PAPER

Proactive Handover Scheme based on Forwarding Router Discovery for Mobile IP Networks

Takeshi TAKAHASHI[†a)], ***Student Member***, **Koichi ASATANI**[††], ***Fellow***, **Jarmo HARJU**[†††], ***Nonmember***, ***and*** **Hideyoshi TOMINAGA**[†], ***Fellow***

SUMMARY 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 a new scheme that minimizes the redundant routing during the process of inter-domain handover by utilizing forwarding routers for each correspondent node. Our proposed scheme consists of forwarding router discovery and proactive handover. We evaluate our proposed scheme in the view of packet misordering and bandwidth consumption, and clarify the efficiency of our proposed scheme. We also evaluate the impact of the forwarding routers' 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.

key words: *Mobile IP, Handover, Mobility, Forwarding Router, Redundant Routing*

1. Introduction

In the forthcoming ubiquitous network era, Mobile IPv6 [1, 2] that provides mobility over IP network has particularly large expectations all over the world and is standardized as the IETF RFC in this June. It 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 still suffers from serious service disruption problem, which is crucial to streaming services and especially to interactive communications such as video conferences with mobile equipments. 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 (handover between domains).

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 correspondent nodes (CNs). For instance, a mobile user watches a TV program while he also records another TV program in background simultaneously. Or, he may have simultaneous communications with several friends. Under these circumstances, we are required to handle handover for each CN individually so that the handover performance can be optimized.

To cope with these problems, we propose a new scheme to minimize the redundant routing during the process of inter-domain handover so that packet misordering and bandwidth consumption will be minimized. Our proposed scheme 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 its new AR (AR_{i+1}) regardless of ARs' unawareness of the network topology while the latter enhances the handover performance with buffering and packet forwarding on FwR. Here, the FwRs are chosen for each CN individually so that the handover performance can be optimized in case MN has multiple connections. Moreover, our proposed scheme is compatible with Fast Handovers for Mobile IPv6 (FMIPv6) [14] with proper enhancement. In evaluation, we evaluate our proposed scheme in the view of packet misordering and bandwidth consumption, and clarify the efficiency of our proposed scheme.

2. Related Works

In this section, several related works are described. Researches on mobility are categorized into two groups: micro (local) mobility and macro (global) mobility.

Manuscript received September 22, 2004.
Manuscript revised December 13, 2004.
Final manuscript received February 13, 2005.

[†]The authors are with the Graduate School of Global Information and Telecommunication Studies, Waseda University, Tokyo Japan.
[††]The author is with the Graduate School of Electrical and Electronic Engineering, Kogakuin University, Tokyo Japan.
[†††]The author is with the Institute of Communications Engineering, Tampere University of Technology, Tampere Finland.
a) E-mail: take@tom.comm.waseda.ac.jp

Micro mobility is intended to be utilized in a local level movement that is usually mobility inside a domain or an access network. Micro mobility provides seamless mobility support in limited geographical areas. HAWAII [5] and Cellular IP [6, 7] represent the researches 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 an MN performs handover between micro mobility areas, i.e. inter-domain handover, MN is required to configure new CoA (NCoA) and to 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 NCoA establishment delay and BU delay (the time needed to exchange BU messages with Home Agent (HA) and CNs).

To minimize the NCoA establishment delay, FMIPv6 [14] is proposed. While an MN is belonging to AR_i, it configures NCoA and checks the validity of the address so that it can utilize the NCoA upon connecting to AR_{i+1}. This feature enables MN to send packets immediately upon connecting to the AR_{i+1}. Therefore, this scheme significantly reduces the NCoA establishment delay. To minimize NCoA establishment delay, our proposed scheme must be compatible with FMIPv6 (See section 3.3).

To alleviate the impact of the BU delay, there are several schemes that performs packet forwarding from AR_i to NCoA or to AR_{i+1} in handover as is clearly described in Smooth handover and FMIPv6 [12–14]. We term this forwarding scheme as "conventional scheme" 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 usually 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. This paper focuses on this issue.

Figure 1 describes the general network architecture among 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 their geographical areas. Most of ISPs' backbone networks have their core domains in metropolitan area and have subdomains in major large cities. The subdomains can be divided into another subdomains 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 a 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. in the case there are no suitable private peering link, the traffic is required to traverse to the most upstream IX to reach the another ISP's domain. In these cases, the redundant routing caused by inter-domain handover is especially problematic.

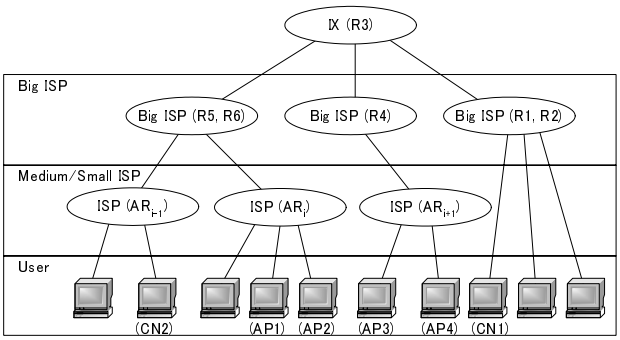


Fig. 1 Network Architecture

3. Proposed Scheme

Our proposed scheme 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, our proposed scheme can be adapted to the network-controlled handover case with proper modification. Here, we describe the FwR discovery scheme in section 3.1, the proactive handover in section 3.2, and then the compatibility with FMIPv6 in section 3.3.

3.1 Forwarding Router Discovery

This section introduces the FwR discovery scheme. FwR is a router that buffers packets and redirects them to AR_{i+1} during the process of handover, 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 PCoA and the one from CN to NCoA 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, our proposed scheme 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 our proposed scheme, 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 that is derived by assigning routers and APs to Fig. 1 as described in the parentheses of the figure. 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 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.

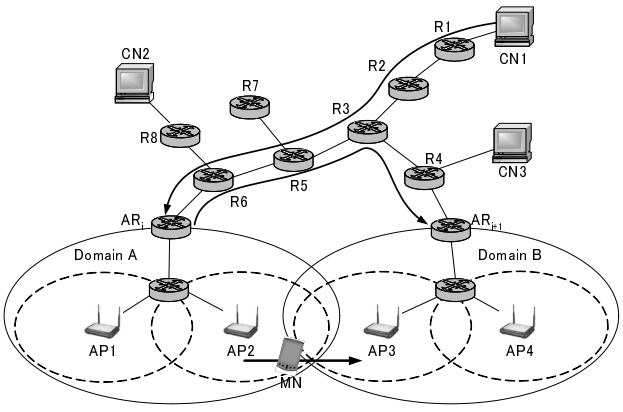


Fig. 2 Forwarding Router Discovery

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 upstream network topology, and CN is not required any modification. Although this searching scheme contains potential deficiency as is later discussed at the end of section 3.1.2, it still chooses much more efficient router as a buffering and forwarding point without requiring CN any protocol specific features than conventional scheme that chooses AR_i as a forwarding point. The details of the discovery scheme is described in the following sections.

3.1.1 FwR Candidates 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.

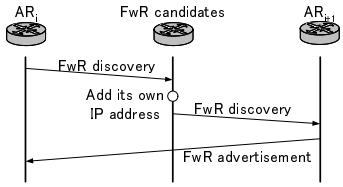


Fig. 3 FwR Discovery with FwR Discovery Message

This discovery scheme should be taken place periodically regardless of MNs' handover process, 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 are limited, it is often more beneficial to cache those result than to conduct discovery scheme for each MN.

3.1.2 FwR Candidates 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 is going to move from previous network belonging to previous AR (AR_{i-1}) to the current network belonging to AR_i, and this information is utilized when the MN moves into next network that belongs to AR_{i+1}, i.e. the next handover.

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 our proposed scheme, AR_i realizes it by receiving Forwarding Request message (See section 3.2) while FMIPv6 utilizes Fast Neighbor Advertisement (FNA) message for that (See section 3.3). Then, the AR_i sends FwR Activation (FwRAct) message to the FwR candidates en route

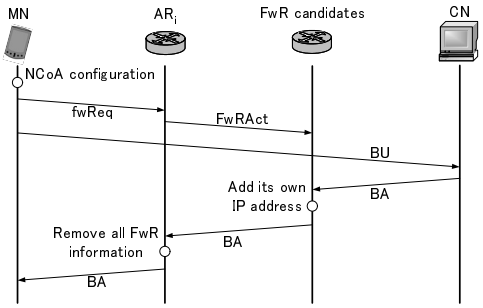


Fig. 4 FwR Discovery with Activation Message

from the AR_i to all the AR_{i+1} candidates that should be known by the periodic procedure described in section 3.1.1. The FwRAct message contains the CN's IP address as well as the MN's NCoA. Upon receiving the FwRAct message, the FwR candidates are activated and start inspecting each arriving packet sent from the CN to the NCoA 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 inserted its IP address inside BA packet or are deactivated after proper timeout period. Upon receiving the BA 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 moves out of the network as described in section 3.2.2. One deficiency of our proposed scheme 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}.

3.2 Proactive Handover

When an MN is going to move out of a network, the MN performs 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. 5, which are also elaborated in the following sections.

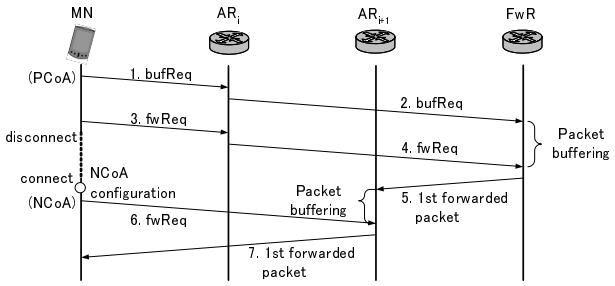


Fig. 5 Proactive Handover Message Flows

3.2.1 Proactive Packet Buffering

By forwarding packets from AR_i to NCoA, handover goes very smoothly provided the related two networks are well-overlapped, and provided the MN can receive packets from both PCoA and NCoA simultaneously. However, otherwise, the packets sent to the MN before the establishment of tunnel will be lost. Therefore, our proposed scheme performs proactive packet buffering that compensates the lost packets before the establishment of tunnel as mentioned in [13]. Different from [13–15], our proposed scheme performs buffering at FwR, which replicates the packets sent from CN to MN. Then the FwR forwards the original packets to the MN while it saves the replicated packets into its buffer. Those saved packets will be forwarded to NCoA 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 obtains the address of AR_{i+1} by looking up its own database. The database should be created by periodic message exchanges with geographically neighboring ARs 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 inserts the address of AR_{i+1} into the message and forwards it to proper FwR that is decided by looking up the result of FwR discovery. 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 3.2.2 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 it to the 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.

3.2.2 Packet Forwarding

When MN is moving 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 PCoA 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 an MN moves into 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 it does not receive any valid fwReq message for certain amount of time, the AR_{i+1} discards those buffered packets.

As described in [14], an MN cannot send any packet to CN with NCoA until it finishes BU procedure. When it sends packets to CN before finishing BU procedure, the source field of the IP header should be PCoA 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.

3.3 Compatibility with FMIPv6

Our proposed scheme 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, it sends fwReq message in our proposal before handover while it sends FBU in FMIPv6. Moreover, it 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, our proposed scheme works with FMIPv6 without MN's noticing our protocol. In this case, our proposed scheme can gain better performance with the help of FMIPv6 though we need some enhancement for the behavior of the AR_i and AR_{i+1} to cooperate with FMIPv6, The detailed feature to cope with FMIPv6 is outside the scope of this paper.

4. Evaluation

In this section, our proposed scheme is evaluated. We evaluate our proposed scheme in the view of packet misordering in section 4.1 while we evaluate it in the view of bandwidth consumption in section 4.2.

4.1 Packet Misordering

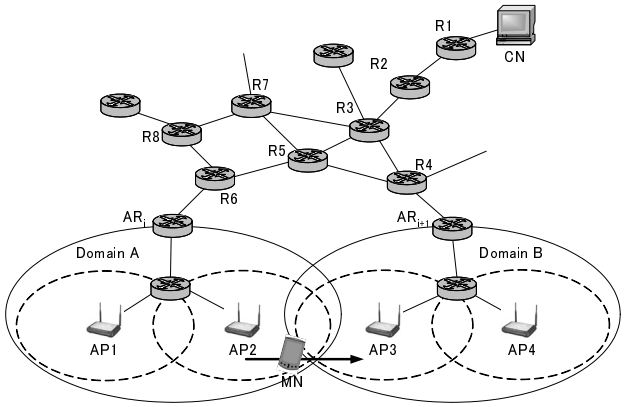


Fig. 6 Simulation Topology

Firstly, we evaluate our proposed scheme 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 3.1.2, FwR discovery sometimes cannot choose CoR if the CoR is not en route from AR_i 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 our proposed scheme 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. Since big ISPs usually have private peering links, different from Fig. 2, Fig. 6 has direct link between R4 and R5. Here, the CN is sending CBR traffic to MN that is connected to AP2. After a while, the MN starts handover to the 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 NCoA. Likewise, upon receiving BU message, the CN starts sending packets to NCoA 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 NCoA and the one from FwR to NCoA. 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.

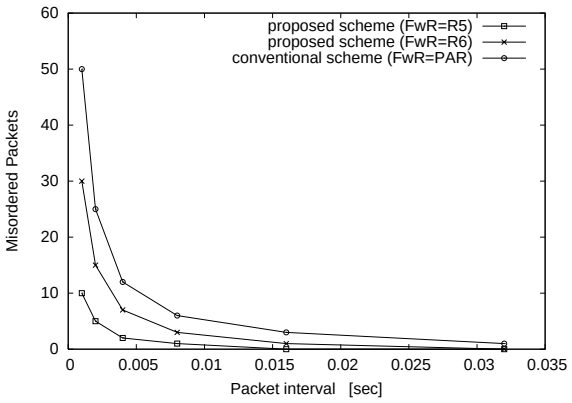


Fig. 7 Packet Misordering (single connection scenario)

Figure 7 shows the result of this simulation. It illustrates the packet misordering for both conventional scheme (FwR=AR_i) and proposed scheme (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 our proposed scheme still suffers from packet misordering, it significantly reduces the amount of misordered packets compared to the conventional scheme that forwards packets from AR_i.

In the Internet, we cannot expect all routers to support our protocol. However, by strategically locating FwR candidates, 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 the CoR or locating FwR candidates around the CoR will efficiently reduce the redundant routing.

Secondly, we evaluate our proposed scheme in the view of packet misordering assuming an MN has multiple connections during its handover process. In our proposed scheme, the MN can utilize FwRs for each connection so that the redundant routing for each connection will be minimized.

In Fig. 2, assuming that an MN has several connections with CN1, CN2, and CN3 during the process of handover, when the MN performs handover, the AR_i chooses FwRs for each CN. Hence R3 is chosen as the FwR for the connection with CN1, R6 is chosen as the FwR for the connection with CN2, and R4 is chosen as the FwR for the connection with CN3. Here, we assume that R3, R4, and R6 are FwR candidates. In this way, the MN can choose the most suitable FwRs for each CN. 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. In Fig. 2, R6 and AR_i are the possible candidates for common FwR. Since R6 is more upstream router than AR_i, R6 is chosen as the FwR.

Table 1 Packet Misordering (multiple connection scenario)

	packet misordering
CN1	40 packets
CN2	0 packet
CN3	60 packets
Total	100 packets

To evaluate the efficiency of multiple FwR support, the number of packet misordering is measured by utilizing the NS2 simulator assuming the topology described in Fig. 2. Here, CN1, CN2, and CN3 are individually sending 128kbps CBR traffic (packet interval=0.001sec) to MN. Table 1 shows the number of packet misordering in case we forbid multiple FwR support. Since CN1 and CN3 cannot utilize CoRs as FwRs, and they utilize R6 as FwR, undesired packet misordering occurs for the connection with CN1 and for the one with CN3. When we utilize multiple FwR support, we utilize R3 as the FwR of CN1, R6 as the FwR of CN2, and R4 as the FwR of CN3, hence no packet misordering occurs for each connection. As can be seen, choosing FwR for each connection significantly reduces the amount of packet misordering.

Note that, although proposed scheme with multiple FwR support still suffers from packet misordering provided CoR is not chosen as an FwR as described in Fig. 6, it reduces the total amount of packet misordering compared to the one without multiple FwR support.

4.2 Bandwidth Consumption

We evaluate our proposed scheme in the view of bandwidth consumption assuming Fig. 6 is our simulation topology. By utilizing FwR discovery, the AR 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 the duration that causes temporal redundant routing caused by handover procedure is 1 second in this simulation model. 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 assumed all FwR has unlimited capacity and one best-located FwR will assist all the MNs' handover. Figure 8 shows the comparison between conventional scheme and proposed scheme in the view of bandwidth consumption of the link between R5 and AR_i. 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, proposed scheme saves bandwidth consumption compared to the conventional scheme all the time.

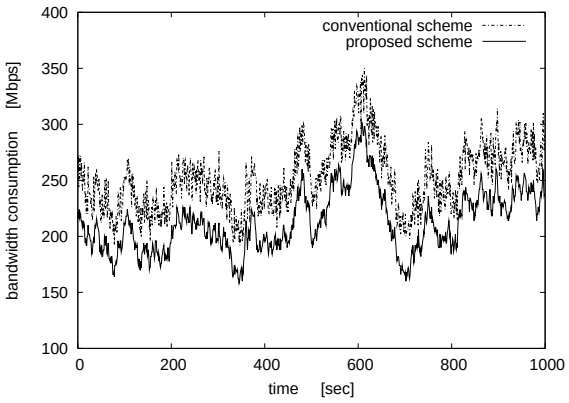


Fig. 8 Bandwidth Consumption

Secondly, we assumed 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 9 shows the relationship between capacity of each FwR and bandwidth consumption for the link between R6 and R5, and for the link between AR_i and R6, in cases of conventional scheme and proposed scheme with FwR discovery individually. 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 saturated minimum value, and the closer to AR_i, the less bandwidth consumption occurs.

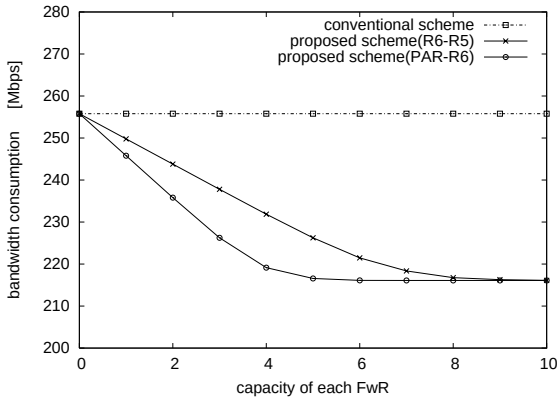


Fig. 9 Impact of FwR's Capacity

5. Conclusion

To enable smooth inter-domain handover, we proposed a scheme 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 ARs' unawareness of the network topology while the latter enhances the handover performance with packet buffering and packet forwarding at FwR. In evaluation, we examined our proposed scheme 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. Our proposed scheme 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 our proposed scheme. Our proposed scheme 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 our proposed scheme 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," *IETF 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," *IETF RFC 3776*, June 2004.
[3] S. Deering and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification," *IETF RFC 2460*, Dec. 1998.
[4] N. Montavont and T. Noel, "Handover Management for Mobile Nodes in IPv6 Networks," *IEEE Communications Magazine*, vol. 40, no. 8, pp. 44–53, 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 Transactions on Networking*, vol. 10, pp. 396–410, Oct. 2002.

[6] A. G. Valko, "Cellular IP : A New Approach to Internet Host Mobility," *ACM SIGCOMM Computer Communication Review*, vol. 29, pp. 50–65, Jan. 1999.

[7] Z. D. Shelby, D. Gatzounas, A. Campbell, and C.-Y. Wan, "Cellular IPv6," *IETF 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, pp. 3307–3312, 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*, pp. 3245–3249, Apr. 2002.

[10] W. Ma and Y. Fang, "Dynamic Hierarchical Mobility Management Strategy for Mobile IP Networks," *IEEE Journal on Selected Areas in Communications*, vol. 22, no. 4, 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*, pp. 42–49, Aug. 2000.

[12] C. Perkins and D. B. Johnson, "Route Optimization in Mobile IP," *Mobile IP Working Group 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.

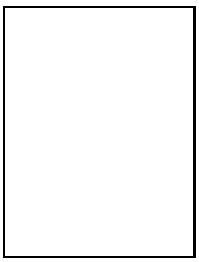
[14] R. Koodli, "Fast Handovers for Mobile IPv6," *IETF Mipshop Working Group Internet Draft (draft-ietf-mipshop-fast-mipv6-02.txt)*, July 2004.

[15] H. Soliman, C. Castelluccia, K. El-Malki, and L. Bellier, "Hierarchical Mobile IPv6 mobility management (HMIPv6)," *IETF Mipshop Working Group Internet Draft (draft-ietf-mipshop-hmipv6-02.txt)*, June 2004.

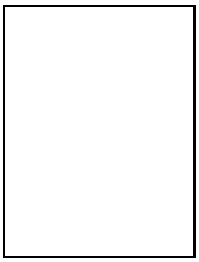
[16] "WIDE Project." [Online]. Available: http://www.wide.ad.jp

[17] K. L. Calvert, M. B. Doar, and E. W. Zegura, "Modeling Internet Topology," *IEEE Communications Magazine*, June 1997.

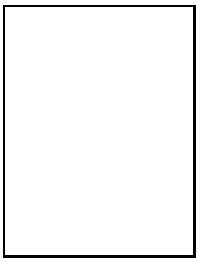
[18] "The Network Simulator, ns-2." [Online]. Available: http://www.isi.edu/nsnam/ns/



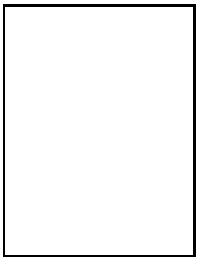
Takeshi Takahashi received his B.Eng. and M.Eng. degrees in 2001 and 2002 respectively from Waseda University, Japan. He became visiting researcher in 2002, and researcher in 2003 in Tampere University of Technology, Finland. In 2004, he became JSPS research fellow and is currently pursuing Ph.D. degree at Graduate School of Global Information and Telecommunication Studies of Waseda University, Japan. His research interests include audiovisual content delivery system and related networking protocols.



Koichi Asatani received his B.Eng., M.Eng. and Ph.D. degrees from Kyoto University in 1969, 1971 and 1974, respectively. From 1974 to 1997, he was engaged in R&D in NTT. Currently he is a professor at Department of Electronic Engineering of Kogakuin University, and a visiting professor at Graduate School of Global Information and Telecommunication Studies of Waseda University. His current interests include Information Networks including broadband networking, Internet interworking, mobile networking and their QoS aspects. He is Fellow of IEEE.



Jarmo Harju received his M.Sc. degree from Helsinki University of Technology in 1979 and Ph.D. degree in mathematics from the University of Helsinki in 1984. In 1985, he joined the Technical Research Center of Finland, working with the development of protocol software. In 1989, he became professor of data communications at Lappeenranta University of Technology. In 1996, he became professor of telecommunications at Tampere University of Technology in the Institute of Communications Engineering, where he is leading the "Networks and Protocols" group. His research interests include mobility and QoS mechanisms in networking.



Hideyoshi Tominaga received his B.Eng., M.Eng. and Ph.D. degrees in 1962, 1964 and 1973 respectively from Waseda University, Japan. He joined NTT in 1964. He became assistant professor in 1971, and professor in 1976 in Waseda University. He founded the Global Information and Telecommunication Institute (GITI) in Waseda University. He was the dean of graduate school of global information and telecommunication studies of Waseda university from 2001 to 2004. His research interests include network engineering and motion picture coding.