行政院國家科學委員會補助專題研究計畫 ■ 成 果 報 告
□ 期中進度報告

全光都會環狀骨幹及其光纖/無線擷取網路整合技術─ 子計畫二：異質無線網路中跨層以網路為基礎快速行動技術與品質服務之研究發展

Study and Development of Cross-Layering Network-Based Fast Mobility Techniques and QoS Provisioning in Heterogeneous Wireless Networks

計畫類別：□ 個別型計畫 ■ 整合型計畫
計畫編號：
執行期間： 100 年 8 月 1 日至 101 年 7 月 31 日

計畫主持人：陳耀宗
共同主持人：
計畫參與人員：施振華、郭俊利、賈文康、黃譽維、李書賢

成果報告類型(依經費核定清單規定繳交)：□精簡報告 ■完整報告

本成果報告包括以下應繳交之附件：
□赴國外出差或研習心得報告一份
□赴大陸地區出差或研習心得報告一份
■出席國際學術會議心得報告及發表之論文各一份
□國際合作研究計畫國外研究報告書一份

處理方式：除產學合作研究計畫、提升產業技術及人才培育研究計畫、列管計畫及下列情形者外，得立即公開查詢
□涉及專利或其他智慧財產權，□一年□二年後可公開查詢

執行單位：國立交通大學資訊工程學系

中 華 民 國 一百零一 年 七 月 三十一日

異質無線網路中跨層以網路為基礎快速行動技術與品質服務之研究發展
Study and Development of Cross-Layering Network-Based Fast Mobility Techniques and QoS Provisioning in Heterogeneous Wireless Networks

計畫編號：NSC 98-2221-E-009-066-MY3
執行期限：98年 8月 1日至 101年 7月 31日
主持人：陳耀宗教授 (國立交通大學資訊工程學系)
計畫參與人員：施振華、郭俊利、賈文康、黃譽維、李書賢

I. 中文摘要

本子計畫在研究發展一個可在異質無線網路下，利用網路導向(Network-based)並運用跨層(Cross-layering)方式以減少換手(Handover)過程延遲與確保服務品質(Quality of Service, QoS)的行動技術，更進一步達到無接縫(Seamless)的換手。在本年度的研究中，我們著重於路由最佳化(route optimization)的問題。目前客戶導向(Client-based)的行動IP(Mobile IPv6, MIPv6)與網路導向(Network-based)的代理行動IP(Proxy MIPv6)各有其不同的路由最佳化的機制。然而這些機制仍然有其缺陷，造成高換手延遲時間(Handover delay)與點對點延遲時間(end-to-end delay)，進而使得無接縫換手無法達成。尤其在行動IP與代理行動IP共存的網路之下，這種無效率的路由最佳化機制更是造成無接縫換手無法達成的主要問題。因此我們針對兩者共存之網路中，路由最佳化的問題提出一有效的解法，此機制能(1)改善行動管理機制的整體效能；(2)減少訊息成本(Signal overhead)及佈建成本；(3)縮短換手與點對點延遲時間；(4)簡化網路元件的軟體複雜度。

關鍵詞：路由最佳化，行動IP，代理行動IP。

II. 英文摘要

Nowadays more and more wireless users are on moving while accessing the Internet, hence provisioning of efficient mobility management in the current Internet becomes increasingly important. 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 mobile environment. In this paper, we proposed a novel unified route optimization scheme based on a simplified MIPv6, 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, achieve lower end-to-end latency, minimize signaling overhead, reduce deployment cost, and lessen software complexity of both network entities and clients, regardless the coexisting MIPv6/PMIPv6 environment in which the MNs reside. The performance of our proposed scheme is evaluated through simulations.

Keywords: Route Optimization, Mobile IPv6 (MIPv6), Proxy Mobile IPv6 (PMIPv6).

III. 計畫緣由與目的

With quick advance in wireless technologies, more and more IP-based wireless user terminals are becoming mobile, and providing mobility support in the IP networks has been a long-standing challenge. Mobility on Internet is an important functionality for future Internet services, hence the most widely known protocol, Mobile IP (MIP), enables a *Mobile Node (MN)* to arbitrarily change its point of attachment to the Internet. Since MIP must be implemented in MNs to serve mobility management by themselves, it is also called Client based MIP (CMIP) [1, 5]. On the other hand, the fast emerging Proxy based Mobile IP (PMIP) [2-4] protocol provides an alternative for mobility management based on the assistance of local 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 multimedia applications [14]; moreover, the most common problem is the *Route Optimization (RO)* [33] 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 [34]. Thus, the 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 [5-6].

CMIP and PMIP will very likely coexist in the future Internet. 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 mobile environment 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 $\rho\omega$ 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 Internet is quite different from today's mobile environment 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.

Previous 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.

From client mode mobile IP towards proxy mode 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 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) [3, 4] working group has initiated tasks in defining a series of Proxy-based MIP (PMIP) 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 to change its original IP address acquired from its home network; Further, the PMIP provides mobility support to MNs located in a restricted and topologically localized portion of the network, 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 etc. [3]. Such concept brings up *Proxy Mobile IPv4 (PMIPv4)* [7] and *Proxy Mobile IPv6 (PMIPv6)* [2] in addition to the legacy client (host) mode *Mobile IPv4 (MIPv4)* and MIPv6 [5], and the MIP is generally called CMIP in PMIP's perspective.

Route optimization between MN and MCN

In addition to bi-directional tunneling operation [5], 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 don't 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, 5-6].

When the MN and CN belong to different mobility management domains (e.g. MIPv6 and PMIPv6) and both moved beyond their home networks, it will result in the most complicated scenario as depicted in Fig. 1. Assume there are four alternative data paths: **Path1**: $MN_{HoA} \leftrightarrow CN_{HoA}$ is a non-optimized route path under double bidirectional tunneling; **Path2**: $MN_{CoA} \leftrightarrow CN_{HoA}$ and **Path3**: $MN_{HoA} \leftrightarrow CN_{CoA}$ are partial route optimization paths with a bidirectional tunneling; **Path4**: $MN_{CoA} \leftrightarrow CN_{CoA}$ 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.

Route optimization operations for MIPv6

When a MN changed its point of attachment 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 end point switched from MN's HoA to CoA as noted previously, *Return Routability (RR)* [6] 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 [8].

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.

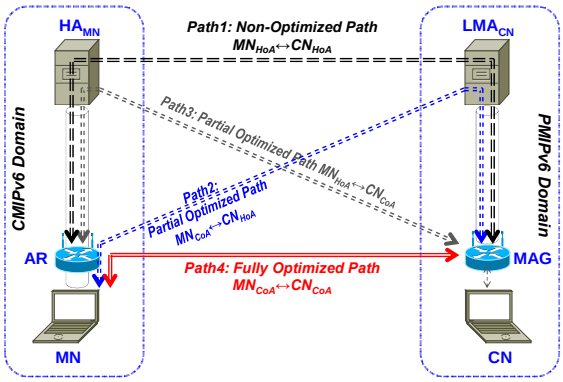

Fig. 1 Hexagonal network reference model in which MN and CN are both mobile and coexist on MIPv6/PMIPv6 mobility management domain.

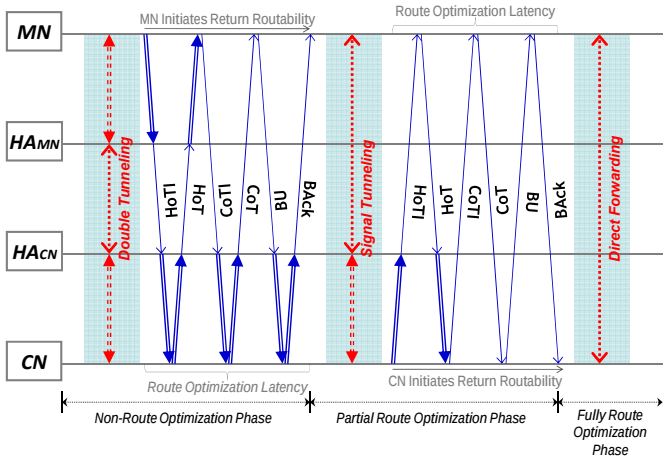

Fig. 2. Return routability operations performed with both MN and (M)CN being mobile.

With the above concerns, a low-latency security mechanism for protecting binding management messages (e.g., signaling related to route optimization) in Mobile IPv6 has been proposed [9], 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.

In Optimizing Mobile IPv6 (OMIPv6) [10] and Optimizing Mobile IPv6+ (OMIPv6+) [11], 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 Cryptographically Generated Addresses (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 all signaling while not moving, and 33% of the per-movement signaling.

Enhanced Route Optimization for Mobile IPv6 [12] 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 [13] 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.

Since the maximum lifetime of the binding cache entry is very short in the specification, MNs must frequently perform binding update. To reduce the number of binding update messages, Lin et al. [32] 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.

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.

Route optimization operations for PMIPv6

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 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 or GRE tunnel [15, 16] 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. S. Jeong et al. [17] pro-

vided the problem statement for route optimization in PMIPv6. 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 [18], 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 [5] return routability test 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}.

The interactions scenarios between PMIPv6 and MIPv6 protocols are first addressed in [19, 20], 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 PMIPv6.

Since the RO path is established and updated through exchanging extra messages between the LMA and the MAG, several researches [21-23] 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) [22] 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 [24], 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 summary, the development of RO in PMIPv6 still lacks the performance concern because new messages are always introduced in all proposed schemes, and the complexity of interoperation between coexisting mobility management domains will increase. It is similar to MIPv6 that many RO setup messages experience same amount of RO latency.

IV. 研究方法

The 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.

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. With this scheme, less network entities of MNs with MIPv6 are supported, and MAGs on PMIPv6 domain are provided with TDPBU function. 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 both binding update and the security procedures, thus the handoff latency can be reduced. Once system is compromised, the average time to implement OPA is estimated from several minutes to hours [29]. The enhanced technique and increased bandwidth will reduce the spent

time. An experienced hacker today can intrude into an unsecure system within minutes in hacking contests [30-31]. 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 CNs.

Network Attachment

Fig. 3 shows a general TDPBU MIPv6 architecture 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.

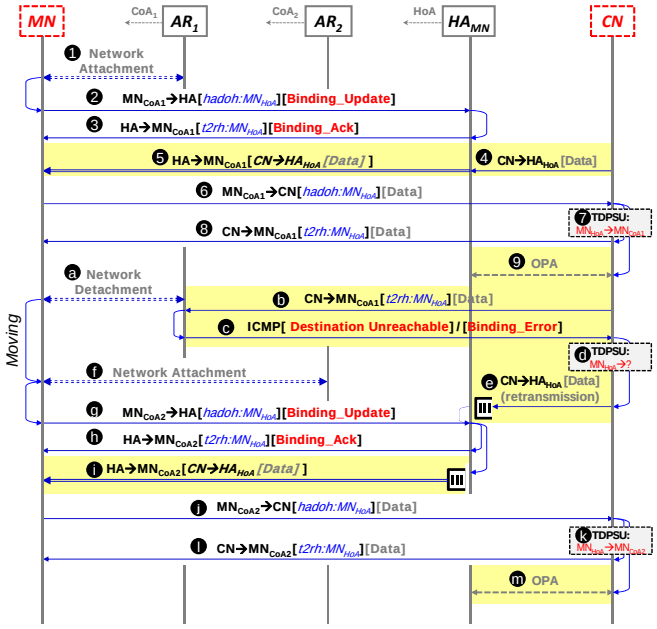

Fig. 3. The basic route optimization operations performed when MN and stationary CN are in TDPBU enabled MIPv6 network. (The marked sections are optional)

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

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 **(6)**.

The datagram packet MN_{CoA}↔CN is piggybacked with the Home Address Destination Options Header 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 procedure immediately **(7)**. If returned packets from CN directly reach the MN_{CoA} **(8)**, and CN does not trust this binding update, the OPA procedure **(9)** will be performed against HA_{MN}. 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_{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 [28], and T2RH has been defined for route optimization of MIPv6 [5]. 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 IPv6 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}.

OPA Procedure

For more strict reason such as 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 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.

MN Handoff

If the MN is moving, it may lead to binding update cached in CN being stale **(8)**, and the datagram will be sent to previous location at the moment **(9)**. The previous AR will detect this phenomenon and respond with an ICMP destination unreachable [25] or binding error message [5] to the CN **(a)**, which then is informed to clear the MN_{CoA} from binding cache entry **(b)**, and originates a retransmission task toward the MN_{CoA} (HA_{MN}) **(c)**. After MN finishes the network attachment procedure in the new point of attachment **(d)~(f)**, those retransmitted packets will be delivered to MN_{HoA} **(g)**, and RO procedure will be restarted by datagram forwarding **(h)~(j)**. Note that the backward packet **(g)** won't trigger the forward packet **(h)** 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) [26] can be applied.

With specific condition, the retransmission procedures **(9)~(c)** and **(g)** may not occur, note that TDPBU relies on normal traffic. Prior to the retransmission procedure triggered by the first downstream datagram packet $CN \rightarrow old\_MN_{CoA}$, the MN may originate an upstream datagram packet $new\_MN_{CoA} \rightarrow CN$ before the downstream packet arrives. Thus, a TDPBU will be triggered by the first upstream datagram packet **(h)~(j)** received by CN.

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.

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 "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 from the remote node will renew the lifetime counter of BCE. After the OPA process is succeeded, the binding state transits to "Secure Binding", the only difference with Early Binding is that the lifetime of BCE can be extended. The only reason for the state transition from "Secure Binding" to "Secure Binding" is that the host receives a packet in HADOH with the same home address coming from a different source address. That means the remote host might have moved. Four reasons for the state transition from "Early Binding" and "Secure Binding" back to "No Binding" are: 1) the 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; 2) 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; 3) host receives a conflict packet such as multiple-source packets carrying the same home address in HADOH; 4) 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; 5) host has not received a packet from the BCE for a long time.

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)* for translating the HoA to CoA and vice versa.

Application Scenarios for Proposed Scheme

The most complicated case occurs when a MN and CN are 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 *InterMIP*, *MIP→PMIP*, *InterPMIP*, and *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 CN are mobile, and the MN has moved away from its home network while the CN has also moved into a foreign network, as shown in Fig. 5, both of these moving nodes need to register their CoAs with their associated HAs.

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// dst is mobile
3:        BindingCache[key].lifetime++
4:        pkt.t2rh←BindingCache[key].HoA
5:        pkt.dst.addr←BindingCache[key].CoA
6:  else                //dst 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:       pkt.hadoh←myHoA
13: endif
```

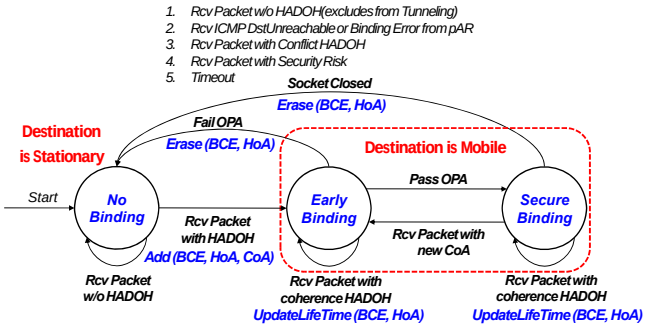

Fig. 4. The FSM for Binding State maintenance in TDPBU enabled MIPv6 Nodes.

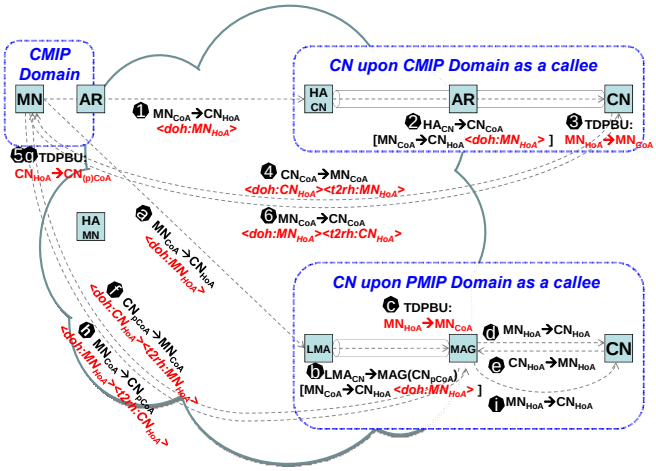

Fig. 5. Proposed scheme operations in the *InterMIP* domain and cross *MIP→PMIP* domain.

The top half of Fig. 5 (step **(1)~(6)**) shows a RO connection established between two generic MIPv6 domains with all the MIPv6 components. Unless the first packet from MN traverses CN's tunnel path via HA_{CN}, the return packets from CN are already on RO path. Route optimization technique offers the biggest advantage when the HA_{MN} and HA_{CN} are far away from the MN and CN respectively, and both of them are based on MIPv6. The bottom half of Fig. 5 (step **(a)~(i)**) shows a RO connection established between MIPv6 and PMIPv6 domains, which contain MIPv6 components and PMIPv6 components, respectively. In this case the MAG assists the MCN 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 CN, respectively.

A CN on PMIPv6 domain may not have mobility support, it means both the HADOH and T2RH cannot be recognized by the CN. Thus MAG should perform TDPBU $MN_{HoA} \rightarrow MN_{CoA}$ address mapping for CN in step **(c)** 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)**, also re-translate the source address from CN_{HoA} to CN_{pCoA}, and the destination address from MN_{HoA} to MN_{CoA} 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 in 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.

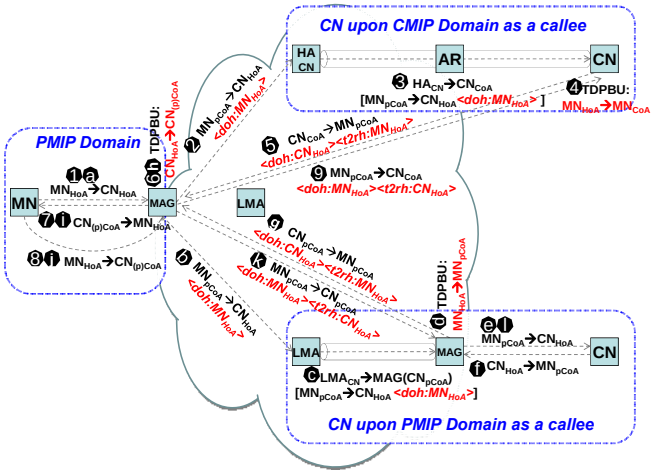

Fig. 6. Proposed scheme operation in *InterPMIP* domain and cross *PMIP→MIP* domains.

The bottom half of Fig. 6 (step **(a)~(l)**) shows a scenario in which the MN and CN are in different PMIPv6 domains. MAG1 and MAG2 are under LMA1 and LMA2 respectively. In this case, route optimization takes place between two MAGs. Since with TDPBU, basically no explicit messages are exchanged among mobile network entities, this fulfills the requirement of unified route optimization solution for coexisting mobility management domains.

V. 研究成果

Performance Evaluation

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. 7 presents the block diagram of the simulation experiment, 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 64ms, 34ms, 34ms and 24ms, respectively. The network topology under consideration is depicted in Fig. 7, 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 128kbps.
- The L2 handoff latency is 500ms.
- The signaling process time is omitted.

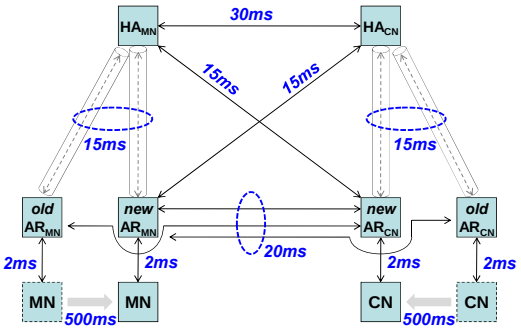

Fig. 7. Network topology for simulation.

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 optimization procedure will be initiated immediately after the handoff procedure (at 110th ms), the result is shown in Fig. 8, the non-optimized route stage (through Path1) continued for about 400ms (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 190ms (from 700th to 1350th 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 500ms (from 1350th to 1850th ms), the communication was disrupted during this period.

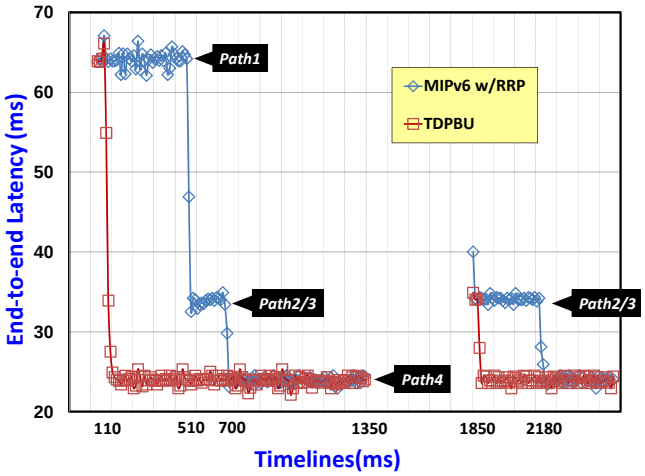

Fig. 8. Comparison of end-to-end latencies for MIPv6/RRP and TDPBU during handoff and route optimization.

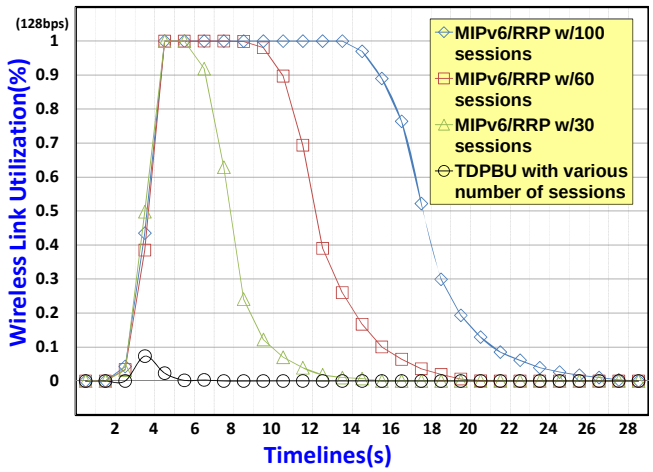

Fig. 9. Comparison of route optimization signaling costs between MIPv6/RRP and TDPBU.

Then MN communicated with mobile CN via the shortest path (through Path4). When the MN moved again while the handoff latency was 500ms (from 1350th to 1850th 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 330ms (from 1850th to 2180th ms).

Signaling Costs during Route Optimization Procedures

We also concerned the number of signaling messages to be reduced during route optimization procedure with TDPBU, and performed a simulation experiment to evaluate the signaling traffic. A MN had established several sessions toward different CNs, and it leaved 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. 9 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.

Network Throughput during Continuous Movement

We also investigated the impact of the end-to-end 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. 10 shows that TDPBU can increase the 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 throughput of TCP would be lower due to the flow control mechanism.

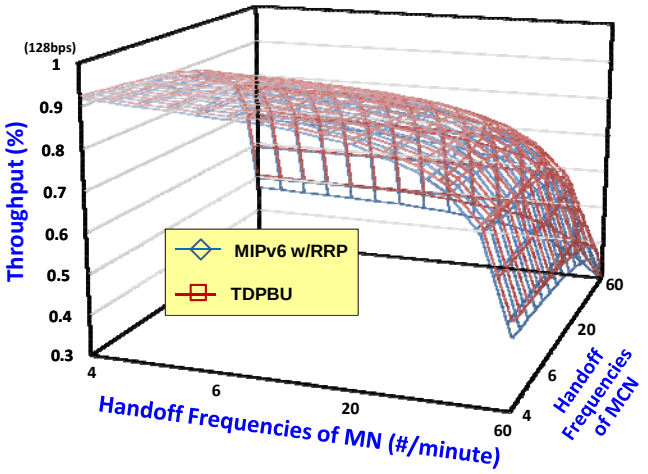

Fig. 10. Comparison of throughput vs. handoff frequencies between MIPv6/RRP and TDPBU.

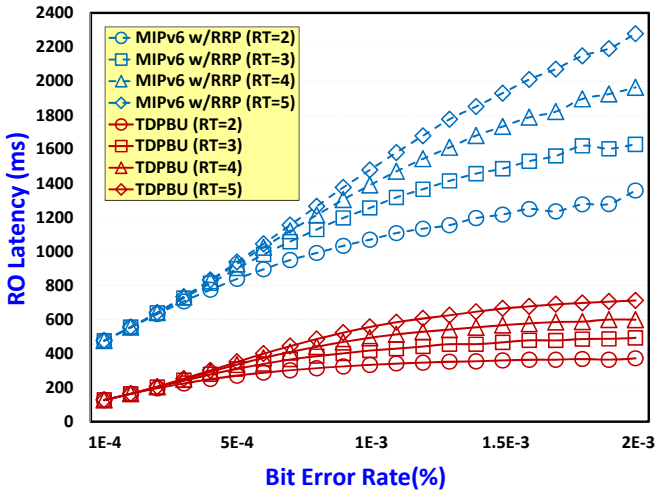

Fig. 11. Comparison of route optimization latency vs. BER between MIPv6/RRP and TDPBU.

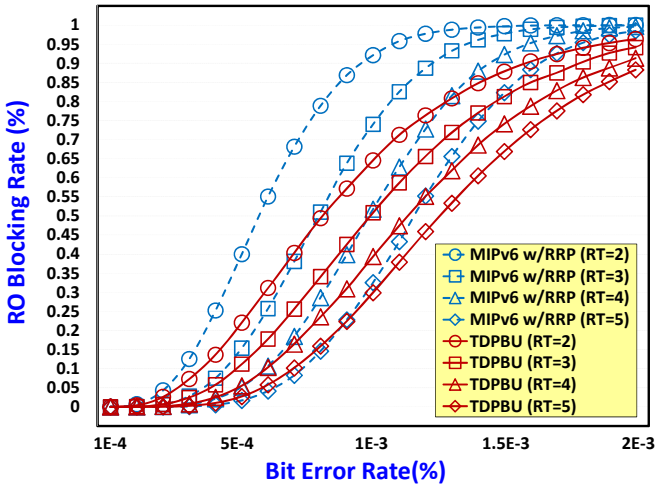

Fig. 12. Comparison of route optimization blocking rate vs. BER between MIPv6/RRP and TDPBU.

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. 11 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. 12 shows the relationship between RO blocking rate and BER in different RO schemes and retransmission 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.

VI. 結論與討論

The next generation IP network has already integrated route optimization as a fundamental part of the mobility support [27]. 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. Further, 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 is unable to send explicit binding update messages to its HA. Our TDPBU scheme will function immediately under such environment.

VII. 參考文獻

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

[2] Gundavelli, S., Leung, K., Devarapalli, V., Chowdhury, K. & Patil, B. (2008). *Proxy Mobile IPv6*. IETF RFC 5213.

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

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

[5] Johnson, D., Perkins, C., & Arkko, J. (2004). *Mobility Support in IPv6*. IETF RFC 3775.

[6] Saxena, P. C. & Jasola, S. (2006). *Performance of intelligent Mobile IPv6," Computer Standards & Interfaces*. 28(6). 737-751.

[7] Leung, K., Dommety, G., Yegani, P., & Chowdhury, K. (2010). *WiMAX Forum / 3GPP2 Proxy Mobile IPv4*. IETF RFC 5563.

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

[9] Perkins, C. (2006). *Securing Mobile IPv6 route optimization using a static shared key*. IETF RFC 4449.

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

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

[12] Arkko, J., Vogt, C. & Haddad, W. (2007). *Enhanced Route Optimization for Mobile IPv6*. IETF RFC 4866.

[13] Vogt, C., Bless, R., Doll, M. & Kfner, T. (2004). *Early Binding Updates for Mobile IPv6*. Expired IETF Internet-Draft: draft-vogtmip6-early-binging-updates-01.

[14] Chen, W. M., Chen, W. & Chao, H. C. (2009). *An efficient mobile IPv6 handover scheme*. Telecommunication Systems. 42(3-4). 293-304.

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

[16] Perkins, C. (1996). *IP Encapsulation within IP*. IETF RFC 2003.

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

[18] Sarikaya, B., Qin, A., Huang, A. & Wu, W. (2008). PMIPv6 route optimization protocol. Internet-Draft: draft-qin-netlmm-pmipro-00.txt (work in progress).

[19] Giaretta, G. Ed. (2007). *Interactions between PMIPv6 and MIPv6: scenarios and related issues*. Internet-Draft: draft-giaretta-netlmm-mip-interactions-02(work in progress).

[20] Velev, G. (2008). *Interactions between PMIPv6 and MIPv6: Route. Optimization Issues*. Internet-Draft: draft-velev-netlmm-mip-pmip-ro-01.

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

[22] Liebsch, M. & Abeille, A. (2007). *Route Optimization for Proxy Mobile IPv6*. Internet-Draft: draft-abeille-netlmm-proxymip6ro-01.

[23] Jeon S. & Kim, Y. (2008). *Fast Route Optimization for PMIPv6 handover*. Internet-Draft: draft-sijeon-netlmm-fastro-pmip6-00.

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

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

[26] Koodli, R. (2008). *Mobile IPv6 Fast Handovers*. IETF RFC 5268.

[27] Perkins, C. (1998). *Mobile IP: Design Principles and Practices*. MA: Addison-Wesley. USA.

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

[29] Jonathan, P. (2002), *SCADA Security Strategy*. Plant Data Technologies. Accessed 25 June 2011.

[30] *Pwn2Own 2010* (2010). http://dvlabs.tippingpoint.com/blog/2010/02/15/pwn2own-2010. Accessed 25 June 2011.

[31] *Black Hat USA 2010* (2010). http://www.blackhat.com. Accessed 25 June 2011.

[32] Lin, Y. W., Chang, H. J., Huang, T. H. (2005). *Performance Evaluation of Threshold Scheme for Mobility Management in IP Based Networks*. Lecture notes in computer science. 3398. 429-438.

[33] Li, C. S., Lin, F. & Chao, H. C. (2009). *Routing optimization over network mobility with distributed home agents as the cross layer consideration*. Telecommunication Systems. 42(1-2). 63-76.

[34] Lee, J. H., Han, Y. H., Gundavelli, S. & Chung, T. M. (2009). *A comparative performance analysis on Hierarchical Mobile IPv6 and Proxy Mobile IPv6*. Telecommunication Systems. 41(4). 279-292.

國科會補助專題研究計畫成果報告自評表

請就研究內容與原計畫相符程度、達成預期目標情況、研究成果之學術或應用價值（簡要敘述成果所代表之意義、價值、影響或進一步發展之可能性）、是否適合在學術期刊發表或申請專利、主要發現或其他有關價值等，作一綜合評估。

1. 請就研究內容與原計畫相符程度、達成預期目標情況作一綜合評估

■ 達成目標

□ 未達成目標（請說明，以 100 字為限）

□ 實驗失敗

□ 因故實驗中斷

□ 其他原因

說明：

本子計畫在研究發展一個可在異質無線網路下，利用網路導向(Network-based)並運用跨層(Cross-layering)方式以減少換手(Handover)過程延遲與確保服務品質(Quality of Service, QoS)的行動技術，更進一步達到無接縫(Seamless)的換手。

在本年度的研究中，我們著重於路由最佳化(route optimization)的問題。目前客戶導向(Client-based)的行動 IP(Mobile IPv6, MIPv6)與網路導向(Network-based)的代理行動 IP(Proxy MIPv6)各有其不同的路由最佳化的機制。然而這些機制仍然有其缺陷，造成高換手延遲時間(Handover delay)與點對點延遲時間(end-to-end delay)，進而使得無接縫換手無法達成。尤其在行動 IP 與代理行動 IP 共存的網路之下，這種無效率的路由最佳化機制更是造成無接縫換手無法達成的主要問題。因此我們針對兩者共存之網路中，路由最佳化的問題提出一有效的解法，此機制能(1)改善行動管理機制的整體效能；(2)減少訊息成本(Signal overhead)及佈建成本；(3)縮短換手與點對點延遲時間；(4)簡化網路元件的軟體複雜度。故這套機制顯著地改善換手過程的中斷時間，有效的改善即時應用(Real-time Application)像是 VoIP 的服務品質，並達到無接縫的換手。

2. 研究成果在學術期刊發表或申請專利等情形：

論文：■已發表 □未發表之文稿 ■撰寫中 □無

專利：□已獲得 □申請中 □無

技轉：□已技轉 □洽談中 □無

其他：（以 100 字為限）

在本年度的研究成果中，A Unified Route Optimization Scheme for Coexisting MIPv6 and PMIPv6 in Future Internet 已發表於 Telecommunication Systems。而其他相關論文也在撰寫中。

Wen-Kang Jia and Yaw-Chung Chen, "A Unified Route Optimization Scheme for Coexisting MIPv6 and PMIPv6 in Future Internet," Telecommunication Systems (TS), Special Issue on Mobility Management in Future Internet, Accepted. (SCI-E, EI) [2010_IF=0.67] <Ranking: TELECOMMUNICATIONS (57/76)=75%>

3. 請依學術成就、技術創新、社會影響等方面，評估研究成果之學術或應用價值（簡要敘述成果所代表之意義、價值、影響或進一步發展之可能性）（以 500 字為限）

在本年度的研究中，我們針對客戶導向(Client-based)的行動 IP(Mobile IPv6, MIPv6)與網路導向(Network-based)的代理行動 IP(Proxy MIPv6)兩者共存之網路中，路由最佳化的問題提出一有效的解法，此機制提供兩者整合之方法，對於之後行動 IP 與代理行動 IP 共存之系統，不只提供一個佈建的參考依據，也為其提供了可選擇的有效路由最佳化機制方案。另一方面，A Unified Route Optimization Scheme for Coexisting MIPv6 and PMIPv6 in Future Internet 已發表於 Telecommunication Systems，此研究成果詳細的探討我們提出之路由最佳化機制的程序，其各種分析與模擬同樣提供學術上的價值。