Journal of Network and Computer Applications 33 (2010) 397–409

Contents lists available at ScienceDirect

Journal of Network and Computer Applications

journal homepage: www.elsevier.com/locate/jnca

Enabling inter-PMIPv6-domain handover with traffic distributors

Feng Zhong *, Chai Kiat Yeo, Bu Sung Lee

Centre for Multimedia and Network Technology, School of Computer Engineering, Nanyang Technological University, N4-B2c-06, Nanyang Avenue, Singapore 639798, Singapore

ARTICLE INFO

Article history:
Received 6 August 2009
Received in revised form
5 January 2010
Accepted 7 March 2010

Keywords:
PMIPv6
HMIPv6
Inter-domain
Traffic distributor

ABSTRACT

As a network-based localized mobility management protocol, *Proxy Mobile IPv6* (PMIPv6) Gundavelli et al. (2008) enables mobile node (MN) to move in a local domain without any involvement in the protocol signaling. In contrast to other mobility protocols (such as cellular IP (CIP) Valkó, 1999, and hierarchical mobile IP (HMIP) Soliman et al., 2005), PMIPv6 does not require any upgrade of MN's protocol stack. Instead, PMIPv6 employs network entities to handle the handover for MN. However, the PMIPv6 can only manage MN's reachability within a local domain. If MN moves beyond the border of PMIPv6 domain, the mobility support will be broken. To provide MN continuous support across domains, we propose a solution to interconnect neighboring PMIPv6 domains. In our proposal, we have introduced a new network entity called *traffic distributor* (TD). The TD is used to deliver the cross-domain traffic. If MN moves across domain borders, LMA will notify the TD and the TD will redirect MN's traffic to the new domain. To evaluate our proposal, we conduct experiments to compare it with Neumann et al.'s (2009a, 2009b) proposal which is another proposal to handle inter-PMIPv6-domain issues. Results show that our proposal is a feasible alternative for inter-domain handover, and it outperforms Neumann's proposal in terms of binding cache entry number, transmission delay and handover delay.

1. Introduction

Next generation network is believed to be an all-IP network wireless network (e.g. 3G network, McCann and Hiller, 2000; Patel and Dennett, 2000, and 4G network Carneiro et al., 2004; Kim et al., 2003), which means all existing networks will evolve to a unified network based on IP protocol. During the unification progress, IP mobility management is one crucial issue. To enable mobile node (MN) can maintain its ongoing communication session, IETF has commissioned a work group to develop mobile IP (MIP) (Johnson et al., 2004; Perkins, 2002; Perkins et al., 2007) protocol. Under MIP, every MN has two addresses—home address (HoA) and care-of-address (CoA). The HoA is acquired by MN in its home network and it is the identification of MN. The CoA is the address used in foreign network. Every time MN moves to a foreign network, MN first gets a new CoA. Then, MN sends a binding update (BU) message to its home agent (HA). After receiving the BU message, HA will set up a mapping entry between HoA and CoA. If HA receives traffic destined at MN's HoA, HA will encapsulate the traffic with MN's CoA and send them out. Because CoA is topologically correct with MN's current location, the traffic will be delivered to MN successfully. Through gluing MN's HoA and CoA, MIP protocol can provide mobility support to MN regardless of its location.

Although MIP protocol solves the handover issue, it has several problems. First of all, MIP protocol suffers a triangular routing problem (Perkins and Johnson, 1998). The packets from the correspondent node (CN) to the MN are first captured by the HA and then tunneled to the MN. Hence, the packet transmission delay will be increased greatly if MN moves far away from its HA. Secondly, MIP's handover delay is too long to satisfy the requirement of some real time applications (e.g. VoIP). Lastly, MIP protocol requires modification to MN's protocol stack. This prevents the immediate deployment of MIP protocol for legacy mobile terminals.

Actually, MIP protocol is a kind of macro-mobility protocol which supports MN roaming in the wide area. It is not suitable for the MN which moves within a limited area and requires high handover performance (e.g. less handover delay and less protocol signaling cost). To improve MIP's performance in the local domain, several micro-mobility protocols (Campbell and Gomez-Castellanos, 2000; Reinbold and Bonaventure, 2003) have been proposed as a complement. Some protocols extend from MIP protocol, such as fast handover for mobile IP (FMIP) (Koodli, 2005; McCann, 2005) and hierarchical mobile IP (HMIP) (Soliman et al., 2005). FMIP (Koodli, 2005; McCann, 2005) is a protocol aiming to reduce the packet loss resulted from handover. To achieve this, FMIP establishes a tunnel between the old access router (AR) and

* Corresponding author.
E-mail address: zhon0026@ntu.edu.sg (F. Zhong).

1084-8045/$ - see front matter © 2010 Elsevier Ltd. All rights reserved.
doi:10.1016/j.jnca.2010.03.001

the new AR. When MN handovers from the old AR to the new AR, it sends a fast binding update message to the old AR. Upon receiving the fast binding update, the old AR will redirect packets to the new AR which buffers the packets temporarily. When MN attaches to the new network, the new AR will deliver the buffered packets to MN. Through buffering process, FMIP can reduce packet loss. Another extension of MIP protocol is HMIP. It is designed to reduce the signaling latency when MN moves within an administrative domain. To achieve this, HMIP organizes the foreign agent (FA) and gateway foreign agent (GFA) in a hierarchy. The MN first registers its CoA with both GFA and HA as soon as it enters the domain. Afterwards, if MN changes its FA within the domain, it will only update its location with GFA by performing a regional binding update (RBU). As GFA is much nearer to MN than HA, HMIP's signaling latency is much shorter than MIP's.

Besides the FMIP and HMIP, there are other mobility protocols to improve the performance of MIP. According to their implementation layer, these protocols can be classified as network-layer protocol and link-layer protocol. For example, cellular IP (CIP) (Valkó, 1999) is a protocol developed at the network layer. Unlike MIP, CIP requires network to have a strict tree structure topology. When MN changes its attaching AR, it will send an update message to the gateway router. Along the way from AR up to the gateway router, each tree node will create a new next-hop routing entry for MN, until the update message reaches the crossover node. At the crossover node, the traffic will be redirected to MN's new location. Through the cooperation of the tree nodes, CIP successfully manages the MN's mobility within a local domain. Another mobility protocol is terminal mobility support protocol (TMSP) (Lim et al., 2009). TMSP is designed to solve the triangular routing issue of MIP. Tapping on the pervasiveness of SIP (Rosenberg et al., 2002) as a location service, TMSP renders IP address change transparent to applications via IP address swapping in the network layer. When MN changes the attaching network, it will notify peers about its new address. If any node wants to send a packet to MN, the source node will update packet's destination with MN's new address. With the help of SIP, TMSP can always deliver traffic to MN via an optimal routing path. In addition to CIP and TMSP which are network layer mobility protocols, there are also link-layer mobility protocols such as secure intra-domain mesh routing protocol (SIMRP) (Kandikattu and Jacob, 2007, 2008). SIMRP is a routing protocol that runs on the link layer. It connects the MN in wireless mesh network together. When MN moves to a different wireless mesh network, SIMRP can also provide connectivity to MN.

All above mentioned protocols are host mobility protocols which only enable a single MN to handover. The host mobility protocols are inefficient when managing the handover for a set of hosts which move as a unit. An example is the passengers in a vehicle move from one AP to another during their journey. To improve the efficiency, researchers extend network mobility from host mobility. The network mobility aims at providing mobility support to a set of hosts which handover simultaneously. The set of hosts is defined as a mobile network. In every mobile network, there is a mobile router (MR) connecting the mobile network to the Internet. Network mobility (NEMO) (Devarapalli and Wakikawa, 2005), session initiation protocol network mobility (SIP-NEMO) (Huang et al., 2006), hybrid-NEMO (Leu, 2009) and terminal-assisted network mobility (TNEMO) (Lim et al., 2009) are examples of network mobility protocols. NEMO is developed by IETF and it is extended from MIP. When the mobile network moves to a new network, MR will register the location with HA. Then, HA will tunnel all traffic of mobile network to MR and MR is responsible for distributing the traffic to MN. Although NEMO can solve mobility issue for mobile network, it suffers from pinball routing effect (Huang et al., 2006). In order to overcome the problem, other network mobility protocols have been proposed. SIP-NEMO is a protocol that is extended from the SIP framework and it can achieve route optimization between two SIP clients even if the mobile network is nested. Hybrid-NEMO is another solution that provides a soft handoff scheme to mobile network. The handoff scheme is based on SIP and SCTP protocols and it ensures a lossless packet-transmission environment and less handoff-delay variation. TNEMO makes use of the IP swapping mechanism in Lim et al. (2009) to enable direct routing between mobile network nodes in the presence of network mobility. It works cooperatively with MRs and access routers to provide seamless connectivity without pinball routing effect and without the need for infrastructure support such as HA. It also eliminates the need to dynamically increase the size of IP header in IP tunneling.

Despite the numerous mobility protocols, deployment is uncommon. The main reason is that these protocols (e.g. HMIP, TMSP and CIP) require an upgrade of MN's protocol stack and they are incompatible with the legacy mobile nodes. In recent years, researchers are trying to develop a network-based solution which allows a quick deployment on legacy devices. Proxy mobile IPv6 (PMIPv6) (Gundavelli et al., 2008) is one of network-based solutions. The PMIPv6 is developed by IETF. It can keep MN agnostic of the movement. When MN changes the attaching network, the whole PMIPv6 domain appears as a single link and MN's IP address remains unchanged. Moreover, PMIPv6 can simplify MN's protocol stack and reduce the power consumption of MN.

To release MN from the process of mobility operation, PMIPv6 employs two new network entities—mobile access gateway (MAG) and local mobility anchor (LMA). The two entities are used to track the movement of MN and to perform the mobility signaling on behalf of MN. MAG is an access router and it is attached by MN directly. LMA is a gateway router of the domain. It is the topological anchor point for the domain. Moreover, LMA maintains the reachability status for MN. When MN moves into a PMIPv6 domain, the MAG will first notice the attachment and send a proxy binding update (PBU) message to LMA, querying MN's configuration parameters (e.g. MN's network prefix). If MN is an authorized user, LMA will reply with a proxy binding acknowledgement (PBA) message to MAG, carrying MN's address configuration. With the PBA message, MAG will construct a router advertisement (RA) message and send to MN unicastly. At the same time, LMA will create a binding cache entry (BCE) for MN. BCE is an entry used to keep MN's information such as the address configuration and current location. All the information is crucial. For example, the current location information can help LMA deliver data packets to MN. The address configuration enables LMA to keep MN's address unchanged. Fig. 1 presents the signaling flow for MN's handover within the domain. When MN moves MAG1 network to MAG2 network, MAG1 will first send a deregister PBU to LMA, informing the MN's detachment. Upon receiving the deregister PBU message, LMA will set a timer to delete the BCE for the MN. If LMA can receive a register PBU from MAG2 before the timer expires, LMA will stop deleting the BCE and update the BCE with MAG2's location. At the same time, LMA will reply with a PBA to MAG2 using the previous address configuration. Because the configuration is the same as MAG1, the RA message sent by MAG2 will remain the same as the message of MAG1. Therefore, MN will not be aware of its movement.

To deliver traffic to MN, LMA will build a bi-directional tunnel whenever MN changes its attaching MAG. Because LMA is the topological anchor point of the domain, LMA will receive data packets before they arrive at MN. When LMA receives the data packets, it will encapsulate the packets and send them to MAG through the tunnel established before. Then, MAG will decapsulate the packets and send them to MN. If MN wants to send out data packets to its communicating peer, the MAG will first tunnel