A Handover Optimized Scheme and Performance Analysis in HMIPv6 Network

Jiao-Min Luo, Ying Li

Department of information engineering, Nanhang Jicheng College, Nanjing, 211156, P. R. China
E-mail:252310217@qq.com

Abstract-**Mobile communication is increasingly oriented towards the usage of all IP networks as fixed network components. The handover performance of mobile IPv6 is one of the key factors which guarantee the QoS of mobile Internet. In this paper, an enhance handover scheme in hierarchical MIPv6 networks by utilizing Passive Duplicate Address Detection (PDAD) to identify duplicate addresses is proposed. Using PDAD, a node examines incoming routing protocol packets to develop hints about address controversies. The simulations are performed using NS-2 to compare the handoff performance. The results show that the proposed scheme can get better performance in terms of packet loss and handoff delay.**

Keywords-Handover Scheme; Hierarchical Mobile IPv6; Passive Duplicate Address Detection;Performance Analysis

I. INTRODUCTION

The Mobile IPv6 specification [1] enables hosts to change their point of attachment to the Internet whilst not breaking existing application sessions. This is achieved primarily through the Mobile Node (MN) always being reachable at its home address (HoA) via its home agent (HA). When a MN changes its point of attachment to the network, it moves from one network to another new network. This process is known as handoff or handover. During this process, the MN usually has disconnected from the old network before connecting to the new network and thus there is a time when the MN has lost connectivity to the Internet. During this period it cannot send or receive IPv6 packets to the detriment of existing application sessions. While many TCP applications are designed to cope with intermittent loss of connectivity by retransmitting unacknowledged packets. Such applications desire what is known as seamless handovers.

There have been numerous proposals for minimizing the handoff latency of MIP. These can be broadly classified into two groups. The first group aims to reduce the network registration time by using a hierarchical network management structure while the second group attempts to reduce the address resolution time through address pre-configuration. The former is generally referred to as hierarchical handoff and the latter as fast-handoff [2]. IETF drafts [3] and [4] incorporate the concepts of hierarchical and fast handoff mechanisms in the IPv6 network, based on Mobile IPv6. However, both of them are not sufficient in providing a packet lossless handoff environment at IP layer, since an approximate delay of 300 to 400 milliseconds has been observed.

In this paper, we propose a scheme to optimize the handover in hierarchical MIPv6 networks by utilize Passive Duplicate Address Detection (PDAD) [5] to identify duplicate addresses. Using PDAD, a node examines incoming routing protocol packets to develop hints about address controversies. Since it is independent of the routing protocol, it produces nearly no protocol overhead and reduces initial delay.

The rest of this paper is organized as follows. Section II discusses some related work. Section III describes the main idea of the proposal, enhanced handover in MIPv6 with the support of MIH services and A-DAD. In Section IV, we present our performance analysis. Finally, in Section V, we conclude this paper and give the future work.

II. RELATED WORK

A. Overview of Mobile IPv6 and Handover

The Mobile IPv6 (MIPv6) specification is a proposed standard by the IETF to provide transparent host mobility within IPv6. The protocol enables a Mobile Node to move from one network to another without the need to change its IPv6 address. A Mobile Node is always addressable by its home address, which is the IPv6 address that is assigned to the node within its home network. When a MN is away from its home network, packets can still be routed to it using the MN's home address. In this way, the movement of a node between networks is completely invisible to transport and other higher-layer protocols. When a MN changes its point of attachment to the Internet from one IPv6 network to another IPv6 network (also referred to as roaming), it will perform the MIPv6 handover procedure. In MIPv6, layer 3 handover latency mainly consists of following three factors: the one is the movement detection latency – in average 1.5 sec, the second is address auto-configuration latency (consists of DAD) – typically takes 1 sec, and the third is binding update latency.

HMIPv6 separate mobility management into micro mobility and macro mobility respectively. The central element of this framework is the inclusion of a special conceptual entity called Mobility Anchor Point (MAP), which replaces Foreign Agent (FA) and helps to decrease the handover latency as a local MAP can be updated more quickly than remote home agent (HA). The main components of handover latency are still movement detection and DAD procedure which belong to the Layer 3 handover. In FMIPv6, decreasing of handover latency is achieved by delivering the packet to the new point of attachment, some of the layer 3 messages exchanging will be performed before the link layer handover. The MN gets

network parameters and configures a new CoA before the handover (in the predictive mode) or just before the handover (in the reactive mode). Both of the MIPv6 extensions require some changes in MN.

B. Handoff in HIMPv6

The system for Inter-domain handoff is based on the following scenario: the MN has a regional Care-of Address RCoA1 and an on-link Care-of Address LCoA3, which is depicted in Fig.1. When the CN sends packets to the MN, the packets will be sent through MAP1 to the MN's LCoA3.
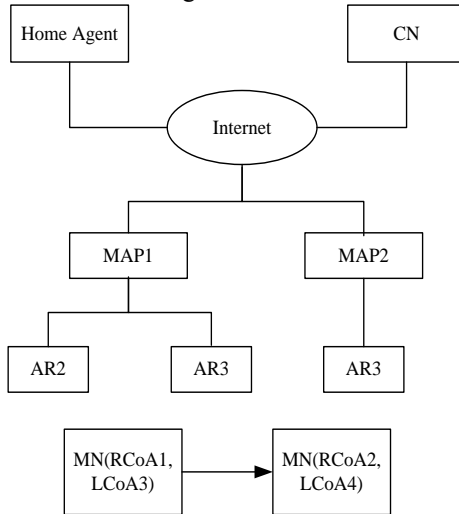

Figure 1. Inter-domain Handoff in HMIPv6.

1) When the MN is about to Move from the MAP1 Domain to the MAP2 Domain:

a)   The MN sends a request control message to MAP1 to construct a multicast group for the MN.

b)   MAP1 forms a multicast group for the MN and sends a multicast group join request to all other neighboring ARs. The neighboring ARs send response messages after receiving these multicast group requests toward MAP1 to show their availability to receive multicast packets from MAP1.

c)   The packets encapsulated by MAP1 are tunneled from the CN to the multicast group members. These ARs buffer the packets. As a final point, these neighboring ARs forward the packets.

2) When the MN Travels from MAP1 Domain to MAP2 Domain:

a)   The MN initially acquires a new address from the MAP2 network (RCoA2, LCoA4). The MN sends a Binding Update to MAP2 through AR4 and sends a message requesting AR4 to forward a multicast message. AR4 receives the request message, and subsequently forwards the buffered packets to the MN.

b)   Whereas AR4 constantly sends multicast packets to MN, MAP2 receives the Binding Update and checks for DAD. MAP2 sends a Binding Update to the MN's Home Agent after receiving the DAD. After that MAP2 waits for a

binding acknowledgment from the Home Agent. MAP2 followed by sends a Binding Acknowledgement to the MN.

c)   The MN receives the Binding Acknowledgement and sends a Binding Update to the CN via MAP2.

d)   After receiving the Binding Update, CN changes the destination address RCoA1 to new RCoA2 and consequently directs the packets to MN in the new network via MAP2 and AR4.

e)   AR4 stops sending multicast packets from MAP1 as soon as it receives new packets intended to the MN. MN at this moment receives packets directly from the CN as with Hierarchical Mobile IPv6.

III.   PROPOSED SCHEME

Our approach uses Passive Duplicate Address Detection (PDAD) [5] to identify duplicate addresses. Using PDAD, a node examines incoming routing protocol packets to obtain hints about address conflicts. PDAD does not use any extra bandwidth. The basic thought is to concern various PDAD algorithms to incoming routing protocol packets [6].

PDAD can also be applied to on-demand routing protocols. The DAD is also on-demand due to their passive nature, as well as can simply identify conflicts between nodes involved in a route discovery or maintenance procedure[7].

In the subsequent, we describe a model of an on-demand routing protocol and present some PDAD algorithms for this model.

In the following, special algorithms for on-demand protocols are presented [8].

1) PDAD-RNS: If a RREQ is received with the receiver's originator address the RREQ-Never-Sent (RNS) algorithm identifies a conflict. However a RREQ has never sent for this destination[9]. In this case, a different node with the same address must have sent the RREQ.

2) PDAD-RwR: If a node receives a RREP meant for its own address the RREP-without-RREQ (RwR) algorithm identifies a conflict, but a RREQ has never sent for this destination.

3) PDAD-2RoR: A singe destination node simply replies one time to a specific RREQ caused by the application of a duplicate message cache. The 2RREPs-on-RREQ (2RoR) algorithm identifies a conflict if more than one RREP has been received from the destination address of a specific RREQ.

4) PDAD-SN: This algorithm exploits the Sequence Numbers (SN) in the routing protocol packets to detect duplicate addresses in the network. The assumptions are that each node uses a sequence number only once within the time interval td, and that each node increments its own and only its own internal sequence number counter.

5) PDAD-SND: A conflict can as well be detected based on the Sequence Number difference (SND). The difference is higher than the maximum possible increment within t1-t2 + td, with t1 and t2 being the points in time when packet 1 and 2 were received, respectively[9]. As a consequence, these packets could not have been sent by the same node.

Intermediate nodes hence can conclude that the originator's address is duplicated.

IV. PERFORMANCE SIMULATION

We use NS2 to simulate our proposed protocol. In our simulation, the channel capacity of mobile hosts is set to the same value: 2 Mbps. We use the distributed coordination function (DCF) of IEEE 802.11 for wireless LANs as the MAC layer protocol. It has the functionality to notify the network layer about link breakage. Table I. summarizes the simulation settings.

TABLE I.   SIMULATION SETTINGS

No. of Nodes	15
Area Size	1000 X 1000
Mac	802.11
Simulation Time	50 sec
Traffic Source	CBR
Packet Size	512
Speed	5,10,15,20
Transmission range	75m
Routing Protocol	AODV

For the simulation, we make use of Hierarchical Mobile IP (HMIP) implementation, which has implemented in Columbia IP Micro-mobility Software (CIMS) [10]. It supports micro mobility protocols for instance Hawaii, Cellular IP, and HMIP extension meant for the NS-2 network simulator based on version 2.1b6. We have additionally included MAP functionality to provide regional registration with the existing CIMS implementations.

The simulation has carried out using the network topology shown in Fig. 1.
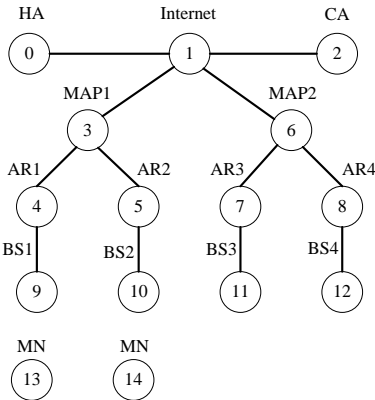

Figure 2.   Network Topology.

Initially the mobile node MN13 was in MAP1 in the domain AR1. During the simulation we perform intra and inter domain handoff on MN13.

Initially, at time t1, the mobile node performs intra domain handoff by moving from AR1 to AR2 within MAP1. Next at time t2, it start moving towards AR3 from AR2, thus by performing inter domain handoff. At time t3, it moves

from AR3 to AR4, within MAP2. Finally at time t4, it moves back to AR1, once again performing inter-domain handoff. In all the movements, PDAD is performed before getting the new CoA.

We evaluate the performance of our scheme based on the following parameters.

- Handoff latency: The handoff latency is defined as the time interval from last packet received form serving BS to and new packet received from target BS.
- Packet loss: The packet loss counts from the MS disconnecting to serving BS to receiving new packets from the target BS.

We move the mobile node to AR1, AR2, AR3 and AR4. Fig.2 shows the packet loss for HMIP handoff with PDAD and DAD schemes. We can see that the packets loss is less in PDAD based handoff.

Figure 3.   Movements Vs Packet Loss.

Fig.3 shows the handoff delay for PDAD and DAD based schemes. Clearly the handoff delay for PDAD is significantly less when compared with DAD.
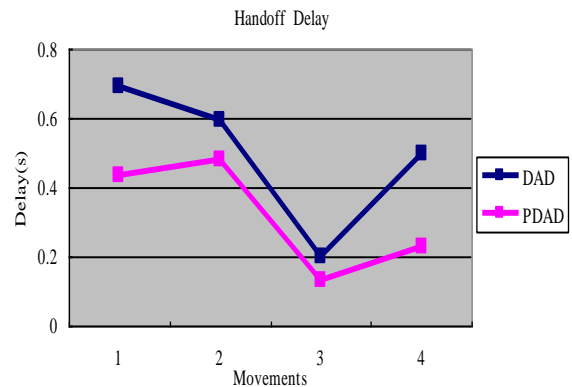

Figure 4.   Movements Vs Handoff Delay.

Next we vary the speed of the MN as 5, 10, 15 and 20 m/s. From Fig.4, we can see that the packet loss is once again less in the case of PDAD scheme when compared with DAD.
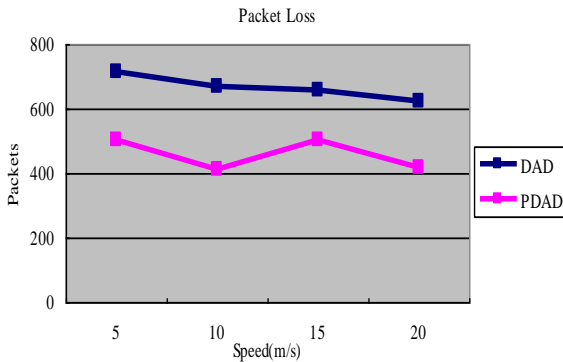
Packet Loss

Figure 5.   Speed Vs Packet Loss.

V.   CONCLUSION AND FUTURE WORK

In Hierarchical Mobile IPv6 (HMIPv6), mobile node's handoff performance is very much impaired by the Duplicate Address Detection (DAD) procedure for the newly formed Care-of Address. In this paper, we proposed a novel cross-protocol design approach for the DAD problem. It uses information from current routing protocol traffic. This utilizes Passive Duplicate Address Detection (PDAD) to identify duplicate addresses. Using PDAD, a node examines incoming routing protocol packets to develop hints about address controversies. Since it is independent of the routing protocol, it produces nearly no protocol overhead and reduces initial delay. By simulation results, we have shown that, the handoff delay and packet loss are reduced in case of PDAD based handoff, when compared with the standard DAD based handoff. Future work includes performance study in real mobile IPv6 networks.

REFERENCES

[1]   D. Johnson, C. Perkins and J. Arkko, "Mobility Support in IPv6," RFC 3775, June 2004.

[2]   Perkins, C., Ed., "IP Mobility Support for IPv4," RFC 3344, August 2002.

[3]   H.S. Flarion, C.Castellucia, K. El-Malki, and L. Bellver, "Hierarchical Mobile IPv6 mobility management (HMIPv6)," IETF RFC 4140, August 2005.

[4]   R. Koodly, "Fast Handovers for Mobile IPv6 (FMIPv6)," IETF RFC 4068, July 2005.

[5]   K. Weniger, PACMAN, "Passive duplicate address detection in mobile ad hoc networks," Proc. of IEEE WCNC 2003, New Orleans, USA, Mar. 2003.

[6]   IEEE 802.21 WG, "Draft Standard for Local and Metropolitan Area Networks: Media Independent Handover Services," IEEE P802.21/D9.0, February 2008.

[7]   Panita Pongpaibool, Pahol Sotthivirat, Sukumal I.Kitisin, Chavalit Srisathapornphat, "Fast Duplicate Address Detection for Mobile IPv6," ICON 2007, 15th IEEE International Conference on Networks, Nov.2007.

[8]   Xinyi Wu, Gang Nie. "Comparative Study and Performance Analysis of the Macro-mobility Protocol," Asia-Pacific Conference on Information Processing (APCIP), pp.497-500, July 2009.

[9]   Gang Nie, Xiuhua Qing. "Analysis and evaluation of an enhanced handover scheme in hierarchical mobile IPv6 networks," International Colloquium on Computing Communication Control and Management (CCCM), pp.329-332, Aug.2009.

[10]   Li Jun ZHANG and Samuel PIERRE, "Evaluating the Performance of Fast Handover for Hierarchical MIPv6 in Cellular Networks," Journal of Networks, Vol. 3, No. 6, June 2008