TDPBU: Route Optimization for Coexisting Mobility Managements in IPv6 Networks

Wen-Kang Jia, Chia-Yao Chen, Yuan-Rung Yang, Yaw-Chung Chen, Senior Member, IEEE
Department of Computer Science and Information Engineering
National Chiao Tung University
{ wkchia, chiayao, yuanrung, yccchen}@cs.nctu.edu.tw

Abstract—Client-based Mobile IPv6 (MIPv6) is the most well known mobility management protocol, and the fast emerging proxy-based Mobile IPv6 (PMIPv6) offers an alternative. Some inherent problems such as route optimization in these protocols have not been really solved. Although various proposals tried to tackle the route optimization problem, none of them has achieved a real success. Furthermore, most of them are not comprehensive solutions for coexisting MIPv6/PMIPv6 mobile environment. In this paper, we proposed a novel unified route optimization scheme - Traffic Driven Pseudo Binding Update (TDPBU) to accommodate various mobility management issues. We evaluated our proposed scheme through simulations, and numerical results show that TDPBU can significantly improve the overall performance of mobility management protocols.

Index Terms—Route Optimization, Mobile IPv6 (MIPv6), Proxy Mobile IPv6 (PMIPv6), Traffic-Driven Pseudo Binding Update (TDPBU), Network Mobility (NEMO).

I. INTRODUCTION

With the quick advance in wireless technologies, IP-based wireless user terminals are becoming mobile, thus providing efficient mobility management has been a long-standing challenge. The most widely known mobility management protocol, Mobile IPv6 (MIPv6), allows a Mobile Node (MN) to arbitrarily change its point of attachment to the Internet. Since MIPv6 must be implemented in mobile nodes to serve mobility management, it is called Client based MIPv6 (CMIPv6) [1, 5]. On the other hand, Proxy based Mobile IPv6 (PMIPv6) [2-4] protocol provides an alternative for mobility management based on the assistance of local networks. However, these protocols have some inherent problems, such as large handoff latency in performing network attachment, and it results in difficulty for supporting real-time multimedia applications. Moreover, due to the high mobility of MNs on Internet, it may incur two predicaments: 1) the mass of correspondent nodes (CNs) is also mobile; 2) the communication path between two MNs changes rapidly. These lead to vastly increased overhead and end-to-end latency due to double tunnel encapsulations and double sub-optimal paths, respectively. Thus, Route Optimization (RO) is necessary, and various solutions have been proposed to accommodate these problems, but it still lacks an efficient solution to deal with the route optimization procedure [5, 6].

CMIP and PMIP will very likely coexist in the future Internet. However, the MIPv6 specification does not fully concern the route optimization induced by the movement of CNs, and it usually assumes that two communicating parties are either all in CMIPv6 domain or all in PMIPv6 domain, but not across both domains. This is not realistic because a MN located at CMIPv6 domain may communicate with a MN on PMIPv6 domain, or vice versa, and it needs an optimized path. Since route optimization in CMIPv6 and PMIPv6 are often implemented independently, a unified RO scheme is required. In this paper, we propose a novel RO solution for coexisting PMIPv6/CMIPv6 domains, based on both Traffic Driven Pseudo Binding Update (TDPBU) scheme and Optional Post Authentication (OPA) scheme. According to the performance evaluation results, we demonstrate that our proposed scheme can achieve route optimization with much lower latency.

The rest of the paper is organized as follows. In Section II, we describe the route optimization problem and related works. In Section III, the proposed scheme is elaborated. Some application scenarios are demonstrated in Section IV; Performance evaluation including simulation, numerical results and comparisons are discussed in Section V. Finally, we conclude the paper in Section VI.

II. RELATED WORKS AND PROBLEM DESCRIPTION

IP mobility concerns the reachability of a MN and persistence of current sessions, as well as connections that fulfill the basic requirements of mobility support. Besides, it needs to fulfill the performance requirement in terms of fast and seamless handoff as well as route optimization.

A. Route optimization operations for Client Mobile IPv6

In addition to bi-directional tunneling mode [5], MIPv6 can operate using route optimization, with which the MN and CN bypass the home agent (HA) and communicate directly with each other to improve data transport efficiency.

A MN owns both Home-Address (HoA) and Care-of-Address (CoA) to represent its current location. For sending datagram to the CN efficiently, a MN can directly send datagram with CoA as the source address. On the other hand, to send datagram to MN, the CN needs to know MN’s current location. If MN’s correct location information can be updated to the CN’s binding cache, the CN can also send datagram to the MN directly via the optimized routing path [1, 5, 6]. When a MN and its CN are both moving away from their home networks which belong to different mobility management domains (e.g. MIPv6 and PMIPv6), it may result in the most complicated data scenario as depicted in Fig. 1. Assume there are four alternative paths: Path1: $MN_{HoA} \leftrightarrow CN_{HoA}$ is the
non-route-optimized path under double bidirectional tunneling; Path2: $MNCNSToCoA^\rightarrow CN_{HoA}$ and Path3: $MN_{HoA}^\rightarrow CN_{CoA}$ are partial route optimized path with one bidirectional tunneling; and Path4: $MNCNSToCoA^\rightarrow CN_{CoA}$ is a fully route optimized path without bidirectional tunneling.

When a MN changed its point of attachment and obtained a new CoA, it sends a Binding Update (BU) message to its associated HA, then all CNs may communicate with the MN using RO. Data traffic from CNs can be first sent to the HA based on MN’s HoA, then tunneled to the MN, or forwarded to the MN’s CoA directly. When the communication switches from MN’s HoA to CoA, a Return Routability (RR) [6] test is used to verify both the right of MN to use a specific HoA and the validity of the claimed CoA. A secure RR mechanism of current Mobile IPv6 has been carefully designed to prevent or mitigate a number of known threats, it requires neither configuration nor trusted entities beyond the HA of MN, and is based on pervasive distrust of the future mobile Internet [8].

The basic RR mechanism consists of two test pairs: The Home Test Init (HoTI) and Care-of Test Init (CoTI) from MNs trigger both tests; the Home Test (HoT) and Care-of Test (CoT) from CNs reply the test, the binding update acts accompanied by both of the tests. As shown in Fig. 2, the RR procedure initiated by MN requires at least 6 messages, including $RTT(\text{Path1})$ and twice $RTT(\text{Path2})$ to achieve the partial RO, also CN requires 6 messages, including $RTT(\text{Path2})$, and twice $RTT(\text{Path4})$ to initiate the RR procedure from another direction. If MN initiates the RR earlier than CN, the Path2 should be selected first; otherwise Path3 should be traversed first. Finally, twice RR procedures (total 12 messages) will be finished by both sides, and the full RO will be selected.

Various schemes such as OMIPv6 [10], OMIPv6+ [11], Enhanced Route Optimization for Mobile IPv6 [12], and Early Binding Updates [13] are proposed. These schemes have limitations in terms of scalability and potential counterfeited binding update due to the lack of CoA test.

B. Route Optimization operations for PMIPv6

In PMIPv6, mobility signaling is controlled through the network entities such as Local Mobility Anchor (LMA), which operates as an HA in MIPv6 and manages the location information of MNs, and Mobile Access Gateway (LAG) which functions like an AR in MIPv6. Once a new MAG (nMAG) detected the movement of a MN, the nMAG sends a Proxy Binding Update (PBU) message to the LMA on behalf of the MN if the MN attached to its associated access link. The MN does not support mobility and always uses the original HoA everywhere; in fact the MN is even not aware of its movement [2].

Similarly, the MN always sends and receives packets using its HoA in PMIPv6 domain. To solve the RO problem in PMIPv6, several researches have been proposed, such as Proxy home test (pHoTI) [15] and Proxy care-of test (pCoTI) [16], and Correspondent Binding Update (CBU) [19]. The interaction between PMIPv6 and MIPv6 protocols are first addressed in [17, 18], which analyze several scenarios when route optimization is used.

III. PROPOSED SCHEME

Our proposed TDPBU is a route-optimized mobility management scheme that cooperates with both PMIPv6 and MIPv6. The basic concept of TDPBU is to reverse both binding update and security procedures. Our assumption is that, if the time duration is short enough, any security threat is unlikely to happen during this short period. Therefore, the RO is always launched instead of being an option, as that in MIPv6. Oppositely, security consideration becomes an option rather than a compulsion. In addition, TDPBU eliminates the explicit BU messages, which are substituted by inherent extension header. For example, Home Address Destination Options Header (HADOH) and Type-2 Routing Header (T2RH) in MIPv6 are carried by the datagram packet. Thus, the signaling cost can be reduced and the time of mass binding update traffic can be postponed.

A. Network Attachment in TDPBU

Figure 3 shows general TDPBU operations with the MIPv6 components, where both MN and CN are with TDPBU support, and both AR and HA play their original roles as in MIPv6. Once the AR detects that a MN has moved into the visited network, the network attachment procedures will be performed. In the original MIPv6, a successful authentication triggers the BU procedure, then the MN sends a BU message to the HA, which updates the existing mobility binding cache entry for the MN and returns a Binding Acknowledgement (BAck) message to the MN. Then a new tunnel between MNCoA and HA is
created, and all connections between MN and CN is established through MN_{HoA} initially. This is so-called “bidirectional tunnel” mode which is usually a non-route-optimized path.

B. Datagram Forwarding in TDPBU

In TDPBU, the MN no longer establishes a connection to CN through bidirectional tunnel path (via source address MN_{HoA}), instead it originates the datapacket with route optimized path directly. Since the packet is originated from source address MN_{CoA}, it should be able to reach the stationary CN as expected (6). With TDPBU, the original network attachment procedure (1) won’t be involved between MN and HA, notes that explicit BU messages (2)−(3) still must be sent to notice HA that MN is moving. And once a CN tries to communicate with MN voluntarily, it sends data packets to the MN using MN’s HoA (MN_{HoA}) (4). The HA intercepts these data-packets, forms a tunnel and forwards them to the MN’s CoA (MN_{CoA}) (5).

The datapacket MN_{CoA}→CN is piggybacked with the Home Address Destination Options Header that contains MN_{HoA}. This implies that a pseudo binding update to CN was received, and CN can perform a pseudo binding update procedure immediately (7). If return packets from CN could directly reach the MN_{CoA} (8), and if CN does not trust this binding update, then the OPA procedure (9) will be performed against MN’s HA (HA_{MN}). The reasons are 1) MN and its HA_{MN} is assumed with trust relationship; and 2) Considering that HA_{MN} is usually a stationary site, it could reduce both the air-link bandwidth consumption and processing load of MN; whether OPA is performed on CN or not, it will significantly speedup the transition to route optimization state. Finally, CN returns the packet to MN_{CoA} directly and piggybacks a type 2 routing header that contains MN_{HoA}. Now, the bidirectional path is optimized. The extension header pair HADOH [23] and T2RH [5] allows the data to be exchanged between the MN_{CoA} and CN directly without being routed through the HA.

When a MN sends an IPv6 datagram to a CN using route optimization with the CoA as the source address, the HADOH must be used for carrying a MN_{HoA} unless the home address appears as the source address in MIPv6. When a CN sends an IPv6 datagram to a MN using route optimization, the destination address field in the IPv6 header contains the MN_{CoA}, while the inserted T2RH contains the MN_{HoA}. IPv6 nodes that process the routing headers must verify whether the IPv6 address in the header corresponds to the HoA of the MN. The detailed process is illustrated in Algorithm 1.

**Algorithm 1. TDPBU:** PacketSend (*pkt*)

**INPUT:** IP Packet from TCP/IP Socket Layer

**OUTPUT:** IP Packet to MAC Layer

1. key←SEARCH(BindingCache, pkt.dst.addr)
2. if key ≠ NIL then // destination is mobile
3. BindingCache[key].lifetime++
4. pkt.t2rh←BindingCache[key].HoA (MN_{HoA})
5. pkt.dst.addr←BindingCache[key].CoA (MN_{CoA})
6. else //destination is stationary
7. endif
8. if my location is in home network then
9. pkt.src.addr←myHoA
10. else if my location is in foreign network then
11. pkt.src.addr←myCoA
12. endif

Therefore, once a CN is also mobile, the forwarded packets MN_{CoA}→CN_{CoA} should carry both two extension headers: the HADOH that contains the MN_{HoA} and T2RH that contains the CN_{HoA}. Those backward packets CN_{CoA}→MN_{CoA} should carry both extension headers too, with HADOH containing the MN_{HoA} and T2RH containing the MN_{HoA}.

C. Security considerations in TDPBU

A frequently moving MN may lead to high cost (including binding update and route optimization procedures) in terms of security needs and excessive mobility signaling messages. With such concern, a low-latency security mechanism to protect binding management messages in MIPv6 is proposed [9], in which it requires configuring a static shared key between the MN and CN, such that RR tests can be avoided. Consider a domain where both the MN and CN share the same trust, the CN has a good reason to trust the MN and vice versa. Hence, once the operator ensures that sufficient security policies are deployed, excessive and complicated security process could be omitted.

For more strict security issue, the OPA procedure (9) and (m) can be redeemed after TDPBU. That optional procedure may be triggered by TDPBU, a binding request will be actively sent from CN to HA_{HoA} to inform the MN performing a real RR test procedure. This is to confirm that the earlier pseudo binding update was legal.

D. Datagram forwarding in TDPBU

If a MN is moving, it may lead to binding cached in CN becoming stale (8); the datagram will be sent to previous location at the moment (9). The previous AR will detect this situation and respond an ICMP destination unreachable [20] or binding error message [5] back to CN (a). CN now is informed to clear the MN_{CoA} from binding cache entry (b), and originates...
a retransmission task toward the MNCoA(HA_{MN}) (c). After MN finished the network attachment procedure in the new point of attachment (d)-(f), those retransmitted packets will be delivered to MN_{HA} (g) and a RO procedure will be restarted by datagram forwarding (h)-(j). Notes that the backward packet (g) won’t trigger the forward packet (h) immediately, it all occurs according to the upper layer applications’ behavior.

To solve the inefficient retransmission problem, assuming that the previous AR (PAR) knows the current location of the MN, the PAR will relay the received datagram to the current AR. Otherwise, the datagram will be sent to the HA and be forwarded to current location of the MN later. The concepts of Fast Mobile IP (FMIP) [21] can be applied.

Under some conditions, the retransmission procedures (9)–(c) and (g) may not occur, notes that TDPBU relies on normal traffic. Before the retransmission procedure is triggered by the first downstream datagram packet CN\rightarrow MN_{newCoA}, the MN may originate an upstream datagram packet MN_{newCoA}\rightarrow CN earlier than the arrival of a downstream packet. Thus, a TDPBU will be triggered by the first upstream datagram packet (h)-(j) received by CN.

E. Binding cache maintenance in TDPBU

The original route optimization mechanism in MIPv6 relies on two data structures — Binding Cache (BC) and Binding Update List (BUL) for binding to current location, and the BUL in the cache must be correct. A CN uses such binding cache entries to store mapping between HoA and CoA of the MN, and persist even after a period of disconnection or loss of state in MNs. A binding update list is therefore kept by the MN, which maintains current binding state on any CN or HA. TDPBU always originates a connection via CoA and HADOH instead of sending the binding update message. Thus, the BUL can be simplified and just for maintaining the HAs.

The binding cache in a TDPBU node contains one entry for every CN with which communication is currently taking place. The binding cache holds four major pieces of per binding information which are essential to the operation of MIPv6. Other non-essential fields are omitted for clarity. Algorithm 1 illustrates the detail process: when a node wants to transmit a packet to a remote host, the HoA field of the binding cache is searched for the IPv6 address of that host. If no match was found, the packet is transmitted according to the routing tables. However, if there was a match, the destination address of packet header is redirected to the CoA specified in the binding cache. This ensures optimal routing to the MN’s current location. The form this encapsulation takes is depending on the state of binding flag stored in the binding cache entry.

With TDPBU, the binding state is illustrated in Fig. 4, in which a simple Finite State Machine (FSM) is driven by incoming packets: once a host receives a packet without HADOH attached from a remote node, it means that node stays in home network, and the binding cache will not record related information of the communication session. Such initial state is called “No Binding”. Once a packet carried a HADOH, it means that the remote node has been moving to a foreign network, so the binding information is added to the Binding Cache Entry (BCE) and the FSM transits to the “Early Binding” state, and the return traffic are through the optimal routing path. Any new arriving packets coming from the remote node will renew the lifetime counter of BCE. After the OPA process is succeeded, the binding state transits to “Secure Binding”, it is different from Early Binding only in that the lifetime of BCE can be extended. The state transition from “Secure Binding” back to “Early Binding” is triggered by the host receiving a packet that carries HADOH with the same HoA coming from a different source address (new CoA). That means the remote node might have moved. There are four reasons for the state transition from “Early Binding” and “Secure Binding” back to “No Binding”: 1) MN receives a packet without piggybacking HADOH, except the tunneled packet from the associated HA; 2) MN receives a binding error or ICMP destination unreachable message from the destination (previous) AR or MAG (meaning that remote node might move away); 3) MN receives a conflict packet, for example, packets with different sources carry the same HoA in HADOH; 4) MN has not received any packet from the BCE for a long time.

F. TDPBU enabled PMIPv6 networks

To adapt TDPBU to a PMIPv6 domain, the basic framework is similar to MIPv6. In Fig. 1, imagine that those MAGs are ARs, LMA is HA, and MN performs TDPBU between the MAGs and itself. So, all mobility management and related signaling will be performed by MAGs on behalf of MN. Since MNs in PMIPv6 might not have mobility support, the HADOH and T2RH might not be recognized by MN themselves, thus the MAGs must perform the Network Address Translation (NAT) between the HoA and CoA.

IV. APPLICATION SCENARIOS FOR ROUTE OPTIMIZATION

When both MN and CN are mobile and under different mobile management domains, our proposed RO technique can be applied to four coexisting MIPv6/PMIPv6 scenarios: InterMIP, MIP\rightarrow PMIP, InterPMIP, and PMIP\rightarrow MIP based on their connection direction. When both MN and its CN have moved away from their home networks, they need to register their CoAs with their associated HAs.

The top half of Fig. 5 (step (1)–(6)) shows a RO connection established between two generic MIPv6 domains. In this case, both MN and CN have moved out of their home areas. Unless the first packet from MN traverses CN’s tunnel path via CN’s HA (HA_{CN}), the return packet from CN are already on RO path.
The bottom half of Fig. 6 (step (a)–(i)) shows a scenario where both the MN and CN are in two different PMIPv6 domains. MAG1 and MAG2 are under LMA1 and LMA2 respectively. In this case, route optimization needs to take place between both MAGs.

Notes that CN on PMIPv6 domain might be without mobility support, and both HADOH and T2RH cannot be recognized by CN; thus, MAG should perform TDPBU $MN_{HoA} \rightarrow MN_{CoA}$ for CN in step (e) when it recognizes the HADOH attached in the incoming packet in step (b). Then MAG should translate the source address from $MN_{CoA}$ to $MN_{HoA}$ in step (d), and translate the destination address from $MN_{CoA}$ to $MN_{HoA}$ and the source address from $CN_{HoA}$ to $CN_{pCoA}$ for step (e) and obtains the packet of step (f). Finally, from step (h) to step (i), the above procedure is reversed.

If the MN was in PMIPv6 domain and the CN was on MIPv6 domains, route optimization should take place between caller-side’s MAGs and MIPv6 enabled MN. The sequence of interactions among different entities is shown in the bottom half of Fig. 6 and the steps are given as (1)–(9) in the figure.

Since in TDPBU there are basically no explicit messages exchanged among mobile network entities, thus it fulfills the requirement of unified route optimization solution for coexisting mobile management domain.

V. PERFORMANCE ANALYSIS

The benefits of TDPBU could be presented by 1) RO latency and 2) signaling cost. Without loss of generality, we make the following assumptions and notations:

1) The network topology under consideration is depicted in Fig. 7, where the one way delay of average-length datagram in which tunneling overhead of each path is included.
2) The average packet length of signaling is 68 bytes (including CoT, CoTI, HoT, HoTI, BU, BAck).
3) The average packet length of datagram is 100 bytes.
4) The wireless bandwidth is 128k bps.
5) The L2 handoff latency is 500ms.

A. Route Optimization Latency

We firstly conducted an experiment to simulate the route optimization latency by observing the variation in end-to-end latency between a MN and a mobile CN, the RO procedure is initiated immediately after handoff procedure, and the result is shown in Fig. 8. The non-route optimized stage (through Path1) continued for about 400ms until the RR procedure was completed, and it entered partial RO (through Path2 or Path3) stage; once in partial RO stage, it costs 190ms to enter full RO stage by reversed RR procedure. Then MN communicated with mobile CN via the shortest path (through Path4). Once the MN has moved, where the handoff latency is 500ms (from 1350th to 1850th ms), the MN still kept the mobile CN’s CoA in its binding cache, the handoff latency can be reduced to 330ms (from 1850th to 2180th ms).

B. Signaling Costs

We perform an experiment to simulate how many signaling messages could be reduced during RO procedure with TDPBU. A MN had established several sessions toward an equal number of CNs. Then it lefted the old AR and attached to a new AR. Once handoff procedure is done, the BU and RO procedures are performed immediately. Four cases were manipulated: case1:
MN with RR procedure of MIPv6 and maintains 100 sessions with different CNs through the new CoA; case 2: with 60 sessions; case 3: with 30 sessions and by case 4: using TDPBU with arbitrary number of sessions. The variation of signaling traffic is compared in Fig. 9. Since in TDPBU it sends a BU message to the HA only once, the RO is nothing to do with the number of sessions. It shows a big difference between RR and TDPBU in signaling costs obviously.

VI. CONCLUSIONS

The next generation IP network has already integrated route optimization as a fundamental part of the mobility support [22]. In this paper, a novel route optimization scheme is proposed with a different view point of security concern. Our proposed scheme has advantages in feasibility of implementation and deployment. Our proposed scheme can achieve much lower handoff and end-to-end latency, ensure immediate route optimization, minimize signaling cost, eliminate binding update message storm, reduce deployment cost, and avoid software complexity of network entities and clients, regardless the coexisting MIPv6/PMIPv6 network environment in which the mobile nodes reside. The performance of our proposed scheme is evaluated through simulations.

Additionally, TDPBU is also useful for Network Mobility (NEMO) environments. Consider a MN which is moving together with the attached mobile network, but it may be unaware that the attached mobile network is moving; such MN has no way of sending explicit binding update messages toward its home agent. The TDPBU will function immediately under such environment.

REFERENCES