Computer Networks 75 (2014) 160–176

Contents lists available at ScienceDirect

Computer Networks

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

A unified MIPv6 and PMIPv6 route optimization scheme for heterogeneous mobility management domains

Wen-Kang Jia

Department of Computer Science, National Chiao Tung University, 1001 University Road, 300 Hsinchu, Taiwan

ARTICLE INFO

Article history:
Received 6 August 2013
Received in revised form 30 June 2014
Accepted 1 October 2014
Available online 12 October 2014

Keywords:
Route optimization
Mobile IPv6 (MIPv6)
Return Routability Procedure (RRP)
Proxy Mobile IPv6 (PMIPv6)
Traffic-Driven Pseudo Binding Update (TDPBU)

ABSTRACT

Nowadays more and more wireless users are on move while accessing the Internet, and providing mobility support in IP networks has been a long-standing challenge. Client-based Mobile IPv6 (MIPv6) is the most widely known mobility management scheme, and fast emerging Proxy-based Mobile IPv6 (PMIPv6) scheme offers an alternative. However, some inherent problems such as route optimization in these schemes have not been totally solved. Although various proposals tried to tackle the route optimization problem, none of them has achieved a satisfactory success. Furthermore, most of them are not a comprehensive solution for coexisting MIPv6/PMIPv6 mobility environments. In this paper, we propose a unified approach to Route Optimization (RO) scheme based on a simplified MIPv6 Return Routability Procedure (RRP) protocol, called Traffic Driven Pseudo Binding Update (TDPBU), which can significantly improve the overall performance of mobility management schemes. Our proposed scheme can ensure immediate route optimization, regardless the heterogeneous MIPv6/PMIPv6 environment in which the MNs reside. Simulation results show that TDPBU can improve the performance in terms of the end-to-end latency, signaling cost, throughput, route optimization latency, route optimization blocking rate, and power consumption compared to original MIPv6 with RRP mechanism. Besides, the deployment cost and software complexity of both network entities and clients, are expected reduction.

1. Introduction

With quick advance in wireless technologies, more and more wireless user clients even servers are becoming mobile, hence provisioning of efficient mobility management in the IP-based wireless networks becomes increasingly important. Mobility management in heterogeneous IP-based wireless access networks is an important functionality for future Internet services since the mobile clients may be moving between multiple types of access networks, which involve several Layer-2 access technologies such as WiFi, WiMAX and UMTS Networks, and multiple Layer-3 mobile management technologies such as Mobile IPv6 (MIPv6) and Proxy Mobile IPv6 (PMIPv6).

In the currently most widely used version of the IP Mobility Protocol—Mobile IPv6 [1,2], enables a Mobile Node (MN) to arbitrarily change its point of attachment to the Internet. Since MIPv6 must be implemented in MNs to serve mobility management by themselves, it is also called Client based MIP (CMIP). On the other hand, the fast emerging Proxy based Mobile IPv6 (PMIPv6) [3–5] protocol provides an alternative for mobility management based on the assistance of local access network.

However, some inherent problems of these protocols have not been totally solved. For example, both of them incur large handoff latency during the period of network attachment, it results in difficulty to support real-time

E-mail address: wkchia@cs.nctu.edu.tw

http://dx.doi.org/10.1016/j.comnet.2014.10.011

multimedia applications [6]; moreover, the most common problem is the Route Optimization (RO) [7] between a MN and its Correspondent Nodes (CNs). RO regards how to route those packets between a MN and a CN efficiently and reliably. Due to the high mobility in future Internet, it may incur two predicaments: (1) mass of CNs is also mobile (so-called Mobile Correspondent Nodes (MCNs)); (2) the communication path between two MNs changes rapidly. These two predicaments bring up problems which are the vastly increased encapsulation overhead and end-to-end latency caused by double tunnel encapsulations and double sub-optimal paths, respectively [7,8]. Thus, route optimization would be compulsory. Subsequently, various solutions have been proposed to accommodate these classic problems, but it still lacks an efficient solution for dealing with the route optimization procedure [2,6].

MIPv6 and PMIPv6 will very likely coexist in the future Internet. In such heterogeneous environments, the bottleneck is often between mobile users. Being able to provide effective route optimization solution between each communication pair is crucial in this environment. Unfortunately, in the standardization process of the route optimization specification, it lacks consideration that CNs are not always stationary, and they may be MNs as well. Further, such specification usually assumes that both communication parties are all CMIP-enabled MNs; the situation of PMIP is analogous to CMIP: assuming that both MNs are under proxy domain. This is not always true in real mobility environments because a MN located at CMIP domain may need to communicate with another MN on PMIP domain and seek an optimized path.

Suppose that N is the number of all active nodes on the Internet, ω is the proportion of MNs, and ρ denotes the proportion of all MNs located in the PMIP domain, so we have $\rho \times \omega$ denoting the proportion of PMIP clients, and $(1-\rho)\omega$ denoting proportion of CMIP clients. Assume that connections between any two nodes are randomized, then at most $2(\rho-\rho^2)\omega^2$ proportion of connections will experience cross domain mobile management. Since growing population of mobile users will result in the increase of ρ and ω in future Internet, assuming that MN and CN were in the same mobile management domain is irrational. Moreover, requesting the network entities to support multiple protocol suites is also unreasonable. Unfortunately, the route optimization management in CMIP and PMIP are often implemented independently, and a unified RO management is required in the future.

Route optimization problem in future IP mobile networks is quite different from today's mobility environments described above. In this paper, a novel route optimization solution for coexisting PMIP/CMIP mobile management domain based on *Traffic Driven Pseudo Binding Update* (*TDPBU*) scheme, and a subsidiary *Optional Post Authentication* (*OPA*) scheme are proposed. According to the performance evaluation results, we demonstrate that our proposed scheme can accomplish the low latency route optimization as expected.

The rest of the paper is organized as follows: In Section 2, we describe the route optimization problem between communication peers within different domains of mobile management and related works. In Section 3, the proposed scheme is elaborated. Application scenarios are demonstrated in detail in Section 4. Performance evaluation including simulation, numerical results and comparison are discussed in Section 5. Finally, Section 6 concludes the work. The Appendix lists the acronyms used in this paper.

2. Related works and problem description

IP mobility concerns the reachability of a MN and persistence of current sessions, as well as connections that conform to the basic requirements for supporting mobility on the Internet. Beyond these basic requirements, IP mobility must be able to support performance requirement in terms of fast handoff and route optimization as well as smoothness of data transport during handover period. In addition, the security issue between roaming MNs and home networks must also be concerned.

2.1. From client-based IP mobility towards proxy-based IP mobility

One of the design principles of the Internet service is intelligent endpoints and simple core network which provides minimum functionality. Client-based MIP (CMIP) is designed based on this principle. Although CMIP ensures seamless mobility for the mobile user session, it introduces some deficiencies, including wasting air-link bandwidth and increasing MN complexity due to signaling overhead and implementing mobile IP protocol suite in client, respectively.

To alleviate the above problems, the IETF network-based local mobility management (NetLMM) [4] working group has initiated tasks in defining a series of Proxy-based MIP (PMIP) [3] protocols, in which local mobility is handled by network side without involvement of the MN. The idea is that a MN moving across multiple *Mobile Access Gateways* (*MAGs*) has not to change its original IP address acquired from its home network; Further, the PMIP provides mobility support to MNs topologically anchored at a *Local Mobility Anchor* (*LMA*) of the access network, which forwards all data for registered MNs, and the MN does not need to participate in any mobility related signaling. In other words, the PMIP enables a mobility environment for all IP-based wireless terminals which lack built-in mobility capability, thereby hiding the mobility of both the IP layer and higher layers.

An additional goal of NetLMM is to simplify the deployment, integrate with and enhance existing solutions if suitable, to the mutual benefit of service operators and end users. The key benefits of PMIP are: decreasing complexity of MNs, enhancing capability for mobility, speeding up the handoff procedure, reducing the air-link consumption, and so on. Such concept brings up *Proxy Mobile IPv4* (*PMIPv4*) [9] and *Proxy Mobile IPv6* (*PMIPv6*) [2] in addition to the legacy client (host) mode *Mobile IPv4* (*MIPv4*) and MIPv6 [2], and the MIP is generally called CMIP in PMIP's perspective.

Today, MIPv6 and PMIPv6 are both candidates for the mobility management in 3GPP System Architecture

Evolution (SAE) which is one of the key challenges for the Long Term Evolution (LTE) of 3G research [14].

2.2. Coexisting deployment of MIPv6 and PMIPv6 networks

Due to their different characteristics, MIPv6 and PMIPv6 can be deployed in hybrid configurations where both types of clients are served in a same network. The interactions scenarios between the two mechanisms are first addressed in [10], which suggest a cooperative model for which PMIPv6 be used for localized mobility and MIPv6 be used for global mobility. In some other deployment scenarios, the MN can be a PMIPv6-enabled client, MIPv6-enabled client or a dual-stack client. An accessory method presents in the [11–13] to decide which entity will manage the signaling of mobile management for the MN, either the MN itself or the network. The usage scenarios and interaction issues of between the two mechanisms in 3G/4G network are also studied in [14]. Moreover, a scenario [10] describes that the dual-stack MN is moving across different access networks, some of them supporting MIPv6 and some others supporting PMIPv6, and that require direct interaction between MIPv6 and PMIPv6. Most of above studies focus on the principles in order to select an appropriate mobility management scheme between MIPv6 and PMIPv6, while others are concerned with the possible usage scenarios of heterogeneous MIPv6 and PMIPv6.

2.3. Route optimization model between mobile nodes

In addition to bi-directional tunneling operation [2], MIPv6 can operate using route optimization mode, with which the MN and CN bypass the *Home Agent* (*HA*) and communicate directly with each other. Without loss of generality, most of direct paths between CNs and MNs would be shorter than routing through the HAs. Thus, route optimization improves data transport rates in mobility environment and especially beneficial when the MNs and CNs are in the near or even same mobility management domain.

In MIPv6, MN owns two valid addresses-*Home-Address* (*HoA*) and *Care-of-Address* (*CoA*) to represent its current location. For sending packets to the CN effectively, a MN can directly send packets using CoA instead of HoA as the source address, thus data traffic do not have to traverse HA. On the other hand, to send packets to the MN effectively, the CN should be aware of the current location (CoA) of MN. If correct MN's location information can be updated to the CN's binding cache, the CN can also directly send packets to the MN's CoA via the optimal route path [1,2,8].

Let us consider that CN are all mobile (a.k.a. MCN) and move along according to the same mobility model. In addition, When the MN and MCN belong to different mobility management domains and both moved beyond their home networks. However, the rule is more complicated than it sounds, and it will result in the most complicated scenario as depicted in Fig. 1. Assume there are four alternative data paths: **Path1**: $(p)MN_{HoA} \leftrightarrow (p)MCN_{HoA}$ is a non-optimized route path under double bidirectional tunneling; **Path2**: $(p)MN_{CoA} \leftrightarrow (p)MCN_{HoA}$ and **Path3**: $(p)MN_{HoA} \leftrightarrow (p)MCN_{CoA}$ are partial route optimization paths with a bidirectional tunneling. However, **Path2** and **Path3** are mutually exclusive depending on which side is firstly initialed for the route optimization. **Path4**: $(p)MN_{CoA} \leftrightarrow (p)MCN_{CoA}$ is a full route optimization path without bidirectional tunneling. Obviously, **Path4** is the best choice based on the shortest hop-counts, and the goal of route optimization is achieved so that the traffic between MN and CN can be shifted from **Path1** to **Path4** through a series of control messages.

2.4. Security concerns during handoff

From the security perspective, any mobility management solution must protect itself against misuses of the mobility features and mechanisms. At least, MIPv6 should not introduce any new security threats to mobile clients from the network and other nodes. The potential security threats of MIPv6 especially in handoff phases can be divided into several types, which were addressed by the [2,15–17].

Among them binding update attack is the most popular one. For instance, an attacker might claim that a certain mobile node is currently at a different location than it really is. If a HA accepts such spoofed binding update request, the victim MN might not get traffic destined to it, and a malicious node might get it illegally. Further and similarly, a malicious MN might also use the HoA of a victim MN in a forged BU message (for route optimization) sent to a victim CN.

Through binding update attacks, which are resulting in Denial of Service (DoS), man-in-the-middle (MITM), Hijacking, Confidentiality, and Impersonation attacks. Most of above threats are caused by the false binding update in the network, so the security objective is to make the routing changes securely, including handoff and route optimization mechanisms [15–17].

To prevent mobile clients from exposing to binding update attacks, the secure mobile management scheme concerns trust and authentication between a MN and a HA. The MN uses services of the HA, so they can exchange some secret such as private authentication in advance, which establish a trust relationship between them. From another aspect, a CN can be arbitrary node in the network, so the MN and the CN will most probably have no relationship beforehand. Several methods were proposed can be used to authenticate the binding messages between the MN and the CN, such as, shared key [18], Public-Key Infrastructure (PKI) [19], Cryptographically Generated Addresses (CGA) [20], Remote Authentication Dial In User Service (RADIUS) [21], Secure Hash Algorithm (SHA) [23], and RRP [2].

Many studies have been reported in this area of research as below: In Optimizing Mobile IPv6 (OMIPv6) [24] and Optimizing Mobile IPv6+(OMIPv6+) [20], it suggests a new route optimization security mechanism for original Mobile IPv6 (MIPv6) based on the longer shared key exchange such as Diffie–Hellman (DH) or CGA algorithms. It proposes to make MIPv6 more optimized with regard to security needs and less redundant in both signaling messages and route optimization delay. The performance improvement achieved is the elimination of

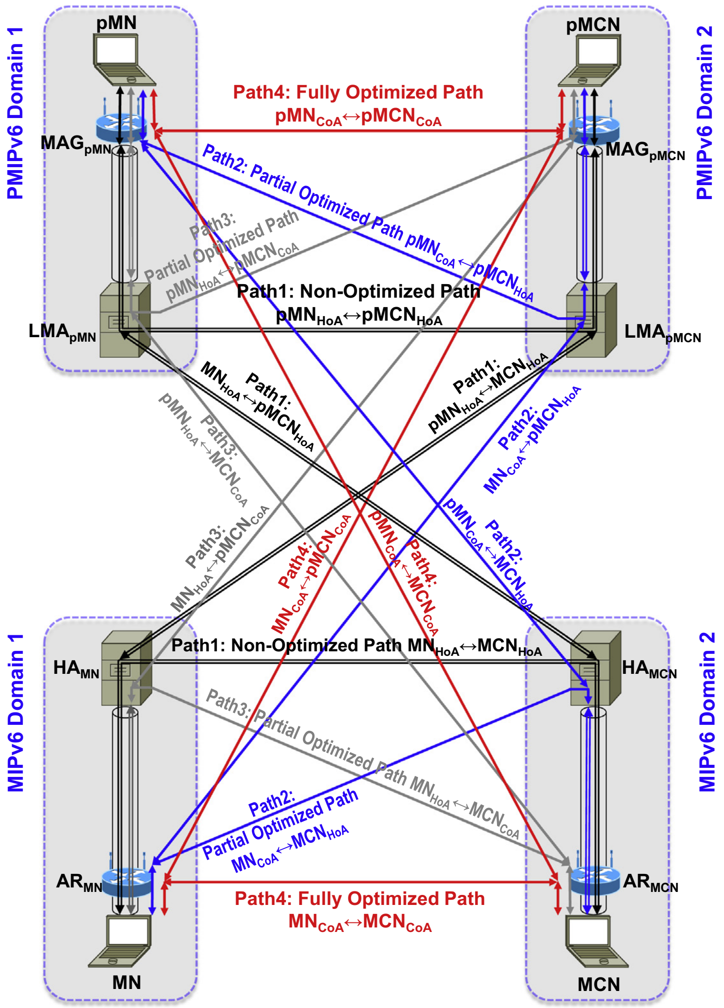

PMIPv6 Domain 1
pMN
PMIPv6 Domain 2
pMCN
Path4: Fully Optimized Path
pMN$_{CoA}$↔pMCN$_{CoA}$
MAG$_{pMN}$
MAG$_{pMCN}$
Path2: Partial Optimized Path pMN$_{CoA}$↔pMCN$_{HoA}$
Path3: Partial Optimized Path pMN$_{HoA}$↔pMCN$_{CoA}$
Path1: Non-Optimized Path
pMN$_{HoA}$↔pMCN$_{HoA}$
LMA$_{pMN}$
LMA$_{pMCN}$
Path1: MN$_{HoA}$↔pMCN$_{HoA}$
Path1: pMN$_{HoA}$↔MCN$_{HoA}$
Path3: pMN$_{HoA}$↔MCN$_{CoA}$
Path2: MN$_{CoA}$↔pMCN$_{HoA}$
Path3: MN$_{HoA}$↔pMCN$_{CoA}$
Path4: MN$_{CoA}$↔pMCN$_{CoA}$
Path4: pMN$_{CoA}$↔MCN$_{CoA}$
Path2: pMN$_{CoA}$↔MCN$_{HoA}$
Path1: Non-Optimized Path MN$_{HoA}$↔MCN$_{HoA}$
HA$_{MN}$
HA$_{MCN}$
MIPv6 Domain 1
MIPv6 Domain 2
Path3: Partial Optimized Path MN$_{HoA}$↔MCN$_{CoA}$
Path2: Partial Optimized Path MN$_{CoA}$↔MCN$_{HoA}$
AR$_{MN}$
AR$_{MCN}$
Path4: Fully Optimized Path
MN$_{CoA}$↔MCN$_{CoA}$
MN
MCN

Fig. 1. Network reference model in which MNs/pMNs are both mobile on different mobility management domains.

all signaling while not moving, and 33% of the per-movement signaling.

Enhanced Route Optimization for Mobile IPv6 [25] specifies an enhanced version of Mobile IPv6 route optimization, it originates an early binding update message that combines the partial return routability tests, provides lower handoff delays, enhances security, and reduces signaling overhead.

Long latency associated with Mobile IPv6's home-address and care-of-address tests can significantly impact delay-sensitive applications. Early Binding Updates [26] proposed an optimization to Mobile IPv6 correspondent registrations that evaded the latency of both address tests. An optimized correspondent registration eliminates 50%, or more, of the additional delay that a standard correspondent registration adds to the network stack's overall latency. The optimization is realized as an optional, and fully backward-compatible, extension to Mobile IPv6.

In order to reconcile both security and handoff performance, a low-latency security mechanism for protecting binding management messages in MIPv6 has been proposed [18], in which it requires configuring a static shared key between the MN and CN, and thus avoid the return routability tests. It can also provide stronger assurance of the home address because it is assumed that the node performing pre-configuration will be with home address. On the other hand [21], describes an extension to the RADIUS protocol that enables an accounting server to notify a Network Access Server (NAS) of a prospective handoff. Thus resulting in the mobile clients potentially reducing handoff latencies.

On the other hand, consider the problem of MIPv6 location privacy described in [22]: the location and movement of the MN can be revealed by the IP addresses used in signaling or data packets. Based on SHA hash function family [23], proposes an efficient and secure techniques to protect location privacy of the MNs.

However, there are obvious limitations in terms of scalability, and a binding update operation cannot be counterfeited due to the absence of a CoA test. In a domain where both the MN and CN share the same trust (e.g., MN and the CN belong to the same HA, or within the same home network), 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.

2.5. Return Routability Procedure (RRP) for MIPv6

When a MN changed its Point of Attachment (PoA) and obtained a new CoA, it sends a *Binding Update* (*BU*) to its associated HA, then all the CNs communicate with it using route optimization approach. The mechanism is simple: let the HA and all CNs know the MN's current point of attachment (CoA), and data packets sent from CNs can first arrive at the HA via MN's HoA, then be tunneled to the MN, or be forwarded to the MN's CoA directly.

When the communication endpoint switched from MN's HoA to CoA as noted previously, *Return Routability* (*RR*) [2] test is used to verify both the right of the MN to use a specific HoA and the validity of the claimed CoA. The secure return routability mechanism of current MIPv6 has been carefully designed to prevent or mitigate a number of known threats. It requires no configuration and no trusted entities beyond the MN's HA, and is based on pervasive distrust of the future mobile Internet [15].

The basic return routability mechanism is triggered by the MN. An intelligent MN can judge the session duration or QoS need to decide whether the route optimization (return routability) is initiated. Once initiated, it consists of two test pairs and four messages: The *Home Test Init* (*HoTI*) and *Care-of Test Init* (*CoTI*) trigger both tests by MNs, the *Home Test* (*HoT*) and *Care-of Test* (*CoT*) reply the test by CNs; the binding update accompanied with both tests are accomplished. If a MN currently communicates with *N* CNs using route optimization approach, the aforementioned procedure will be performed *N* times. The procedures will probably be executed twice if *N* CNs were also mobile.

The return routability procedure is very costly for both MN and CN, especially when both of them are mobile. Regardless the latency of network attachment procedure, the return routability procedure initiated by MN requires at least 6 messages, including RTT_{Path1} and twice RTT_{Path2} to achieve the partial route optimization. Also CN requires 6 messages, including RTT_{Path2}, and twice RTT_{Path4} to initiate the return routability procedure from another direction. If MN initiates the return routability mechanism earlier than CN, the **Path2** should be selected first; otherwise **Path3** should be first traversed. Finally, twice return routability procedures (total 12 messages) have been accomplished by both sides, and the full route optimization will be selected. The whole procedure is depicted in Fig. 2.

Consider that each MN may be moving fast, it causes both MN/CN experiencing a long non-optimized route and/or partial route optimization duration. However, this efficiency of route optimization comes with high cost (e.g., binding update storm and high-latency route optimization) in terms of security needs and excessive mobility signaling messages.

With the above concerns, many low-latency security mechanisms for protecting binding management messages (e.g., signaling related to route optimization) in MIPv6 has been proposed as mentioned in the previous subsection.

Since the maximum lifetime of the Binding Cache Entry (BCE) is very short in the specification, MNs must frequently perform binding update. To reduce the number of binding update messages [27], is recommended to adjust the lifetime of BCE depending on the frequency of mobility, which reduces a lot of signaling overheads.

Furthermore [28], proposed "on demand scheme" and "threshold scheme" in addition to "always push scheme". The simulation results show that the mobility binding update strategy significantly impacts the overall performance of mobile systems, and the threshold scheme proposed in this paper outperforms aforementioned schemes for the route optimization in IP mobile networks. Further, the binding update message storm can also be avoided.

2.6. State of the art: PMIPv6 route optimization protocols

In PMIPv6, all mobility signaling is controlled through the network entities such as the Local Mobility Anchor (LMA) and the Mobile Access Gateway (MAG). The LMA

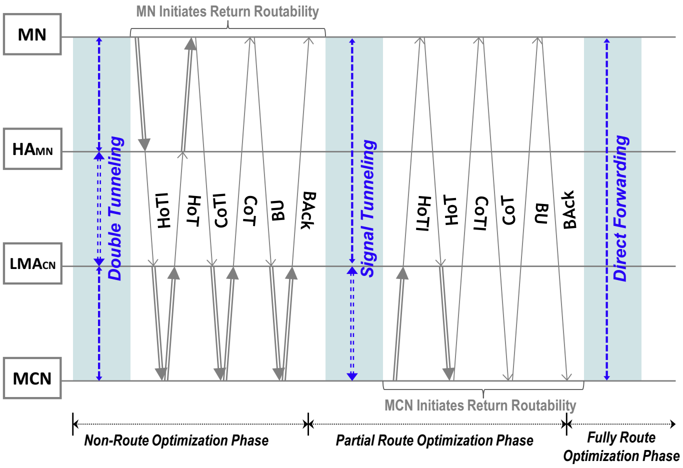

MN Initiates Return Routability
MN
HAMN
LMACN
MCN
Double Tunneling
HoTI
HoT
CoTI
CoT
BU
BAck
Signal Tunneling
HoTI
HoT
CoTI
CoT
BU
BAck
Direct Forwarding
MCN Initiates Return Routability
Non-Route Optimization Phase
Partial Route Optimization Phase
Fully Route Optimization Phase

Fig. 2. Return routability operations performed with both MN and MCN being mobile.

operates as an HA used in MIPv6 and manages the location information of the MN registered to it. The MAG functions like an AR in MIPv6. Once a new MAG (nMAG) detected the movement of a MN, it sends a Proxy Binding Update (PBU) message to its LMA on behalf of the MN if the MN was attached to its access link. A MN without supporting mobility always maintains the original HoA everywhere, including the MN located at the home network, and the MN moving across MAGs in multiple foreign networks. In fact, the MN is even not aware of its movement [2].

Similar to the bi-directional tunneling of MIPv6, the MN always sends and receives packets using its HoA in the PMIP domain. When a MN sends a packet to the CN, the packet is transmitted through a bidirectional IP-in-IP [29] or GRE tunnel [30] which has been created between the MAG and the LMA. The LMA de-encapsulates the packet and forwards it to the CN. Also, when a CN sends a packet to the MN, the packet will be intercepted by the LMA through the reverse tunnel and the MAG transmits the packet to the MN.

To solve such RO problem in PMIPv6, several researches have been performed. Jeong et al. provide the problem statement for route optimization in PMIPv6 [31]. It also investigated design goals and requirements for route optimization with consideration of the characteristics of PMIPv6. Firstly, since a MN is unaware of its topological location, even its proxy Care-of-Address (pCoA), it is not possible for the MN to perform correspondent binding update. Secondly, unlike Mobile IPv6, a MN does not participate in binding management procedures, and signaling is contained within the network entities in Proxy Mobile IPv6. Hence the MN cannot perform optimization procedures and binding update procedures for CNs. Since MAG is an intermediate node of MN–CN communication, it seems not easy to initiate Mobile IPv6 route optimization on behalf of the MN. Finally, In Mobile IPv6, a CN validates whether a MN is reachable through the MN's HoA and CoA and sets up trust relationship between the two nodes. However, the CN cannot establish trust relationship with a MN in Proxy Mobile IPv6 domain.

In the proposed RO protocol in PMIPv6 [32], only network entities exchange the messages for RO configuration, thus it is different from previous RO protocol used in the MIPv6. When MAG initiates Client MIPv6-based return routability test [2] between MN and CN, MAG_{MN} sends Proxy home test (pHoTI) and Proxy care-of test (pCoTI) messages to MAG_{CN} as defined in MIPv6. Since MN does not have CoA in PMIPv6, MAG_{MN} sets the source addresses of Proxy CoTI as its pCoA. Other parameters for authenticating the MN will be set the same as that in MIPv6. In order to acquire information about which MAG_{MN} serves the CN, MAG_{MN} queries LMA_{MN} before initiating return routability procedures, and so does between MAG_{CN} and LMA_{CN}.

Since the RO path is established and updated through exchanging extra messages between the LMA and the MAG, several researches [33–35] proposed novel protocol that focuses on efficient set up and maintenance of an optimized route path between two MNs for complex mobility scenarios as well as networks with multiple mobility anchors. To establish the optimal RO path, the LMA is endowed with the function of Route Optimization control (ROC) [34] and they are established under two modes, the "Direct Mode" and the "Proxy Mode". A series of new control messages are introduced for the novel scheme such as **RO Init**, **RO Report**, **RO Setup**. As a result, the optimized path provides an efficient mobility service to mobile user in the PMIPv6.

In [36], a LMA initiated route optimization protocol based on Correspondent Binding Update (CBU) message is proposed, it features a smooth transition from the serving MAG to the neighboring MAG without sending the CBU message to LMA in PMIPv6. The proposed protocol simplifies the return routability procedures, and it can reduce the handover latency and achieve fast recovery of the optimized path after handover.

In PMIPv6, mobile nodes are topologically anchored at a LMA, which forwards all data for registered MNs. In the case where two MNs belong to different PMIP domains, in order to setup a localized routing path between two MAGs [37], presents a method, which allows forwarding of data packets between two MNs' MAGs without involvement of their each LMA in forwarding. Hence the localized routing path inside an access network is optimization.

Today's mobile management protocol suite employs a turnkey RO solution which renders them complex and hard to implement, and limits the choice of protocols combination. Hence they are often not widely deployed and are of little practical value. Some studies are also investigating more complex scenarios where the mobility of coexisting mobile management domains, this also needs to be analyzed as a possible deployment scenario.

In summary, the development of RO in PMIPv6 still lacks the performance concern because new messages are always introduced in each proposed scheme, and the complexity of interoperation between coexisting and heterogeneous mobility management domains will increase. It is similar to MIPv6 that many RO setup messages experience same amount of RO latency.

In this paper, we do not address the challenges that hybrid PMIPv6/MIPv6 access network present to dual mobile management supported MNs, such as [10–13] which is mentioned previous subsections. On the contrary, a unified MIPv6/PMIPv6 route optimization scheme is proposed between heterogeneous MIPv6 and PMIPv6 domains, which analyze several scenarios when route optimization is used. The analysis could be used to identify possible issues that should be considered in designing extensions for route optimization in heterogeneous MIPv6/PMIPv6 environment.

3. Proposed scheme

In this section, the proposed schemes are discussed. We briefly address the network attachment procedure and handoff procedure. Also we devise a new type of message-less binding update scheme-*Traffic Driven Pseudo Binding Update* (*TDPBU*) scheme which is automatically triggered by first upstream datagram packet from MN to CN, and propose a related *Optional Post Authentication* (*OPA*) scheme that assists CN to create trust relationship with HA_{MN} on demand.

3.1. Design concept

The design concept of TDPBU is threefold: Firstly, the TDPBU is inherent route optimized mobility management scheme cooperating in both PMIPv6 and MIPv6 domains. In order to support route optimization between MNs, both MIPv6 MN and MAG should mandating support the proposed scheme for the additional protocols, which detailed protocol formats are omitted here. The role and structure of the PMIPv6 MN, HA and LMA will remain essentially the same as before. For security reasons, a minimal change is introduced to AR, but it is optional. Security consideration becomes optional rather than compulsory. Oppositely, the RO is always launched between MN and CN, and no longer an option like that in MIPv6.

Secondly, 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 definition are carried by the datagram packet. Thus, the signaling cost can be reduced and the time spent for massive binding update can be ignored.

Finally, in OPA part, the basic idea is to reverse the binding update and the security procedures, thus the handoff latency can be reduced. An experienced hacker today can intrude into an unsecure system within minutes in hacking contests. On average, it takes estimated from several minutes to hours for the hacker to trespass into an ordinary secure system once which is compromised [38–40]. Further, the enhanced technique and increased bandwidth will reduce the spent time.

Therefore, we must be aware that security still faces some infinitesimal threats that should not be neglected. In rule of OPA, the authority of initiation of the new connections has been temporarily and thoroughly suspended in the time duration of OPA. In other words, MNs who are relocated to a new PoA, they can communicate their existing CNs with TDPBU through route optimization path, but they are not authorized to initial new connections towards non-preexisting CNs temporarily until they finished the OPA procedure.

Nonetheless, security threats depend on not only the system robustness, but also the time duration to break in. If the time duration before OPA is short enough, any security threat is unlikely to happen during such a short period (i.e. several milliseconds). Besides, such security threats can be detected and eliminated easily by existing CNs.

3.2. Network attachment

Generally, PMIPv6 and MIPv6 are each going to visit their respective access networks through their respective network attachment procedures. Fig. 3 shows a general TDPBU MIPv6 call-flow diagram with the MIPv6 components, where both MN and CN are with TDPBU support, and both AR and HA play the original role as in MIPv6. Once the AR detects that MN has moved into the visited network, the network attachment such as link acquisition, movement detection, IP configuration, authentication and authorization, and binding update procedures, will be performed when MN leaves the home network and attaches to the foreign network. In the original MIPv6, the successful authentication triggers the binding update procedure. The MN sends a BU message, which contains the new CoA obtained from the new AR, to the HA. The HA updates the existing mobility binding cache entry for the MN and returns the Binding Acknowledgement (BAck) message to the MN. Then the new tunnel between MN_{CoA} and HA is created, and all connections between MN and CN is established through HAHOA initially. This is so-called "bidirectional tunnel" mode, which usually is a non-optimized route path.

With TDPBU, the original network attachment procedure **(1)** will not be involved between MN and HA, and explicit BU messages **(2)** and **(3)** still must be sent to notify HA that MN is moving. Once a MN tries to communicate with CN, it sends data packets to the CN through tunneling using the MN's home address (MN_{HoA}), which tunneled by MN's current care-of-address (MN_{CoA}) **(4)** and **(5)**. Once a CN tries to communicate with MN voluntarily, it sends data packets to the MN using the MN's home address (MN_{HoA}) **(6)**. The HA intercepts these data-packets, forms a tunnel and forwards them to the MN's current care-of-address (MN_{CoA}) **(7)**.

3.3. Datagram forwarding

If a MN wanted to improve the transmission performance, a return routability mechanism is adopted as discussed previously, and it changes the communication target from logical HoA to physical CoA. This is called "route optimization" mode. In general, it is a better path comparing with that in aforementioned schemes.

But with TDPBU, the MN no longer establishes a connection to CN through bidirectional tunnel path (via source address MN_{HoA}) at the beginning, instead it originates the datagram packet with route optimization path (via source address MN_{CoA}) directly, because many border routers discard such packets if they do not contain a source IP address configured for one of the internal networks, the so-called "ingress filtering". Since the packet is originated from source address MN_{CoA}, the packet should be able to reach the stationary CN as expected (step **(8)**).

The datagram packet $MN_{CoA} \leftrightarrow CN$ is piggybacked with the Home Address Destination Options Header (HADOH) that contains MN_{HoA} as mentioned above, this implies that a pseudo binding update to CN will be received and CN can perform a pseudo binding update (early binding) procedure immediately **(9a)**. Moreover, the explicit binding update message can be omitted. If returned packets from CN directly reach the MN_{CoA} **(a)**, and CN does not trust this binding update, the OPA procedure **(b)** will be performed against HA_{MN}, then enter trust mode (secure binding) **(9b)**. The reasons are (1) that MN and its HA_{MN} is assumed to have trust relationship; and (2) since HA_{MN} is usually a stationary site, this design will reduce both air-link bandwidth and process load of MN. Whether OPA is performed on CN's or not, it will significantly speedup the connection transition to route optimization state. Finally, according to the rule of MIPv6, CN returns the packet to MN_{CoA} directly and piggybacks a type 2 routing header that contains

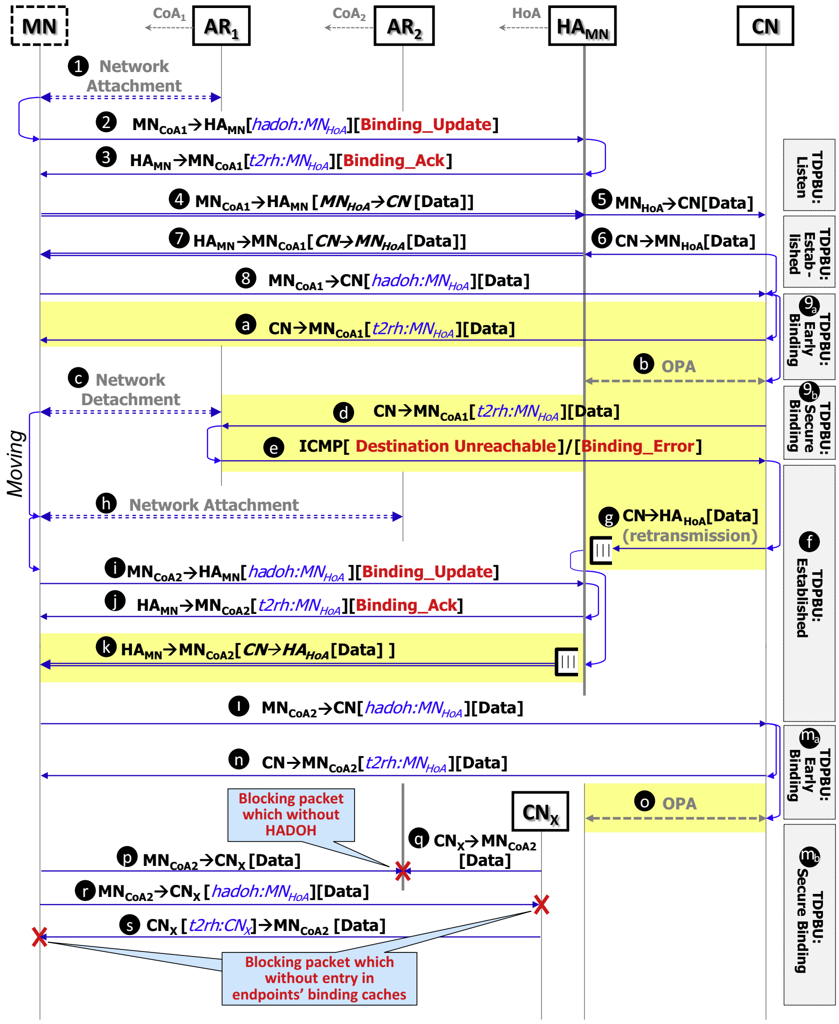

MN
CoA1
AR1
CoA2
AR2
HoA
HAMN
CN
1 Network Attachment
2 MNCoA1→HAMN[hadoh:MNHoA][Binding_Update]
3 HAMN→MNCoA1[t2rh:MNHoA][Binding_Ack]
4 MNCoA1→HAMN [MNHoA→CN [Data]]
5 MNHoA→CN[Data]
6 CN→MNHoA[Data]
7 HAMN→MNCoA1[CN→MNHoA[Data]]
8 MNCoA1→CN[hadoh:MNHoA][Data]
a CN→MNCoA1[t2rh:MNHoA][Data]
b OPA
c Network Detachment
d CN→MNCoA1[t2rh:MNHoA][Data]
e ICMP[Destination Unreachable]/[Binding_Error]
Moving
h Network Attachment
g CN→HAHoA[Data] (retransmission)
i MNCoA2→HAMN[hadoh:MNHoA][Binding_Update]
j HAMN→MNCoA2[t2rh:MNHoA][Binding_Ack]
k HAMN→MNCoA2[CN→HAHoA[Data]]
l MNCoA2→CN[hadoh:MNHoA][Data]
n CN→MNCoA2[t2rh:MNHoA][Data]
o OPA
CNX
Blocking packet which without HADOH
q CNX→MNCoA2 [Data]
p MNCoA2→CNX [Data]
r MNCoA2→CNX [hadoh:MNHoA][Data]
s CNX [t2rh:CNX]→MNCoA2 [Data]
Blocking packet which without entry in endpoints' binding caches
TDPBU: Listen
TDPBU: Estab-lished
9a TDPBU: Early Binding
9b TDPBU: Secure Binding
f TDPBU: Established
ma TDPBU: Early Binding
mb TDPBU: Secure Binding

Fig. 3. The basic route optimization operations performed when MN and stationary CN are in TDPBU enabled MIPv6 network. (The marked sections are optional.)

MN_{HoA}. Now, the bidirectional path is optimal. Note that first data packet is accompanied with HADOH and T2RH between MN and CN, but it is not always generated immediately. The HADOH has been defined in IPv6 specification [41], and T2RH has been defined for route optimization of MIPv6 [2]. This extension header pair allows the data to be exchanged between the MN_{CoA} and CN directly without being routed through the HA.

The destination options have the characteristic that they are only interpreted by the destination in IPv6. When a MN sends an IPv6 datagram to a CN using route optimization with the care-of-address as the source address, the HADOH is used to carry a MN_{HoA}. In other words, a HADOH must be contained in the packets unless the home address appears as the source address in MIPv6.

When a CN sends an IP datagram to a MN using route optimization, the destination address field in the IPv6 header contains the MN_{CoA}, while the T2RH inserted contains the MN_{HoA}. IPv6 nodes that process these routing headers must verify whether the IPv6 address contained corresponds to the home address of the MN. The detailed process is illustrated in Algorithm 1. As a result, once a CN is also mobile, the forwarded packets $MN_{CoA} \rightarrow CN_{CoA}$ should carry both two extension headers, the HADOH that contains MN_{HoA} and T2RH that contains CN_{HoA}. The backward packets $CN_{CoA} \rightarrow MN_{CoA}$ should carry both extension headers too, where the HADOH contains the CN_{HoA} and T2RH contains the MN_{HoA}.

3.4. OPA procedure

For more strict reason such as security issue, the OPA procedure **(b)** and **(o)** can be redeemed after TDPBU. That optional procedure may be triggered by TDPBU, a binding request will then be actively sent from CN to HA_{HoA} to inform the MN performing a real return routability test procedure. This is to confirm that the earlier pseudo binding update was legal. Besides, this OPA messages and user datagram are sent in parallel resulting in shorter RO latency for proposed scheme.

As mentioned previously, the OPA procedure aims to protect preexisting CN's privacy. In other situations, it may harm non-preexisting CN's privacy; hackers (MN side) have attempted to use the security flaw in targeted attacks on third side CNs. Hence, the proposal scheme should justify which packets could not pass through the AR. Fortunately it is quite easy for AR/MAG to block an outbound packets in they without HADOH (step **(p)** and **(q)**). In other words, MN's packets destined for the CN_X go through the HA of MN at first, which applies to reverse tunneling. Once the attacked packet with HADOH which can pass through the AR and directly arrival at the victim CN_X like in step **(r)**, it is not a problem at all, it is quite easy for CN_X to drop an inbound packets in they without entries in CNx's binding cache. Once again, if an outbound attacked packet without tunneling comes from a non-preexisting CN_X, it also blocked by AR/MAG as same rule (step **(s)**).

3.5. MN handoff

If the MN is moving, it may lead to binding update cached in CN being stale **(c)**, and the datagram will be sent to previous location at the moment **(d)**. The previous AR will detect this phenomenon and respond with an ICMP destination unreachable [42] or binding error message [2] to the CN **(e)**, which then is informed to clear the MN_{CoA} from binding cache entry **(f)**, and originates a retransmission task toward the MN_{CoA} (HA_{MN}) **(g)**. After MN finishes the network attachment procedure in the new point of attachment **(h)–(j)**, those retransmitted packets will be delivered to MN_{HoA} **(k)**, and RO procedure will be restarted by datagram forwarding **(l)–(n)**. Note that the backward packet **(k)** will not trigger the forward packet **(l)** immediately, it all occurs according to the behavior of upper layer applications.

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 forwarded to the current location of MN later. Here the concepts of Fast Mobile IP (FMIP) [43] can be applied.

With specific condition, the retransmission procedures **(d)–(e)** and **(g)** may not occur, note that TDPBU relies on normal traffic. Prior to the retransmission procedure triggered by the first downstream datagram packet CN → old_MN_{CoA}, the MN may originate an upstream datagram packet new_MN_{CoA} → CN before the downstream packet arrives. Thus, a TDPBU will be triggered by the first upstream datagram packet **(l)–(n)** received by CN.

3.6. Binding cache maintenance

In the MIPv6 specification, every MN maintains at least two data structures-*Binding Cache* (*BC*) and *Binding Update List* (*BUL*). The original route optimization mechanism in MIPv6 relies on these data structures for binding to the current location, and maintaining correct BUL in the cache. Such binding cache entries are used by a CN to store mapping between HoA and CoA of the MN, and still kept a certain period even after the disconnection or loss of state in MNs. Therefore a binding update list will be kept by MNs, which maintains current binding state on CNs or HAs.

TDPBU always originates a connection via care-of-address and HADOH instead of sending the binding update message. Thus the binding update list can be simplified for solely dealing with the HA.

The binding cache in a TDPBU node contains one entry for every CN with which communication is taking place. The binding cache contains four major fields of information, which are central to the operation of MIPv6, for each binding. Other non-essential fields are omitted for clarity. Algorithm 1 illustrates the detailed process: when a MN wants to transmit a packet to a remote host, the home address field in the binding cache entry is searched to find the IPv6 address of that host. If no match was found, the packet is transmitted according to the routing tables. Otherwise, if there is a match then the destination address in the packet header will be altered to the care-of-address 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.

Algorithm 1. TDPBU_PacketSend (*pkt).

```
INPUT: IP Packet from Input_Interface TCP/IP Socket Layer
OUTPUT: IP Packet to MAC Layer
key $\leftarrow$ SEARCH (BindingCache, pkt.dst.addr)
if key $\neq$ NIL then      // dst is mobile and in foreign network
        BindingCache[key].lifetime++
        ADD_EXTENSION (pkt.t2rh, BindingCache[key].dstHoA)
        pkt.dst.addr $\leftarrow$ BindingCache[key].dstCoA
        if my location is in home network then
              pkt.src.addr $\leftarrow$ myHoA
        else //  my location is in foreign network
              pkt.src.addr $\leftarrow$ myCoA
              ADD_EXTENSION (pkt.hadoh, myHoA)
        endif
else                 //dst is stationary or in home network
        pkt $\leftarrow$ TUNNELING (myHA, pkt)
endif
FORWARD (Output_Interface, pkt);
```

The binding state with TDPBU 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 attached HADOH from a remote node, it means that node is either stationary or stays in home network, and the binding cache does not record related information of the communication session. Such initial state is called "**Listen**". If the host that has received a packet without piggybacking HADOH, it will drop this packet and then keep itself on "**Listen**" state. The state will transit to "**Established**" when a packet without carried a HADOH arrival at MN and expected that a TCP/UDP connection is established immediately following. Once a packet carried a HADOH, it means that the remote node has been moving to a foreign

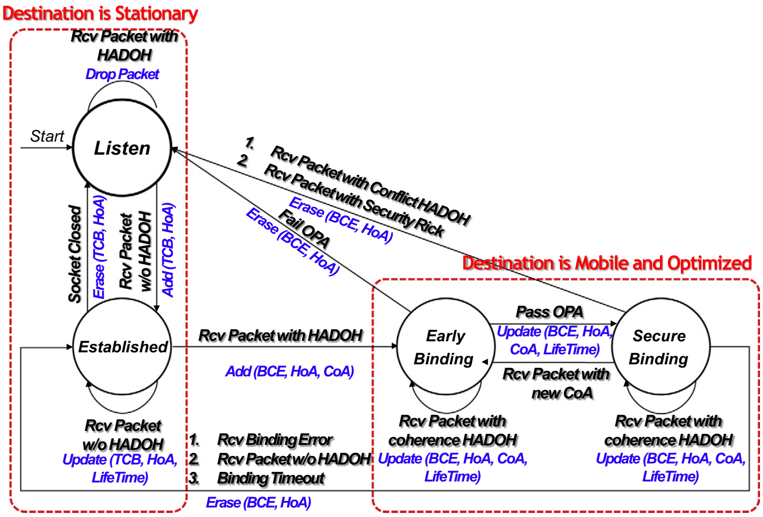


Fig. 4. The FSM for Binding State maintenance in TDPBU enabled MIPv6 Nodes (MN and MAG).

network, so the binding information is added to the Binding Cache Entry (BCE) and the FSM transits to the "**Early Binding**" state (cross reference to step **(9$_a$)** and **(m$_a$)** in Fig. 3), and the return traffic are through the optimal routing path. Any new arriving packets from the remote node will renew the lifetime counter of BCE. After the OPA procedure is succeeded, the binding state transits to "**Secure Binding**" (cross reference to step **(9$_b$)** and **(m$_b$)** in Fig. 3), the only difference with "**Early Binding**" is that the lifetime of BCE can be extended. Else if the OPA procedure was fail, it then transitions to the "**Listen**" state.

The only reason for the state transition from "**Secure Binding**" to "**Early Binding**" is that the host receives a packet with the same home address in HADOH coming from a different source (new CoA) address. That means the remote host might have moved.

Two reasons for the state transition from "**Secure Binding**" back to "**Listen**" are: (1) the host receives a conflict packet such as multiple-source packets carrying the same home address in HADOH; (2) host detects a packet with high risk in security, such as a packet generated by either a new TCP establishment or a port number change after movement.

A host should transit from the "**Secure Binding**" state to the "**Established**" state based on following reasons: (1) the host receives a binding error or "ICMP destination unreachable" message from the destination (previous) AR or MAG, this means that remote node might move away; (2) host receives a packet without piggybacking HADOH, it means that the remote node returns to home network. But it excludes the tunneled packets from the associated HA, this might be caused by host itself moves; (3) host has not received a packet from the BCE for a long time (a.k.a timeout).

3.7. TDPBU enabled PMIPv6 networks

To adapt TDPBU to the PMIPv6 network, the basic framework is similar to MIPv6. In Fig. 1, imagine that these MAGs are ARs, LMA is HA, and MN performs TDPBU between the MAGs and itself. All mobility management and related signaling are performed by MAGs on behalf of the MN. Since MNs in PMIPv6 might not have mobility support, the HADOH and T2RH might not be recognized by MNs themselves, thus the MAGs must play the role analogous to *Network Address Translation* (*NAT*) [44] for translating the HoA to CoA and vice versa.

The translation operates in conjunction with routing function on the proxy side, so that translator can simply be enabled on a MAG when translation is desired. A dynamic form of translation can be configured for some inside-to-outside (pMN → LMA) traffic. Once a HADOH and/or T2RH extension header(s) is carried, a source address (pMN_{CoA}) matching one of those on a translation list will be replaced with pMN_{HoA} address from HADOH, and a destination address (pMCN_{CoA}) will be replaced with pMCN_{HoA} address from T2RH in the meantime. Similar, in the outside-to-inside (LMA → pMN) direction, a source address (pMCN_{HoA}) matching one of those on a translation list will be replaced with pMCN_{CoA} address and a HADOH carry pMCN_{HoA} will be attached automatically. Simultaneously, a destination address (pMN_{HoA}) matching one of those on a translation list will be replaced with pMN_{CoA} address and a T2RH carry pMN_{HoA} also will be attached.

4. Application scenarios for proposed scheme

The most complicated case occurs when a MN and CN are both mobile and in different mobility management domains. In this section, four coexisting MIPv6/PMIPv6 scenarios to which the proposed scheme can be applied are discussed. These scenarios can primarily be classified as four scenarios: (1) *Inter-MIP*, (2) *MIP → PMIP*, (3) *Inter-PMIP*, and (4) *PMIP → MIP* according to their connection direction. Our proposed route optimization scheme can be applied to all of these scenarios.

Assuming both the MN and the MCN are mobile, and the MN has moved away from its home network while the MCN has also moved into a foreign network, as shown in Figs. 5 and 6, both of these moving nodes need to register their

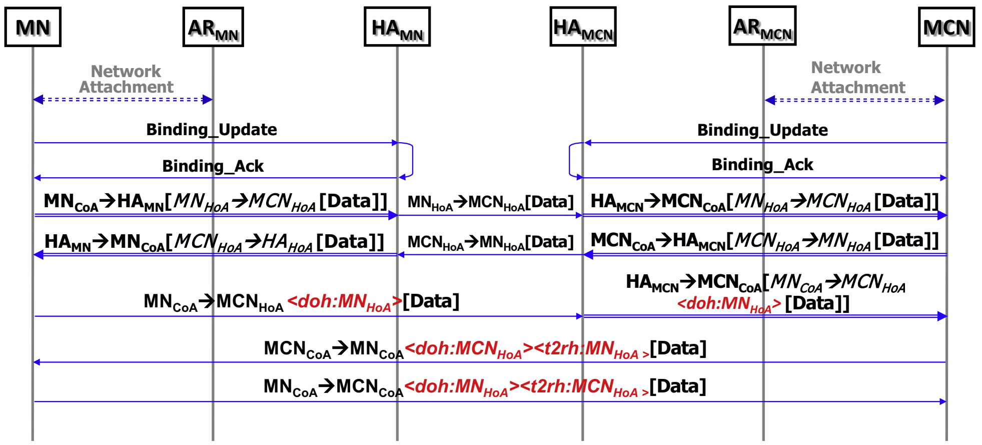

MN
AR_{MN}
HA_{MN}
HA_{MCN}
AR_{MCN}
MCN
Network Attachment
Network Attachment
Binding_Update
Binding_Ack
Binding_Update
Binding_Ack
MN_{CoA}→HA_{MN}[MN_{HoA}→MCN_{HoA}[Data]]
MN_{HoA}→MCN_{HoA}[Data]
HA_{MCN}→MCN_{CoA}[MN_{HoA}→MCN_{HoA}[Data]]
HA_{MN}→MN_{CoA}[MCN_{HoA}→HA_{HoA}[Data]]
MCN_{HoA}→MN_{HoA}[Data]
MCN_{CoA}→HA_{MCN}[MCN_{HoA}→MN_{HoA}[Data]]
MN_{CoA}→MCN_{HoA} <doh:MN_{HoA}>[Data]
HA_{MCN}→MCN_{CoA}[MN_{CoA}→MCN_{HoA} <doh:MN_{HoA}> [Data]]
MCN_{CoA}→MN_{CoA}<doh:MCN_{HoA}><t2rh:MN_{HoA} >[Data]
MN_{CoA}→MCN_{CoA}<doh:MN_{HoA}><t2rh:MCN_{HoA} >[Data]

Fig. 5. Proposed scheme operations in the Inter-MIPv6 domains.

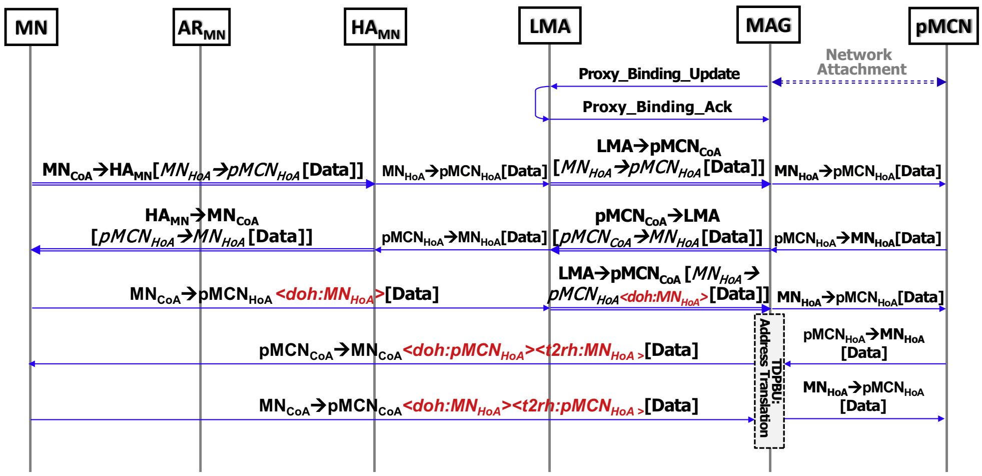

MN
AR_{MN}
HA_{MN}
LMA
MAG
pMCN
Network Attachment
Proxy_Binding_Update
Proxy_Binding_Ack
MN_{CoA}→HA_{MN}[MN_{HoA}→$pMCN_{HoA}$[Data]]
MN_{HoA}→$pMCN_{HoA}$[Data]
LMA→$pMCN_{CoA}$ [MN_{HoA}→$pMCN_{HoA}$[Data]]
MN_{HoA}→$pMCN_{HoA}$[Data]
HA_{MN}→MN_{CoA} [$pMCN_{HoA}$→MN_{HoA}[Data]]
$pMCN_{HoA}$→MN_{HoA}[Data]
$pMCN_{CoA}$→LMA [$pMCN_{CoA}$→MN_{HoA}[Data]]
$pMCN_{HoA}$→MN_{HoA}[Data]
MN_{CoA}→$pMCN_{HoA}$ <doh:MN_{HoA}>[Data]
LMA→$pMCN_{CoA}$ [MN_{HoA}→ $pMCN_{HoA}$<doh:MN_{HoA}>[Data]]
MN_{HoA}→$pMCN_{HoA}$[Data]
TDPBU: Address Translation
$pMCN_{CoA}$→MN_{CoA}<doh:$pMCN_{HoA}$><t2rh:MN_{HoA} >[Data]
$pMCN_{HoA}$→MN_{HoA} [Data]
MN_{CoA}→$pMCN_{CoA}$<doh:MN_{HoA}><t2rh:$pMCN_{HoA}$ >[Data]
MN_{HoA}→$pMCN_{HoA}$ [Data]

Fig. 6. Proposed scheme operations in between MIPv6 and PMIPv6 domains.

CoAs with their associated HAs. The Fig. 5 shows a RO connection established between two generic MIPv6 domains with all the MIPv6 components. Unless the first packet from MN traverses MCN's tunnel path via HA_{MCN}, the return packets from MCN are already on RO path. Route optimization technique offers the biggest advantage when the HA_{MN} and HA_{MCN} are far away from the MN and MCN respectively, and both of them are based on MIPv6. The Fig. 6 shows a RO connection established from MIPv6 toward PMIPv6 domains, which contain MIPv6 components and PMIPv6 components, respectively. In this case the MAG assists the proxy MCN (pMCN) to perform the RO procedure. Here route optimization technique will offer the biggest advantage when the HA_{MN} and LMA are far away from the MIPv6-based MN and PMIPv6-based pMCN, respectively.

A pMCN on PMIPv6 domain may not have mobility support, it means both the DOH and T2RH cannot be recognized by the CN. Thus MAG should perform TDPBU $MN_{HoA} \rightarrow MN_{CoA}$ address translating for pMCN in LMA when it recognizes the DOH attached in the incoming packet from MN_{CoA} to $pMCN_{CoA}$, then MAG should translate the source address from MN_{CoA} to MN_{HoA} (extract from DOH). In the backward direction, the MAG retranslates the source address from $pMCN_{HoA}$ to $pMCN_{CoA}$, and retranslates the destination address from MN_{HoA} to MN_{CoA} (extract from address translation table), and attaches the DOH (contains $pMCN_{HoA}$) and T2RH (contains MN_{HoA}) to the packet. Finally, the above procedure is reversed.

If the pMN was in PMIPv6 domain and the MCN was in MIPv6 domains, route optimization should take place between caller-side's MAGs and MIPv6 enabled MCN. The sequence of interactions among different entities is shown in Fig. 7.

Fig. 8 shows a scenario in which the pMN and MCN are in different mobile management domains. MAG_{pMN} and MAG_{pMCN} are under LMA_{pMN} and LMA_{pMCN} respectively. In this case, route optimization takes place between two MAGs. Since with TDPBU, basically no explicit messages

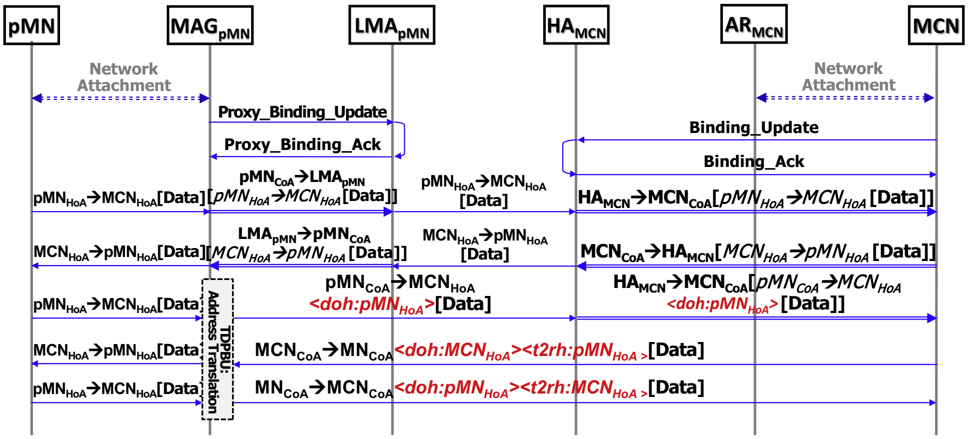

pMN
MAG_{pMN}
LMA_{pMN}
HA_{MCN}
AR_{MCN}
MCN
Network Attachment
Network Attachment
Proxy_Binding_Update
Proxy_Binding_Ack
Binding_Update
Binding_Ack
$pMN_{HoA} \rightarrow MCN_{HoA}$[Data]
$pMN_{CoA} \rightarrow LMA_{pMN}$ [$pMN_{HoA} \rightarrow MCN_{HoA}$[Data]]
$pMN_{HoA} \rightarrow MCN_{HoA}$ [Data]
$HA_{MCN} \rightarrow MCN_{CoA}$[$pMN_{HoA} \rightarrow MCN_{HoA}$ [Data]]
$MCN_{HoA} \rightarrow pMN_{HoA}$[Data]
$LMA_{pMN} \rightarrow pMN_{CoA}$ [$MCN_{HoA} \rightarrow pMN_{HoA}$ [Data]]
$MCN_{HoA} \rightarrow pMN_{HoA}$ [Data]
$MCN_{CoA} \rightarrow HA_{MCN}$[$MCN_{HoA} \rightarrow pMN_{HoA}$ [Data]]
$pMN_{HoA} \rightarrow MCN_{HoA}$[Data]
$pMN_{CoA} \rightarrow MCN_{HoA}$ <doh:pMN_{HoA}>[Data]
$HA_{MCN} \rightarrow MCN_{CoA}$[$pMN_{CoA} \rightarrow MCN_{HoA}$ <doh:pMN_{HoA}> [Data]]
TDPBU: Address Translation
$MCN_{HoA} \rightarrow pMN_{HoA}$[Data]
$MCN_{CoA} \rightarrow MN_{CoA}$<doh:$MCN_{HoA}$><t2rh:$pMN_{HoA}$>[Data]
$pMN_{HoA} \rightarrow MCN_{HoA}$[Data]
$MN_{CoA} \rightarrow MCN_{CoA}$<doh:$pMN_{HoA}$><t2rh:$MCN_{HoA}$>[Data]

Fig. 7. Proposed scheme operation in Inter-PMIPv6 domains.

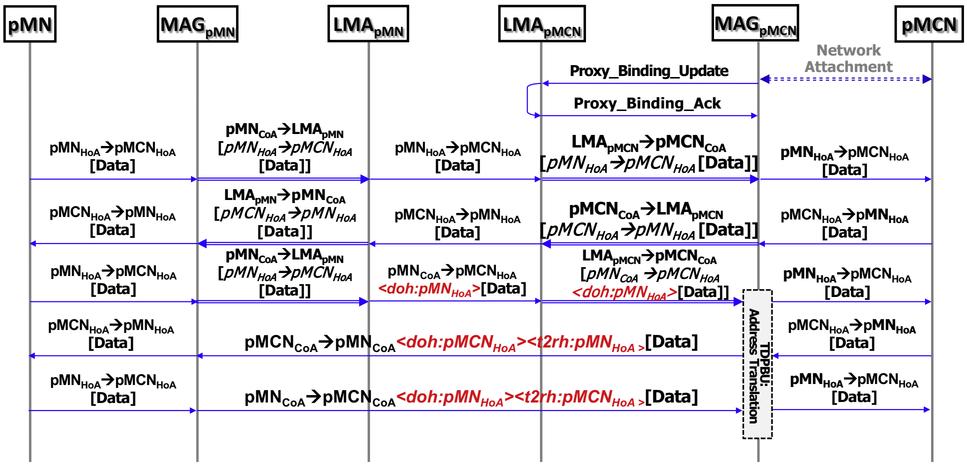

pMN
MAG_{pMN}
LMA_{pMN}
LMA_{pMCN}
MAG_{pMCN}
pMCN
Network Attachment
Proxy_Binding_Update
Proxy_Binding_Ack
$pMN_{HoA} \rightarrow pMCN_{HoA}$ [Data]
$pMN_{CoA} \rightarrow LMA_{pMN}$ [$pMN_{HoA} \rightarrow pMCN_{HoA}$ [Data]]
$pMN_{HoA} \rightarrow pMCN_{HoA}$ [Data]
$LMA_{pMCN} \rightarrow pMCN_{CoA}$ [$pMN_{HoA} \rightarrow pMCN_{HoA}$ [Data]]
$pMN_{HoA} \rightarrow pMCN_{HoA}$ [Data]
$pMCN_{HoA} \rightarrow pMN_{HoA}$ [Data]
$LMA_{pMN} \rightarrow pMN_{CoA}$ [$pMCN_{HoA} \rightarrow pMN_{HoA}$ [Data]]
$pMCN_{HoA} \rightarrow pMN_{HoA}$ [Data]
$pMCN_{CoA} \rightarrow LMA_{pMCN}$ [$pMCN_{HoA} \rightarrow pMN_{HoA}$ [Data]]
$pMCN_{HoA} \rightarrow pMN_{HoA}$ [Data]
$pMN_{HoA} \rightarrow pMCN_{HoA}$ [Data]
$pMN_{CoA} \rightarrow LMA_{pMN}$ [$pMN_{HoA} \rightarrow pMCN_{HoA}$ [Data]]
$pMN_{CoA} \rightarrow pMCN_{HoA}$ <doh:pMN_{HoA}>[Data]
$LMA_{pMCN} \rightarrow pMCN_{CoA}$ [$pMN_{CoA} \rightarrow pMCN_{HoA}$ <doh:pMN_{HoA}>[Data]]
$pMN_{HoA} \rightarrow pMCN_{HoA}$ [Data]
TDPBU: Address Translation
$pMCN_{HoA} \rightarrow pMN_{HoA}$ [Data]
$pMCN_{CoA} \rightarrow pMN_{CoA}$<doh:$pMCN_{HoA}$><t2rh:$pMN_{HoA}$>[Data]
$pMCN_{HoA} \rightarrow pMN_{HoA}$ [Data]
$pMN_{HoA} \rightarrow pMCN_{HoA}$ [Data]
$pMN_{CoA} \rightarrow pMCN_{CoA}$<doh:$pMN_{HoA}$><t2rh:$pMCN_{HoA}$>[Data]
$pMN_{HoA} \rightarrow pMCN_{HoA}$ [Data]

Fig. 8. Proposed scheme operation in between PMIPv6 and MIPv6 domains.

are exchanged among mobile network entities, this fulfills the requirement of unified route optimization solution for coexisting mobility management domains.

5. Performance evaluation

5.1. Simulation methodology

In this section, we evaluated the performance of TDPBU whose benefits could be illustrated by (1) end-to-end latency during route optimization; (2) signaling costs; (3) throughput; and (4) route optimization latency and blocking rate in an error-prone link. Fig. 9 presents the network topology for the experiments, note that CN is also mobile (a.k.a. MCN). Without loss of generality, we make the following assumptions and notations:

- The one way delay for average-length datagram of $T_{MN \rightarrow AR\_MN}$, $T_{CN \rightarrow AR\_CN}$, $T_{AR\_MN \rightarrow HA\_MN}$, $T_{AR\_CN \rightarrow HA\_CN}$, $T_{HA\_MN \rightarrow HA\_CN}$, $T_{HA\_MN \rightarrow AR\_CN}$, $T_{HA\_CN \rightarrow AR\_MN}$ and TA$_{R\_MN \rightarrow AR\_CN}$ are 2, 2, 15, 15, 30, 15, 15 and 20, respectively; It means that **Path1**: $MN_{HoA} \leftrightarrow CN_{HoA}$, **Path2**: $MN_{CoA} \leftrightarrow CN_{HoA}$, **Path3**: $MN_{HoA} \leftrightarrow CN_{CoA}$ and **Path4**: $MN_{CoA} \leftrightarrow CN_{CoA}$ have one way delay with 64 ms, 34 ms, 34 ms and 24 ms, respectively. The network topology under consideration is depicted in Fig. 9, in which tunneling overhead is included.
- The average packet length of signaling is 68 bytes (including CoT, CoTI, HoT, HoTI, BU, and BAck).
- The average packet length of datagram is 100 bytes.
- The wireless bandwidth is 54 Mbps.
- The L2 handoff latency is 500 ms.
- The signaling process time is omitted.

5.2. End-to-End Latency during Route Optimization

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 during handoff and route optimization phases. The route

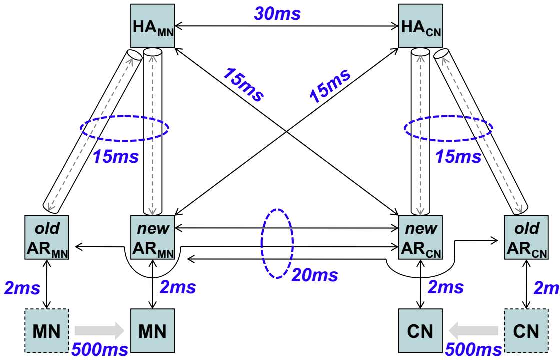


Fig. 9. Network topology for simulation.

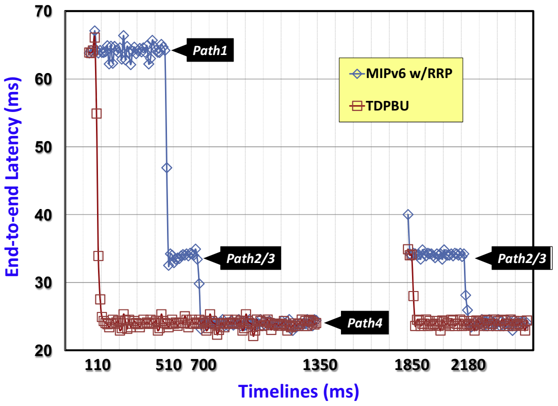


Fig. 10. Comparison of end-to-end latencies for MIPv6/RRP and TDPBU during handoff and route optimization.

optimization procedure will be initiated immediately after the handoff procedure (at 110th ms), the result is shown in Fig. 10, the non-optimized route stage (through **Path1**) continued for about 400 ms (from 110th to 510th ms) until the unidirectional return routability procedure was completed, and it enters into partial route optimization (through **Path2** or **Path3**). Once in the partial route optimization stage, it took 190 ms (from 700th to 1,350th ms) to transit to fully route optimization stage through the bidirectional reversed return routability procedure. Then MN communicated with mobile CN via the shortest path (through **Path4**). When the MN moved again while the handoff latency was 500 ms (from 1,350th to 1,850th ms), the communication was disrupted during this period. After that, the MN re-attached to the AR and still kept the mobile CN's CoA in its binding cache. As a result, the unidirectional route optimization procedure was reduced to 330 ms (from 1,850th to 2,180th ms).

5.3. Signaling costs during route optimization procedures

We also concerned the number of signaling messages to be reduced during route optimization procedure with

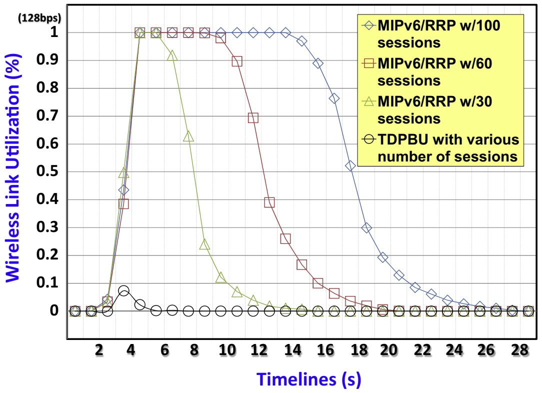


Fig. 11. Comparison of route optimization signaling costs between MIPv6/RRP and TDPBU.

TDPBU, and performed a simulation experiment to evaluate the signaling traffic. A MN had established several sessions toward different CNs, and it left the old AR and attached to a new one. Once the handoff procedure is done, the binding update and route optimization procedures are performed immediately. Four cases were manipulated: (1) MN with return routability procedure MIPv6 and switched 100 sessions (CNs) to the new CoA; (2) 60 sessions (CNs); (3) 30 sessions (CNs); (4) TDPBU method with various numbers of sessions (CNs). We measure the variation of signaling traffic, and Fig. 11 depicts a comparison of aforementioned results. Since TDPBU sends a binding update message to its HA only once, its route optimization is nothing to do with the number of sessions (CNs). Obviously it shows a huge difference between MIPv6/RRP and TDPBU in signaling costs.

5.4. Network throughput during continuous movement

We also investigated the impact of the end-to-end TCP and UDP throughput during the continuous movement of MNs and MCNs. All MNs are now set to operate with different handoff frequencies (a.k.a. mobile speeds) whose unit is number of handoffs per minute. Both MNs and CNs move to the destination and stay there for certain duration (1/mobile speed), then move again. The handoff occurs randomly, and the duration is normally distributed. The model is more suitable to movement found in mobile networks that may be typical in future Internet. Fig. 12 shows that TDPBU can increase the UDP throughput (reduce the signaling cost) of MNs, especially that moves frequently. Note that end-to-end throughput was measured with UDP traffic; the maximum theoretical UDP throughput of MIPv6 (without RO) would be lower due to the long RTT.

Fig. 13 shows the TCP Vegas [45] throughputs of each of the three mobility schemes as a function of varying handoff frequencies of both the MN and MCN, and with window size = 32,768 and buffer size = 16 M bytes as parameters. Fig. 14 presents TCP Reno [46] throughputs as a function of varying handoff frequencies, and is similar to the previous simulation.

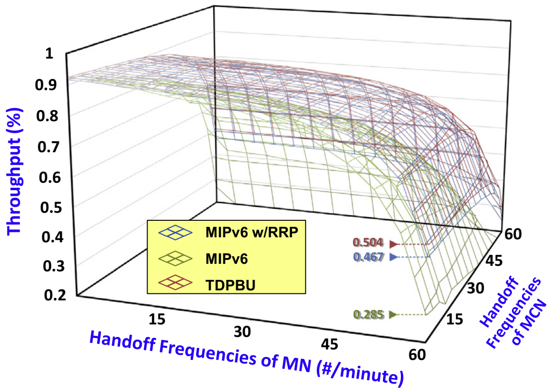


Fig. 12. Comparison of UDP throughput vs. handoff frequencies between mobility schemes.

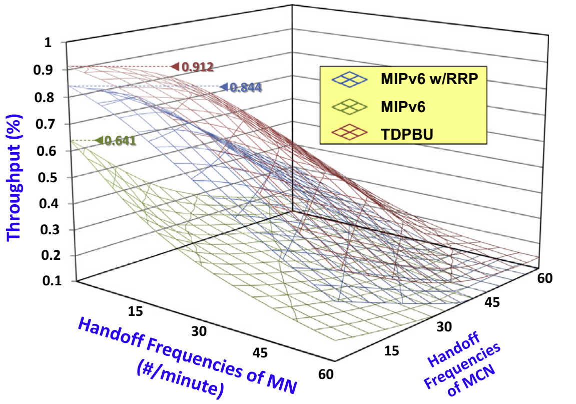


Fig. 14. Comparison of TCP Reno throughput vs. handoff frequencies between mobility schemes.

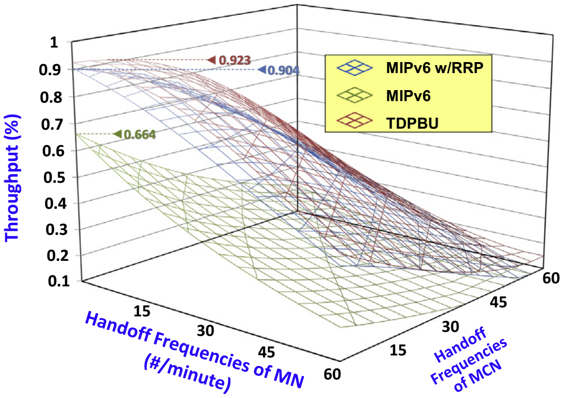


Fig. 13. Comparison of TCP Vegas throughput vs. handoff frequencies between mobility schemes.

For the case that the handoff frequencies are increasing progressively, the suboptimal path delay (represented by RTT) and Packet Loss Rate (PLR) of the TCP flows will be influenced, and it impacts the throughput of TCP connection. Even for a small mobility probability there is very little RTT and PLR in the network. The TCP flows still spend most of their available bandwidth in congestion avoidance mechanism. The result is that the UDP flow has higher throughput and also suffers high mobility probability than TCP. In addition, as the handoff frequency increases, the MIPv6 with RRP and TDPBU have similar performance. Finally, when handoff frequency of both sides becomes heavier TCP Vegas outperforms Reno since it employs more intelligent congestion control mechanisms.

5.5. Route optimization latency and blocking rate in an error-prone link

In reliable networks and protocols, error control schemes must be embedded. We assume that error detection schemes such as *Cyclic Redundancy Check* (*CRC*) are performed in each mobile component. Once an erroneous signaling message was detected by receivers, or timeout was detected by senders, the automatic retransmission mechanism is originated immediately. However, it will cause longer delay to combat the channel errors. Generally, reducing either quantity of messages or length of the message could reduce the error probability in an error-prone wireless link.

Before evaluating the performance of the proposed scheme, some background conditions must be set. First, the bit error occurs randomly with normal distribution. If a bit error in a control message is detected, the message must be retransmitted. Once retransmission reaches 3 times for a message, we assume that route optimization procedure is blocked. We define the RO latency as the duration from initiating the RO procedure between a MN and the CN to the successful arrival of the first datagram. Fig. 15 displays the RO latency of TDPBU and MIPv6/RRP vs. varying Bit Error Rate (BER) in different RO schemes and retransmission times. Obviously, in high BER environment, the TDPBU can efficiently reduce the RO latency.

Fig. 16 shows the relationship between RO blocking rate and BER in different RO schemes and retransmission

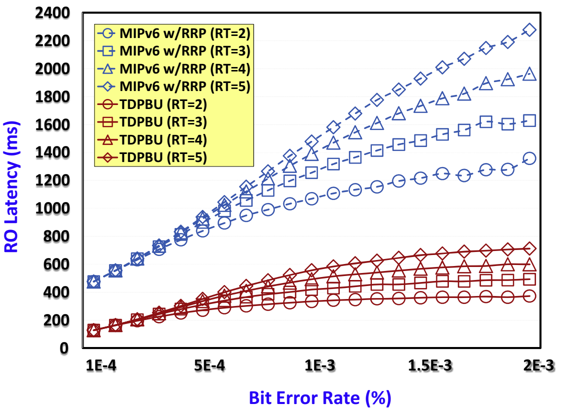


Fig. 15. Comparison of route optimization latency vs. BER between MIPv6/RRP and TDPBU.

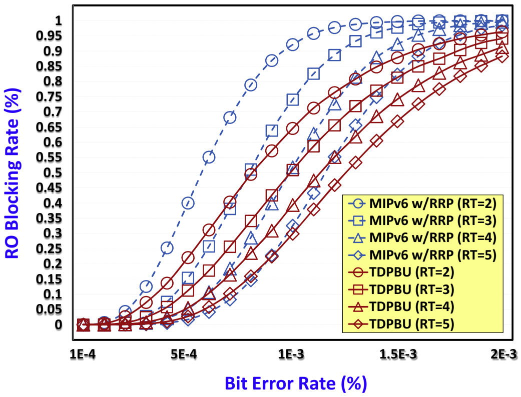


Fig. 16. Comparison of route optimization blocking rate vs. BER between MIPv6/RRP and TDPBU.

times. TDPBU can significantly reduce the blocking rate in a high BER radio environment. According to the discussion above, our proposed scheme is more suitable for poor wireless environment than the original MIPv6.

5.6. Energy saving during continuous movement

In this subsection, we extend our work to provide energy efficient to wireless mobile networks. Additionally, let us assume the main cause of additional power consumption in AR/MAG is transmitting data and signaling packets. We consider the Average Energy Efficiency (AEE) metric which is defined as

$$\text{AEE} = \frac{\textit{energy consumption for transmit packets}}{\textit{total energy consumption}} \tag{1}$$

This AEE metric has been first adopted in previous works such as [47]. Our goal is to maximize the AEE metric across all MNs receiving the same data size in the coverage area of AR/MAGs. We evaluate and compare the energy savings resulted from our proposed scheme to that of the original scheme. In Fig. 17, we present the comparison between the three mobile management and route optimization schemes when the handoff frequencies and number of MNs varies, respectively.

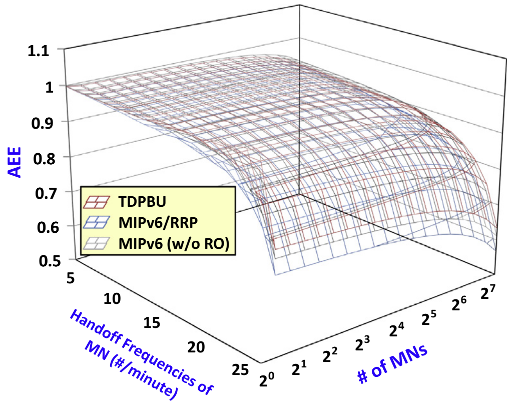


Fig. 17. Energy efficiency vs. handoff frequencies and number of MNs.

The figures show that the proposed scheme achieves high values for the AEE metric (close to 1) and remains significantly more efficient than the MIPv6-RO (with RRP) and original MIPv6 (without route optimization) schemes when the handoff frequency increases. In addition, the results also show that the energy consumption increases when the number of MN increases. Moreover, if the MN selects the MIPv6/RRP scheme, the energy consumptions are significantly worsened in all expected AEEs, because of the performance raise by reducing tunnel overhead will be offset by the great amounts of RRP procedures.

6. Conclusions and future works

The next generation IP network has already integrated route optimization as a fundamental part of the mobility support [1,48]. Both MIPv6 and PMIPv6 mobility management techniques have provided various route optimization mechanisms. However, some inherent problems of those mechanisms have not been totally solved. These include the ineffective route optimization procedures which usually are not comprehensive solutions for coexisting MIPv6/PMIPv6 mobility management environment. In this paper, a novel route optimization scheme is proposed with different view point of security concern. Our proposed scheme features advantages in feasible implementation and deployment, much lower handoff and end-to-end latency, immediate route optimization, minimizing signaling cost, eliminating binding update message storm, reducing deployment cost, and avoiding software complexity of network entities and clients, regardless the coexisting MIPv6/PMIPv6 network environment in which the MNs reside. The performance of our proposed scheme is evaluated through simulations.

One of the TDPBU design goals is to address most of the mobility challenges in one unified architectural view by appropriately balancing both client-side and network-side requirements. However, we must admit that as a big whole architecture, behind many high level descriptions and discussions, especially about the concept of inter-mobility-domains negotiation, QoS insurance during handoff, and provision of Authentication, Authorization and Accounting (AAA) services among mobility-domains, significant research and experiments are still needed to be done in the future.

In the future, we will also work in the description of TDPBU of 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 is unable to send explicit binding update messages to its HA. Our TDPBU scheme will function immediately under such environment. Consequently, proposed scheme is expecting useful for NEMO environments.

Appendix A. Acronym Table

Acronym	Definition
AAA	Authentication, Authorization and Accounting
AEE	Average Energy Efficiency
AR	Access Router
BAck	Binding Acknowledge
BCE	Binding Cache Entry
BE	Binding Error
BU	Binding Update
nAR	new Access Router
MN	Mobile Node
CMIP	Client based MIP
CN	Correspondent Node
CoA	Care-of Address
CoT	Care-of Test
CoTI	Care-of Test Init
HA	Home Agent
HADON	Home Address Destination Options Header
HoA	Home Address
HoT	Home Test
HoTI	Home Test Init
LTE	Long Term Evolution
LMA	Local Mobility Anchor
MAG	Mobile Access Gateway
MCN	Mobile Correspondent Node
MIPv6	Mobile Internet Protocol Version 6
NEMO	Network Mobility
nMAG	new Mobile Access Gateway
OPA	Optional Post Authentication
PBU	Proxy Binding Update
pCoA	proxy Care-of Address
pHoA	proxy Home Address
PMIPv6	Proxy Mobile Internet Protocol Version 6
pMN	Proxy Mobile Node
PoA	Point of Attachment
RO	Route Optimization
RRP	Return Routability Procedure
T2RH	Type-2 Routing Header
TCP	Transmission Control Protocol
UDP	User Datagram Protocol

References

[1] R.S. Koodli, C.E. Perkins, Mobile Inter-Networking with IPv6: Concepts, Principles and Practices, Wiley-Interscience, USA, 2007.

[2] C. Perkins, D. Johnson, J. Arkko, Mobility Support in IPv6, IETF RFC 6275, 2011.

[3] S. Gundavelli, K. Leung, V. Devarapalli, K. Chowdhury, B. Patil, Proxy Mobile IPv6, IETF RFC 5213, 2008.

[4] J. Kempf (Ed.), Goals for Network-based Localized Mobility Management (NETLMM), IETF RFC 4831, 2007.

[5] J. Kempf (Ed.), Problem Statement for Network-Based Localized Mobility Management (NETLMM), IETF RFC 4830, 2007.

[6] W.M. Chen, W. Chen, H.C. Chao, An efficient mobile IPv6 handover scheme, Telecommun. Syst. 42 (3–4) (2009) 293–304.

[7] Z. Yan et al., Design and implementation of a hybrid MIPv6/PMIPv6-based mobility management architecture, Math. Comput. Model. 53 (2011) (2011) 421–442.

[8] P.C. Saxena, S. Jasola, Performance of intelligent Mobile IPv6, Comput. Stand. Interfaces 28 (6) (2006) 737–751.

[9] K. Leung, G. Dommety, P. Yegani, K. Chowdhury, WiMAX Forum/3GPP2 Proxy Mobile IPv4, IETF RFC 5563, 2010.

[10] G. Giaretta, Interactions between Proxy Mobile IPv6 (PMIPv6) and Mobile IPv6 (MIPv6): Scenarios and Related Issues, IETF RFC 6612, 2012.

[11] D. Damic et al., Proxy Mobile IPv6 Indication And Discovery. Internet-Draft: draft-damic-netlmm-pmip6-ind-discover-03, 2008.

[12] B.-J. Han, J.-H. Lee, T.-M. Chung, Hybrid PMIPv6 indication mechanism for interaction between MIPv6 and PMIPv6, in: International Conference on Mobile Technology, Applications, and Systems (Mobility '08), 2008.

[13] G. Velev, K. Weniger, Interactions between PMIPv6 and MIPv6: route. optimization issues, Internet-Draft: draft-velev-netlmm-mip-pmip-ro-01, 2008.

[14] ETSI, Architecture enhancements for non-3GPP accesses, 3GPP TS 23.402 version 11.6.0 Release 11, 2013.

[15] P. Nikander, J. Arkko, T. Aura, G. Montenegro, E. Nordmark, Mobile IP Version 6 Route Optimization Security Design Background, IETF RFC 4225, 2005.

[16] T. Aura, J. Arkko, MIPv6 BU Attacks and Defenses, Internet-Draft: draft-aura-mipv6-bu-attacks-01, 2002.

[17] C. Vogt, J. Arkko, A Taxonomy and Analysis of Enhancements to Mobile IPv6 Route Optimization, IETF RFC 4651, 2007.

[18] C. Perkins, Securing Mobile IPv6 Route Optimization using a Static Shared Key, IETF RFC 4449, 2006.

[19] M. Roe, T. Aura, G. O'Shea, J. Arkko, Authentication of Mobile IPv6 Binding Updates and Acknowledgments, Internet-Draft: draft-roe-mobileip-updateauth-02.txt, 2002.

[20] W. Haddad, Applying Cryptographically Generated Addresses to Optimize MIPv6 (CGA-OMIPv6), Expired IETF Internet-Draft: draft-haddad-mip6-cga-omipv6-04, 2005.

[21] A. Arbaugh, B. Aboba, Handoff Extension to RADIUS, Internet-Draft: draft-irtf-aaaarch-handoff-04, 2003.

[22] R. Koodli, IP Address Location Privacy and Mobile IPv6: Problem Statement, IETF RFC 4882, 2007.

[23] Y. Qiu, F. Zhao, R. Koodli, Mobile IPv6 Location Privacy Solutions, IETF RFC 5726, 2010.

[24] W. Haddad, F. Dupont, L. Madour, S. Krishnan, S. Park, Optimizing Mobile IPv6, (OMIPv6), Expired IETF Internet-Draft: draft-haddad-mipv6-omipv6-01, 2004.

[25] J. Arkko, C. Vogt, W. Haddad, Enhanced Route Optimization for Mobile IPv6, IETF RFC 4866, 2007.

[26] C. Vogt, R. Bless, M. Doll, T. Kfner, Early Binding Updates for Mobile IPv6, Expired IETF Internet-Draft: draft-vogt-mip6-early-binding-updates-00, 2004.

[27] F. Zhao et al., Extensions to Return Routability Test in MIP6, Internet-Draft: draft-zhao-mip6-rr-ext-01, 2005.

[28] Y.W. Lin, H.J. Chang, T.H. Huang, Performance evaluation of threshold scheme for mobility management in IP based networks, Lect. Notes Comput. Sci. 3398 (2005) 429–438.

[29] C. Perkins, IP Encapsulation within IP, IETF RFC 2003, 1996.

[30] D. Farinacci et al., Generic Routing Encapsulation (GRE), IETF RFC 2784, 2000.

[31] S. Jeong et al., Problem Statement and Requirements for Route Optimization in PMIPv6, Expired IETF Internet-Draft: draft-jeong-netlmm-pmipv6-roreq-01, 2007.

[32] B. Sarikaya, A. Qin, A. Huang, W. Wu, PMIPv6 Route Optimization Protocol, Internet-Draft: draft-qin-netlmm-pmipro-00, 2008.

[33] S. Jeong, R. Wakikawa, Route Optimization Support for Proxy Mobile IPv6 (PMIPv6), Internet-Draft: draft-jeong-netlmm-ro-support-for-pmip6-00, 2007.

[34] M. Liebsch, L. Le, J. Abeille, Route Optimization Support for Proxy Mobile IPv6 (PMIPv6), Internet-Draft: draft-abeille-netlmm-proxymip6ro-01, 2008.

[35] S. Jeon, Y. Kim, Fast Route Optimization for PMIPv6 Handover, Internet-Draft: draft-sijeon-netlmm-fastro-pmip6-00, 2008.

[36] A. Dutta et al., Proxy MIP Extension for Inter-MAG Route Optimization, Internet-Draft: draft-dutta-netlmm-pmipro-01, 2008.

[37] S. Krishnan et al., Localized Routing for Proxy Mobile IPv6, IETF RFC 6705, 2012.

[38] P. Jonathan, SCADA Security Strategy, Plant Data Technologies, 2002.

[39] Pwn2Own 2010, 2010 <http://dvlabs.tippingpoint.com/blog/2010/02/15/pwn2own-2010> (accessed 25.06.11).

[40] Black Hat USA 2010, 2010 <http://www.blackhat.com> (accessed 25.06.11).

[41] S. Deering, R. Hinden, The Internet Protocol version 6 (IPv6) Specification, IETF RFC 2460, 1998.

[42] A. Conta, S. Deering, M. Gupta, Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification, IETF RFC 4443, 2006.

[43] R. Koodli, Mobile IPv6 Fast Handovers, IETF RFC 5268, 2008.

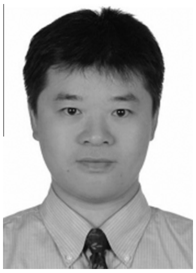
[44] G. Tsirtsis, P. Srisuresh, Network Address Translation – Protocol Translation (NAT-PT), IETF RFC 2766, 2000.

[45] L.S. Brakmo, L.L. Peterson, TCP vegas: end to end congestion avoidance on a global Internet, IEEE J. Sel. Areas Commun. 13 (8) (1995) 1465–1480.

[46] W. Stevens, TCP Slow Start, Congestion Avoidance, Fast Retransmit, and Fast Recovery Algorithms, IETF RFC 2001, 1997.

[47] V. Erceg et al., Channel models for fixed wireless applications, IEEE 802.16 Broadband Wireless Access Working Group, 2003.

[48] C. Perkins, Mobile IP: Design Principles and Practices, Addison-Wesley, MA, USA, 1998.



Wen-Kang Jia received his Ph.D. degree from the Department of Computer Science, National Chiao Tung University, Hsinchu, Taiwan. Before returned to school, he had been a senior engineer and manager since 1991 in various networking areas including ICT Manufacturer, Network Integrator, and Telecomm Service Provider. His research interests include TCP/IP protocol design, IP mobility, IP convergence, error resilience coding, multimedia communications, NAT traversal, routing and switching, multicasting and broadcasting, teletraffic engineering, P2P Networks, and wireless networks. He is a member of IEEE.