A Backward Fast Handover Control Scheme for Mobile Internet (BFH-MIPv6)

Meng-Shu Chiang[1], Chung-Ming Huang[2]

[1] Department of Computer Science and Information Engineering, Far East University, Taiwan
[2] Laboratory of Multimedia Mobile Networking, Department of Computer Science and Information Engineering, National Cheng Kung University, Taiwan
chiangms@gmail.com; huangcm@locust.csie.ncku.edu.tw

Abstract

The fast handover scheme provides a handover preparation mechanism, which retrieves a new care-of-address (CoA) in advance and forwards packets to MN's new visiting access router, to improve the handover performance over wireless network. However, if the handover preparation cannot be finished before the current link becoming unavailable, the handover latency will be increased. In this paper, we propose a backward fast handover control scheme for mobile Internet (BFH-MIPv6) to resolve the aforementioned problems. In the proposed BFH-MIPv6 scheme, a new CoA is formed by the new access router (NAR) and a tunnel is established in advance when MN moves into the domain of NAR. As a result, MN can move smoothly to the new network domain to shorten the handover latency.

Keywords: Fast handover, Care-of-address, Handover latency, New access router

1 Introduction

Mobile IPv6 [13, 18] was proposed to continuously access data for mobile node (MN) over the wireless network, i.e., when MN switches from one network to another during handover, MN can retrieve data continuously. However, Mobile IPv6 suffers from long handover latency and packet loss [9]. The delay time caused by handover is called handover latency. The handover latency consists of the time interval of layer 2 (L2) handover and layer 3 (L3) handover. The L2 handover delay includes the time intervals of (1) scanning and (2) re-association operations [11].

After the L2 handover is complete, L3 handover can occur. The L3 handover latency includes the time period of (1) a CoA acquisition and (2) registration. (1) a CoA acquisition operation: MN formulates a new CoA address after receiving the router advertisement from NAR; (2) Registration: Upon obtaining a new CoA, MN sends a binding update message to notify its HA of its new location. HA replies a binding update acknowledgement to MN and intercepts packets to MN's new location. The L3 handover is complete after MN receives the first packet from NAR. Since Mobile IPv6 performs the above procedures step by step during handover, the handover latency gap is significant and it is not suitable for time-sensitive network applications [1, 17].

Several extensions have been proposed to reduce handover latency in the past years. These proposed methods can be classified into (1) L2, (2) L3, and (3) the cooperation of L2 and L3 originated behaviors. (1) The L2 originated behaviors are intended to reduce the scanning time by (1) scanning with the reduced no. of channels or (2) scanning with a shorter time interval [14]. (2) The L3 originated behaviors constructs a tree-like structure, i.e., hierarchical based structure, to reduce the no. of registration messages and time [5]. In addition, a network-based mobility management protocol, which does not need MN's involvement in mobility management, has been developed [19, 20]. (3) Fast Mobile IPv6 (FMIPv6) [2-4, 6-8, 10, 16] combines L2 and L3 protocols to improve handover performance.

The problem of FMIPv6 is as follow: MN may disconnect with previous access router (PAR) before getting a new CoA and establishing the tunnel, which is because MN stays in PAR's domain without enough time for handover preparation [15]. In this paper, we propose a backward fast handover control scheme for mobile Internet (BFH-MIPv6) to improve the handover performance. In the fast handover control scheme, a tunnel is built from PAR to NAR when L2 trigger occurs, which can be regarded as a "forward" scheme. For the "forward" scheme, the handover preparation is handled by PAR. On the other hand, the proposed "backward" scheme is handled by NAR and a tunnel is built from NAR to PAR. The benefit of the "backward" scheme can be depicted as follows: each time when MN detects a new access point (NAP), MN sends a probe request message, which contains

*Corresponding Author: Chung-Ming Huang; E-mail: huangcm@locust.csie.ncku.edu.tw
DOI: 10.3966/160792642018031902005

network prefix and its MAC address, to NAP/NAR. NAR forms a new valid CoA for MN based on the information and sends a tunnel requirement, which contains the valid CoA, to PAR in advance. Therefore, when MN detects the signal strength of the PAR's domain is going down, i.e., a L2 trigger occurs, PAR can confirm the requirement of the tunnel. In summary, the "forward" scheme needs longer time to wait for the tunnel establishment when a L2 trigger occurs. On the other hand, the "backward" scheme has processed tunnel establishment in advance. Therefore, MN needs less overhead when a L2 trigger occurs. As a result, the proposed BFH-MIPv6 control scheme can improve the handover performance. To have convenient reading of this paper, Table 1 lists these symbols used in this paper.

Table 1. The abbreviations used in this paper

abbr.	meaning	abbr.	meaning	abbr.	meaning
BFH-MIPv6	Backward Fast Handover for Mobile IP	FMIPv6	Fast Handovers for Mobile IP	PAP/NAP	Previous/New Access Point
CN	Correspondence Node	HA	Home Agent	PAR/NAR	Previous/New Access Router
CoA	Care-of-Address	HAck	Handover Acknowledge	PrRtAdv	Proxy Router Advertisement
DAD	Duplicate Address Detection	HI	Handover Initiation	RtSolPr	Router Solicitation Proxy
FBack	Fast Binding Acknowledge	L2/L3	Layer 2/3	UNA	Unsolicited Neighbor Advertisement
FBU	Fast Binding Update	NAACK	Neighbor Advertisement Acknowledge		

The rest of this paper is organized as follows: Section 2 describes related works and problems of the fast handover control scheme. Section 3 depicts the operation of the proposed backward fast handover control scheme for mobile Internet (BFH-MIPv6). Section 4 gives analytical formation and experimental results to evaluate and simulate the performance of our proposed scheme. Section 5 has the conclusion remarks.

2 Problem Formulation

In this Section, operations of FMIPv6 are introduced in detail. Afterwards, we address problems of FMIPv6. Finally, our proposed BFH-MIPv6 is briefly presented to resolve these problems.

There are two modes, which are predictive and reactive, in FMIPv6. Operations of the predictive mode are described as follows:

When a L2 trigger occurs, MN and PAR exchange messages of Router Solicitation Proxy (RtSolPr)/Proxy Router Advertisement (PrRtAdv) to retrieve a new CoA. Then, MN sends a fast binding update (FBU) message to PAR for initializing the handover preparation. PAR and NAR exchange Handover Initiate (HI) and Handover Acknowledge (HAck) messages with NAR to build a tunnel and verify the new CoA. When the Hack message is back to PAR, PAR sends a fast binding Acknowledge (FBack) message to MN and NAR for the handover preparation acknowledgement. From now on, MN can switch to the NAR's domain at any time. Since the handover preparation is successfully complete before MN disconnects from PAR's domain, the handover latency is reduced. Figure 1 depicts the handover steps for the predictive mode of FMIPv6.

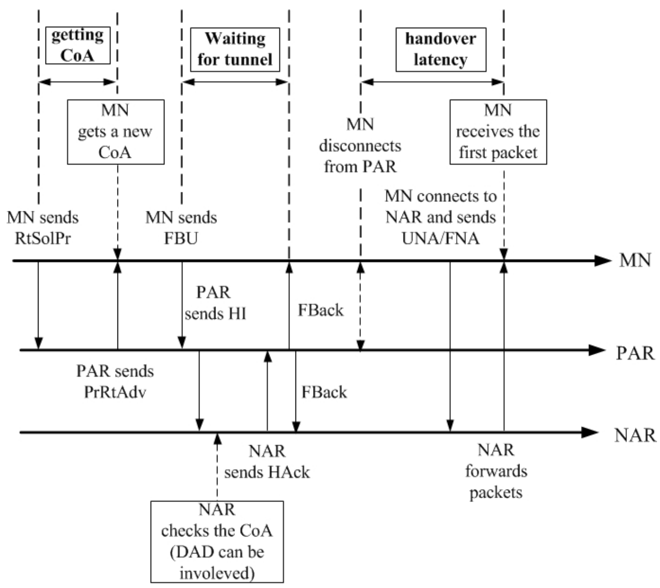

Figure 1. The handover procedure of the predictive mode

On the other hand, in the reactive mode of FMIPv6, MN disconnects from the PAR's domain without completing the handover preparation. As a result, the handover latency of the reactive mode is longer than that of the predictive mode. The reactive mode is as follows: when MN disconnects from the PAR's domain and attaches the NAR's domain, MN sends the Unsolicited Neighbor Advertisement (UNA) message, which includes a FBU message in it. When NAR receives the UNA message, it retrieves the FBU message and then exchanges HI/HAck messages with PAR. PAR starts to forwards packets to NAR. Figure 2 depicts the handover steps for the reactive mode of FMIPv6.

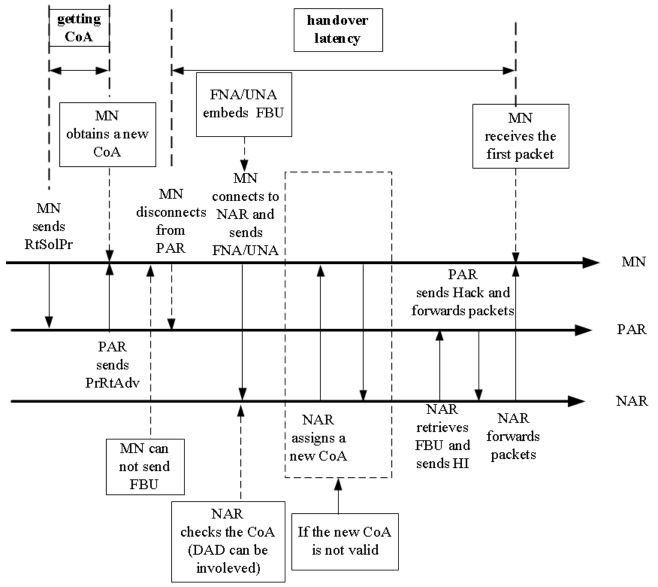

Figure 2. The handover procedure of the reactive mode

There are two problems in FMIPv6:

The time of duplicate address detection (DAD) [12]**.** PAR sends a HI message to NAR for the purpose of (1) checking the validation of a new CoA and (2) requesting a tunnel for handover between PAR and NAR. In order to verify the uniqueness of the new CoA, the procedure of DAD will be performed in NAR. Therefore, in order to obtain a new valid CoA, MN spends time to wait for the message exchanging of HI/Hack messages.

The return of the FBack message. MN may not receive the FBack message in PAR's domain. This situation depends on the factors of MN's moving speed and staying time in PAR's domain. If the FBU message is not processed properly, MN should send UNA, which encapsulates the FBU information, to NAR when MN reconnects with the NAR's domain. Upon receiving the UNA message, NAR will verify the uniqueness of the new CoA, which is included in the FBU message. If the new CoA is not valid, it sends a router advertisement with the Neighbor Advertisement Acknowledge (NAACK) option to MN. The NAACK option contains an alternate IP address for MN. MN uses the new IP address to re-send a FBU message. As a result, MN takes extra handover delay during handover.

3 The Proposed BFH-MIPv6

A new message type of a modified probe request is used in the proposed BFH-MIPv6 to forward PAR's IP address to NAP/NAR. A type and a subtype of frame control, which are set as 00 and 0111 (reserved), are defined; a frame body, which includes PAR's IP address, is also defined. The frame format of the modified probe request is depicted in Figure 3.

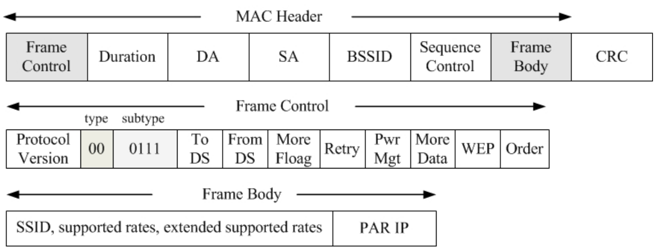

Figure 3. The frame structure of the extended probe request message used in BFH-MIPv6

Figure 4 shows the message exchanging flow chart. Operations are described as follows.

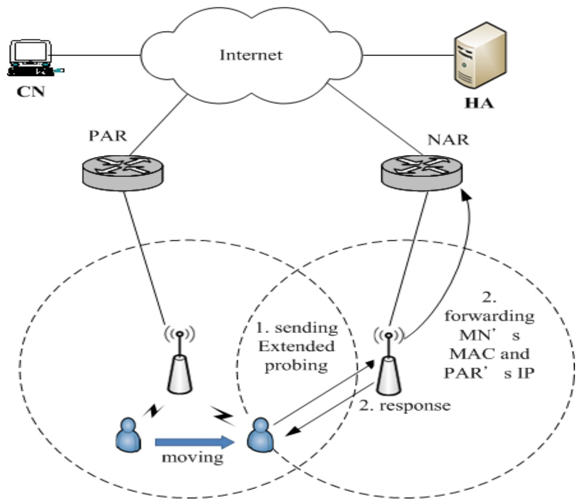

Figure 4. The message exchanging flow using the modified probe request message

MN's operation: when MN receives a new beacon message from a nearby AP, it starts to broadcast a modified probe request frame to nearby APs. After receiving the probe response from NAP, MN stops sending the modified probe request frame.

NAP's/NAR's operation: upon receiving the modified probe request message, NAP sends a probe response message to MN. Meanwhile, NAP extracts MN's L2 address and PAR's IP address from the modified probe request frame. NAP then forwards these two messages to NAR. NAR performs two operations: (1) It forms a new CoA for MN according to its network prefix and MN's MAC address; the new CoA can be verified for DAD procedure, in the NAR's domain in advance. (2) It starts a handover preparation/request for MN. HI/HAck messages are used to start and confirm the handover procedure. The scenario of the proposed BFH-MIPv6 scheme is depicted in Figure 5.

Step 1. Sending the modified probe request from MN: when MN detects a beacon sent from a NAP/NAR, MN sends a modified probe request to the NAP/NAR.

Step 2. Tunnel requirement from NAR: when NAR receives MN's information, it forms a new CoA and sends a HI message, which contains the new CoA, to PAR.

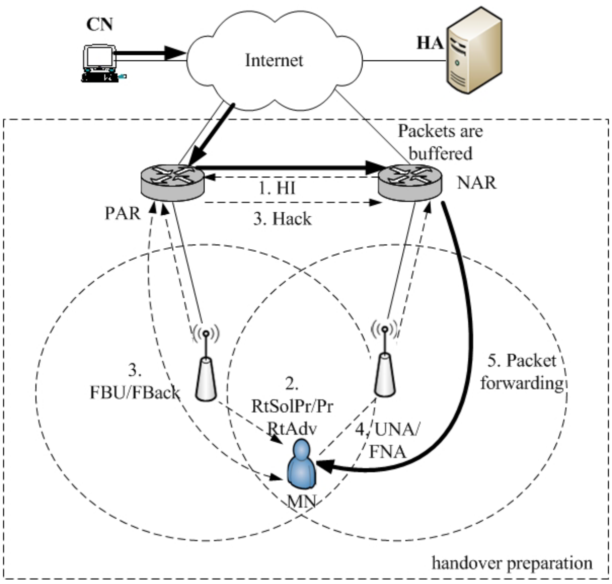

Figure 5. The scenario of the proposed BFH-MIPv6 scheme

Step 3. L2 trigger to get a new CoA: when MN detects the signal strength of PAP is going down than the pre-defined threshold, MN exchanges RtSolPr/PrRtAdv messages with PAR to obtain the new CoA, which is sent from NAR.

Step 4. Tunnel acknowledgement: PAR sends a FBack message, i.e., "handover preparation is ready" message, to MN. At the same time, PAR sends a HAck message to confirm the tunnel request to NAR.

Generally speaking, MN can finish handover preparation before the connection is broken. if some exception case occur, e.g., the sudden disconnection of MN or MN moves in very high speed suddenly, PAR can send a ping message to test whether MN is still reachable or not.

Step 5. MN's present in the new domain: If MN gets a FBack message from PAR's domain, it disconnects from PAR's domain and switches to the NAR's domain. Then, MN sends a UNA message to NAR. On the other hand, if MN is unable to receive the FBack message from PAR, it sends a UNA message, which is embedded with a FBU message, to NAR. Upon receiving the UNA message, NAR sends a FBU message to inform PAR. When PAR receives the FBU message, it reserves this tunnel and disconnects with other tunnels.

Step 6. Packet forwarding: NAR forwards packets to MN when it receives MN's UNA message. Figure 6 depicts the flow chart of the proposed BFH-MIPv6.

The proposed BFH-MIPv6 scheme has the following advantages:

(1) Providing available information: in our proposed scheme, PAR and NAR exchange information with each other using MN's probe request and response messages.

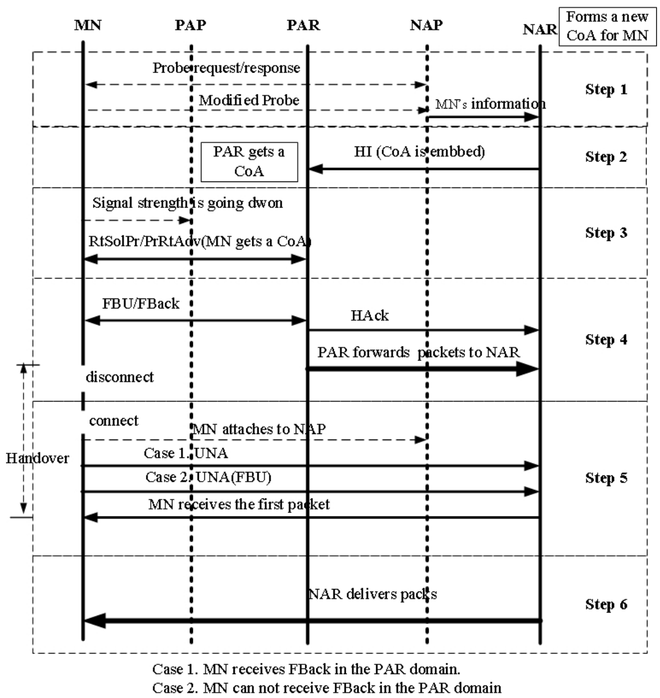

Figure 6. The flow chart of the proposed BFH-MIPv6 scheme

(2) Obtaining a new valid CoA ahead: In FMIPv6, a new CoA is formed by PAR. Hence, the new CoA must be sent to NAR to check the uniqueness. In our proposed scheme, NAR forms a new valid CoA and passes it to PAR. As a result, MN can obtain a new valid CoA from PAR immediately.

(3) Quick response for handover request: in FMIPv6, MN must wait for procedures of tunnel establishment and a new CoA verification after it sending the FBU message. Therefore, MN may not receive the response in PAR's domain if MN's staying interval is too short. In our proposed scheme, the valid CoA has been passed to PAR and the request of tunnel establishment also has been sent to NAR early. If MN sends a FBU message, PAR can send response back to MN immediately. With the quick response time, the failure case of FMIPv6 can be improved.

(4) Exception consideration of packet forwarding: PAR starts to test MN's connection after receiving MN's FBU message. If MN disconnects with PAR without sending a FBU message, PAR forwards packets to all places that MN may visit, i.e., PAR bi-casts to all tunnels. PAR will stop bi-casting as it is notified by MN's new position message. As a result, the packet loss can be reduced with the proposed bi-casting mechanism.

4 Analysis of the Proposed Scheme

In this Section, we first analyze costs of FMIPv6 and the proposed BFHMIPv6 schemes, and then some performance results of the proposed BFH-MIPv6 scheme are given. The notations used in the expression are listed in Table 2.

Table 2. The symbols used in the analysis of FMIPv6 and BFH-MIPv6

symbol	meaning
T_{HO}	the total handover latency
T_{PREP}	the time interval of handover preparation
T_{WAIT}	the waiting time from sending a FBU message to receiving a FBack message in PAR's domain
T_{stay}	the time interval from the time that MN starts a L2 trigger to the time that MN disconnects from PAR

4.1 Analysis of the FMIPv6 Scheme

Figure 7 depicts the timing flow chart of message exchanging before and during handover in FMIPv6, where α is the time interval of transmitting messages between MN and PAR, β is the time interval from the time that MN receives a PrRtAdv message to the time that MN sends a FBU message, γ is the time interval of transmitting messages between two access routers.

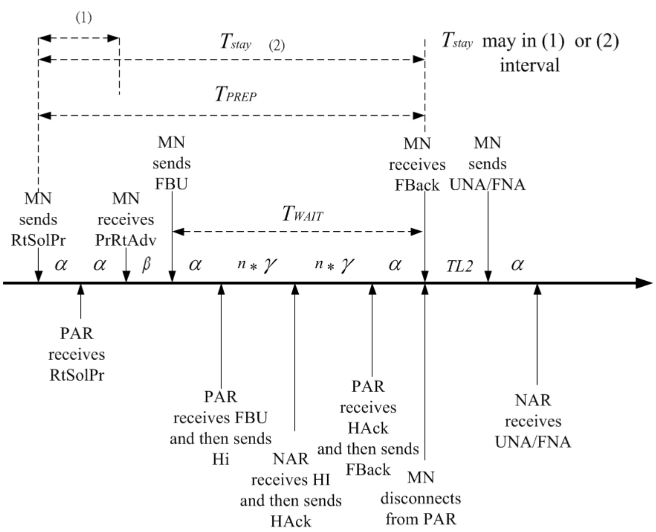

Figure 7. The timing flow chart of FMIPv6

If there are n hops from PAR to NAR, the transmission time is $n*\gamma$. T_{L2} is the time interval of L2 handover. T_{L3} is the time interval of L3 handover. T_{RA} is the time interval of router advertisement. T_{PREP} is the time interval of handover preparation, which includes the time interval of the new CoA acquisition and tunnel establishment between PAR and NAR. Therefore, $T_{PREP} = \alpha$ (MN sends a RtSolPr message to PAR) + α (PAR replies a PrRtAdv message to MN) + β (the delay time for sending a FBU message) + α (MN sends a FBU message to PAR) + $n*\gamma$ (PAR sends a HI message to NAR) + $n*\gamma$ (NAR replies a Hack message to PAR) + α (PAR sends a FBack message to MN) = $4*\alpha + \beta + 2*n*\gamma$. T_{WAIT} is the waiting time from sending a FBU message to receiving a FBack message in PAR's domain. Therefore, $T_{WAIT} = 2*\alpha + 2*n*\gamma$. The quick response time, i.e., less T_{WAIT}, makes MN be able to start handover earlier.

Let (1) T_{stay} denote the time interval from the time that MN starts a L2 trigger to the time that MN disconnects from PAR, (2) T_{HO} denote the total handover latency, and (3) β would be 0 if the MN sends a FBU message immediately when it receives a PrRtAdv message.

The conditions of FMIPv6 can be analyzed as follows:

(1) If $T_{stay} < 2*\alpha$: It means that MN can not obtain a new CoA from PAR before the link is broken. In this case, MN scans nearby available APs and selects one as NAP to attach. Then, it receives router advertisement from NAR to form a new CoA. After obtaining the new CoA, MN sends a FBU message to PAR for receiving tunneled packets between PAR and NAR. At the same time, MN can send a binding update to HA to perform a L3 handover. The handover procedure is finished when MN receives the first packet from NAR. Therefore, $T_{HO} = T_{L2} + T_{RA} + max(2*\alpha + 2*n*\gamma, T_{L3}$.

(2) If $T_{stay} >= 2*\alpha$ and $T_{stay} < T_{PREP}$: In this case, MN can obtain a new CoA from PAR. MN sends a FBU message but it can not receive a FBack message in PAR's domain. Therefore, MN can not make sure whether the tunnel and a new CoA are ready or not. MN sends a UNA/FNA message embedded with a FBU message to NAR. This can be classified into two subcases. Subcase 1: The new CoA is valid in the NAR's domain. $T_{HO} = T_{L2} + \alpha$ (MN sends a UNA/FNA message embedded with a FBU message to NAR) + max(T_{L3}, n*γ (NAR sends a FBU message to PAR) + n*γ (PAR forwards packets to NAR)) + α (NAR sends packets to MN). Therefore, $T_{HO} = T_{L2} + 2*\alpha + \max(T_{L3}, 2*n*\gamma)$. Subcase 2: The new CoA is not valid in the NAR's domain. $T_{HO} = T_{L2} + \alpha$ (MN sends a UNA/FNA message) $+\alpha$ (NAR sends a NAACK message) + α (MN re-sends a FBU message) + max(T_{L3}, 2*n*γ (NAR forwards a FBU message and PAR sends packets to NAR)) + α (NAR forwards packets to MN). Therefore, $T_{HO} = T_{L3} + 4*\alpha + \max(T_{L3}, 2*n*\gamma)$.

(3) If $T_{stay} >= 4*\alpha + \beta + 2*\gamma$: MN can receive the FBack message from PAR's domain. Therefore, MN disconnects from PAR's domain and reconnects to the NAR's domain. At the same time, PAR starts to forward packets to NAR. The total handover time depends on the time of MN's L2 handover time and PAR's tunnel forwarding time. $T_{HO} = \max(n*\gamma, T_{L2} + 2*\gamma)$. In summary, the expressions are listed in Table 3.

Table 3. The numerical analysis of FMIPv6

name	value	condition
T_{PREP}	$4*\alpha+\beta+2*n*\gamma$	no
T_{WAIT}	$2*\alpha+2*n*\gamma$	no
T_{HO}	$T_{L2}+T_{RA}+\max(2*\alpha+2*n*\gamma, T_{L3})$	If $T_{stay}<2*\alpha$
T_{HO}	$T_{L2}+2*\alpha+\max(T_{L3},2*n*\gamma)$	$T_{stay}>=2*\alpha$ & $T_{stay}<T_{PREP}$ valid CoA
T_{HO}	$T_{L3}+4*\alpha+\max(T_{L3},2*n*\gamma)$	$T_{stay}>=2*\alpha$ & $T_{stay}<T_{PREP}$ & not valid CoA
T_{HO}	$\max(n*\gamma, T_{L2}+2*\gamma)$	If $T_{stay}>=4*\alpha+\beta+2*\gamma$

4.2 Analysis of the Proposed BFH-MIPv6 Scheme

Figure 8 depicts the timing flow chart of message exchanging before and during handover in the proposed BFH-MIPv6 scheme, where δ is the time interval of channel scanning. T_{L2_prep} denotes the time interval from the time that MN starts scanning channels to the time that MN sends a RtSolPr message. $T_{PREP}=\alpha$ (MN sends a RtSolPr message to PAR) + α (PAR replies a PrRtAdv message to MN) + β (the delay time for sending a FBU message) + α (MN sends a FBU message to PAR) + max (α (PAR replies a FBack message to MN), $n*\gamma$ (PAR replies a Hack message to NAR)) = $2*\alpha+\beta+n*\gamma$. $T_{WAIT}=2*\alpha$ (MN sends a FBU message to PAR, PAR replies a FBack message to MN immediately). The conditions of the proposed BFH-MIPv6 scheme can be classified as follows: (1) If $T_{L2\_prep}+\alpha>=\delta+\alpha+n*\gamma$, i.e., $T_{L2\_prep}>=\delta+n*\gamma$. In this case, a new valid CoA is forwarded from NAR to PAR and MN can get the new valid CoA from PAR.

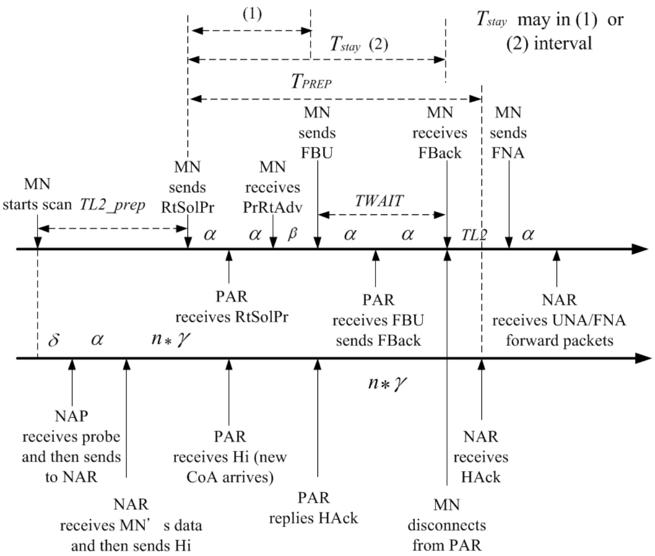

Figure 8. The timing flow chart of the proposed BFH-MIPv6 scheme

There are three subcases: Subcase 1: If $T_{stay}>=\alpha+\alpha+\beta+\alpha+\alpha$, i.e., $T_{stay}+T_{L2}>T_{PREP}$, MN can receive a FBack message from PAR and the tunnel is ready. The handover time is similar to the time of predictive FMIPv6. Therefore, $T_{HO}=\max(n*\gamma, T_{L2}+2*\alpha)$. Subcase2: If $T_{stay}+T_{L2}<T_{PREP}$ and $T_{stay}>2*\alpha+\beta$: MN sends a FBU message from PAR, but it can not receive a FBack message from PAR. Since MN has obtained a new valid CoA from PAR, no NAACK is needed to be sent. Therefore, T_{HO} is equal to $\max(n*\gamma, T_{L2}+2*\alpha)$. Subcase 3: $T_{stay}<2*\alpha+\beta$: MN can not send a FBU message from PAR. Since PAR sets a timer for waiting MN's FBU message, PAR can detect MN's disconnection within \$$2*\alpha+\beta$. PAR starts to forward packets to all possible NARs when PAR detects MN's leaving. Therefore, $T_{HO}<2*\alpha+\beta+\max(n*\gamma, T_{L2}+2*\alpha)$. (2) If $T_{PREP}<\delta+n*\gamma$, MN has requested a new CoA from PAR, but PAR still does not receive a new valid CoA from NAR. We can conjecture that MN moves away from PAR's domain with very high speed. Thus, MN stays within PAR's domain in a very short period, i.e., T_{stay} is very small. In this case, MN can not get a new valid CoA from PAR. The proposed BFH-MIPv6 scheme works like the reactive mode of FMIPv6. In summary, the expressions are listed in Table 4.

4.3 Performance Testing

The performances of FMIPv6 and our proposed BFH-MIPv6 scheme are compared using the ns-2 simulator [21]. The experimental environment for performance testing is depicted in Figure 9. MN is set to move linearly from PAR, which is the original network, to NAR, which is the destination network. The wireless coverage of PAP and NAP are overlapped to test handover preparation for FMIPv6 and BFH-MIPv6 control schemes. Generally speaking, the signal strength of Wi-Fi will be downgraded and unsuitable to connect when MN is away from it. Therefore, the coverage range of AP in this testing is set to 50m to make sure that MN can send and receive packets normally.

Table 4. The numerical analysis of the proposed scheme

name	value	condition
T_{PREP}	$2*\alpha+\beta+*n*\gamma$	no
T_{WAIT}	$2*\alpha$	no
T_{HO}	$\max(n*\gamma, T_{L2}+2*\alpha)$	$T_{stay}+T_{L2} > T_{PREP}$
T_{HO}	$\max(n*\gamma, T_{L2}+2*\alpha)$	$T_{stay}+T_{L2} < T_{PREP}$ & $T_{stay} > 2*\alpha+\beta$
T_{HO}	$T_{HO} < 2*\alpha+\beta+\max(n*\gamma, T_{L2}+2*\alpha)$	$T_{stay} < 2*\alpha+\beta$

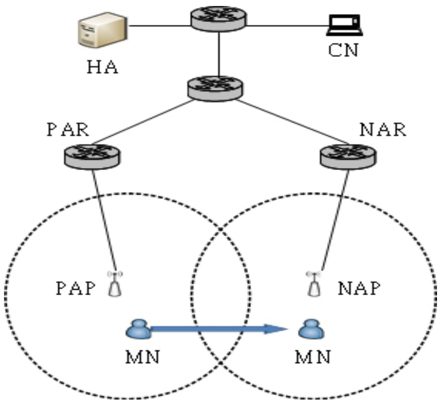

Figure 9. The experimental topology of the handover performance testing

The staying time in the PAR's domain depends on the overlapped area of PAP/NAP and MN's moving speed. The time of the tunnel establishment depends on the routing path between PAR and NAR, i.e., how many hops the corresponding routing path has.

Initially, the overlapped area is set to 10m and MN's moving speed is set 5. Therefore, the staying time in PAR's domain is about 2 second. In this case, although the hop counts between PAR and NAR are increased to 6, both of FMIPv6 and BFH-MIPv6 control schemes are successful for handover preparation. In order to test the situation of handover preparation, the overlapped area is set from 10m to about 0 and the hop counts are increased from 2 to 6 in the following experiment. Generally speaking, a larger packet size will raise the situation of packet loss during handover. A higher packet loss rate causes a longer handover latency. Therefore, the packet size is set 512 bytes to test the strength of FMIPv6 and BFH-MIPv6 control schemes.

A correspondence node (CN) is used as a source agent, which is an FTP server to provide packets for MN. A home agent (HA) is needed for MN to record it's initial situation.

Table 5 depicts these parameters. All simulations have time duration of 100 seconds and initially there are 5 seconds for the warm-up step, i.e., MN initially stays in HA's domain to record its HA information. MN is set to move into PAR's domain at the 10th second, and MN then moves linearly towards the NAR's domain.

Table 5. The experimental parameters used in the test

Parameters	value
MN's moving speed	5m/s
coverage range of AP	50m
packet size	512 bytes
Intersection of two APs	10m

Figure 10 depicts the average handover preparation time of FMIPv6 and our proposed method. FMIPv6-2, FMIPv6-4, and FMIPv6-6 are tested under 2, 4, and 6 hop counts between PAR and NAR in FMIPv6 respectively; BFH-MIPv6-2, BFH- MIPv6-4, and BFH- MIPv6-6 are tested under 2, 4, and 6 hop counts between PAR and NAR in our proposed BFH-MIPv6 scheme respectively.

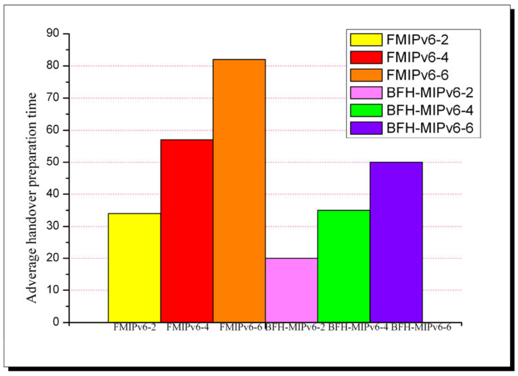

Figure 10. The handover preparation time of FMIPv6 and our proposed schemes

In FMIPv6, the handover preparation starts from the time that a RtSolPr message is sent to the time that a FBack is received by MN. Because HI/Hack messages are passed between PAR and NAR, the time will be increased when the hop number increases. Since MN receives a FBack message after MN sends a FBU message immediately in our proposed BFH-MIPv6, a Hack message is traveled only half of the hop counts in our proposed scheme, comparing with FMIPv6. As a result, the time of handover preparation of our proposed method is about half time of that of FMIPv6. In FMIPv6, the handover preparation time depends on hop counts between PAR and NAR. As the hop counts between PAR and NAR increase, MN needs more remaining time in PAR for handover preparation due to passing HI/Hack messages to wait for the new CoA verification. However, in our proposed scheme, the handover preparation time of our proposed scheme is less than that of FMIPv6 because of without waiting for the new CoA verification. Thus, MN requires less handover preparation time to stay in PAR's domain.

Figure 11 and Table 6 depicts the average handover latency of more handovers. The handover latency starts from the time that MN disconnects with PAR's domain and ends with the time that MN receives the first packet from the NAR's domain. If MN's staying time in the PAR domain is long enough, MN has a better chance to prepare for handover successfully and the handover latency will be reduced. Otherwise, the handover latency will be increased.

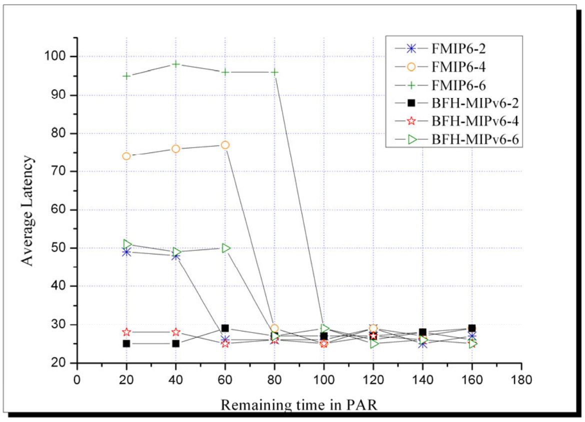

Figure 11. The handover latency of FMIPv6 and our proposed schemes

Table 6. The average handover latency of FMIPv6 and our proposed schemes

Staytime	FMIPv6-2	FMIPv6-4	FMIPv6-6	BFH-MIPv6-2	BFH-MIPv6-4	BFH-MIPv6-6
20	51.06	77.18	99.66	26.03	29.29	53.4
40	49.73	78.81	101.82	25.88	29.04	50.91
60	26.78	79.23	98.98	29.9	32.25	51.5
80	26.7	29.81	98.78	27.7	26.7	27.78
100	26.6	25.58	29.78	27.62	25.58	29.67
120	29.61	29.67	26.6	27.57	27.59	25.6
140	25.45	27.46	28.56	28.48	26.49	26.47
160	27.41	29.49	26.44	29.44	25.35	25.38

Figure 12 depicts the packet delivery time. The delivery time starts from the time that CN sends a packet to the time that MN receives it. During handover, packets destined to MN will be transferred from PAR to NAR. In the column of Interval1 for packet delivery time, MN moves normally from the PAR's domain to the NAR's domain. FMIPv6 and our proposed BFH-MIPv6 schemes have the similar packet delivery time interval. In the column of Interval2 for packet delivery time, MN moves quickly from the PAR's domain to the NAR's domain. Our proposed BFH-MIPv6 has better packet delivery time than the FMIPv6 scheme has.

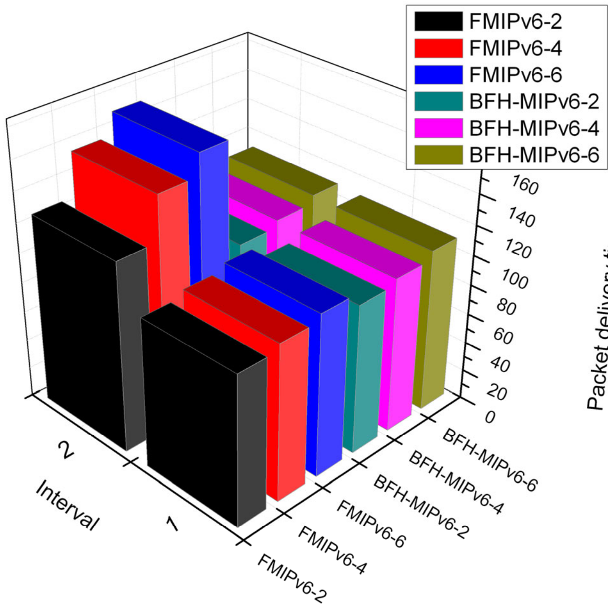

Figure 12. The packet delivery time interval of FMIPv6 and our proposed schemes during handover

5 Conclusion

If MN prepares for the handover successfully, i.e., in the predictive mode, the handover latency is reduced. On the other hand, MN has longer handover latency when MN is in the reactive mode of FMIPv6. In this paper, we have proposed a backward fast handover for Mobile Internet (BFH-MIPv6) control scheme to reduce the time of handover preparation. In the proposed BFH-MIPv6 scheme, MN can obtain a new valid CoA in advance and prepare for handover before link is broken. In this way, our proposed BFH-MIPv6 can prepare for handover with much more time than the fast handover. Therefore, the proposed method can have better chance to be in the predictive mode. As a result, the handover latency can be improved.

Acknowledgment

This research is supported by the National Science Council of the Republic of China, Taiwan under the contract number NSC 102-2221-E-006 -114 -MY3.

References

[1] V. Amarsinh, D. Satish, Seamless Video Streaming Using Improved Handover Prediction and Session Handover in Mobile Networks, *International Journal of Computer Engineering & Technology* (IJCET), Vol. 5, No. 4, pp. 105-118, April, 2014.

[2] M. Boutabia, H. Afifi, Maximizing Predictive Mode Probability in Fast Handovers for Mobile IP, *Proceeding of the 20th International Conference on Telecommunications* (ICT), Casablanca, Morocco, 2013, pp. 1-5.

[3] Y.-H. Cheng, Y.-H. Lin, S.-J. Kao, Incorporating MIP and SIP for Cross-Layer Fast Handoff in IPv6 Networks, *Journal of Internet Technology*, Vol. 4, No. 11, pp. 509-517, July, 2010.

[4] M.-S. Chiang, C.-M. Huang, D. D. Tuan, The Multi-Node Fast Handover Control Scheme Using the Group-Based Approach, *IET Networks*, Vol. 4, No. 1, pp. 44-53, January, 2015.

[5] R. Hsieh, Z. G. Zhou, A. Seneviratne, S-MIP: A Seamless Handoff Architecture for Mobile IP, *Proceedings of IEEE INFOCOM*, San Francisco, CA, 2003, pp. 1774-1784.

[6] R. Koodli, Ed., *Mobile IPv6 Fast Handovers*, IETF RFC 5268, June, 2008.

[7] H. Li, S. Habibi, G. Ascheid, Handover Prediction for Long-term Window Scheduling Based on SINR Maps, *IEEE 24th International Symposium on Personal Indoor and Mobile Radio Communications* (PIMRC), London, UK, 2013, pp. 917-921.

[8] R. Li, J. Li, K. Wu, Y. Xiao, J. Xie, An Enhanced Fast Handover with Low Latency for Mobile IPv6, *IEEE Transactions on Wireless Communications*, Vol. 7, No. 1, pp. 334-342, January, 2008.

[9] J.-H. Lee, J.-M. Bonnin, I. You, T.-M. Chung, Comparative Handover Performance Analysis of IPv6 Mobility Management Protocols, *IEEE Transactions on Industrial Electronics*, Vol. 60, No. 3. pp. 1077-1088, March, 2013.

[10] C. Makaya, S. Pierre, An Architecture for Seamless Mobility Support in IP-Based Next-Generation Wireless Networks, *IEEE Transactions on Vehicular Technology*, Vol. 57, No. 2, pp. 1209-1225, March, 2008.

[11] A. Mishra, M. Shin, W. Arbaugh, An Empirical Analysis of the IEEE 802.11 Mac Layer Handoff Process, *ACM SIGCOM Computer Communications Review*, Vol. 33, No. 2, pp. 93-102, April, 2003.

[12] N. Moore, *Optimistic Duplicate Address Detection*, IETF RFC 4429, April, 2006.

[13] C. Perkins, D. Johnson, *Mobility Support in IPv6*, IETF RFC 3775, 2004.

[14] I. Ramani, S. Savage, SyncScan: Practical Fast Handoff for 802.11 Infrastructure Networks, *Proceedings of IEEE INFOCOM*, Miami, Fla, 2005, pp. 675-684.

[15] D. Su, S. J. Yoo, Failure Case Analysis of Fast Handover in Hierarchical Mobile IPv6 Networks, *Proceedings of IEEE International Symposium on Communications and Information Technology* (ISCIT), Piscataway, NJ, 2005, pp. 226-229.

[16] T. Taleb, K. Letaief, A Cooperative Diversity Based Handoff Management Scheme, *IEEE Transactions on Wireless Communications*, Vol. 9, No. 4, pp. 1462-1471, April, 2010.

[17] X. Wang, D. Le, Y. Yao, A Cross-layer Mobility Handover Scheme for IPv6-based Vehicular Networks, *International Journal of Electronics and Communications*, Vol. 69, No. 10, pp. 1514-1524, October, 2015.

[18] T.-Y. Chi, H.-C. Chao, Pseudo MIPv6 for Anycast and Fault Tolerance Services, *Journal of Internet Technology*, Vol. 7 No. 3, pp. 215-223, July, 2006.

[19] H. Zhou, H. Zhang, Y. Qin, A Fast Handover Scheme of PMIPv6 and Performance Analysis, *Journal of Internet Technology*, Vol. 8, No. 4, pp. 535-543, October, 2007.

[20] J. Bong, S. Park, Y. Shin, Fast Handover Method by Using L2 Trigger Supporting Multi-interface in PMIPv6, *Seventh International Conference on Ubiquitous and Future Networks* (ICUFN), Sapporo, Japan, 2015, pp. 378-381.

[21] ns-2, *Main Page*, http://nsnam.sourceforge.net/wiki/index.php/Main_Page.

Biographies

Meng-Shu Chiang received the M.S. degree from Institute of Computer Science and Information Engineering, National Cheng Kung University, Taiwan, R.O.C. He is currently an assistant Professor of Department of Computer Science and Information Engineering, Far East University, Tainan, Taiwan. His research interests include Wireless and Mobile Networks.

Chung-Ming Huang received the Ph.D. degree in computer and information science from The Ohio State University. He is currently a Distinguished Professor of Dept. of Computer Science and Information Engineering, National Cheng Kung University, Tainan, Taiwan, R.O.C. He currently serves as the Chair of IEEE Vehicular Technology Society Tainan Chapter.