAG. Figure 2.4 explains the working of the FMIPv6. When a mobile node detects that has to handoff to another MAG, it reports the mobile node identifier(MN-ID) and the new access point Identifier to the access point/access network which indicates the PMAG about the MN's handoff tot he new access point. The P-AN can also determine the new AP-ID if needed. The PMAG derives the NMAG address using the N-AN ID. Then the PMAG sends a handoff initiate(HI) message to the NMAG. The HI message should contain all the required information like the HNP, MN-ID and LLA-ID. The NMAG sends a handoff acknowledgment(HACK) to the PMAG and a bidirectional tunnel is established between the PMAG and the NMAG and packets from PMAG destined to the mobile node are forwarded to the NMAG. When the network is ready for the handoff the mobile node is allowed to perform a handoff to the N-AN. The MN establishes the L2 connection with the N-AN. The PMAG determines whether to the MN LL-ID received on the N-AN and from the PMAG match. The NMAG starts forwarding the packets destined for the MN. While this in progress the NMAG sends the PBU to the LMA. After the NMAG receives a PBA the packets from the LMA are directly sent to the NMAG.

In the reactive mode of operation the NMAG sends the HI message to the PMAG since the MN cannot send a FBU or a UNA message. For this to happen the MN has to provide the PMAG information to the NMAG. Figure 2.5 show the working of the reactive mode in FPMIPv6. Here the mobile node handoff to the N-AN and establishes a L2 connection with the N-AN. It sends the MN-ID and the P-AN ID to the N-AN which in turn sends this information to the NMAG. Now the NMAG sends a HI message to the PMAG which include the MN-ID. The PMAG sends a HACK message to the NMAG which includes the HNP corresponding to the MN. After validating the information send by the PMAG the NMAG establishes the tunnel between the PMAG and the NMAG. Now all the packets destined to the MN are forwarded to the NMAG. The process after this is similar to that of the predictive mode operation.

Another method which is concerned with packet disruption period integrated with FPMIPv6 was proposed for seamless handovers in PMIPv6 [6]. In this method a

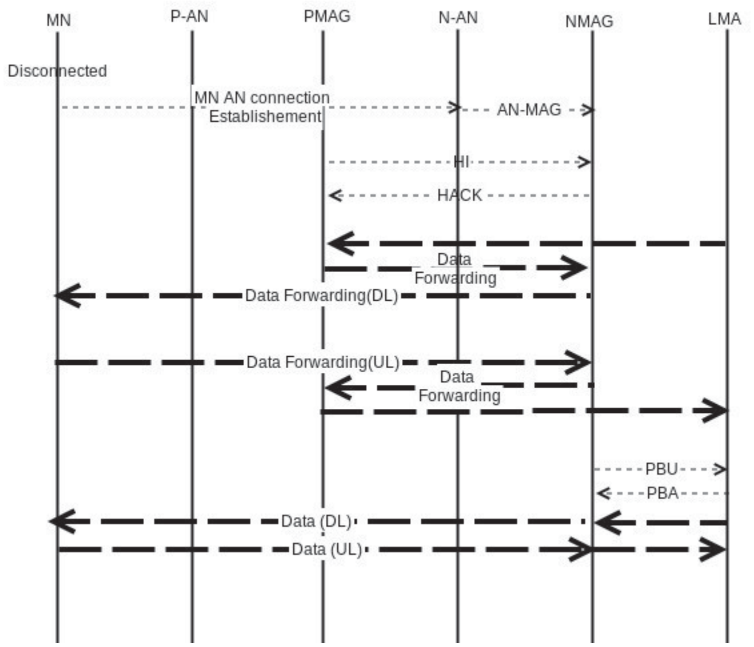


Fig. 2.5. Fast Proxy Mobile IPv6 Architecture(Reactive Mode)

smart buffering mechanism is applied where the PMAG buffer packets while the MN is about to get disconnect. When the MN connects to the NMAG, the NMAG sends a flush request/reply message(FRM) to the PMAG. The PMAG then sends a FRM reply to the NMAG and forwards all the buffered packets to the NMAG. In the mean time the NMAG starts buffering packets from the LMA and performs a reordering on the packets based on the control information sent by the PMAG. When the MN is authenticated and authorized then the NMAG forwards all the buffered packets to the MN in order.

Another method also relies on buffering the packets but at the LMA and also performs a proactive handoff mechanism [7]. Here the PMAG detects the LGD trigger and sends a deregistration PBU with 0 lifetime. The LMA after receiving the De-Reg PBU activates the pre-registration along with the pre-access authentication. In the Pre-registration phase the LMA sends a polling message to all the neighboring MAGs about the MNs movements. When one of the MAG attaches to the MN it sends a PBU with a finite lifetime. Here the MAG can bypass the access authentication procedure by comparing the MNs profile with the profile advertised by the LMA. Now the LMA updates the BCE of the MN with the NMAG. There are similar methods proposed like fast handoff scheme in PMIPv6 and a scheme to reduce packet loss in PMIPv6 [8]. In this scheme the PMAG plays the active role during handoff by sending a De-Reg PBU which piggybacks the registration of the NMAG, which allows a conditional registration and a tunnel to be setup before the MN can authenticate itself enable a faster handoff process.

3. HYPOTHESIS

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 below show the handoff process in the PMIPv6 domain.

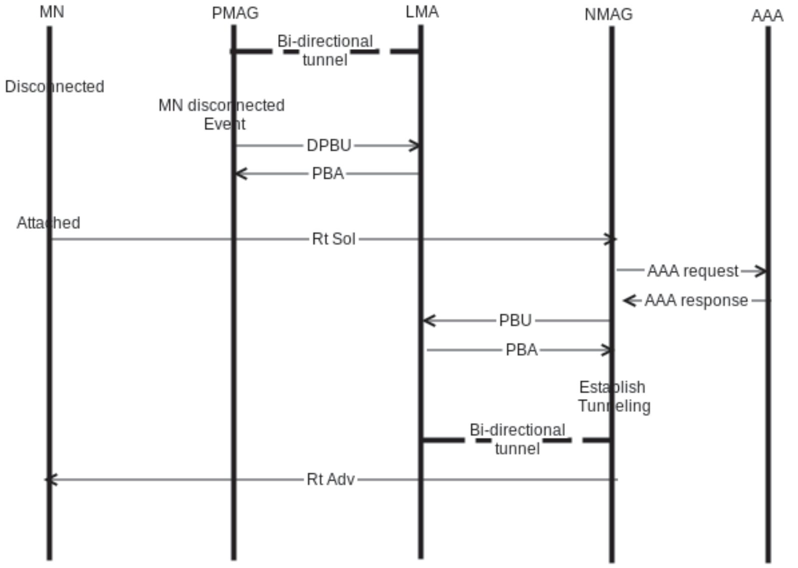


Fig. 3.1. Proxy Mobile IPv6 Signaling

In Figure 3.1 the 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.

This sequential process can also be illustrated using a Petrinet(State transition system). Figure 3.2 shows the Petrinet of PMIPv6 signaling.

3.1 Petrinet Representation of PMIPv6 Signaling

Petrinet is one of many ways to discribe 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 3.2 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.

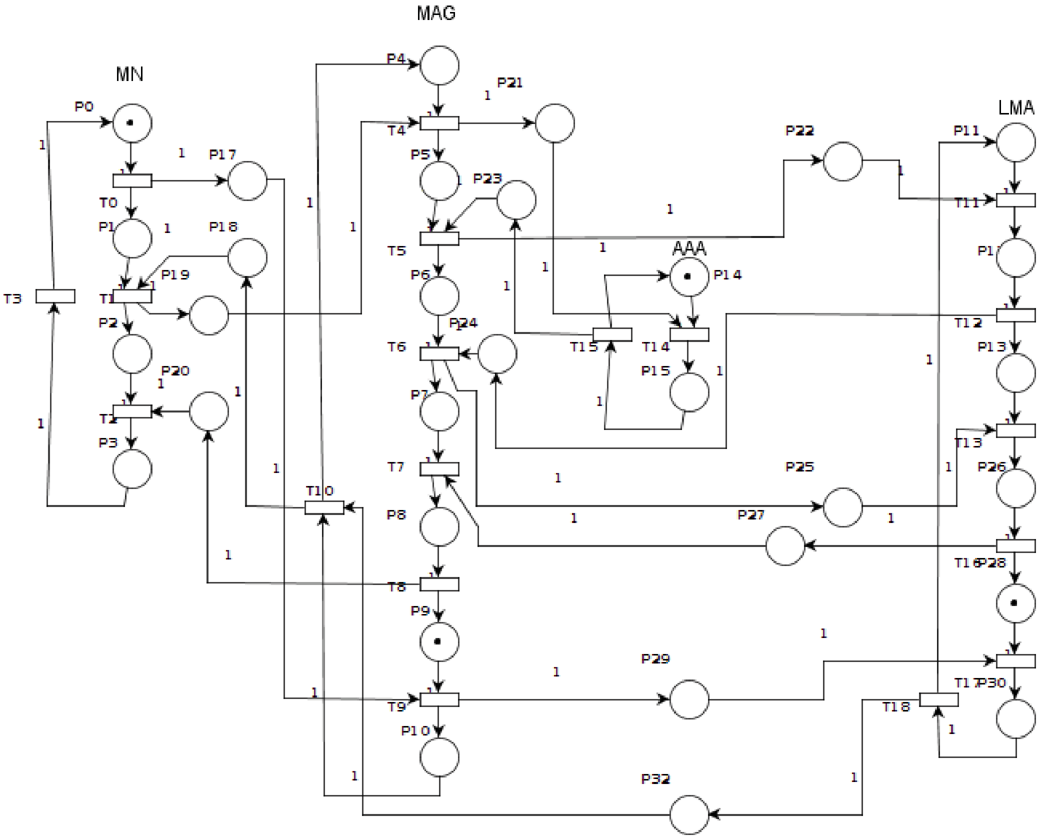


Fig. 3.2. Petrinet of PMIPv6 Signaling

Table 3.1
Place Definitions

Place	**Name**
P0	MN Connected
P1	Disconnected(Looking for a new connection)
P2	L2 connection Established
P3	Received Route Adv
P4	MAG Initial 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 Initial State
P12	Performing Registration
P13	Waiting for Tunnel Establishment
P14	AAA server initial State
P15	Authentication Process
P26	waiting for Tunnel Request Ack
P28	New node authentication done
P30	Deregistration

3.1.1 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 inturn 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.

3.1.2 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.

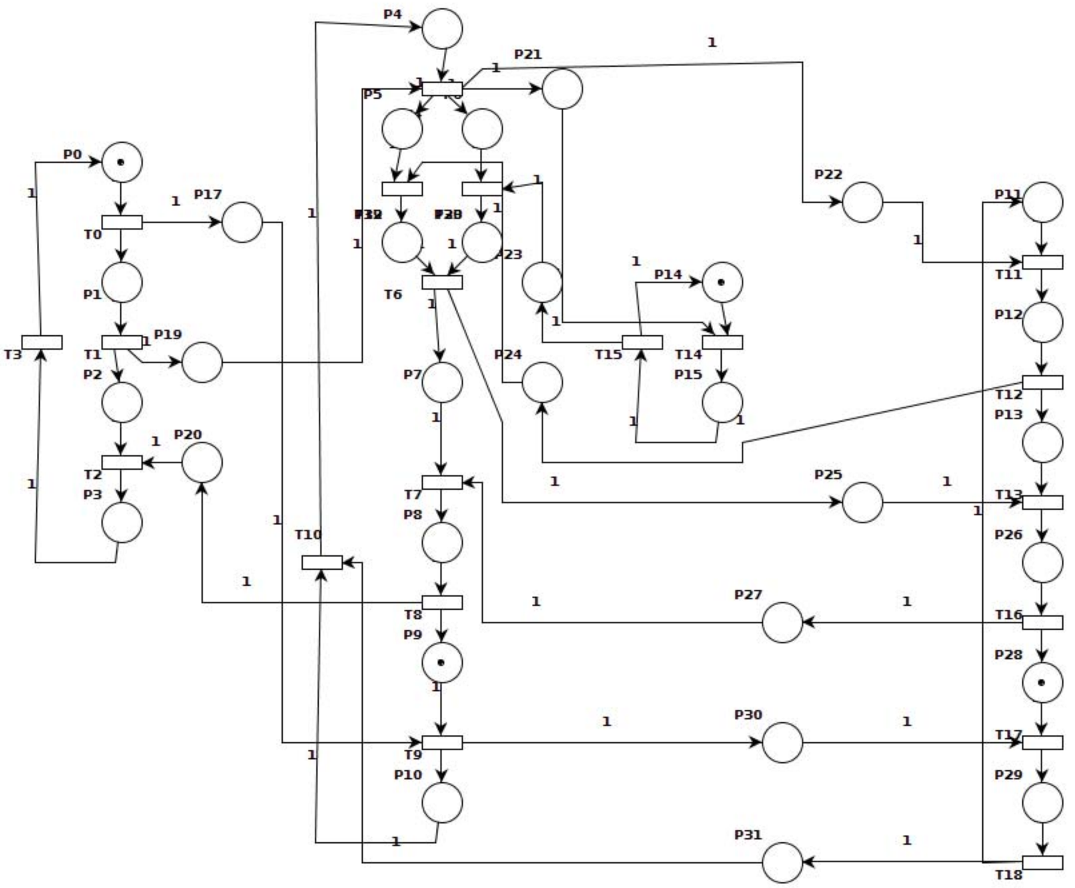


Fig. 3.3. Petrinet of PMIPv6 Signaling(Proposed Approach)

The Proposed approach is shown in Figure 3.3 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.
Case 1: The AAA response arrives before the PBA
Case 2: The PBA arrives before the AAA response

Case 1:
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:
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 reponse 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.

3.2 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

$$T_{L3HO} = T_{AUTH} + T_{REG} + T_{TUN} \tag{3.1}$$

The AAA server authentication delay is given by

$$T_{AUTH} = T_{MAG-AAA} + T_{AAA-MAG} + P_{AAA} \tag{3.2}$$

And the LMA registration delay is given by

$$T_{REG} = T_{MAG-LMA} + T_{LMA-MAG} + P_{LMA} \tag{3.3}$$

Substituting (3.2) and (3.3) in (3.1) ....

$$T_{L3HO} = T_{MAG-AAA} + T_{AAA-MAG} + P_{AAA} + T_{MAG-LMA} + T_{LMA-MAG} + P_{LMA} + T_{TUN} \tag{3.4}$$

Table 3.2
Parameter Descriptions

Parameter	**Description**
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.

$$T_{L3HO} = T_{REG} + T_{TUN} \tag{3.5}$$

Because the MAG waits for the PBA message from the LMA. (3.5) can also be written as

$$T_{L3HO} = T_{MAG-LMA} + T_{LMA-MAG} + P_{LMA} + T_{TUN} \tag{3.6}$$

Case 2: When PBA arrives before AAA response.

$$T_{L3HO} = T_{AUTH} + T_{TUN} \tag{3.7}$$

Which can also be written as

$$T_{L3HO} = T_{MAG-AAA} + T_{AAA-MAG} + P_{AAA} + T_{TUN} \tag{3.8}$$

$$T_{L3HO} = Max((T_{MAG-AAA}+T_{AAA-MAG}+P_{AAA}),(T_{MAG-LMA}+T_{LMA-MAG}+P_{LMA}))+T_{TUN} \tag{3.9}$$

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

4. SIMULATION

In order to verify the theoretical results obtained in our proposed approach we have decided to simulate our proposed model. We have used network simulator 3(NS3) [9] for all our simulations. NS3 is an open source discrete event network simulator developed for network research and education with support for various protocols and scope for development.

4.1 Extensions and Modifications in NS3

We have used the PMIPv6 extension created for NS3 [10]. The focus was basically on building an independent PMIPv6 module which can be later integrated to other versions of NS-3. To support this flexibility most of the functionality was rewritten even with the code re-usability feature in NS3. Minimum implementation of MIPv6(mobility headers) was also implemented in PMIPv6 module since NS3 did not support MIPv6. Binding update process begins with the MN attaching to the link layer of access point and the MAG sending a PBU to the LMA. A simple topology was created to test the available features in the PMIPv6 module. The topology created is in Figure 4.1.

The pcap traces of the simulation is show in Figure 4.2. This trace belongs to MAG2 interface 1 which is connected to the switch. At 5.32 seconds MAG starts the registration process without any authentication of the mobile node. The available module only allowed us to create pmip specific nodes such as MAG and LMA. The current PMIP module required some modifications to be made before we can simulate the proposed model. The PMIPv6 extension for NS3 does not support AAA authentication and directly starts the registration process with the LMA. We included a AAA

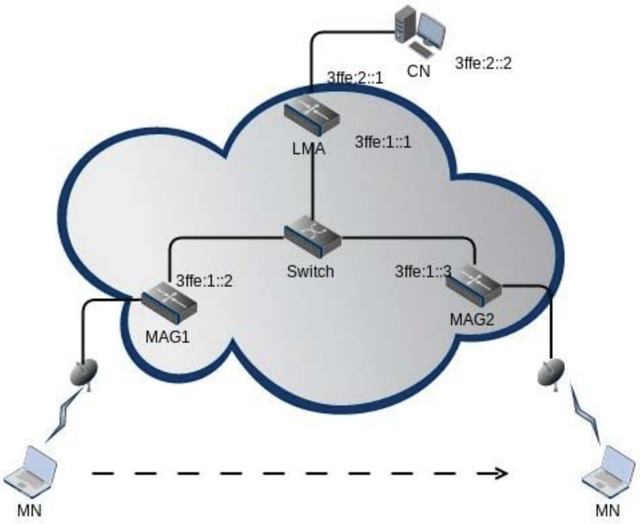
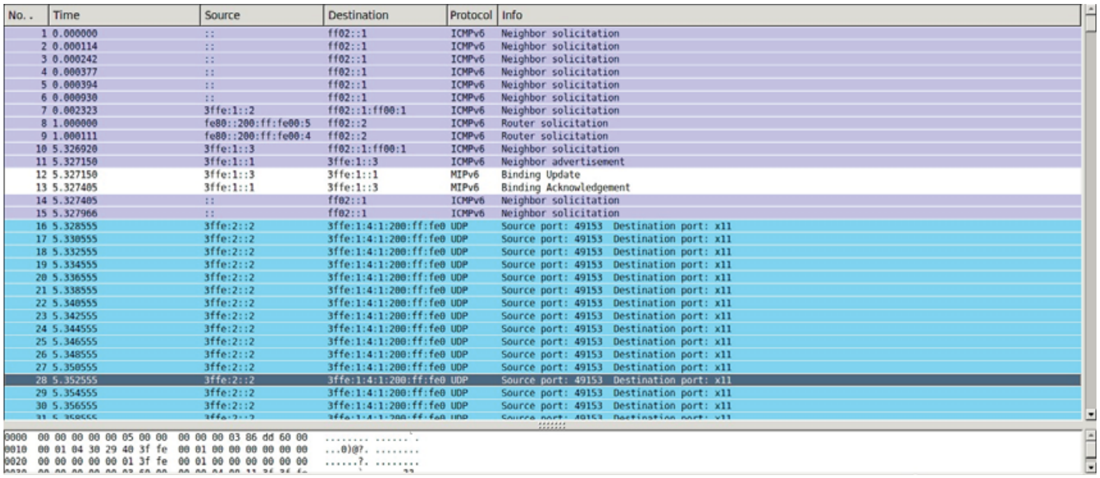


Fig. 4.1. PMIPv6 Topology without any modifications



No. .	Time	Source	Destination	Protocol	Info
1	0.000000	::	ff02::1	ICMPv6	Neighbor solicitation
2	0.000114	::	ff02::1	ICMPv6	Neighbor solicitation
3	0.000242	::	ff02::1	ICMPv6	Neighbor solicitation
4	0.000377	::	ff02::1	ICMPv6	Neighbor solicitation
5	0.000394	::	ff02::1	ICMPv6	Neighbor solicitation
6	0.000930	::	ff02::1	ICMPv6	Neighbor solicitation
7	0.002323	3ffe:1::2	ff02::1:ff00:1	ICMPv6	Neighbor solicitation
8	1.000000	fe80::200:ff:fe00:5	ff02::2	ICMPv6	Router solicitation
9	1.000111	fe80::200:ff:fe00:4	ff02::2	ICMPv6	Router solicitation
10	5.326920	3ffe:1::3	ff02::1:ff00:1	ICMPv6	Neighbor solicitation
11	5.327150	3ffe:1::1	3ffe:1::3	ICMPv6	Neighbor advertisement
12	5.327150	3ffe:1::3	3ffe:1::1	MIPv6	Binding Update
13	5.327405	3ffe:1::1	3ffe:1::3	MIPv6	Binding Acknowledgement
14	5.327405	::	ff02::1	ICMPv6	Neighbor solicitation
15	5.327966	::	ff02::1	ICMPv6	Neighbor solicitation
16	5.328555	3ffe:2::2	3ffe:1:4:1:200:ff:fe0	UDP	Source port: 49153 Destination port: x11
17	5.330555	3ffe:2::2	3ffe:1:4:1:200:ff:fe0	UDP	Source port: 49153 Destination port: x11
18	5.332555	3ffe:2::2	3ffe:1:4:1:200:ff:fe0	UDP	Source port: 49153 Destination port: x11
19	5.334555	3ffe:2::2	3ffe:1:4:1:200:ff:fe0	UDP	Source port: 49153 Destination port: x11
20	5.336555	3ffe:2::2	3ffe:1:4:1:200:ff:fe0	UDP	Source port: 49153 Destination port: x11
21	5.338555	3ffe:2::2	3ffe:1:4:1:200:ff:fe0	UDP	Source port: 49153 Destination port: x11
22	5.340555	3ffe:2::2	3ffe:1:4:1:200:ff:fe0	UDP	Source port: 49153 Destination port: x11
23	5.342555	3ffe:2::2	3ffe:1:4:1:200:ff:fe0	UDP	Source port: 49153 Destination port: x11
24	5.344555	3ffe:2::2	3ffe:1:4:1:200:ff:fe0	UDP	Source port: 49153 Destination port: x11
25	5.346555	3ffe:2::2	3ffe:1:4:1:200:ff:fe0	UDP	Source port: 49153 Destination port: x11
26	5.348555	3ffe:2::2	3ffe:1:4:1:200:ff:fe0	UDP	Source port: 49153 Destination port: x11
27	5.350555	3ffe:2::2	3ffe:1:4:1:200:ff:fe0	UDP	Source port: 49153 Destination port: x11
28	5.352555	3ffe:2::2	3ffe:1:4:1:200:ff:fe0	UDP	Source port: 49153 Destination port: x11
29	5.354555	3ffe:2::2	3ffe:1:4:1:200:ff:fe0	UDP	Source port: 49153 Destination port: x11
30	5.356555	3ffe:2::2	3ffe:1:4:1:200:ff:fe0	UDP	Source port: 49153 Destination port: x11
31	5.358555	3ffe:2::2	3ffe:1:4:1:200:ff:fe0	UDP	Source port: 49153 Destination port: x11

```
0000   00 00 00 00 00 05 00 00   00 00 00 03 86 dd 60 00   ........ ......`.
0010   00 01 04 30 29 40 3f fe   00 01 00 00 00 00 00 00   ...0)@?. ........
0020   00 00 00 00 00 01 3f fe   00 01 00 00 00 00 00 00   ......?. ........
```

Fig. 4.2. Pcap trace of mobile access gateway

server module to the PMIPv6 extension in NS3, which only checks for the MN-ID and returns a response to the MAG.

4.1.1 RADIUS

Remote Authentication Dial In User Service(RADIUS) [11] is one of the networking protocol that provides centralized authentication authorization and Accounting(AAA) services to the clients that connect to a network and use the service. Radius is an application layer protocol which uses UDP as its transport protocol and listens on port 1812 for incoming connections. AAA services using Radius are provided in two phases 1) Authentication and Authorization and 2)Accounting which are collectively called AAA transact.

When a mobile node requests access to the networking services via the MAG, the MAG is responsible for sending an access request message to the Radius server. The request consists of access specific security information such as username, password or security certificates or other information which the Radius server can use to identify the MN. Different authentication schemes are available to verify the information sent by the MAG such as PAP(Password Authentication Protocol), EAP(Extensible Authentication Protocol), and CHAP(Challenge-Handshake Authentication Protocol). Upon receiving the request and verifying the information in the request the Radius server can send one of the three messages 1)Access Accept, 2)Access Reject or 3) Access Challenge depending upon the type of authentication scheme used. Figure 4.3 shows the Authentication and Authorization phase in the AAA transact.

Access-Accept

This message is sent to the Radius client(MAG) after the Radius server has successfully authenticated the MN with the information provided in the access-request message. The server also checks if the requesting node is authorized to use the services requested.

Access-Reject

This message is sent to the Radius client(MAG) if the Radius server cannot successfully authenticate the MN. The reason for authentication failure can be due to improper identification of the MN or the MN is not registered with the Radius server and it cannot authenticate the MN.

Access-Challenge

This message is sent to the Radius client(MAG) to request additional information if the Radius server is set to use more sophisticated security mechanisms where the user needs to provide information such as secondary password, token, pin etc.

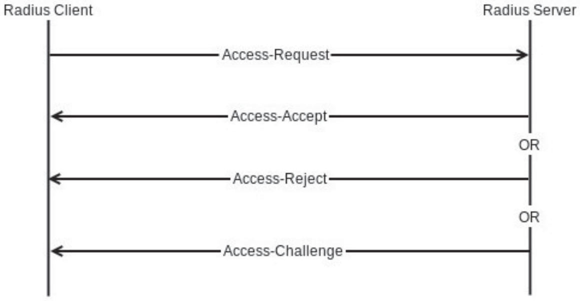


Fig. 4.3. Radius AAA Transact Phase I

The second phase of the AAA transact is accounting. When a MN is granted access to the networking services the Radius client sends a accounting request message to the radius server with Acct-Status-Type value set to ”start”. This record generally contains information such as MN identification, network address, POA(point of attachment) and a session identifier. The Radius client sends periodical updates to the Radius server know as the interim update records with Acct-Status-Type set to value ”interim update”. This message is used to sends updates about the current session of the mobile node. The Radius client sends a Radius accounting request message with Acct-Status-Type set to ”stop” when the MN access to the network service is terminated. The accounting part in the radius server is basically used for network monitoring and billing purpose. Figure 4.4 shows the Accounting phase in the AAA transact.

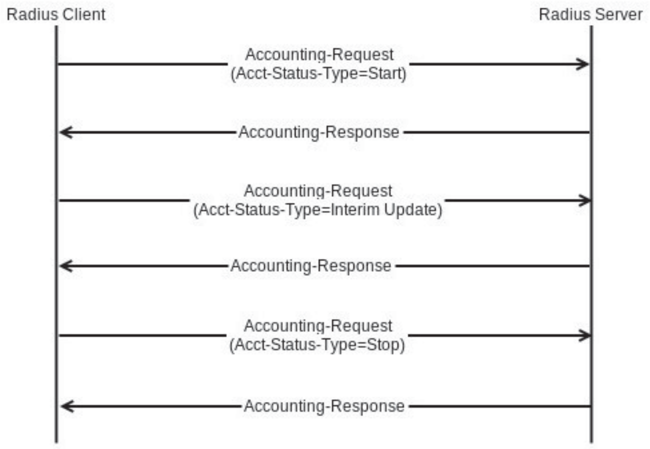


Fig. 4.4. Radius AAA Transact Phase II

As mention earlier Radius uses UDP as its transport protocol and listens on port 1812 for authenticating and authorizing and port 1813 for accounting. The size of the radius header is 20 bytes and includes fields such as 1)Code(1 Byte) 2)Identifier(1 Byte) 3)Length(2 Bytes) and 4)Authenticator(16 Bytes). Figure 4.5 shows the structure of a radius Packet.

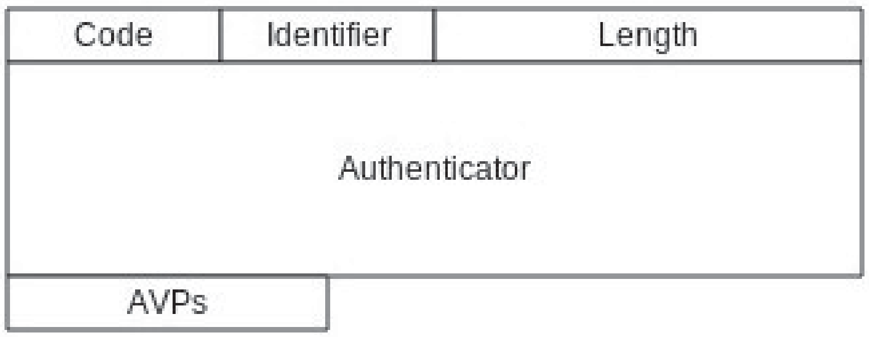


Fig. 4.5. Radius Packet Structure

Table 4.1
Radius Header code

Code	Type of Message
1	Access-Request
2	Access-Accept
3	Access-Reject
4	Accounting-Request
5	Accounting-Response
11	Access-Challenge
12	Status-Server
13	Status-Client
255	Reserved

Code

The code field is used to recognize the type of packet the server or the client received. If either of the two receive a radius packet with an invalid code the packet is silently discarded. Table 4.1 shows all the valid codes and their assignment.

Identifier

Identifier is 1 byte long and generally used for matching the request with the response.

Length

Length field is 2 bytes longs and specifies the total length of the radius packet which includes the header as well as the Radius Attributes.

Authenticator

The authenticator field is 16 bytes longs and contains information regarding the security parameters exchanged between the client and the server.

Attribute Value Pairs

The Radius AVPs carry information regarding authentication, authorization and accounting in the radius packets. This amount of information being sent can be determined by the length field in the radius header. Figure 4.6 shows the attribute value pairs structure. It consists of 1)Type(1 byte) 2)Length(1 byte) and 3)Value(variable length).

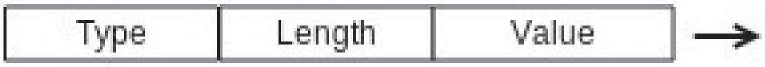


Fig. 4.6. Radius Attribute Value Pair Structure

For our simulations we chose Radius as our AAA server. We implemented a simplest form of a radius server with only the first part of AAA transact i.e Authentication and Authorization. The radius server implemented only authenticates and authorizes the MN but does not support accounting. The authentication is done based on the username which is just the plain MN identifier. The implemented radius header is derived from the header class of NS3 allowing us to use the serialize and deserialize features in those class for realistic packets. Also the code for the header and the radius attributes is generic and can be extended for other attributes as well. The Radius server implementation was integrated to the existing PMIP module in NS3 and radius server available with AAAhelper class. This allowed us to create a AAA node in the PMIPv6 module and to study the behavior of the simulation. The Topology after including the AAA server is show in Figure 4.7.

This is the same topology as show in Figure 4.7 but with an addition of the AAA server. In this simulation when the MN attaches to the link layer of the MAG then the MAG would first send out a Radius request and only after it receives the radius

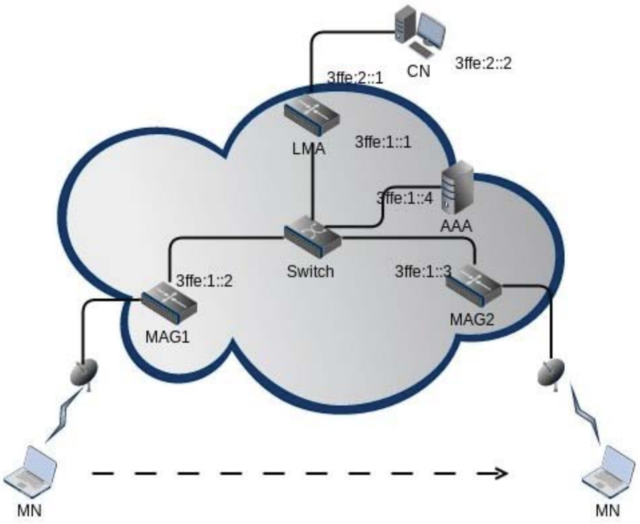
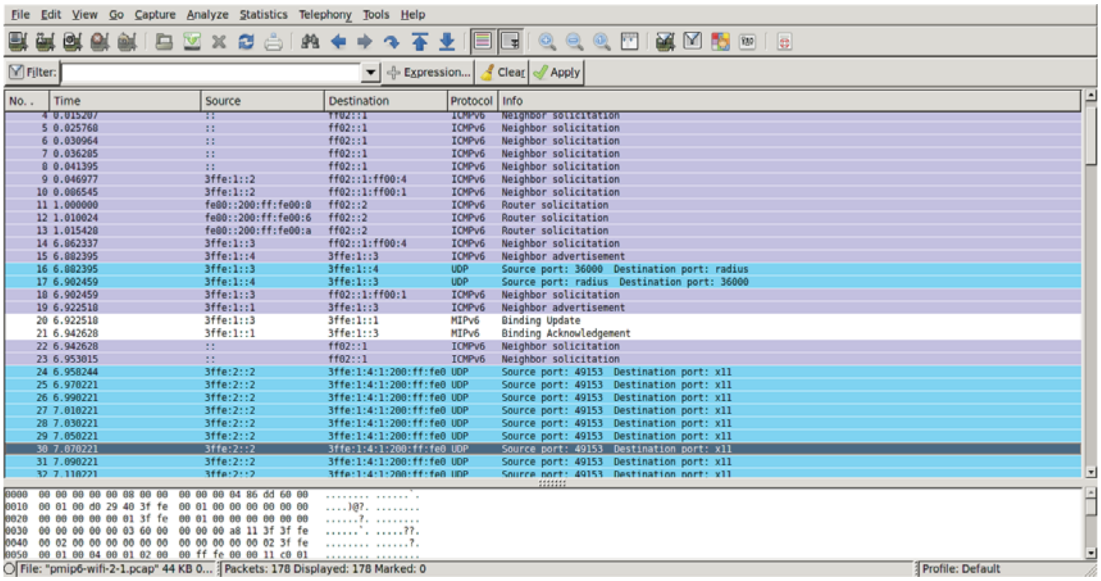


Fig. 4.7. PMIPv6 Topology with the Radius Server

response it initiates the LMA registration process. The simulation result can be seen through the trace of MAG2 interface1 shown in Figure 4.8


File Edit View Go Capture Analyze Statistics Telephony Tools Help
Filter:
Expression...
Clear
Apply

```
No. .  Time       Source              Destination           Protocol Info
    4 0.015207    ::                  ff02::1               ICMPv6   Neighbor solicitation
    5 0.025760    ::                  ff02::1               ICMPv6   Neighbor solicitation
    6 0.030964    ::                  ff02::1               ICMPv6   Neighbor solicitation
    7 0.036285    ::                  ff02::1               ICMPv6   Neighbor solicitation
    8 0.041395    ::                  ff02::1               ICMPv6   Neighbor solicitation
    9 0.046977    3ffe:1::2           ff02::1:ff00:4        ICMPv6   Neighbor solicitation
   10 0.086545    3ffe:1::2           ff02::1:ff00:1        ICMPv6   Neighbor solicitation
   11 1.000000    fe80::200:ff:fe00:8 ff02::2               ICMPv6   Router solicitation
   12 1.010024    fe80::200:ff:fe00:6 ff02::2               ICMPv6   Router solicitation
   13 1.015428    fe80::200:ff:fe00:a ff02::2               ICMPv6   Router solicitation
   14 6.862337    3ffe:1::3           ff02::1:ff00:4        ICMPv6   Neighbor solicitation
   15 6.882395    3ffe:1::4           3ffe:1::3             ICMPv6   Neighbor advertisement
   16 6.882395    3ffe:1::3           3ffe:1::4             UDP      Source port: 36000  Destination port: radius
   17 6.902459    3ffe:1::4           3ffe:1::3             UDP      Source port: radius  Destination port: 36000
   18 6.902459    3ffe:1::3           ff02::1:ff00:1        ICMPv6   Neighbor solicitation
   19 6.922518    3ffe:1::1           3ffe:1::3             ICMPv6   Neighbor advertisement
   20 6.922518    3ffe:1::3           3ffe:1::1             MIPv6    Binding Update
   21 6.942628    3ffe:1::1           3ffe:1::3             MIPv6    Binding Acknowledgement
   22 6.942628    ::                  ff02::1               ICMPv6   Neighbor solicitation
   23 6.953015    ::                  ff02::1               ICMPv6   Neighbor solicitation
   24 6.958244    3ffe:2::2           3ffe:1:4:1:200:ff:fe0 UDP      Source port: 49153  Destination port: x11
   25 6.970221    3ffe:2::2           3ffe:1:4:1:200:ff:fe0 UDP      Source port: 49153  Destination port: x11
   26 6.990221    3ffe:2::2           3ffe:1:4:1:200:ff:fe0 UDP      Source port: 49153  Destination port: x11
   27 7.010221    3ffe:2::2           3ffe:1:4:1:200:ff:fe0 UDP      Source port: 49153  Destination port: x11
   28 7.030221    3ffe:2::2           3ffe:1:4:1:200:ff:fe0 UDP      Source port: 49153  Destination port: x11
   29 7.050221    3ffe:2::2           3ffe:1:4:1:200:ff:fe0 UDP      Source port: 49153  Destination port: x11
   30 7.070221    3ffe:2::2           3ffe:1:4:1:200:ff:fe0 UDP      Source port: 49153  Destination port: x11
   31 7.090221    3ffe:2::2           3ffe:1:4:1:200:ff:fe0 UDP      Source port: 49153  Destination port: x11
   32 7.110221    3ffe:2::2           3ffe:1:4:1:200:ff:fe0 UDP      Source port: 49153  Destination port: x11
```

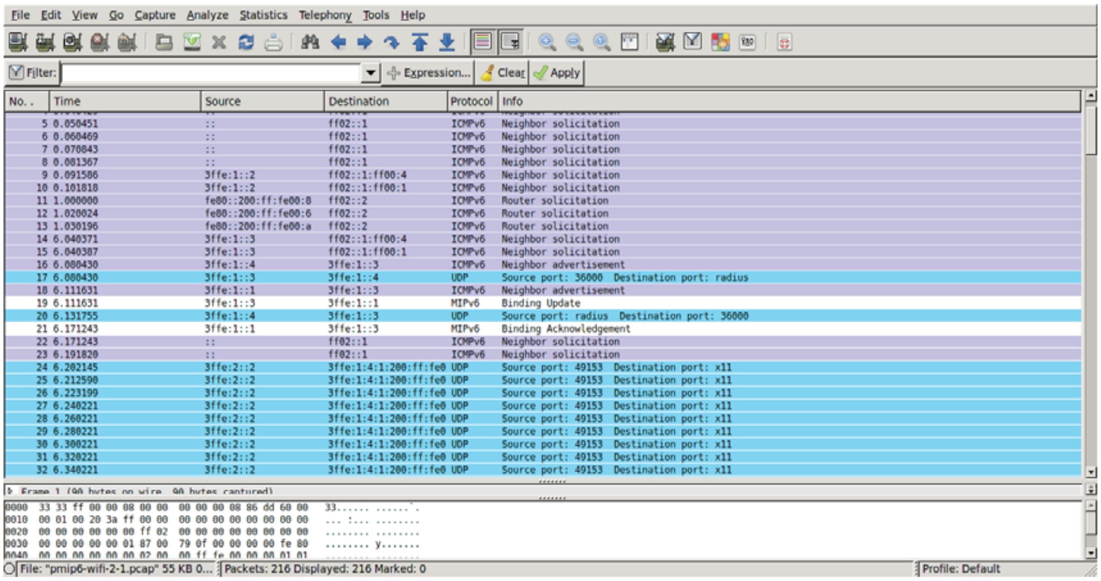
```
0000  00 00 00 00 00 08 00 00  00 00 00 04 86 dd 60 00   ........ ......`.
0010  00 01 00 d0 29 40 3f fe  00 01 00 00 00 00 00 00   ....)@?. ........
0020  00 00 00 00 00 01 3f fe  00 01 00 00 00 00 00 00   ......?. ........
0030  00 00 00 00 00 03 60 00  00 00 00 a8 11 3f 3f fe   ......`. .....??.
0040  00 02 00 00 00 00 00 00  00 00 00 00 00 02 3f fe   ........ ......?.
0050  00 01 00 04 00 01 02 00  00 ff fe 00 00 11 c0 01   ........ ........
```

File: "pmip6-wifi-2-1.pcap" 44 KB 0... Packets: 178 Displayed: 178 Marked: 0 Profile: Default

Fig. 4.8. Pcap Trace of MAG2 (Current Approach)

We can see that at 6.882395 seconds the MAG sends out a radius access request to the AAA server and receives a response at 6.982459 seconds. Only after receiving this response the MAG sends a registration message to the LMA and the registration process continues.

To implement the proposed approach in PMIP module the Binding Update List can be modified to indicate the AAA authentication and the LMA registration is completed. In case 1, if the AAA response arrives before the LMA response the the boolean value field in the BUL m_aaareg can be set and when the LMA registration responses arrives the MAG can go ahead and establish the tunnel and start forwarding the packets. In case 2, is the LMA registration response arrives before the AAA authentication response the boolean value field in BUL m_lmareg can be set and after the AAA authentication is received the MAG gateway can go ahead and setup the tunnel and forward the packets. These m_aaareg and m_lmareg boolean values can be used to achieve the proposed mechanism. The Pcap trace of one of the MAG for the proposed approach is shown in Figure 4.9.



```
No. .  Time      Source               Destination          Protocol Info
     5 0.050451  ::                   ff02::1              ICMPv6   Neighbor solicitation
     6 0.060469  ::                   ff02::1              ICMPv6   Neighbor solicitation
     7 0.070843  ::                   ff02::1              ICMPv6   Neighbor solicitation
     8 0.081367  ::                   ff02::1              ICMPv6   Neighbor solicitation
     9 0.091586  3ffe:1::2            ff02::1:ff00:4       ICMPv6   Neighbor solicitation
    10 0.101818  3ffe:1::2            ff02::1:ff00:1       ICMPv6   Neighbor solicitation
    11 1.000000  fe80::200:ff:fe00:8  ff02::2              ICMPv6   Router solicitation
    12 1.020024  fe80::200:ff:fe00:6  ff02::2              ICMPv6   Router solicitation
    13 1.030196  fe80::200:ff:fe00:a  ff02::2              ICMPv6   Router solicitation
    14 6.040371  3ffe:1::3            ff02::1:ff00:4       ICMPv6   Neighbor solicitation
    15 6.040387  3ffe:1::3            ff02::1:ff00:1       ICMPv6   Neighbor solicitation
    16 6.080430  3ffe:1::4            3ffe:1::3            ICMPv6   Neighbor advertisement
    17 6.080430  3ffe:1::3            3ffe:1::4            UDP      Source port: 36000  Destination port: radius
    18 6.111631  3ffe:1::1            3ffe:1::3            ICMPv6   Neighbor advertisement
    19 6.111631  3ffe:1::3            3ffe:1::1            MIPv6    Binding Update
    20 6.131755  3ffe:1::4            3ffe:1::3            UDP      Source port: radius  Destination port: 36000
    21 6.171243  3ffe:1::1            3ffe:1::3            MIPv6    Binding Acknowledgement
    22 6.171243  ::                   ff02::1              ICMPv6   Neighbor solicitation
    23 6.191820  ::                   ff02::1              ICMPv6   Neighbor solicitation
    24 6.202145  3ffe:2::2            3ffe:1:4:1:200:ff:fe0 UDP     Source port: 49153  Destination port: x11
    25 6.212590  3ffe:2::2            3ffe:1:4:1:200:ff:fe0 UDP     Source port: 49153  Destination port: x11
    26 6.223199  3ffe:2::2            3ffe:1:4:1:200:ff:fe0 UDP     Source port: 49153  Destination port: x11
    27 6.240221  3ffe:2::2            3ffe:1:4:1:200:ff:fe0 UDP     Source port: 49153  Destination port: x11
    28 6.260221  3ffe:2::2            3ffe:1:4:1:200:ff:fe0 UDP     Source port: 49153  Destination port: x11
    29 6.280221  3ffe:2::2            3ffe:1:4:1:200:ff:fe0 UDP     Source port: 49153  Destination port: x11
    30 6.300221  3ffe:2::2            3ffe:1:4:1:200:ff:fe0 UDP     Source port: 49153  Destination port: x11
    31 6.320221  3ffe:2::2            3ffe:1:4:1:200:ff:fe0 UDP     Source port: 49153  Destination port: x11
    32 6.340221  3ffe:2::2            3ffe:1:4:1:200:ff:fe0 UDP     Source port: 49153  Destination port: x11

▷ Frame 1 (90 bytes on wire, 90 bytes captured)

0000  33 33 ff 00 00 08 00 00  00 00 00 08 86 dd 60 00   33...... ......`.
0010  00 01 00 20 3a ff 00 00  00 00 00 00 00 00 00 00   ... :... ........
0020  00 00 00 00 00 00 ff 02  00 00 00 00 00 00 00 00   ........ ........
0030  00 00 00 00 00 01 87 00  79 0f 00 00 00 00 fe 80   ........ y.......
0040  00 00 00 00 00 00 02 00  00 ff fe 00 00 08 01 01   ........ ........

File: "pmip6-wifi-2-1.pcap" 55 KB 0...  Packets: 216 Displayed: 216 Marked: 0  Profile: Default
```

Fig. 4.9. Pcap Trace of MAG2 (proposed Approach)

As we can see in the trace the MAG does not wait for the AAA response instead sends a PBU to the LMA at 6.111631 seconds. The MAG receives the AAA response at 6.131755 seconds which is after the PBU message is sent. Later the PBA is received at 6.171243 seconds. This approach reduces the L3 handoff latency approximately by 50% and is discussed in detail in the next section.

5. RESULTS

5.1 Setup

The simulation was carried out on a simple topology with all the required nodes like the Local Mobility Anchor, Mobile Access Gateway, AAA server, Correspondent Node and the Mobile node. The Topology is shown in Figure 5.1.

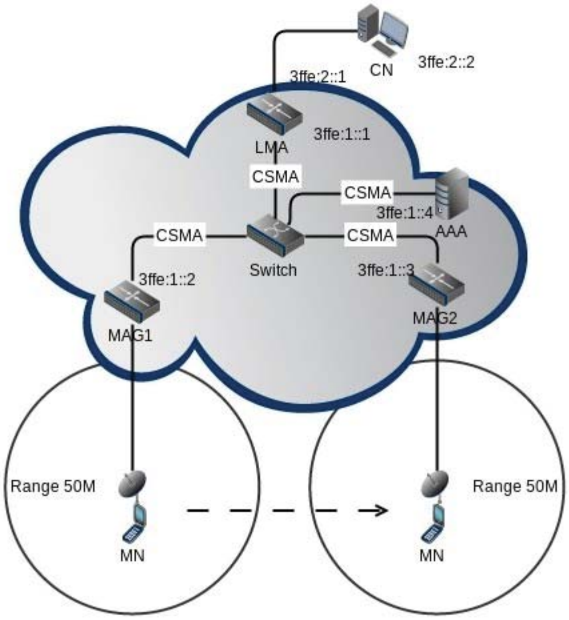


Fig. 5.1. Simulated Topology with current and proposed approach

We can divide the topology into three individual segments. The outer-net which consists of the correspondent node and one of the LMA interfaces as shown in Figure 5.1. The outer-net has only one CSMA link with the datarate of 50Mbps and a delay of 0.1 ms. The outer-net belongs to 3ffe::2::/64 subnet. The second segment will be the backbone Network consisting of the LMA, MAG's and the AAA server. They are all connected to a L2 switch individual CSMA links. The bandwidth of all the CSMA links on the backbone network is 50Mbps. The link delay is varied from 1ms to 10ms during the simulation. The backbone network belongs to 3ffe::1::/64 sunbet. The third and the final segment contains the MAG1-net and MAG2-net. A unified MAC adddress of 00:00:AA:BB:CC:DD is assigned to the interfaces on MAG1 and MAG2 facing the MAG 1-net and MAG2-net respectively so that the MN does not change the default gateway even after changing the access point for seamless connectivity. This way the same link local address fe80::200:aaff:febb:ccdd is assigned to both the interfaces.

The access point connected to the MAG have a range of 50 meters and are separated by a distance of 110 meters. The MN starts from the location of access point 1 and moves towards access point 2 at a speed of 10m/s(36Km/hr). The communication between the CN and the MN starts at 1.5 seconds. We have studied the 1) L3 handoff latency with no data traffic, 2) L3 handoff latency with Voip data traffic, and 3) Packet loss.

5.2 Simulation Results

1. **L3 Handoff Latency without Data Traffic**

   Figure 5.2 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 5.1 shows the values obtained for the simulation with out data traffic.

Table 5.1
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

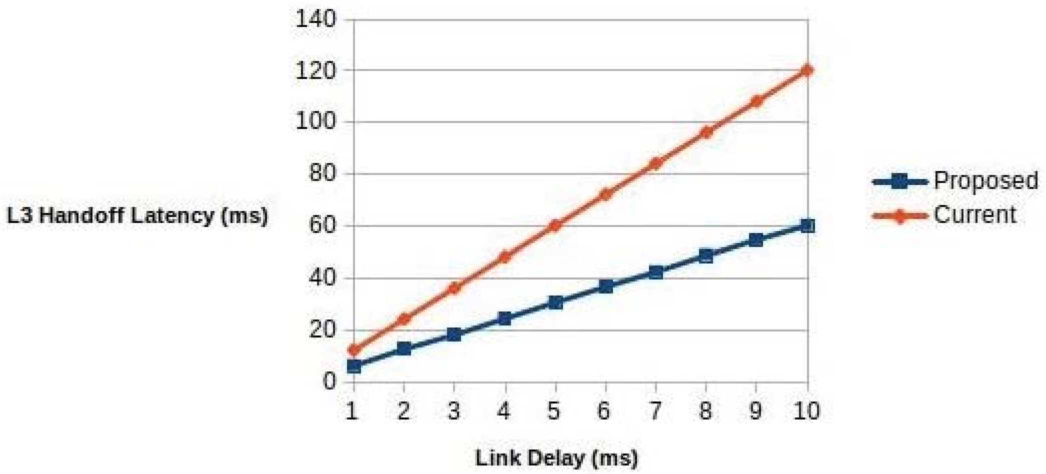


Fig. 5.2. L3 Handoff Latency without Data traffic

2. **L3 Handoff Latency with Data Traffic**

Figure 5.3 shows the link delay vs L3 handoff latency comparison for both the current approach and the proposed approach with Voip traffic present. The Voips taffic 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 senarios we can see that the proposed approach still performs better than the current approach. Table 5.2 shows the values obtained for the simulation with Voip data traffic.

Table 5.2
L3 Handoff Latency Readings(Voip data Traffic)

Link Delay(ms)	**Proposed Approach(ms)**	**Current Approach(ms)**
5	30.186	60.233
6	41.418	73.746
7	50.758	92.524
8	58.167	107.414
9	55.728	115.272
10	91.593	157.789

3. **Packet Loss with Data Traffic**

Figure 5.4 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. Table 5.3 gives the packet loss data results during simulation.

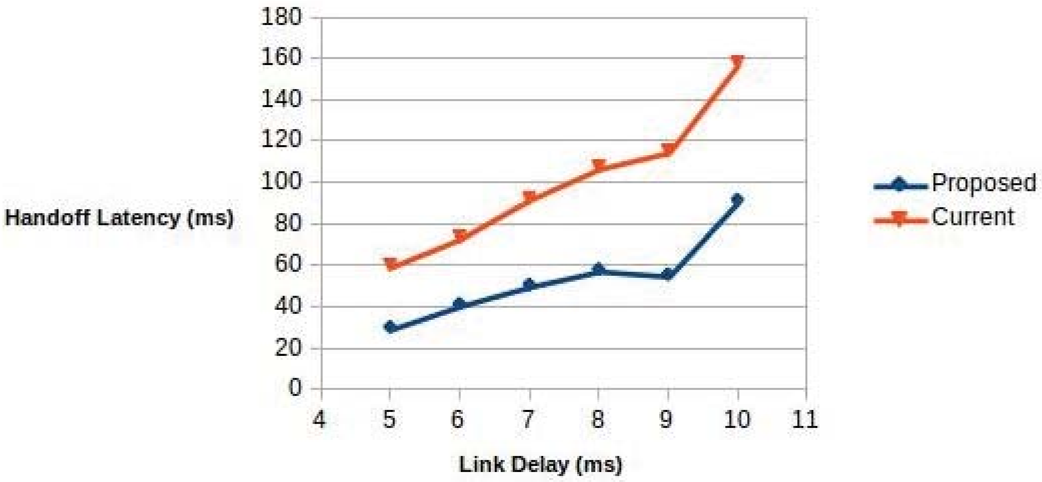


Fig. 5.3. L3 Handoff Latency with Data traffic

Table 5.3
Packet loss Readings

Link Delay(ms)	**Proposed Approach**	**Current Approach**
5	55	56
6	55	57
7	55	58
8	56	59
9	56	59
10	60	63

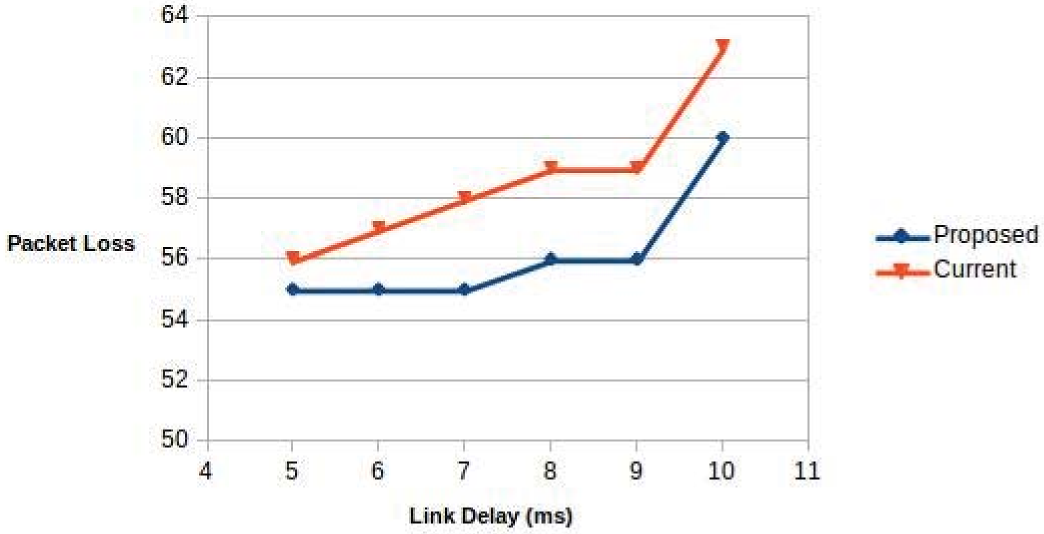


Fig. 5.4. Packet Loss with Data traffic

6. CONCLUSION AND FUTURE

6.1 Conclusion

In my thesis we studied the proxy mobile ipv6 protocol in detail and also different approaches proposed to reduce the handoff latency and packet loss. After carefully reviewing we came up with a idea which we thought would reduce the L3 handoff latency and also reduce packet loss. The idea was to change 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%. We have performed all our simulations in network simulator 3 with PMIPv6 module add-on. We had to make 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 our theoretical calculations and that the proposed version always performs better than the current version.

6.2 Future Scope

Though 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.

LIST OF REFERENCES

LIST OF 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] "Network simulator 3 description." http://www.nsnam.org/. Last date accessed: January 25, 2012.

[10] 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/. Last date accessed: September 09, 2013.