Distributed Data Path and Mobility Function Scheme for PMIPv6 in Flattened Networks

Petro P. Ernest[1], Olabisi E. Falowo[1] and H. Anthony Chan[2]
[1]Department of Electrical Engineering, University of Cape Town, Rondebosch 7701, South Africa
[2]Futurewei Technologies, Plano, Texas, USA
Tel: +27 21 6502813, Fax: +27 216503465
pernest@crg.ee.uct.ac.za; bisi@crg.ee.uct.ac.za; h.a.chan@ieee.org

Abstract— Proxy Mobile IPv6 is a most promising mobility management solution to pave a way toward all IP-based networks for the next generation networks. Many researchers are paying attention to PMIPv6 because of its network-based mobility feature. However, PMIPv6 relies on centralized and hierarchical mobility management approach that make it difficult to break away from problems such as single point of failure and bottleneck, and non-optimal routing path. To address these problems, a distributed mobility management scheme for PMIPv6 is proposed. The proposed scheme separates user's data plane from control plane. It establishes a data path for an MN data along the shortest path between different access networks. The paper presents the scheme's design, operational mechanism and performance evaluation. The performance evaluation of the scheme has been conducted using mathematical models. The numerical results show that the proposed scheme has a much significant better packet delivery latency than PMIPv6.

Index Terms— PMIPv6, IP mobility management, distributed mobility management

I. Introduction

The current rapid growth in number of mobile users, smart-phones and other mobile broadband capable devices is expected to push a huge volume of mobile data traffic in the next generation network (NGN). The NGNs will be fully IP-based network that will use IP mobility management solutions for mobility support of the mobile nodes (MNs). Moreover, the NGNs will be flat network due to the current trends in both wireless and mobile networks toward flat network architecture. Therefore, IP mobility management solution suitable for flat network architecture and able to accommodate the increasing data traffic volume is a desirable solution.

The existing IP mobility management solutions rely on a central mobility anchor such as a Home Agent in Mobile IPv6 [1] to manage both control and data traffic. The central mobility anchor introduces a single point of failure and bottleneck. Furthermore, the central mobility anchor centralizes the routing path which can result in non-optimal routing path [2]. Consequently, it may be difficult to accommodate the increasing mobile data traffic volume while using the current IP mobility management solution as they lead to all traffic being pushed to the core network for the mobility sake.

One promising solution for mobility management support in flattened network is the use of the distributed mobility management approach. Hence, an enhancement of the existing IP mobility management solutions with a distributed mobility management approach is needed [2] [3].

Proxy Mobile IPv6 (PMIPv6) [4] is one of the most promising mobility management solution to pave a way toward an all IP-based networks, and it has received considerable attention from many researchers and adoption by WiMAX forum [5] and in 3GPP standards, such as Evolved Packet Core (EPC) [6].

PMIPv6 is a network-based localized mobility management solution standardized by the IETF. It is composed of a Local Mobility Anchor (LMA) and several Mobile Access Gateways (MAGs). In basic PMIPv6 standard [4], data packets toward and from the MNs are encapsulated in bidirectional tunnels between MAGs and LMA. All communication between MNs and correspondent nodes (CNs) traverses the LMA which imposes a processing burden on LMA. Moreover, the binding updates for all MNs are serviced by the LMA that also increase load on LMA as the number of MNs in PMIPv6 domain increase [2], [7]. Hence, it may become difficult for PMIPv6 to break away from a single point of failure and bottleneck issue, and triangle routing problems.

Although PMIPv6 is the promising mobility management solution, it still needs enhancement to fit well with the flattened network architecture. This paper therefore proposes a distributed mobility management scheme for PMIPv6. The proposed scheme is named Distributed Data Path and Mobility Function scheme for PMIPv6 (DDMPMIPv6). DDMPMIPv6 distributes mobility functions of the LMA to the access part of the network that is at the MAG level. This relieves LMA from being responsible for all mobility management functions of all MNs that in turn reduce the bottleneck and single point of failure problems. Moreover, DDMPMIPv6 scheme distributes the data routing path to the access part of the network, hence, it addresses the triangle routing problem and improves packet delivery latency. Furthermore, the scheme uses two cache memories to enable MN reachability inside and outside the distributed DDMPMIPv6 domain.

The contribution of this paper includes (i) detailed explanation of the design and functional operation of the proposed scheme, (ii) a mechanism that enables a network to differentiate the MN first attachment from handover, and the new network to know IP address of the old network the MN has detached from, and (iii) a method that address the MN reachability in a distributed mobility management architecture.

The rest of this paper is organized as follows. Section II presents the related work. Section III describes the proposed DDMPMIPv6 scheme. Section IV presents the performance evaluation and analytical results of the proposed scheme and compares it to PMIPv6. Finally, Section V concludes the paper.

II. RELATED WORK

PMIPv6 [4] addresses the MIPv6 [1] limitations by removing the mobility management functions from MN and moving them to the network. This alleviates the need for the protocol stack modification of the MN. However, the mobility challenge issues such as the traffic concentration on LMA, non-optimal routing path, and single point of failure have not been solved by PMIPv6 due to the use of centralized mobility management approach [2]. Distributed mobility management (DMM) is one of the approaches to address these problems. DMM relieves the mobility management functions from the central mobility anchor and place them in the access part of the network. The mobility management function of the central anchor can be fully distributed or partially distributed [3]. In fully DMM, the mobility management functions of the central anchor are fully distributed to the access part of the network. On the other hand, partially DMM separates the user data plane from control plane where the data plane can be distributed to the access part of the network.

In the literature [8], [9], routing optimization schemes for PMIPv6 have been proposed. The schemes distribute data path to MAGs by building tunnels between the source and the destination MAGs. However, the schemes mechanism still inherits the centralized mobility management approach.

Fabio, et al. [10] has proposed two DMM schemes that re-use the concept of PMIPv6. The schemes allow an MN to configure different IP addresses from different mobility anchors. However, the authors do not discuss how CN can reach the MN that configures different IP addresses from different networks. Thus, it may be difficult for the CN to know which IP address the MN is using at a given instant in order to send packets to MN via optimal path. Otherwise, the packets will always traverse the network that owns the IP prefix of the destination address which may not be the optimal path.

Bertin, et al. [11] discussed a distributed dynamic and mobility management scheme for flat architecture. However, the scheme depends on the MN uplink data traffic in order to discover the previous MN's network information and setup tunnel. This may result in increased delay for the downlink data traffic, if the MN has nothing to send in the uplink after it has moved to a new network.

III. ARCHITECTURE OF THE PROPOSED DDMPMIPV6

In this Section, the proposed DDMPMIPv6 scheme is presented. The scheme is based on DMM concepts; it distributes the data routing path to the access part of the network. This relieves traffic concentration from a single network element. The scheme is built on PMIPv6 by pushing mobility functions of LMA to the access part of the network, at the access router level. Each access router (AR) is capable of performing both LMA and MAG functions depending on whether the MN is registered to that AR or is visiting the AR. The new network element called Mobility Tracking Manager (MTM) is introduced. MTM enables a correspondent node (CN) to reach the MN for data delivery as well as the new network to know the address of the old network the MN has detached from during handover.

The DDMPMIPv6 functional architecture is mainly composed of two network elements namely; Distributed Mobility Access Router (DMAR) and Mobility Tracking Manager (MTM) as illustrated in Fig. 1.

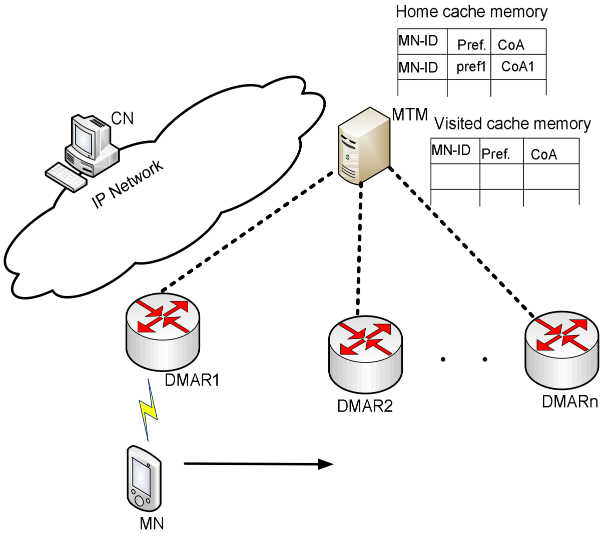

Fig. 1. DDMPMIPv6 Architecture.

The DMAR is an access router that is capable of performing both LMA and MAG functions. Each DMAR allocates a home network prefix (HNP) to an MN attached to its network, caches the MN's binding information, intercepts packet for a registered MNs when they move away from its network and de-capsulates the data traffic for the visiting MNs.

The MTM is responsible for tracking the MN's mobility information. It holds two cache memories, which are Home Cache Memory (HCM) and Visited Cache Memory (VCM). HCM stores the MN's home network binding information. VCM keeps the MN's visiting network binding information. The binding in VCM includes a care-of-address the MN is currently reachable when it moves away from its home network. The binding information in VCM is updated each time the MN changes networks. On the other hand, the binding information in HCM does not change when the MN changes network. This enables the MN to keep the same IP address assigned during its registration in the domain.

A. *Initial MN Registration Procedure and Communication Establishment*

When an MN enters DDMPMIPv6 domain for the first time, it attaches to DMAR, for example DMAR1. The MAG functions in DMAR1 detect the MN attachment and get the MN identifiers (MN-ID). Then, DMAR1 proposes an IP prefix (i.e., pref1) to assign to the MN from its IP prefix range. Next, the MN attachment is verified if the attachment is a first attachment or a handover through sending a binding request (BReq) message to MTM. The BReq message includes MN-ID and pref1as illustrated in Fig. 2. It is assumed that all DMARs in the domain know the MTM. This can be preconfigured by the network administrator. Hence, each DMAR knows where to send BReq message.

When MTM receives BReq message, it extracts the MN-ID and uses the MN-ID to find the MN's binding information from the HCM. Since the MN is attaching to the domain for the first time, HCM has no binding information for the MN. Hence, MTM caches the MN-ID, pref1, and the address of DMAR1 in its HCM. Then, MTM responds to the request by sending a binding reply (BRep) messages to DMAR1 as shown in Fig. 2.

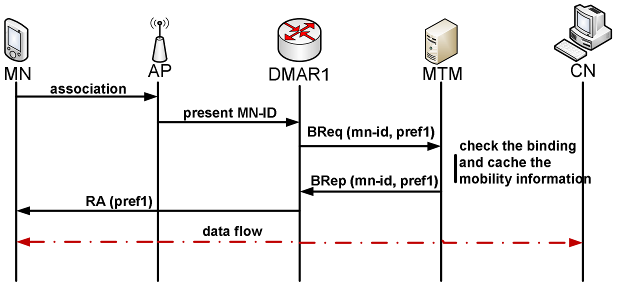

Fig. 2. MN registration signaling flow.

Upon receiving the BRep message, DMAR1 extracts pref1 included in the message. Given that the pref1 is the prefix that has been proposed, DMAR1 realizes that the MN is attaching to the domain for the first time. Then DMAR1 sends a router advertisement (RA) including pref1 to the MN. Finally, the MN configures the IP address (HoA1) using pref1.

After the MN has configured HoA1, it can establish a communication to a Correspondent Node (CN) using HoA1 as the source IP address. The MN sends packet to DMAR1. When DMAR1 receives packet from MN, it uses the routing table to forward the packet to CN. As long as the MN remains attached to DMAR1, the packets are forward directly to CN without tunneling. Thus, there is no packet that traverses MTM. That is, the burden of the traffic concentration at a single point is reduced.

B. *Handover scenario*

The MN registered to DMAR1 can move to another DMAR such as DMAR2 as shown in Fig. 3.

When an MN changes a network, for example from DMAR1 to DMAR2, the MAG functions in DMAR2 detect its attachment. Then, DMAR2 gets the MN-ID and proposes an IP prefix (i.e., pref2) to assign to the MN from its IP prefix range. Then, DMAR2 sends a verification message to MTM so as to verify if the MN is attaching to the network for the first time or the MN has performed handover as illustrated in Fig. 4.

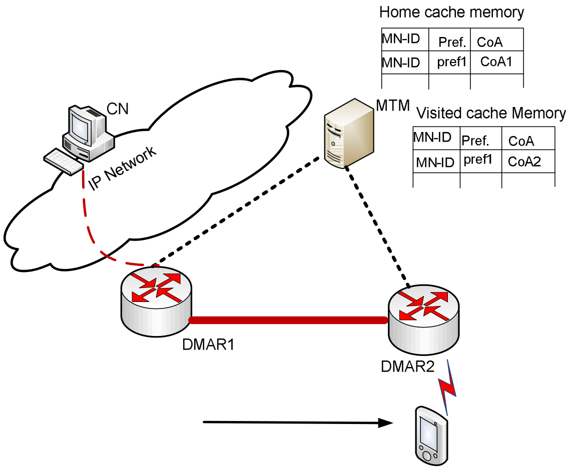

Fig. 3. MN moved to visited network.

Upon receiving the BReq message, MTM gets the MN-ID and uses the MN-ID to search for MN's binding information from the HCM. Because the MN has performed handover its binding information is available in HCM. Then, MTM caches the new MN's location, DMAR2 address, to VCM as shown in Fig.3. Now, MTM sends a reply message, BRep, to DMAR2. The BRep message includes pref1 and address of DMAR1 (CoA1). This enables DMAR2 to know the network the MN has detached from.

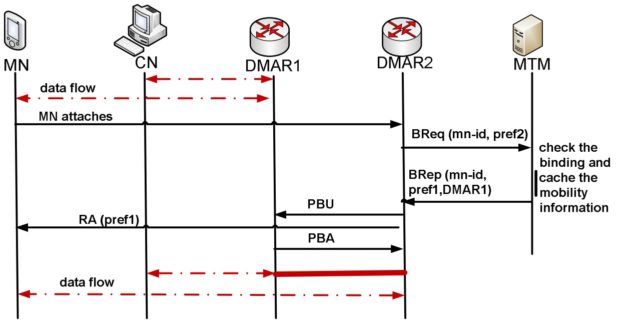

Fig. 4. Handover signaling flow in DDPMIPv6.

When DMAR2 receives BRep message, it compare the IP prefix included in the message with the prefix it has proposed. Since the prefix in the BRep message is pref1, DMAR2 realizes that the MN has performed handover to its network. Hence, the MAG functions collocated in DMAR2 is activated for pref1 and DMAR2 establishes a tunnel to DMAR1 through exchange of PBU and PBA messages as in [4]. In parallel, DMAR2 sends a RA that includes pref1 to the MN. When an MN receives the RA, it knows that it is still in the same network and does not configure a new HoA. This enables a MN to retain the same IP address regardless of the network the MN has moved to within the domain.

When DMAR1 receives PBU message from DMAR2, it updates the MN's binding and setup a tunnel end point for pref1 to DMAR2. In this regard, DMAR1 performs the role of LMA where DMAR2 assumes the role of MAG. The packets now flow from CN to DMAR1, and then DMAR1 tunnels them to DMAR2. Then DMAR2 de-capsulate packets and deliver them to MN as illustrated in Fig. 4.

C. MN Reachability Procedure and Data flow

Reachability is a significant component of any mobility management scheme that allows the CN to locate the MN for data delivery. In this sub-section, we consider two scenarios, the first scenario addresses the reachability problem when both MN and CN are inside the DDMPMIPv6 domain and the second scenario considers the MN reachability from outside the DDMPMIPv6 domain.

i. Both MN and CN inside the DDMPMIPv6 domain

In this scenario both MN and CN are located in the same DDMPMIPv6 domain, for example, the CN is attached to another DMAR (DMAR3) inside the DDMPMIPv6 domain as shown in Fig.5. In the following explanation DMAR1 is the MN home network and HoA1 is the HoA of the MN.

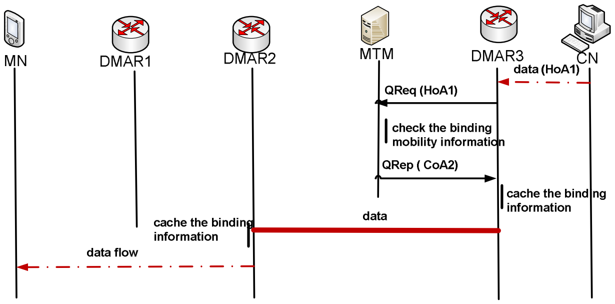

Fig. 5. Reachability signaling flow inside the DDPMIPv6 domain.

When CN sends packet destined for HoA1 the packet arrives at DMAR3, where the CN is attached, see Fig. 5. Then DMAR3 on receiving packet checks if it has binding information for HoA1 in its cache. If no binding information is found DMAR3 sends location query (QReq) message for HoA1 to MTM. On receiving the QReq, the MTM checks the MN binding information from both HCM and VCM. If the MN HoA1 binding information is only found in HCM, MTM returns the address of DMAR1 (CoA1) to DMAR3. If the MN HoA1 binding information is found in both HCM and VCM the MTM returns the address of DMAR2 (CoA2) to DMAR3. In this regards the MN has moved to a visited network with a care-of-address found in VCM. For example, in this scenario the MN is visiting DMAR2; hence, MTM returns CoA2.

When DMAR3 receives the query reply (Qrep) message it caches the binding information for HoA1 and encapsulates the packet to DMAR2. It is important to note that once DMAR3 obtains MN's binding information, it behaves as the LMA while the destination DMAR assumes the MAG roles. Therefore, packets do not go through DMAR1 to which the HoA belongs but are tunneled directly to the current point where the MN is currently attached. Hence, the packet always follows a shorter path. To mitigate the packet loss during the query process the scheme buffers packets at DMAR3.

ii. CN outside the DDMPMIPv6 domain

When the CN is outside the DDMPMIPv6 domain, the packets are routed to DMAR that the HoA belongs. For example, in this scenario the packets are routed to DMAR1. DMAR1 upon receiving the packets checks the MN's binding from its cache memory. If the MN is within its network, it delivers the packet to MN. If the MN has moved away from DMAR1 network, DMAR1 tunnels the packet to the network where the MN is currently attached.

IV. PERFORMANCE EVALUATION

In this section we analyze the performance of DDMPMIPv6 and compare it with PMIPv6. The metrics used in the analysis are handover delay and packet delivery latency. We assume a negligible processing delay at each network element. Furthermore, LMA and MTM are co-located in the network topology because of some functional similarities. Moreover, layer 2 handover latency is assumed to be the same for both schemes. The network topology presented in Fig. 6, and signaling flow represented in Fig. 4 are used for the analysis. The following abbreviations are used:

- The delay between the DMAR/MAG and MTM/LMA is $t_{DMAR/MAG,\ MTM/LMA}$, which is the time required for the packet to travel between DMAR/MAG and MTM/LMA.
- The delay between DMARs/MAGs is $t_{DMAR/MAG,\ DMAR/MAG}$, which is the time the packet takes to travel between DMARs/MAGs.
- The delay between MN and DMAR/MAG is $t_{DMAR/MAG,\ MN}$, which is the time the packet takes to travel from DMAR/MAG to MN through the air interface.

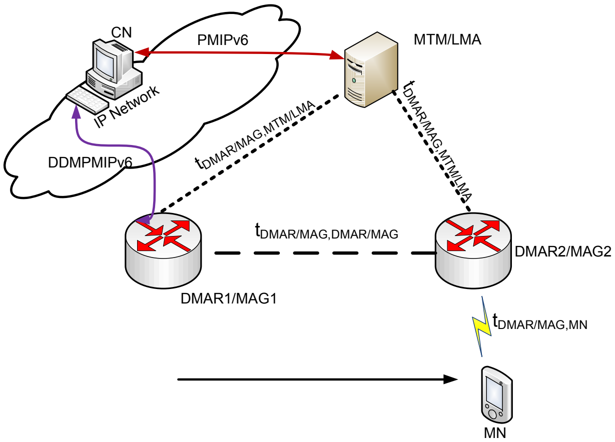

Fig. 6. Evaluation topology.

A. Handover delay performance

During handover in DDMPMIPv6, the new DMAR (nDMAR) sends RA message to MN and PBU message to previous DMAR (pDMAR) at the same time as shown in Fig. 4. Thus, downlink packets and uplink packets experience different handover delay. We define handover delay as the time during which the MN is not able to send or receive packets. The handover delay for down link packet is defined as the time elapsed between when an MN received the last packet through the previous network and the time the MN receives the first packet through the new network. The handover delay for the uplink packets is defined as the time elapsed between when the MN was able to send the last uplink packet through the previous network, before connection break, and when the MN is capable to send the first uplink packet via the new network.

i. Handover latency for the down link packet in DDMPMIPv6

We represent the total handover delay by T_d .When the MN moves to nDMAR, it performs layer 2 handover that constitutes a layer 2 handover delay (t_{L2}). Then nDMAR acquires MN's previous binding information from MTM and sends location update for MN to pDMAR. Lastly, packets flow from pDMAR to nDMAR and then to MN as illustrated in Fig.4. Hence, the handover latency is calculated from Fig.4 and is given in equation (i).

$$T_d = t_{L2} + 2\,(t_{DMAR/MAG,\ MTM/LMA} + t_{DMAR/MAG,\ DMAR/MAG}) + t_{DMAR/MAG,\ MN} \qquad \text{(i)}$$

ii. Handover delay for the uplink packets in DDMPMIPv6

The MN is capable to send the uplink packets on handover as soon as it receives the RA message because the MN does not configure a new IP address. Thus the following delay will occur before the MN is able to send a new uplink packet after handovers to nDMAR;

$$T_d = t_{L2} + 2\,t_{DMAR/MAG,\ MTM/LMA} + t_{DMAR/MAG,\ MN} \qquad \text{(ii)}$$

iii. Handover delay for the down link packets in PMIPv6

When MN handovers to a new MAG (nMAG), it performs layer 2 handover. Then, nMAG acquires MN-ID and sends PBU to LMA. Then LMA updates the tunnel end point to nMAG and responds with PBA. Hence, the handover latency for down link packet is presented as follows:

$$T_d = t_{L2} + 2\,t_{DMAR/MAG,\ MTM/LMA} + t_{DMAR/MAG,\ MN} \qquad \text{(iii)}$$

iv. Handover latency for the uplink packet in PMIPv6

Similarly, the MN can send the uplink packet after it has received the RA message, thus the uplink packet handover delay is:

$$T_d = t_{L2} + 2\,t_{DMAR/MAG,\ MTM/LMA} + t_{DMAR/MAG,\ MN} \qquad \text{(iv)}$$

B. Packet delivery latency

We assume that packet experiences equal latency before it arrives to either DDMPMIPv6 domain or PMIPv6 domain. Moreover, we consider two scenarios. The first scenario is when the MN is attached to a network that assigns IP address to MN (home network). The second scenario is when the MN is attached to a visited network.

i) When the MN is in home network

In DDMPMIPv6, when the MN is attached to DMAR in its home network, the packet is routed from CN network directly to DMAR. Then DMAR forward the packet to MN. Hence, the packet delivery latency for DDMPMIPv6 scheme is:

$$T_d = t_{DMAR/MAG,\ MN} \qquad \text{(v)}$$

In PMIPv6, the MN uses HoA with IP prefix belongs to LMA in all of its communication regardless of where the MN is attached in the domain. Hence, packet traverses the LMA which encapsulates the packet to MAG where the MN is attached. Then, MAG de-capsulate packet and forwards it to MN. The following equation expresses the packet delivery latency for PMIPv6 scheme:

$$T_d = t_{DMAR/MAG,\ MTM/LMA} + t_{DMAR/MAG,\ MN} \qquad \text{(vi)}$$

ii) When an MN is in visited network

In DDMPMIPv6, the packet is first routed to pDMAR. Then, pDMAR encapsulates the packet to nDMAR. Then, nDMAR de-capsulates packet and forward it to MN. Thus, the packet delivery latency for DDMPMIPv6 scheme is expressed as shown in equation below.

$$T_d = t_{DMAR/MAG,DMAR/MAG} + t_{DMAR/MAG,\ MN} \qquad \text{(vii)}$$

In PMIPv6, the packet traverses LMA which encapsulate the packet to MAG. The MAG on receiving a packet, de-capsulates the packet and deliver it to MN as presented in equation below for PMIPv6 scheme.

$$T_d = t_{DMAR/MAG,\ MTM/LMA} + t_{DMAR/MAG,\ MN} \qquad \text{(viii)}$$

C. Numerical result

In this subsection, the numerical results based on the above analysis for the packet delivery latency is presented. We setup a delay between DMAR/MAG and MTM/LMA to 10ms, and a delay between DMAR/MAG and MN to 12ms. The two delay parameters are according to [12]. To investigate the impact of the delay between DMARs/MAGs on the packet delivery latency, the delay between DMARs/MAGs is varied from 2ms to 8ms and the results are shown in Fig.7. Moreover, the effect of the delay between DMAR/MAG and MTM/LMA on packet delivery latency is investigated where the delay parameter between DMAR/MAG and MTM/LMA is varied from 5ms to 15ms as shown on Fig. 8.

Fig.7 and Fig.8 compare the packet delivery latency performance of PMIPv6 and DDMPMIPv6 schemes. From the results, when the MN is in its home network, DDMPMIPv6 shows better packet delivery latency compared to PMIPv6. This is because DDMPMIPv6 anchors packets directly to DMAR where the MN is attached. However, we notice that when the MN moves to a visited network, the packet delivery latency for DDMPMIPv6 increases as the distance between DMARs/MAGs increase as shown in Fig. 7. On the other hand, the packet delivery latency in PMIPv6 increases as the distance between DMAR/MAG and MTM/LMA increases as illustrated in Fig.8.

From these results, the proposed DDMPMIPv6 scheme demonstrates a better packet delivery latency performance compared to PMIPv6. This is because in PMIPv6 the packet delivery time is influenced by the delay between LMA and MAG. Typically, LMA is located far away from MAGs. Hence, the data path between MAG and LMA is longer than the data path between MAG and MAG. Since DDMPMIPv6 uses the data path between DMAR/MAG and DMAR/MAG, it achieves significant better packet delivery latency.

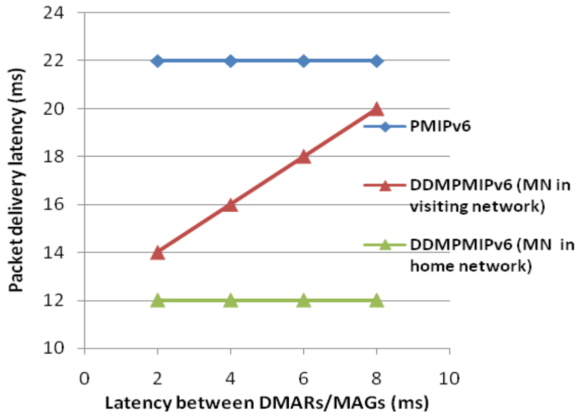

Fig. 7. The impact of the delay between DMARs/MAGs on packet delivery latency.

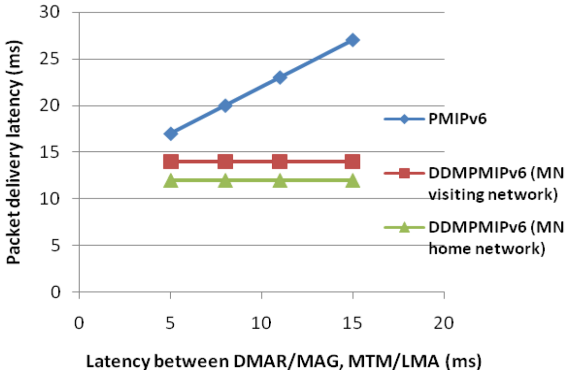

Fig. 8. The influence of the delay between DMAR/MAG and MTM/LMA on packet delivery latency.

V. Conclusion

In this paper, we have proposed DDMPMIPv6 scheme that provides an efficient support for optimizing data path. We used two cache memories in MTM to enable the reachability of the MN. By distributing the data routing path at the access part of the network, the packet delivery latency is improved and the high task burden on LMA in PMIPv6 is removed. Through the performance evaluation results, DDMPMIPv6 has shown a much better packet delivery latency compared to PMIPv6.

References

[1] D. Jonson, C. Perkins, and J. Arkko, “Mobility Support for IPV6,” IETF RFC 6275, July, 2011.

[2] H. A. Chan, Editor, “Problem statement for distributed and dynamic mobility management,” draft-chan-distributed-mobility-ps-05 (work in progress), October, 2011.

[3] H. Yokota, et al., “Use case scenarios for Distributed Mobility Management,”IETF draft-yokota-dmm-scenario-00 (work in progress), October 2010.

[4] S. Gundavelli, K. Leung, V. Devarapalli, K. Chowdhury, and B. Patil, “Proxy Mobile IPv6,” IETF RFC 5213, August,2008.

[5] WiMAX Forum, http://www.wimaxforum.org/, August, 2011.

[6] 3GPP TR 23.882 2.0.0, “3GPP system architecture evolution (SAE): report on technical option and conclusion,” 2008

[7] H.N.Nguyen and C. Bonnet, “ PMIPv6 for Cluster Based Heterogeneous Wireless Mesh Networks,” Proceeding of 5th IEEE International Conference on Mobile Ad Hoc and Sensor Systems,(MASS 2008), Atlanta, GA, USA, September 2008.

[8] Q. Wu and B. Sarikaya, “An extension to proxy mobile IPv6 for local routing optimization,” draft-wu-netext-local-ro-05 (work in progress), February. 2010.

[9] S.Krishnan, R. Koodli, P. Loureiro, Q. Wu, and A dutta, “ Localized routing for proxy mobile IPv6,” draft-ietf-netext-pmip-lr-08, (work in progress), January, 2012.

[10] G. Fabio, O. Antonio, J. B. Carlos, and R.P.F. Costa, “ A Network-based Localised Mobility Solution for Distributed Mobility Management,”, WPMC Workshop on Mobility Management for Flat Networks (WPMC 2011),Brest France, October, 2011.

[11] P. Bertin, S. Bonjour and J. Bonnin “A Distributed Dynamic Mobility Management Scheme Designed for Flat IP architectures,” Proceeding of 3rd International Conference on New Technology, Mobility and Security, (NTMS 2008), April 2008.

[12] K. Kong, W. Lee, Y. Han, M, Shin, and H. You, “Mobility Management for All-IP Mobile Networks: Mobile IPv6 Vs. Proxy Mobile IPv6,” Wireless Communications, vol.5, pp 36-45, April 2008.

Petro P. Ernest received his Master of Science in Electronic Engineering from University of Stellenbosch in 2005. He is currently a PhD candidate in the Department of Electrical Engineering, University of Cape Town. His research interest is mobility management in next generation networks.