Distributed Mobility Management Scheme using Lightweight Fast Handover

Taj Elsir H. Suliman
Sudan University of Science and Technology (SUST)
Sudan Academy for Banking & Financial Sc.(SABFS)
Khartoum, Sudan
Email: tagsir@gmail.com

Eltayeb Salih Abuelyaman
Computer Science Department
Nizwa University, Oman
Email: Abuelyaman@Unizwa.edu.om

***Abstract*—Distributed Mobility Management solutions are aimed at addressing limitations of their centralized counterparts. Among these limitations, the identification of the location of a target node during handover and the corresponding data delivery are critical. Many distributed mobility management schemes have been proposed to address these limitations. However, the resulting solutions are not scalable to large coverage areas. As such, this paper addresses the scalability issue by reducing both handover latency and packet losses. To that end, a Lightweight fast handover technique is proposed. The technique piggy bags routing information in the option-field of the header of an IPv6 packet. Superiority of the proposed scheme over two of the leading solutions is demonstrated in two areas: the handover latency and packet losses.**

***Keywords*—lightweight; Fast; DMM; CM**

i. INTRODUCTION

The Distributed Mobility Management (DMM) approach aims at minimizing the drawbacks of the current centralized approach. Solutions, such as Mobile IPv6 and its extensions (e.g. HMIPv6, FMIPv6) basically depend on the existence of a central entity (e.g. HA, GGSN). These entities assign IP addresses to, and manage mobility of, nodes. Most of the mobility management issues are convincingly addressed by the Mobile IP protocol family and its extensions. Nevertheless, some limitations that require further attention are identified. These include costly routing which results in scalability problems and packet losses.

Several DMM approaches have recently been proposed. Some, including the one proposed in this document, depend on leading network-based mobility protocols the likes of Proxy Mobile IPv6 (PMIPv6).

The proposed solution is characterized by the following:

- Introduction of a Control component to the Media Access Gateway (MAG). The resulting system combines functionalities of a plain IPv6 access router, a MAG and a Local Mobility Anchor (LMA). For convenience of referencing, the Control MAG system will be referred to hereafter by the acronym CM.
- Reduction of handover latency and packet losses.
- Extension of the PMIPv6 signaling
- Reducing of the overall signaling overhead.

The rest of the paper is organized as follows. In Section II related work is presented and assessed. Section III and section IV are devoted to the proposed solution. Results are presented in section V followed by the conclusion in section VI.

II. RELATED WORK

To overcome the limitations of centralized approaches, the Mobility EXTension for IPv6 (MEXT)) working group under the Internet Engineering Task Force (IETF) considered distributed mobility management._To that end, various distributed mobility management solutions are proposed. The solutions distribute the mobility functions by moving them closer to the MNs. This section presents a glimpse at four such solutions.

In reference [1], the author proposes two schemes for DMM in Proxy Mobile IP (PMIP) based mobile networks. The schemes are: Signal-driven PMIP (S-PMIP) and Signal-driven Distributed PMIP (SD-PMIP). The former is viewed as a partially distributed mobility management approach. It enables separation of the control plane from the data plane. Nevertheless, it still suffers from packet losses during handover. Such is the case because no mechanism for setting up a new tunnel between the MAGs was considered. As such, a packet remains tunneled only to the MN’s old MAG, hence, the probability of losing it increases.

A distributed dynamic mobility management scheme for flat IP architecture is proposed in [2]. The scheme dynamically anchors MN’s traffic to appropriate access nodes (AN). However, during handover, an MN’s traffic remains anchored to its previous AN. When an MN has a long term traffic that moves from one AN to another, a long route is formed by the increased distance between the AN's.

In [3] the author proposed a scheme based on Mobile IPv6 (MIPv6) with operation mechanisms similar to the mechanism described in [2]. However, the scheme still suffers from long routes that limit its scalability.

Two enhanced schemes are proposed in [4]. They are aimed at addressing the limitations found in [1], [2] and [3]. The first is based on reference [1] and enhances the handover mechanism via a de-registration message that reports to the Control Function (CF) detached MNs.

However the scheme still suffers from long handover latencies and signaling overhead. The second scheme is based on both [2] and [3] and adds an entity called Intelligent Mobility Router (IMR) to the core network to control the signaling (location management). However, the added entity presents a bottleneck due to being a single point of failure.

A solution to the handover latency and packet loss is presented next.

III. PROPOSED L-FH-PMIPV6 ARCHITECTURE

Figure1 depicts the proposed architecture.

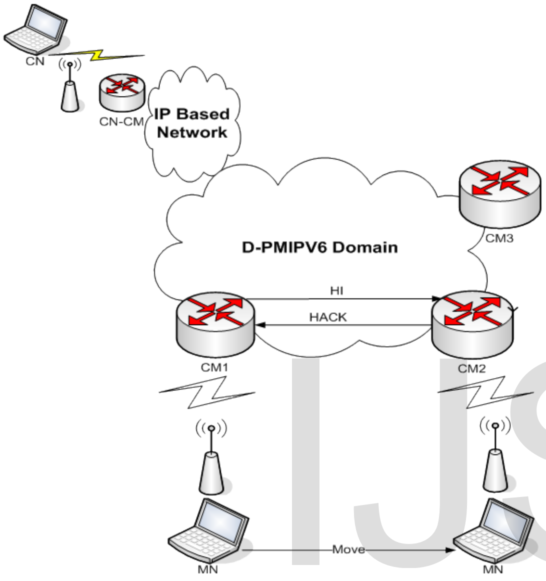


Figure 1: Proposed DMM Architecture

This paper proposes a PMIPv6-based DMM architecture with a CM deployed at the access level. The architecture, as shown in figure 1, covers a wide area and is constrained to a single service provider. The DMM assigns IP addresses via its CM and the standard PMIPv6. Its mobility management functions are fully distributed at the CMs to bring mobility closer to the MN.

Figures 2 and 3 demonstrate functions of the proposed architecture. Emphasis of further discussions in this section is on two operations: registration and handover. Each of these operations is elaborated on next.

A. *Registration(initial) Process:*

When an MN enters the domain (D-PMIPv6 domain), a CM (e.g., CM1) detects its presence on the link connecting both. The CM then creates a binding entry for the MN and sends to it an RA(HNP) named(pref1).

The MN uses the prefix(pref1) to configure an IPv6 address (e.g MN-HoA) following the stateless configuration mechanism. The MN then uses the address to communicate with the CN without the need for tunneling as shown in figure 2.

When CM1 receives data sent by an MN, it mimics a standard IPv6 router by forwards the data to its address (CM-CN) without encapsulation.

Upon receiving the data, CN-CM relays it to its destination CN.

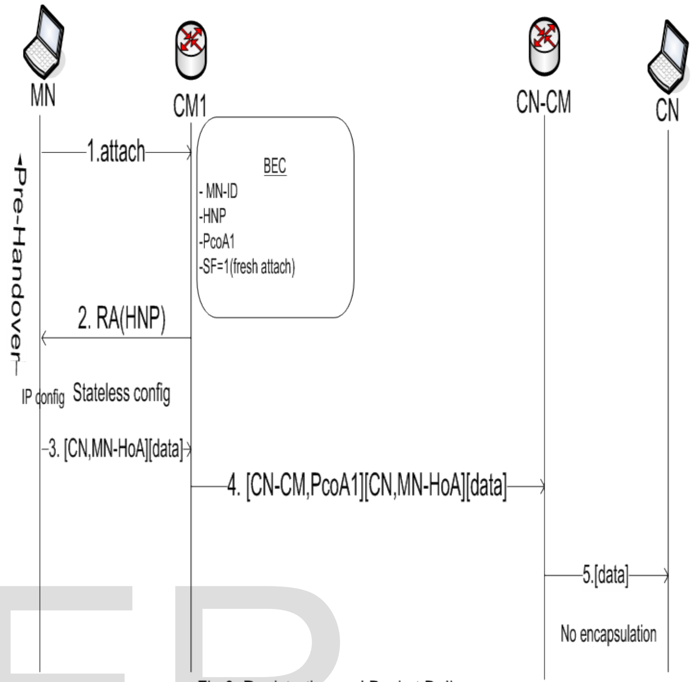


Fig 2: Registration and Packet Delivery

B. *Handover Procedure (with active session):*

The handover process consists of two phases: the pre-handover phase and lightweight-fast handover phase, figure 3 shows how a handover is performed. When an MN handovers with an ongoing—active session involving two CMs, here is what takes place:

1. Before an MN leaves its current CM (e.g CM1) to another (e.g CM2), the former sends a Handover Initiation message (HI) to latter. The message includes the authentication information {MN-ID, the proxy Care of Address (pCoA1) and the Home Network Prefix(pref1)}.
2. Upon receiving the HI, CM2 binds it and replies with a HACK message containing its pCoA2. It then builds a bi-directional tunnel connecting it with CM1 and sets itself ready for receiving packets when the tunneling begins.
3. Upon receiving the HACK, CM1 forwards the MN's packets to CM2 which buffers them to prevent packet loss as shown in (step3).
4. When CM2 realizes its connection with the MN, it verifies registration of the MN in its binding list. Upon verification, CM2 sends RA to the MN to configure an IP address. Step (4).

5. Upon receiving the RA with a new prefix (e.g pref2), the MN retains the same home address by using stateless configuration mechanism, and starts downloading the buffered packets according to their arrival times (newest to oldest).(step 5).
6. After configuring the home address while communicating with the CN, the MN sends a new Packet to CM2 that is destined to the CN (step 7).
7. Since CM2's pCoA2 is unknown to CN-CM, the latter will reject delivered packets from the former. In such a case, this paper suggests inserting the previous pCoA1 of the predecessor CM into the Header's option filed of the IPv6 packet. Once the CN-CM receives a new packet, it checks the header's option field and accepts the packet only if its corresponding pCoA1 is verified. The CN-CM also recognizes the move by the MN to a new CM whose location address is (pCoA2). Consequently, it forward the received packet to CN (step 8).
8. The CN then sends new packets destined to MN via CN-CM, which in turn forwards them directly to the corresponding CM (CM2). The latter delivers the packers to the target MN (steps 9, 10).

As mentioned earlier, the above scenario focuses on a handover process that takes place during an ongoing session. However, the second handover's scenario which does not involve any active session, follows the steps of the standard PMIPv6 using a pre-handover phase to reduce the handover latency and packet loss.

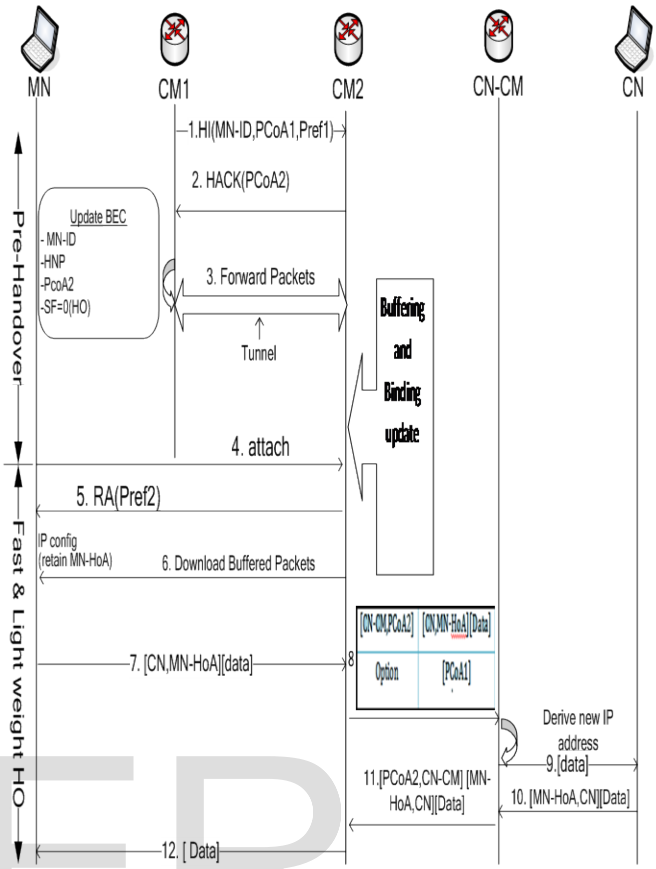


Fig 3: Handover Procedure

IV. PERFORMANCE ANALYSIS

This section presents a comparison among the handovers of the PMIPv6, the PL-MIPv6 and the L-FH-PMIPv6 based on their handover latencies and signaling costs. The model in figure 1 is used in the process.

A. Handover Latency (HL):

Handover latency is contributed by three processes: link switching, IP connectivity and location updating. A link switching latency is caused by a layer2 handoff (L2). An IP connectivity latency is due to movement detection and a new IP address configuration after an L2 handoff. Upon establishment of connectivity, an MN becomes capable of sending or receiving packets through another CM. The handover latencies of the *PMIPv6*, the *PL-PMIPv6* and the *L-FH-PMIPv6* (the proposed scheme) can be expressed as follows:

$$T_{PMIPv6} = t_{link\text{-}switching} + t_{AAA\text{-}auth} + t_{p\text{-}reg} + t_{RS\text{-}RA} \quad (1)$$

$$T_{MIPV6} = t_{link\text{-}switching} + t_{AAA\text{-}auth} + t_{RS} \quad (2)$$

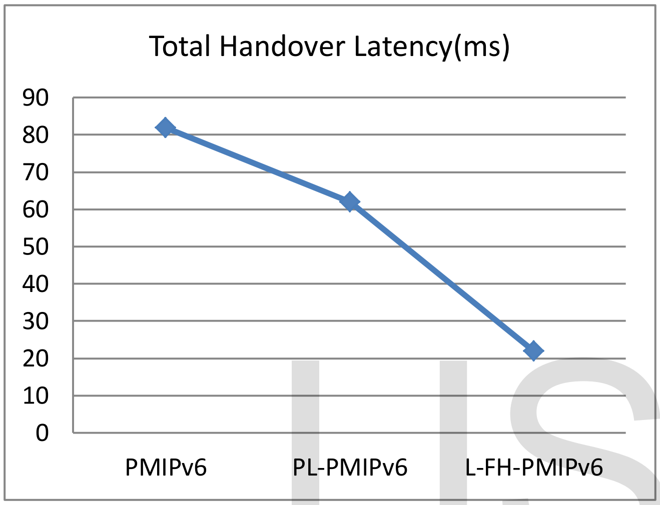
$$T_{L\text{-}FH\text{-}PMIPV6} = t_{link\text{-}switching} + t_{RS\text{-}RA} \quad (3)$$

Table 1 is comparing in figures the total handover for the mentioned schemes using the above formulas.

Table 1: Total Handover Latency (ms)

Assumptions: $L2_{HO}$ =2ms, $t_{MN,MAG}$ = 10 ms, $t_{MAG,MAG}$=2m $T_{MAG,H N}$=10 ms

Scheme	$L2_{HO}$	$t_{AAA\text{-}auth}$	$t_{p\text{-}Registration}$	$t_{RS\text{-}RA}$	Total (ms)
		2*(tMN,MAG + tMAG,HN)	2*(tMAG,HN)	2*(tMN,MAG)	
PMIPv6	2	40	20	20	82
PL-PMIPv6	2	40	0	20	62
L-FH-PMIPv6	2	0	0	20	22



The handover latency of the proposed scheme is the lowest compared to those of the *PMIPv6* and *PL-PMIPv6*. Such is the case because *L-FH-PMIPv6* deploys a fast and lightweight mechanism that reduces the handover latency.

B. Signaling Cost (SC):

The signaling cost is measured by the number of signals sent during a handover. The signaling cost of handover for the three schemes is as follows.

(1) $SC_{PMIPv6} = 10$.
(2) $SC_{PL\text{-}PMIPv6} = 9$.
(3) $SC_{L\text{-}FH\text{-}PMIPv6} = 4$.

The lowest SC among all three belongs to the proposed scheme while the highest belongs to the PMIPv6 scheme.

V. CONCLUSION AND FUTURE WORK

This paper presented a novel solution for two distributed mobility issues: handover and related packet losses. The solution optimized handover by reducing both its latency and the consequent packet losses. In particular, the solution is focused on the intra-domain movement and is based on the standard localized mobility solution PMIPv6. Results of preliminary analysis of handover latencies and related packet losses favored the proposed scheme—L-FH-PMIPv6 over two of the leading contenders.

Future work includes simulation of the proposed scheme using OMENT++ (v4) and further improvement of both the handover latencies and their associated costs.

ACKNOWLEDGMENT

A special thanks to Dr. Muhana Magboul from Shagra University-KSA, Dr. Rashid Saeed vice dean of scientific Research at Sudan University and Dr. Adil Yousif assistance professor at University of Kassala for their valuable comments.

REFERENCES

[1] Koh S., Kim J., Jung H., and Han Y., “Use of Proxy mobile IPv6 for Distributed Mobility Control” IETF draft-sjkoh-mext-pmip-dmc-01(workin progress), March 2011.

[2] 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.

[3] Fabio G., Antonio O., Carlos J. B., “Flat Access and Mobility Architecture: an IPv6 Distributed Client Mobility Management Solution”, Mobility Management in the Network of the Future World (MobiWorld), and IEEE 2011.

[4] Petro P. Ernest, Olabisi E. Falowo, H. Anthony Chan," Enhanced Distributed Mobility Management Schemes for NGWNs ", GLOBCOM, 2012.

[5] Perkins, C., Johnson, D., and J. Arkko, "Mobility Support in IPv6", RFC 6275, July 2011.

[6] Gundavelli, S., Leung, K., Devarapalli, V., Chowdhury, K., and B. Patil, "Proxy Mobile IPv6", RFC 5213, August 2008.

[7] Bernardos, C. and F. Giust, "A IPv6 Distributed Client Mobility Management approach using existing mechanisms",draft-bernardos-mext-dmm-cmip-00(work in progress),March 2011.

[8] Chan, A., "Problem statement for distributed and dynamic mobility management",draft-chan-distributed-mobility-ps-03 (work in progress),July 2011.

[9] Giust, F., de la Oliva, A., Bernardos, CJ., and RP.Ferreira Da Costa, "FA Network-based Localized Mobility Solution for Distributed Mobility Management", under submission , 2011.

[10] R. Koodli, “Fast Handover for Mobile IPv6,” IETF RFC 4068, July 2005.

[11] D. Jonson et al., “Mobility Support for IPV6”, IETF RFC 3775, June 2004

[12] S. Gundavelli et al., “Proxy Mobile IPv6”, IETF RFC 5213, August 2008

[13] Yokota, et al., "Use case scenarios for Distributed Mobility Management "IETF draft-yokota-dmmscenario-00 (work in progress), October 2010.

[14] Chan H.A., H. Yokota, J. Xie, P. Seite, and D. Liu "Distributed and Dynamic Mobility Management in Mobile Internet: Current Approaches and Issues", Journal of Communications, Vol. 6, No. 1, 2011.

[15] Seonggeun Ryu, Gye-Young Kim, Byunggi Kim Youngsong Mun, "A Scheme to Reduce Packet Loss during PMIPv6 Handover considering Authentication", ICCSA 2008.

Taj Elsir Hassan Suliman IS an ABD-PhD Candidate at Sudan University of Science and Technology. He received the M.Sc in 2006 from the School of Mathematical Sciences of Khartoum University-Sudan. .His current research interests are in the areas of Distributed Mobility Management, WAP applications and information security. He supervised over forty senior design projects in various areas in the Computer Science realm.

Eltayeb Abuelyaman is a professor of Computer Networking and the Planning Officer for the University of Nizwa, Sultanate of Oman. His MS and PhD degrees are in Electrical Engineering from Oregon State University 1984 and the University of Arizona-1988. He held various teaching positions at reputable Universities in the United States and the Middle East. He also held administrative jobs ranging from Head of a department to Dean of a college. Professor Abuelyaman's areas of research are Computing networks, Computing Security and Data Mining.