A Routing-Aware Handover Scheme for Mobile IP

Takeshi Takahashi*, Jarmo Harju†, Koichi Asatani‡*, Hideyoshi Tominaga*
* Graduate School of Global Information and Telecommunication Studies, Waseda University, Tokyo, Japan
Email: take@tom.comm.waseda.ac.jp
† Institute of Communications Engineering, Tampere University of Technology, Tampere, Finland
‡ Graduate School of Electrical and Electronic Engineering, Kogakuin University, Tokyo, Japan

***Abstract*— One of the main issues of Mobile IPv6 is handover latency that causes service disruption time. Although plenty of proposals significantly reduce the service disruption time, they suffer from redundant routing that causes packet misordering and bandwidth consumption during the process of inter-domain handover. In this paper, we propose R-MIP, a routing-aware handover scheme for Mobile IP, that minimizes the redundant routing during the process of inter-domain handover by utilizing forwarding routers. R-MIP consists of forwarding router discovery and proactive handover. We evaluate R-MIP in the view of packet misordering and bandwidth consumption, and clarify its efficiency. We also evaluate the impact of the forwarding router's capacity since routers have limited resources. By strategically locating forwarding routers, e.g. next to the router that has peering to another domain, the redundant routing caused by inter-domain handover will be efficiently suppressed.**

I. Introduction

In the forthcoming ubiquitous network era, Mobile IPv6 [1], [2] that provides mobility over IP network is a promising technology, which specifies the operation of the IPv6 [3] Internet with mobile nodes (MNs). Each MN is always identified by its home address regardless of its current point of attachment to the Internet. While situated away from its home, an MN is also associated with a care-of address (CoA), which provides information about the MN's current location. IPv6 packets addressed to an MN's home address are transparently routed to its CoA [4].

However, Mobile IPv6 suffers from serious service disruption problem, which is crucial to streaming services and especially to interactive communications. To cope with this problem, plenty of researches have been proposed [5–15]. Although those proposals significantly reduce the service disruption time, they suffer from redundant routing that causes packet misordering and bandwidth consumption during the process of inter-domain handover.

On the other hand, most of the proposals so far conduct packet forwarding at single router regardless of the number of connections. However, mobile users will have several connections and will consume more network bandwidth than ever in the forthcoming future, e.g. by receiving several audiovisual contents simultaneously from several correspond nodes (CNs). Under these circumstances, we are required to handle handover for each CN respectively so that the handover performance can be optimized.

To cope with these problems, we propose a Routing-aware handover scheme for Mobile IP (R-MIP) to minimize the redundant routing during the process of inter-domain handover so that packet misordering and bandwidth consumption will be minimized. R-MIP consists of forwarding router (FwR) discovery and proactive handover. The former enables MN to utilize FwR located between its current access router (current AR, AR_i) and new AR (AR_{i+1}) regardless of the AR's unawareness of the network topology while the latter enhances the handover performance with packet buffering and packet forwarding on FwR. Here, the FwRs are chosen for each CN respectively so that the handover performance can be optimized in case MN has multiple connections. Moreover, R-MIP is compatible with Fast Handovers for Mobile IPv6 (FMIPv6) [14] with proper enhancement. In evaluation, we evaluate R-MIP in the view of packet misordering and bandwidth consumption, and clarify its efficiency.

II. Related Works

Researches on mobility are categorized into two groups: micro (local) mobility and macro (global) mobility.

Micro mobility is intended to be utilized in a local level movement that is usually mobility inside an domain or an access network. It provides seamless mobility support in limited geographical areas. HAWAII [5] and Cellular IP [6], [7] represent the research on micro mobility. For instance, Cellular IP provides IP forwarding, minimal signaling, and soft-state location management by incorporating a number of important cellular system design principles such as paging in support of passive connectivity [11].

When MN hands over between micro mobility areas, i.e. inter-domain handover, it must configure new CoA (CoA_{i+1}) and update location information with Binding Update (BU) procedure. This type of mobility is called macro mobility. Hence, the handover latency for inter-domain handover consists of CoA establishment delay and BU delay (the time needed to exchange BU messages with Home Agent (HA) and CNs).

To minimize CoA establishment delay, FMIPv6 [14] is proposed. When an MN is belonging to an AR_i, it configures CoA_{i+1} and checks the validity of the address so that it can utilize the CoA_{i+1} upon connecting to the AR_{i+1}. This feature enables MN to send packets immediately upon connecting to the AR_{i+1}. Therefore, this scheme significantly reduces CoA establishment delay. To minimize CoA establishment delay, R-MIP must be compatible with FMIPv6 (See Section III-D).

To alleviate the impact of the BU delay, there are several schemes that performs packet forwarding from AR_i to CoA_{i+1} or to AR_{i+1} in handover as is clearly described in Smooth handover and FMIPv6 [12–14]. We term these forwarding schemes as "conventional schemes" in this paper. Although these conventional schemes significantly reduce the service disruption time caused by BU delay, the packet forwarding from AR_i causes redundant routing that causes packet misordering and bandwidth consumption. In micro mobility, MN does not suffer from these problems since all the routers in the network are under administration and since they can implement protocol specific features. However, macro mobility schemes cannot usually utilize routers between handover networks except AR_i and AR_{i+1} since routers between AR_i and AR_{i+1} are unknown to them and are not under administration. Our research focuses on this issue.

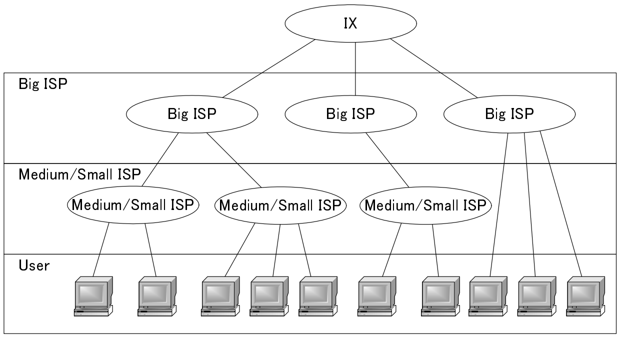


Fig. 1. Network architecture

Figure 1 describes the general network architecture between ISPs [16], [17]. Big ISPs are connected via Internet Exchange (IX) each other while medium/small ISPs are usually connected via big ISPs. Moreover, the networks inside Big ISPs are usually divided into subnetworks according to the geographical area. Most of ISPs' backbone networks have their core networks in metropolitan area and have subnetworks in major large cities. The subnetwork can be divided into another subnetworks even further in some cases. Although private peerings can be established between ISPs, the established peering point is usually between networks in major cities so that ISPs can gain enough benefit from establishing it. Hence, the subdomains elsewhere and middle/small ISPs usually do not have direct private peering one another. Therefore, if an user connected to a network of Medium/Small ISP or subdomains in small cities conducts inter-domain handover, the traffic is required to traverse to the upstream ISP/domain so that it can pass through the private peering link even though the two domains are geographically adjacent. In the worst case, i.e. there is no suitable private peering link, the traffic is required to traverse to the IX to reach the other ISP's domain. In these cases, the redundant routing caused by inter-domain handover is especially problematic.

III. R-MIP : Routing-Aware Handover Scheme

R-MIP consists of FwR discovery and proactive handover. Since Mobile IP is more likely to be utilized in MN-controlled handover circumstances such as Time Division Multiple Access (TDMA) network, we assume handover is controlled by MN. However, R-MIP can be adapted to network-controlled handover cases with proper modification. Here, we describe FwR discovery in Section III-A, proactive handover in Section III-B, state information required for R-MIP in Section III-C and then the compatibility with FMIPv6 in Section III-D.

A. Forwarding Router Discovery

This section introduces the FwR discovery scheme. FwR is a router that buffers packets and redirects them to AR_{i+1}, and FwR candidate is a router that can work as FwR. One of the most efficient places to buffer packets is in the router where the routing path from CN to current CoA (CoA_i) and the one from CN to CoA_{i+1} divert, called Cross over Router (CoR). However, since the location of CoR is always changing depending on the CN's location, it is undesirable to configure all the CoR addresses manually for each CN or to cache all the information for all CNs in large network. Therefore, R-MIP searches FwR for each handover.

In order to obtain the IP address of the ideal FwR, i.e. CoR, it is desirable to search a router that locates en route from CN to AR_i as well as en route from CN to AR_{i+1}. However, since it is infeasible to require CN any of our protocol specific features, and since it is AR_i that we can control the best, in R-MIP, AR_i searches FwR candidates en route from CN to itself as well as the ones en route from itself to AR_{i+1} respectively as described in Fig. 2. Then the AR_i compares the searching results and chooses the common and most upstream FwR candidate between the two searching results just before the MN moves out of the network with handover procedure. For instance, in Fig. 2, assuming that an MN has connection with CN1, and that R2, R3, R5 and R8 are FwR candidates, AR_i finds R2, R3, and R5 as FwR candidates en route from CN1 to AR_i while it also finds R3 and R5 as FwR candidates en route from AR_i to AR_{i+1}. Since the most upstream common router between the two searching results is R3, R3 is chosen as FwR. If AR_i cannot find any common router between the two searching results, then the AR_i itself is chosen as FwR.

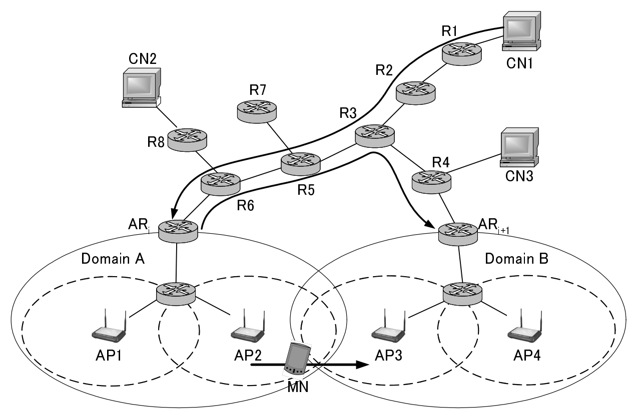


Fig. 2. Forwarding router discovery

In case that the CoR does not work as FwR candidate due to the lack of functionality or due to some failure, FwR candidate that is closest to the CoR will be chosen as FwR. In this example scenario, if R3 is not FwR candidate, R5 is chosen as FwR.

Note that none of AR_i, AR_{i+1}, and MN is required to be aware of the topology of upstream network, and CN is not required any modification. Although this searching scheme contains potential deficiency as is later discussed at the end of Section III-A.2, it still chooses much more efficient router as a buffering and forwarding point than AR_i without requiring CN any specific features. The details of the discovery scheme is described in the following sections.

1) FwR Candidate Discovery en route from AR_i to AR_{i+1}: Figure 3 illustrates the FwR discovery scheme en route from AR_i to AR_{i+1}. AR_i sends FwR discovery message with hop-by-hop option of IPv6 [3] to all the AR_{i+1} candidates (ARs that locate next to AR_i geographically and can be AR_{i+1}

next time). When an FwR candidate receives FwR discovery message, it inserts its IP address inside the message and forwards the packet to the next router. Upon receiving FwR discovery message, the AR_{i+1} replies with FwR advertisement message that contains those FwR candidates' IP addresses.

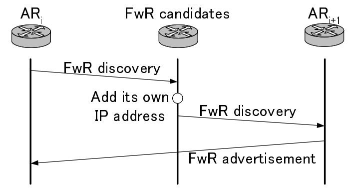


Fig. 3. FwR discovery with FwR discovery message

This discovery scheme should be taken place periodically, and the discovered information should be cached inside AR_i so that the discovery scheme is not required to be taken place so frequently. Since it is very rare that the topology between AR_i and AR_{i+1} candidates changes, and since the number of AR_{i+1} candidates is limited, it is often more beneficial to cache those result than to conduct discovery scheme for each MN.

2) FwR Candidate Discovery en route from CN to AR_i:

The most efficient and easiest way to discover FwR candidates en route from CN to AR_i is the one that CN sends FwR advertisement message to AR_i. However, since we cannot expect CN any of our protocol specific features, we assign more features on AR_i and FwR candidates instead and utilize BU messages and Binding Acknowledgement (BA) messages. FwR candidate discovery en route from CN to AR_i is conducted when an MN hands over from previous AR (AR_{i-1}) to AR_i, and this information is utilized when it hands over to AR_{i+1}, i.e. the next handover.

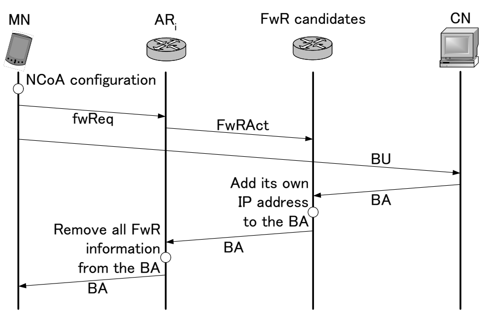


Fig. 4. FwR discovery with activation message

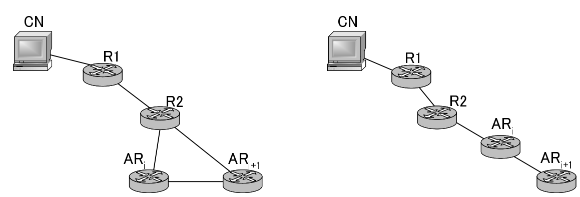
Figure 4 illustrates the FwR discovery scheme en route from CN to AR_i. The discovery starts when the AR_i realizes new MN's connectivity. In R-MIP, AR_i realizes it by receiving fwReq message while FMIPv6 utilizes Fast Neighbor Advertisement (FNA) message for that (See Section III-D). Then, the AR_i sends FwR Activation (FwRAct) message to the FwR candidates en route from the AR_i to all the neighboring ARs that should be know by this time as described in Section III-A.1. The FwRAct message contains the CN's IP address as well as the MN's CoA_i. Upon receiving the FwRAct message, the FwR candidates are activated and start inspecting each arriving packet sent from the CN to the CoA_{i+1} and check whether the packet is BA message or not. When an activated FwR candidate receives BA, it inserts its own IP address inside the packet and forwards the packet to the next router. Here, those activated FwR candidates are deactivated when they once insert its IP address inside BA packet or after proper timeout period. Upon receiving the FwRAct message, the AR_i stores those information concerning FwR candidates and deletes those information from the BA, which is then forwarded to the MN.

Provided the capacity of an FwR is almost full, and the burden to the FwR is significant, the FwR candidate is not required to notify its presence to AR_i. It is also not required to notify its presence if the FwR does not work due to some failure. Therefore, the FwR candidate simply forwards the BA message without any further action. This feature enables us to create some double, or triple FwR structure, which establishes the balanced burden router system.

As can be seen, the FwR candidates en route from CN to AR_i are discovered though the searching range is limited between the AR_i and all the AR_{i+1} candidates. The final selection of FwR will be conducted by comparing the FwR candidates en route from AR_i to AR_{i+1} and the ones en route from CN to AR_i when the MN hands over to AR_{i+1} as described in Section III-B.2. One deficiency of R-MIP is that AR_i cannot choose CoR as FwR if the CoR is not en route from AR_i to AR_{i+1}. In this case, AR_i simply chooses the FwR that is closest to the CoR and that is en route from AR_i to AR_{i+1}. When AR_i needs to seek for more efficient FwR, then the further process described in the next section can be taken place though it is an optional feature.

3) FwR Rediscovery:

Depending on the topology, the FwR discovery mentioned above sometimes cannot find any FwR in case the interface for packets coming from CN and the one for packets going to AR_{i+1} is different as described in Fig. 5(a). It also cannot find the best FwR in case that the topology has several routes as described in Fig. 6. This type of network topology is very reasonable since ISPs are connected via IXs as well as private peerings, which is usually located between the core networks of each ISP. Hence, we provide an optional scheme, named FwR rediscovery, to seek for more efficient FwR. FwR rediscovery is invoked by AR_i, and can be invoked any time during MN's staying at the current network, or can be invoked by some certain signals such as bufReq message introduced in Section III-B.1.



(a) (b)

Fig. 5. Network topologies

FwR rediscovery starts with AR_i's sending FwR rediscovery message that contains the address of single AR_{i+1} candidate. The AR_i sends FwR rediscovery message only to the FwR candidates en route from CN to AR_i that should have been known by this time as described in Section III-A.2. Different from FwR discovery, FwR rediscovery requires AR_i to specify single AR_{i+1} address and to look up the routing table of FwR candidates.

Upon receiving the message, the FwR candidate looks up its routing table and checks the next hop to the AR_{i+1}'s address ($nh(AR_{i+1})$), the one to the AR_i's address ($nh(AR_i)$), and the previous hop from CN to AR_i ($ph(AR_i)$). $ph(AR_i)$ can be obtained by waiting for any incoming traffic sent from CN to AR_i instead of looking up the routing table even though some router does not have the $ph(AR_i)$ information. If the $nh(AR_{i+1})$ is the same as $nh(AR_i)$, the FwR candidate sends FwR readvertisement message to AR_i with "follow" flag. If the $nh(AR_{i+1})$ is the same as $ph(AR_i)$, it sends the message with "reverse" flag. Otherwise, it sends the message with "divert" flag.

Upon receiving the messages from all the FwR candidates en route from CN to AR_i, the AR_i sorts the messages so that the AR_i can check the message that is sent from the nearest FwR candidate first, and so that it can check the message that is sent from the furthest FwR candidate last. When the AR_i finds "follow" flag after "divert" flag or after "reverse" flag, the FwR candidate that sends the message with "follow" flag is FwR. When the AR_i finds "divert" flag or "reverse" flag and cannot find "follow" flag, then the FwR candidate that sends the last message with those flags is FwR. When the AR_i finds neither "divert" flag nor "reverse" flag, then the AR_i is the FwR. In this case, the AR_i can be en route from CN to AR_{i+1} as described in Fig. 5(b) or no FwR candidates are available en route from CN to AR_i.

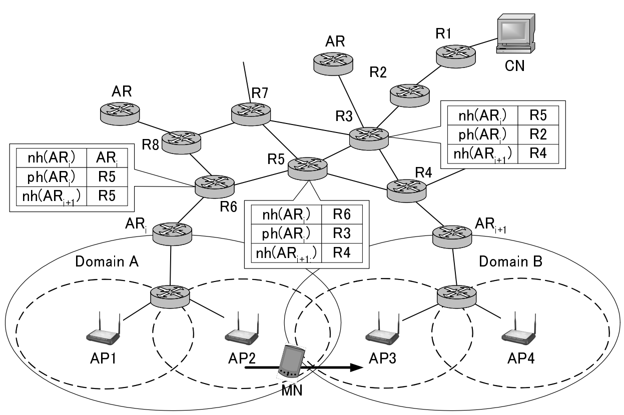


Fig. 6. FwR rediscovery

For instance, assuming all the routers in Fig. 6 are FwR candidates, and assuming all ARs in this figure are AR_{i+1} candidates, the AR_i can know that R3, R5 and R6 are FwR candidates en route from CN to AR_i. FwR rediscovery starts with FwR rediscovery messages sent from AR_i to R3, R5, and R6. Upon receiving the message, R6 sends FwR readvertisement message with "reverse" flag while R5 and R3 sends the message with "divert" flag. Therefore, according to the algorithm mentioned above, R3 is chosen as FwR and is better FwR than R5 that is chosen by FwR discovery.

B. Proactive Handover

When an MN hands over to new network, it initiates proactive handover with the help of FwR. The proactive handover consists of proactive packet buffering and packet forwarding, which are described in the following sections. The message flows utilized in proactive handover are described in Fig. 7, which is also elaborated in the following sections.

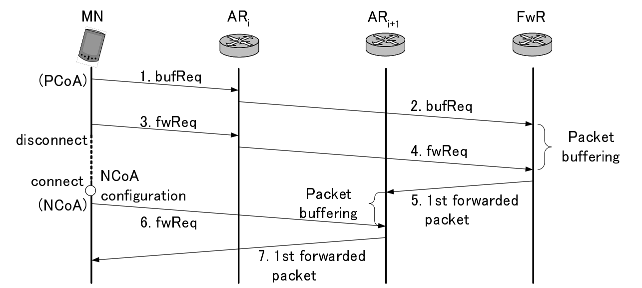


Fig. 7. Proactive handover message flows

1) Proactive Packet Buffering:

By forwarding packets from AR_i to CoA_{i+1}, handover goes very smoothly provided the related two networks are well-overlapped, and provided the MN can receive packets from both CoA_i and CoA_{i+1} simultaneously. However, otherwise, the packets sent to the MN before the establishment of tunnel will be lost. Therefore, R-MIP performs proactive packet buffering that compensates the lost packets before the establishment of tunnel as mentioned in [13]. Different from [13–15], R-MIP performs buffering at FwR, which replicates the packets sent from CN to CoA_i. Then it forwards the original packets to CoA_i while it saves the replicated packets into its buffer. Those saved packets will be forwarded to AR_{i+1} upon receiving Forwarding Request (fwReq) message.

The proactive handover begins with a buffering request (bufReq) message sent by an MN to AR_i when the MN detects a candidate network for next handover point by L2 trigger, which should be defined depending on each network. The bufReq message includes the new AP identifier, with which the AR_i knows the address of AR_{i+1} by looking up its own database. The database should be created by periodic message exchanges with neighboring APs or by manual configuration or by other schemes though the scheme is outside the scope of this paper. Upon receiving the message, the AR_i forwards the message to proper FwR that is decided by looking up the result of FwR discovery/rediscovery scheme with the address of AR_{i+1}. Here, note that MN is not required to know the existence of FwR at all while AR_i knows it.

Upon receiving the bufReq message, the FwR starts buffering and continues buffering until it receives fwReq message introduced in Section III-B.2 or until it gets timeout expired. FwR simply discards buffered packets after timeout expired. The MN may retransmit the bufReq message when necessary. During the handover decision process, the MN may receive another L2 trigger that suggests different network for handover. Then it sends bufReq message to the AR_i, which forwards the message to proper FwR. If the FwR is the same one as before, it simply updates the timeout value. The FwR discovered by a failed L2 trigger will simply discard the buffered packets after timeout expired.

Here, the buffer size of FwR can be configured depending on the policy of administrator. The discussion concerning the buffer size is outside the scope of this paper.

2) Packet Forwarding:

When an MN hands over to new network, it sends fwReq message to AR_i just before switching connection to new network. Upon receiving the fwReq message, the AR_i forwards it to proper FwR, which in return starts forwarding packets sent from CN to CoA_{i+1} to AR_{i+1} preceded by the buffered packets inside the FwR. Upon receiving the packets, the AR_{i+1} starts buffering those forwarded packets until it realizes the MN's existence under its network.

When the MN get connection with the new network, it sends fwReq message to AR_{i+1}. Upon receiving the message, the AR_{i+1} starts forwarding packets sent from FwR preceded by the buffered packets inside the AR_{i+1} itself. If the AR_{i+1} does not receive any valid fwReq message for certain amount of time, it discards those buffered packets.

As described in [14], an MN cannot send any packet to CN with CoA_{i+1} until it finishes BU procedure. When it sends packets to CN before finishing BU procedure, the source field of the IP header should be CoA_i as is described in FMIPv6. Upon receiving the packet, the AR_{i+1} encapsulates the packet and forwards the packet to FwR by tunneling. Then the FwR decapsulates the packet and sends the original packet to CN. In this way, MN can also avoid the redundant routing not only in the packet receiving scenario but also in the packet sending scenario. Therefore, packet misordering, packet loss, and bandwidth consumption are suppressed as well.

C. State Information

R-MIP requires FwR candidates, FwRs, and ARs to maintain protocol specific state information. FwR candidates maintain state entries consisting of $\{$CN's address, CoA_i, timeout$\}$ and inspect each packet sent from CN specified in any of the state entries to its corresponding CoA until it detects BA or until the timeout expires. FwR, to perform packet buffering and forwarding, maintains state entries consisting of $\{$CN's address, CoA_i, AR_{i+1}'s address, flag, timeout$\}$. Flag is either on (forwarding) or off (buffering), and this state is effective until the timeout expires. AR_i maintains state entries consisting of $\{$CN's address, CoA_i, FwR candidates' addresses en route from CN to $\mathrm{AR}_i\}$. To discover the FwR candidates en route from CN to AR_i, the CoA_i and CN's address are referenced, and the discovered FwR candidates en route from CN to AR_i will be stored in the table. Note that we assume ARs have database that has the mapping from AP identifiers to their belonging AR's IP addresses as is also assumed in FMIPv6 [14].

D. Compatibility with FMIPv6

R-MIP displays better performance by cooperating with FMIPv6. The required features for MN in our proposal can be observed as an extension to the one in FMIPv6. In our proposal, MN sends bufReq message while it sends RtSolPr message in FMIPv6. Also, MN sends fwReq message in our proposal before handover while it sends FBU in FMIPv6. Moreover, MN sends fwReq message in our proposal after handover while it sends FNA in FMIPv6.

By substituting bufReq message with RtSolPr message, fwReq message before handover with FBU message, and fwReq message after handover with FNA, R-MIP works with FMIPv6 without MN's noticing our protocol. In this case, R-MIP can gain better performance with the help of FMIPv6 though it requires some enhancements for the behavior of ARs to cooperate with FMIPv6, The detailed feature to cope with FMIPv6 is outside the scope of this paper.

IV. Evaluation

We evaluate R-MIP in the view of packet misordering in Section IV-A and in the view of bandwidth consumption in Section IV-B, and then discuss its deployability in Section IV-C.

A. Packet Misordering

Firstly, we evaluate R-MIP in the view of packet misordering assuming an MN communicates with single CN. Ideally, CoR should work as FwR, which completely avoids packet misordering. However, as described in Section III-A.2, FwR discovery sometimes cannot choose CoR if the CoR is not en route from AR_{i1} to AR_{i+1}, hence some packet misordering will occur. Although this misordering can be re-ordered in the MN provided the MN implements special function for that, otherwise those misordered packets are simply discarded or invoke packet retransmission depending on the higher layer protocols. Therefore, we evaluate R-MIP in the case CoR is not en route from AR_i to AR_{i+1}.

We utilized NS2 simulator [18] for this simulation and established simulation topology as described in Fig. 6. Here, the CN is sending CBR traffic to MN that is connected to AP2. After a while, the MN hands over to domain B. Here, domain A network and domain B network are overlapping though the MN cannot receive packets from both networks simultaneously. Upon receiving BU message, the FwR starts forwarding packets to the AR_{i+1}. Likewise, upon receiving BU message, the CN starts sending packets to CoA_{i+1} directly. By utilizing FwR discovery, R5 is chosen as an FwR while R3 is CoR. Here, we analyzed the packet misordering caused by the difference between the route from CN to CoA_{i+1} and the one from FwR to CoA_{i+1}. In this simulation, the delay for each link was set to 10 msec and the bitrate was set to 128 kbps. We measured the number of misordered packets when we changed the value of packet interval. The packet size was also changed so that the bitrate is always fixed on 128 kbps.

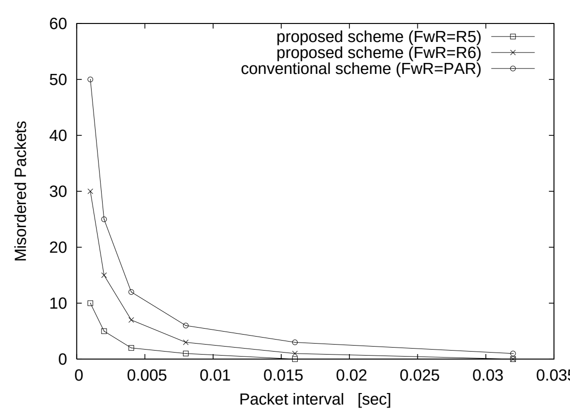


Fig. 8. Packet misordering (single connection scenario)

Figure 8 illustrates the amount of misordered packets in the simulation for both conventional scheme (FwR=AR_i) and R-MIP (FwR=R5). It also shows the case that R6 is working as the FwR instead of R5. The X-axis represents the packet interval in the unit of second while the Y-axis represents the number of misordered packets. As can be seen, when the packet interval is smaller, the misordering happens more. Although R-MIP also suffers from packet misorderings, the amount of misordered packets is significantly reduced compared to the conventional scheme that forwards packets from AR_i.

Now, by utilizing FwR rediscovery scheme, R3 is chosen as FwR, and the packet misordering is suppressed to zero. By utilizing FwR rediscovery, AR_i can discover better FwR than the one discovered by FwR discovery though the use of FwR rediscovery is optional. Provided the CoR resides en route from AR_i to its neighboring ARs, and provided the CoR is FwR candidate, FwR rediscovery enables AR_i to choose CoR as FwR.

In the Internet, we cannot expect all routers to support our protocol. However, by strategically locating forwarding routers, the redundant routing caused by inter-domain handover will be efficiently suppressed. Since the traffic is diverted on the CoR that contains peering to another domain, implementing our protocol over CoR or locating FwR around CoR will efficiently reduce the redundant routing.

Secondly, we evaluate R-MIP in the view of packet misordering assuming an MN has multiple connections during its handover process. In R-MIP, an MN can utilize FwR for each connection so that the redundant routing for each connection will be minimized. Depending on the policy of the network, the multiple FwR support can be enabled or disabled. Provided the multiple FwR support is disabled, the AR_i must choose the common FwR for all connections.

To evaluate the efficiency of R-MIP with multiple FwR support (R-MIP with mFwR), the number of packet misordering is measured by utilizing NS2 simulator with the topology described in Fig. 2 in comparison with the case of conventional scheme and with the case of R-MIP without multiple FwR support (R-MIP without mFwR). In Fig. 2, CN1, CN2, and CN3 are sending 128kbps CBR traffic (packet interval=0.001sec) to MN respectively, all routers are FwR candidates, and is handing over between two networks. When it initiates handover, the conventional scheme chooses AR_i as the FwR for all the connections, and R-MIP without mFwR chooses R6 as the FwR for all the connections while R-MIP with mFwR chooses R3 as the FwR of the connection with CN1, R6 as the FwR for the connection with CN2, and R4 as the FwR for the connection with CN3.

TABLE I

PACKET MISORDERING (MULTIPLE CONNECTION SCENARIO)

	CN1	CN2	CN3	Total
Conventional	60	20	80	160
R-MIP without mFwR	40	-	60	100
R-MIP with mFwR	-	-	-	-

Table I shows the simulation result. In case of conventional scheme, since AR_i is the single packet forwarding point, all of the 3 connections suffer from packet misordering. In case of R-MIP without mFwR, the connection with CN2 is free from packet misordering since R6 is the CoR for the connection However, undesired packet misorderings occur for the connection with CN1 and for the one with CN3 since CN1 and CN3 cannot utilize their CoRs as FwRs. In case of R-MIP with mFwR, no packet misordering occurs for each connection since each connection utilized CoR as FwR. Note, though MN still suffers from packet misordering depending on network topology as mentioned above with Fig. 6, the amount of misordered packet is greatly reduced by R-MIP with mFwR. As can be seen, choosing FwR for each connection significantly reduces the amount of packet misordering.

B. Bandwidth Consumption

We evaluate R-MIP in the view of bandwidth consumption assuming Fig. 6 is our simulation topology. By utilizing FwR discovery and FwR rediscovery, AR_i in domain A knows that R3, R5 and R6 are FwR candidates for the handover from Domain A to Domain B, while the AR in domain B knows that R3 and R4 are FwR candidates for the handover from Domain B to Domain A. All MNs are receiving 2 Mbps traffic from CN all the time, and they are moving between Domain A and Domain B. We assume CoA establishment delay caused by handover procedure is 1 second in this simulation model while we assume the link delay is 10 msec. The number of MNs moving from one network to another is described as uniform pseudorandom number and is calculated by Box-Muller transformation (average=10, standard deviation=2) in this evaluation.

Firstly, we assume all FwRs have unlimited capacity and one best-located FwR assists all the MNs' handover. Figure 9 shows the comparison between conventional scheme and R-MIP in the view of bandwidth consumption of the link between AR_i and R5. The X-axis shows the time after this simulation starts while the Y-axis shows the bandwidth consumption between AR_i and R5 in the unit of bitrate. As can be seen, R-MIP saves bandwidth consumption compared to the conventional scheme all the time. Here, the average bandwidth consumption with R-MIP is 216 Mbps while the one in the conventional scheme is 256 Mbps. Hence, though the bandwidth consumption saving gain varies depends on the topology, R-MIP saves bandwidth consumption by 15.6 % compared to the conventional scheme in this simulation.

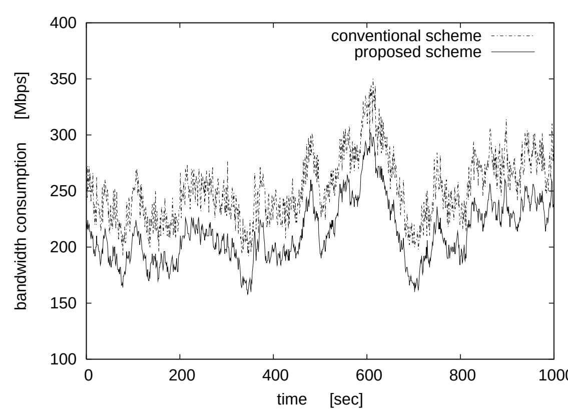


Fig. 9. Bandwidth consumption

Secondly, we assume FwR has limited capacity and each FwR supports up to certain amount of handovers at the same time. Here, we name "capacity" as the number of handover processes that one FwR can handle at the same time. Since forwarding and buffering inside FwR are extra burden for routers, it is natural that each FwR's capacity is limited. Figure 10 shows the relationship between capacity of each FwR and bandwidth consumption for the link between R5 and R6, and for the one between AR_i and R6, in cases of conventional scheme, R-MIP with FwR discovery, and R-MIP with FwR rediscovery respectively. X-axis shows the capacity of each FwR while Y-axis shows the bandwidth consumption in the unit of Mbps. Note that R3 is the FwR that helps handover from Domain A to Domain B as well as the one from Domain B to Domain A. As can be seen, the more capacity each FwR has, the more we can save bandwidth consumption until the bandwidth consumption reaches minimum value, and the more closer to AR_i, the less bandwidth consumption happens. Utilizing FwR rediscovery saves bandwidth better than utilizing only FwR discovery since the number of FwRs that support handover is increased.

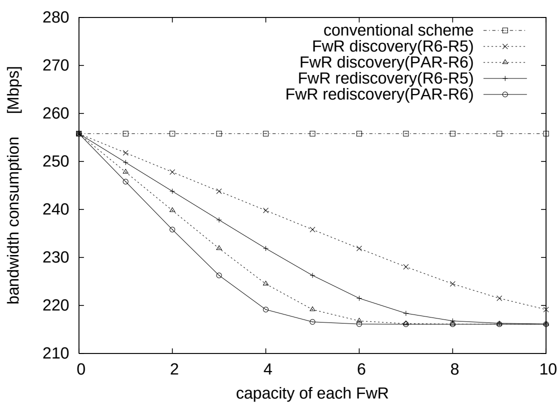


Fig. 10. Impact of FwR's capacity

C. Deployability

From the viewpoint of MN, assuming an MN supports FMIPv6, R-MIP is transparent from the MN. If the AR_i supports R-MIP, it invokes R-MIP. If it does not support R-MIP but supports FMIPv6, it invokes FMIPv6. Otherwise, Mobile IP will be conducted without any help from ARs. Since all the functionality of R-MIP is achieved by network intelligences, the gradual deployment is available.

In the view of FwR deployment, R-MIP provides one-by-one deployment since it enables FwR to coexist with non-FwRs. Although we cannot expect all routers to support R-MIP in the Internet at this moment, by strategically locating a couple of FwR candidates in the network, e.g. around the router that has peering to another domain, plenty of MNs can benefit from R-MIP.

However, the bottleneck of R-MIP deployability is the R-MIP support over ARs. Although the modification over ARs are very minimal over FMIPv6, the current trend of the Internet development tends to avoid any modification over ARs. Current trend of the Internet development asks end nodes to have all necessary functionality while it asks network routers including ARs to simply forward packets to their destinations. Under the circumstances, it will be very hard to widely implement R-MIP as well as FMIPv6 over ARs. Hence, an enhanced R-MIP without AR supports should be considered to be capable of R-MIP's wide deployment.

V. CONCLUSION

To enable smooth inter-domain handover, we proposed R-MIP consisting of forwarding router discovery and proactive handover. The former enables MN to utilize FwR located between AR_i and AR_{i+1} regardless of the AR's unawareness of the network topology while the latter enhances the handover performance with packet buffering and packet forwarding at FwR. In evaluation, we examined R-MIP in the view of packet misordering and bandwidth consumption as well as the impact of each FwR's capacity. Moreover, our evaluation clarified that choosing FwR for each connection is efficient for the MN with several connections during the process of handover. R-MIP alleviated the redundant routing caused by handover process and minimized packet misordering and bandwidth consumption. Although we cannot expect all routers to support our protocol in the Internet, by strategically locating a couple of FwR candidates in the network, e.g. around the router that has peering to another domain, plenty of MNs can benefit from R-MIP. R-MIP is compatible with FMIPv6 with proper enhancement and is expected to reduce handover latency even more by cooperating with the protocol.

As a future work, we will implement R-MIP over Linux environment and evaluate the protocol overhead under real environments.

REFERENCES

[1] D. B. Johnson, C. E. Perkins, and J. Arkko, "Mobility Support in IPv6," *RFC 3775*, June 2004.
[2] J. Arkko, V. Devarapalli, and F. Dupont, "Using IPsec to Protect Mobile IPv6 Signaling Between Mobile Nodes and Home Agents," *RFC 3776*, June 2004.
[3] S. Deering and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification," *RFC 2460*, Dec. 1998.
[4] N. Montavont and T. Noel, "Handover Management for Mobile Nodes in IPv6 Networks," *IEEE Commun. Mag.*, vol. 40, Aug. 2002.
[5] R. Ramjee, K. Varadhan, L. Salgarelli, S. R. Thuel, S.-Y. Wang, and T. L. Porta, "HAWAII : A Domain-Based Approach for Supporting Mobility in Wide-Area Wireless Networks," *IEEE/ACM Trans. Networking*, vol. 10, Oct. 2002.
[6] A. G. Valko, "Cellular IP : A New Approach to Internet Host Mobility," *ACM SIGCOMM Computer Communication Review*, vol. 29, Jan. 1999.
[7] Z. D. Shelby, D. Gatzounas, A. Campbell, and C.-Y. Wan, "Cellular IPv6," *Internet Draft (draft-shelby-seamoby-cellularipv6-00.txt)*, Nov. 2000.
[8] Q. Gao and A. Acampora, "Connection Tree Based Micro-mobility Management for IP-centric Mobile Networks," *IEEE International Conference on Communications*, vol. 5, Apr. 2002.
[9] E. Shim, H. yu Wei, Y. Chang, and R. D. Gitlin, "Low Latency handoff for Wireless IP QoS with NeighborCasting," *IEEE International Conference on Communications*, Apr. 2002.
[10] W. Ma and Y. Fang, "Dynamic Hierarchical Mobility Management Strategy for Mobile IP Networks," *IEEE J. Select. Areas Commun.*, vol. 22, May 2004.
[11] A. T. Campbell, J. Gomez, S. Kim, A. G. Valko, and C. yih Wan, "Design, Implementation, and Evaluation of Cellular IP," *IEEE Personal Communications*, Aug. 2000.
[12] C. Perkins and D. B. Johnson, "Route Optimization in Mobile IP," *Internet Draft (draft-ietf-mobileip-optim-09.txt)*, Feb. 2000.
[13] C. E. Perkins and K.-Y. Wang, "Buffer Management for smooth handoffs in Mobile IPv6," *The Fourth IEEE Symposium on Computers and Communications*, July 1999.
[14] R. Koodli, "Fast Handovers for Mobile IPv6," *Internet Draft (draft-ietf-mipshop-fast-mipv6-02.txt)*, July 2004.
[15] H. Soliman, C. Castelluccia, K. El-Malki, and L. Bellier, "Hierarchical Mobile IPv6 mobility management (HMIPv6)," *Internet Draft (draft-ietf-mipshop-hmipv6-02.txt)*, June 2004.
[16] "WIDE Project." [Online]. Available: http://www.wide.ad.jp
[17] K. L. Calvert, M. B. Doar, and E. W. Zegura, "Modeling Internet Topology," *IEEE Commun. Mag.*, June 1997.
[18] "The Network Simulator - ns-2." [Online]. Available: http://www.isi.edu/nsnam/ns/