PFC: A packet forwarding control scheme for vehicle handover over the ITS networks

Chung-Ming Huang a,*, Meng-Shu Chiang a, Tz-Heng Hsu b

a Laboratory of Multimedia Mobile Networking, Department of Computer Science and Information Engineering, National Cheng Kung University, Tainan, Taiwan, ROC
b Department of Computer Science and Information Engineering, Southern Taiwan University, Tainan, Taiwan, ROC

Available online 23 December 2007

Abstract

When a vehicle moves on roads, it can receive messages from base stations (BSs) and other vehicles. After it moves far away the transmission range, the vehicle tries to find an available link for continuing packet transmission. The disconnecting from the old link and reconnecting with the new link is called vehicle handover in this paper. How to reduce the message transmission time during vehicle handover becomes an important issue for delivering packets over the intelligent transportation system (ITS) networks. The packet transmission time would be long if the transmission path crosses more hops over the ITS network, which makes more transmission time and increases the handover latency. In order to resolve the above problem, we propose a packet forwarding control (PFC) scheme to select a common ahead point (CAP) as the tunnel source to forward packets. The CAP can forward packets to PAR and NAR with the short transmission path. During vehicle handover, packets sent from the data center to vehicles can be forwarded through CAP to NAR directly without having to travel to PAR. As a result, packets can be sent through a shorter delivery path during handover in the proposed PFC scheme. Simulation results show that our proposed method has less packet transmission time and short handover delay.

Keywords: Fast handover; Mobile node; Previous access router; New access router

1. Introduction

Intelligent transportation systems (ITSs) are gradually deployed. An ITS is an application which combines electronic sensor, computer hardware and software, and communication technologies to improve the effectiveness of transportation system. Goals of ITS are to provide drivers with safe, efficient and comfortable driving and infotainment during journey. The raising demand for ITS has been driven on many dimensions such as traffic surveillance, traffic congestion control, vehicle location and navigation, electronic toll collection, mobility, infotainment, and so on.

With the advance of computer technologies, vehicle telematics is introduced to direct about transport’s communications and information. Drivers can send or receive traffic or personalized messages via vehicle to vehicle or vehicle to infrastructure communications over broadband wireless technologies. Fig. 1 depicts the communication scenario of vehicles.

Drivers can get communication information such as traffic, news, travel, shopping, and even video and music multimedia data via telematics services. Although the cellular networks such as GPRS and 3G can provide vehicles with telematics services, it has drawbacks of high cost and low transmission bandwidth. A feasible alternative is to provide 802.16 based wireless communication infrastructure along roadside. Usually, vehicles have short connection time from a roadside base station (BS). The vehicle’s connection time depends on the communication range of a roadside base station and the moving speed of the
A vehicle handover can simply be considered as that a vehicle disconnects with a previous BS and reconnect with a new BS when it moves into the converge area of these two roadside base stations (BSs). When a vehicle enters into the service range of a new BS, it has little time to prepare for handover between the previous BS and the new BS. The handover duration, which is called handover latency, causes packet loss. How to provide vehicles with seamlessly data accessing between two network domains becomes an important issue.

Two factors that affect the handover duration are (i) the time to connect the new BS and (ii) the time to receive original data from the new BS. In order to shorten the connecting time, vehicles can start to scan available roadside BSs when the signal quality of the current serving roadside BS is getting worse. Nowadays, a new technology based on IEEE 802.16e standard [28,29], which is called WiMAX (the world-wide interoperability for microwave access), can be applied to reduce the connection time of BS. WiMAX outperforms traditional 802.11 wireless networks with higher capacity and long distance range. In order to let vehicles to receive original data from the new BS, mobile IP based technologies are used to provide data continuity. Mobile IP [6,17,19] supports IP layer mobility between different subnets over wireless communication technologies. However, it suffers from an unacceptable handover delay and hence causes a lot of packet loss. Several methods were proposed to resolve the handover related issues in the past [2,9,10,12,13,15,18,24].

Redundant packet transmission over the ITS network causes the triangle packet transmission problem: Packets sent from the data center will be transferred to the vehicular previous network, and then be forwarded to the vehicular newly connecting network. The triangle transmission path suffers from two disadvantages. (1) Redundant packet transmission: it wastes the bandwidth of wireless communication and downgrades the network performance over the ITS network. Especially when many vehicles on the road, and multimedia information are transmitted between vehicles and roadside BSs. (2) Long packet transmission time: The packet transmission time is the time period between (i) the time at which the packet is sent from the data center and (ii) the time at which the packet is received by vehicles. The packet transmission time would be long if the transmission path crosses more hops over the ITS network. Therefore, the redundant tunnel transmission path causes more transmission time and increases the handover latency. The fast handover scheme can reduce handover latency by predicting a new access router (NAR), and pre-building a tunnel between NAR and previous access router (PAR). However, the proposed scheme causes a redundant transmission during handover. Fig. 2 depicts the redundant transmission in the fast handover scheme.
In this paper, a packet forwarding control (PFC) scheme for vehicle handover is proposed to improve handover performance. In order to resolve the triangle packet transmission problem, the PFC scheme selects a common ahead point (CAP) as the tunnel source for forwarding packets. The CAP is the closest parent of PAR and NAR, it can forward packets to PAR and NAR with the short transmission path. In Fig. 2, the access router, which is the closest parent of PAR and NAR, is selected as the CAP. During handover, packets sent from the data center to vehicles can be forwarded through CAP to NAR directly without traveling to PAR.

The rest of this paper is organized as follows: Section 2 describes related handover control schemes over ITS. Section 3 specifies problems of the fast handover over the WiMAX wireless networks. Section 4 depicts the operation of the proposed packet forwarding control (PFC) scheme for vehicle handover. Section 5 evaluates the performance of the proposed control scheme. Section 6 has the conclusion remarks.

2. Preliminary

ITS provides various information services for vehicles. Vehicles can exchange data and road’s conditions with other vehicles traveling on the road, or traffic control center. Information exchanging between vehicles is called inter-vehicle communication, and information exchanging between vehicle and data center is called vehicle-to-infrastructure communication. When a vehicle moves to the boundary between two roadside BSs, traffic information destined to the vehicle may be delayed or lost due to handover. In this section, researches that focus on the improvement of the vehicle-to-infrastructure communication are introduced. Several researchers have proposed different approaches for the improvements of MN/vehicle handover [3,7–10,12,13,16,20,23–27]. These researches can be classified as the layer 2 [3,7,13,20,23,25,26], hierarchical [9,24], multicast [12,27], proxy of application [16], and the hybrid layer 2 and layer 3 scheme [8,10].

The layer 2 based methods are proposed to reduce the data link layer’s delay time and anomaly. In [25], a selective scanning algorithm is proposed to reduce the scanning delay. Channels can be aggregated into several groups, and MN scans BSs group by group. If an available BS is found, MN connects to the BS and stops the scanning procedure. In [20], the SyncScan is proposed to reduce scanning time by a pre-arranged timing for MN and BSs. Every BS is synchronized and starting to broadcast beacons when MN switches to it. Therefore, if MN switches to the next channel, MN can quickly detect the beacon message. Although it can reduce the layer 2 scanning handover, 802.11 protocols are required to be modified to receive extra information for management. In [7], the authors proposed a mechanism named MV-MAX to improve the performance anomaly of 802.11. When multiple vehicles are within the same BS, the vehicle with poor signal strength will downgrade the performance of all vehicles which reside in the same BS. The MV-MAX scheme will disconnect the vehicle with poor signal strength, which provides a better performance for other vehicles. However, the unfairness approach will cause a vehicle to disconnect with a new BS unless it moves closer to a new area. Thus, the handover latency would be long.

The hierarchical based scheme is proposed to reduce the registration time [9,24]. A mobility anchor point (MAP) is used to manage an administrative network. When MN changes to a new network of the same administrative domain, the MAP will catch a binding update that is sent from MN, and send a binding update acknowledgement directly to MN instead of forwarding the binding update to HA. As a result, the registration time is reduced when MN roams at the same administrative domain.

The multicast-based scheme is proposed to reduce packet loss during handover. MN can request the retransmission of the lost packets from the source. If the source is far from MN, the duplicated packets will become the burden of the network. In [12], a candidate access router (CAR) [11] record is dynamically changed when MN visits or leaves a multicast group. A MAP is selected as the multicast source to send packets to the access routers which are in the CAR record. In [30], the Dedicated Short Range Communications Group (DSRC) defines different layer protocols, layer 1, layer 2, and layer 7, for vehicles. The DSRC group defines the management of data transmission between layer 2 and layer 7 and addresses problems such as location-based multicast. In [27], the traffic message can be transmitted using the multicast-based scheme over the DSRC technology. The roadside BS can join a multicast group to receive multicast messages and then send these messages to MN. If MN needs packets to be retransmitted, a cached BS of the same multicast group can forward these packets to MN. The multicast-based scheme may cause duplicate message transmission.

The proxy of application based scheme provides a proxy of MN to buffer packets when MN is disconnected from the previous network to reduce packet loss. In [16], a Drive-thru Internet system is proposed to maintain the connectivity using Drive-thru client and Drive-thru proxy mechanisms. The Drive-thru client acts as an application layer gateway of the high level application protocol. The Drive-thru proxy provides relay information from corresponding node (CN) to MN when MN is connected, and buffers data for MN when MN is disconnected. Although it can provide mobility on the application, the handover latency seems to be long.

The hybrid layer 2 and layer 3 schemes are proposed to improve the handover latency and packet loss. In [8,10], when MN receives a poor signal quality from the previous BS located at the PAR’s domain, MN is notified by layer 2 trigger to find a new available BS among nearby BSs located at the NAR’s domain. After finding a new candidate BS, packets can be forwarded by the tunnel between PAR and NAR, and would be buffered by NAR. Although
these control schemes can improve handover performance, they have the problem of redundant packet transmission, which is introduced in Section 1.

3. The fast handover tunneling problems

Our proposed PFC method is based on the fast handover scheme over 802.16e technology. In this Section, the 802.16e technology is introduced first, and then the fast handover over 802.16e is presented. Finally, problems of the fast handover is pointed out concisely.

3.1. 802.16e Technology

In the 802.16e scheme, MN can have information of its neighbor BSs by (1) listening to the layer 2 neighbor advertisement or (2) demanding the serving BS for scanning available channels [5,21]. Using these two mechanisms, the handover latency of layer 2 can be reduced. Neighbor BSs can periodically broadcast the layer 2 neighbor advertisement named MOB_NBR-ADV message, which includes the BSID and channel information, to announce their networks. With the information of the MOB_NBR-ADV, MN can proceed synchronization operation with neighbor BSs instead of scanning the available channels. If a MN requests the severing BS to achieve scanning the available channels, the severing BS will schedule the scanning intervals or sleep intervals for MN. During channel scanning, the severing BS buffers packets when the link is disrupted temporarily.

3.2. Mobile IP fast handovers over 802.16e

In 802.16e, handover is initiated when (1) MN sends a MOB_MSHO-REQ to the serving BS or (2) the severing BS sends the MOB_BSHO-REQ to MN. After MN receiving the response message of MOB_BSHO-RSP or MOB_BSHO-REQ message, a layer 2 trigger named Link_Going_Down (LGD) notifies MN to send a Fast Binding Update message (FBU) to PAR. PAR exchanges Handover Initiate (HI) and Handover Acknowledge (Hack) messages with NAR to verify the new prospective CoA and builds a tunnel between them. Then, PAR sends a Fast Binding Acknowledgement (FBack) to MN. After receiving the FBack, MN sends a MOB_HO-IND message to PAR for indication of forwarding packets to NAR through the tunnel. The Link_Switch trigger (LSW) can be applied for sending MOB_HO-IND message immediately when the FBack message is arrived at MN. After MN changing to the new link, MN synchronizes with NAR by exchanging messages. If PAR has transferred MN’s context to NAR, the synchronization time with NAR can be reduced. The initial service flow (ISF), pre-provisioned service before transferring packets, must be established by the network. A Link_Up (LUP) trigger will inform MN to send Fast Neighbor Advertisement (FNA) to NAR. Finally, after NAR receives FNA, it starts to send buffered packets to MN to complete the handover procedure. The message flow diagram of fast handover is depicted in Fig. 3.

3.3. Problems of the fast handover scheme

Although the 802.16e technology and mobile IP fast handover over 802.16e can reduce layer 2 and layer 3 handover latency, the packet transmission time would be long if the transmission path crosses more hops over the ITS networks. Considering three cases of the handover scenario which are depicted in Fig. 4.

- Case 1: When a vehicle moves between AR7 (PAR) and AR8 (NAR) networks. A tunnel is built between AR7 and AR8 during handover. The packet flow sent from the data center to AR8 is the sequence of f0-f1-f2-f3-f4-f5. The sequences of f3 and f4 are redundant transmission when packets can be sent directly from AR1 to AR8.
- Case 2: When a vehicle moves between AR8 (PAR) and AR9 (NAR) networks. A tunnel is built between AR8 and AR9 during handover. The packet flow sent from the data center to AR8 is the sequence of f0-f1-f2-f5-f6-f7-f8-f9. The sequence of f2, f3, f6, and f7 is redundant transmission when packets can be sent directly from AR3 to AR9.
Case 3: When a vehicle moves from AR7 to AR8, and then from AR8 to AR9 quickly before the registration is complete. Assuming the first tunnel between AR7 and AR8, and the second tunnel between AR8 and AR9 are established successfully. Packets sent to AR7 will arrive at AR8 and then finally to AR9. Since packets travel through several tunnels, the redundant transmission causes more network burden and the handover delay would be increased.

Redundant packet transmission over the ITS network causes the triangle packet transmission problem. In order to resolve the above problem, we propose the PFC scheme to select a good forwarding point for delivering packets through the tunnel. It can forward packets to PAR and NAR with the short transmission path. Details of the proposed PFC scheme is depicted in next Section.

4. The proposed packet forwarding control (PFC) scheme

In our proposed PFC scheme, a common ahead point (CAP) locates at the upstream position, which has the minimal distance to PAR and NAR. In the proposed scheme, CAP is located at the intersection of two packet transmission paths over the ITS network. The first transmission path is the normal packet deliver path whose source is data center and the destination is PAR. The second transmission path is the tunnel forwarding path whose source is PAR and the destination is NAR. Flow label information and Hop-by-Hop option header of IPv6 are used in the proposed PFC scheme. A flow label, which is assigned by the flow’s source node, combines with the source address can be used to uniquely identified a flow. Packets with the same flow will be sent from the same source address to the same destination address. The Hop-by-Hop option header is used to deliver optional information that must be checked by each node located at the routing delivery path [4]. The Hop-by-Hop option header of the PFC scheme contains three parts: option type, option length and option data. The Hop-by-Hop option header is used in the HI and HAck messages. Furthermore, the PFC scheme proposes an option data field named “PFC option” that contains flow-checked bit, CAP-FLAG bit and CAP-IP field. The PFC option is defined as follows.

- bit 0 (flow-checked bit): “0” denotes that routers do not check the flow label field in the IPv6 header; “1” denotes that routers must search for flow label in the cache entry and compare it with the flow label in the IPv6 header.
- bit 1 (DFP-found): “0” denotes that no candidate CAP is found; “1” denotes that candidate CAP is found.
- bit 2-129 (DFP-IP): The field contains the IP address of candidate CAP.

Step 1: when a MN receives the MOB_NBR-ADV message from PAR, it can start to find the new AR information using RtSolPr and PrRtAdv messages to get the BSSID from the new BS and a network prefix from NAR to form a new CoA.

Step 2: A Link_Going_Down is triggered after MN requests for handover or the handover is indicated by PAR. On receiving the Link_Going_Down, MN sends a FBU message to PAR for tunnel establishment. When PAR receives the FBU message, it sends a HI message.

![Fig. 4. The handover scenario for tunnel transmission.](image)
with the Hop-by-Hop option header to NAR. The option header contains flow-checked bit, which is set as 1 and CAP-FLAG bit, which is set as 0. Because of the Hop-by-Hop option header, each access router \( AR_m \) located at the routing path between PAR and NAR will examine the PFC option. In the HI message, the flow-checked bit is set as 1 for finding CAP. \( AR_m \) fetches the flow label information from the IPv6 header and searches for the cache entry. If the entry is found in its cache, it means that \( AR_m \) is a candidate CAP. \( AR_m \) must set the CAP-FLAG bit as 1 and replaces the CAP-IP field with its IP address. If \( AR_m \) cannot find the flow label in its cache entry, it passes the HI message to the next hop. The HI message is processed along the routing path until it arrives at NAR.

- Step 3: When NAR receives the HI message with the Hop-by-Hop option header, three possible conditions should be checked.

Subcase 1: NAR can find the flow label in its cache. NAR replies the HAck message with the Hop-by-Hop option header. The Hop-by-Hop option header is for the HAck message, which contains its IP address, CAP-FLAG bit, which is set as 1, and flow-checked bit, which is set as 0.

Subcase 2: NAR cannot find the related flow label in its cache and the CAP-FLAG bit is set as 1. NAR replies the HAck message with the Hop-by-Hop option header. The HAck’s Hop-by-Hop option header contains IP address fetched from the CAP-IP field of the HI message, CAP-FLAG bit, which is set as 1, and flow-checked bit, which is set as 0.

Subcase 3: NAR can find neither the specified flow label in its cache nor 1 in the CAP-FLAG. It means that there is no CAP between PAR and NAR. In this case, the PFC scheme works like the fast handover scheme.

With the Hop-by-Hop option header, each \( AR_m \) located at the routing path between PAR and NAR checks the PFC option. If \( AR_m \) found the CAP-FLAG bit is set as 1, it gets the IP address from the PFC option and compares with its IP address. If these two IP addresses are equal, it means that \( AR_m \) is the CAP. A tunnel between \( AR_m \) and NAR can be built. Otherwise, \( AR_m \) passes the HAck message to the next hop. After PAR receiving the HAck message, if CAP-FLAG is 0, then a tunnel is built between PAR and NAR. PAR replies FBack to MN.

- Step 4: When MN receives the FBack message, it can switch to NAR at any time. If MN is ready to leave the PAR domain, it can send MOB_HO-IND to PAR for forwarding packets from CAP or PAR to NAR through the pre-established tunnel. If there are some reasons that it is necessary for bicasting, the bicasting source, which is the CAP, can have less transmission duplication than other source nodes because the CAP has the minimal distance to PAR and NAR.

- Step 5: When MN is triggered by Link_UP, it can connect to NAR domain. If MN moves to NAR linearly, i.e., without changing its direction, it can send a FNA message to inform its appearance. After receiving the FNA message, NAR informs CAP of stopping bicasting and starts to send buffered packets, which were forwarded from CAP, to MN. When MN receives packets from NAR, the handover procedure is complete.

### Algorithm 1. The algorithm of the PFC scheme

**Symbols definition:**
- \( path_{\text{PAR-NAR}} \): the routing path from PAR to NAR
- \( CAP_{\text{PAR-NAR}} \): parent of PAR and NAR. It is located at the intersection of \( path_{\text{PAR-NAR}} \) and \( path_{\text{PC-N}} \)

**End definition:**
- Step 1: New BS is found from neighbor router advertisement
- MN gets MOB_NBR-ADV from PAR
- MN exchanges RtSolPr/PrRtAdv messages to get a new CoA
- \( path_{\text{PAR-NAR}} \)

**Step 2: locating the CAP**
- MN sends F-BU to PAR when the Link Going Down triggers
- PAR notifies the CAP of forwarding packets through tunnel or bicasting

**Step 3: HI message arrives at NAR**
- if CAP-FLAG bit = 1 then
  - NAR sets the PFC option that sets flow-check as 0, CAP-FLAG as 1 and put HI’s CAP-IP into HAck’s CAP-IP field
- NAR replies the HAck message with the Hop-by-Hop option header

**Step 4: MN switches to NAR**
- if CAP-FLAG bit = 1 then
  - \( AR_m = \text{CAP}_{\text{PAR-NAR}} \)
    - if \( AR_m \)’s IP = CAP-IP then
      - \( \text{CAP}_{\text{PAR-NAR}} = AR_m \)
      - \( AR_m \) builds a tunnel to NAR
  - NAR builds a tunnel between it and NAR

**Step 5: MN switches to NAR**
- MN connects to NAR when a Link_UP triggers
- MN sends F-NA to inform NAR of its attachment
- NAR sends the bicasting stop message to CAP if it is necessary
- MN receives packets from NAR
5.1. Analysis of handover overhead

Posed PFC scheme are given.

5. Performance analysis
to MN when it is appeared in NAR’s domain. The CAP will intercept packets destined to MN and then wise, the intermediate node identifies it as the CAP. Then the PFC option, it just forwards the H Ack message. Other-IP address is different from the IP address embedded in address embedded in the PFC option. If it finds that its and NAR. Each intermediate node again checks the IPmediate nodes, which locate at the path between PARIP address into the CAP option and sends back the CAP’s IP address into the CAP option and gets the IP address of CAP. NAR puts the HI message with the Hop-by-Hop option header. The H Ack message is also received and checked by inter-

data center

![](image)

5. Packets

3. HI with hop-by-hop option

CAP

4. Hack with hop-by-hop option

PAR

2. FBU

1. RtSolPr/ PrRtAdv

Fig. 5. The scenario of the proposed DFP scheme.

![Image](image)

Fig. 5 depicts the scenario of the proposed PFC scheme. When MN moves to a new network, it uses RtSolPr/PrRtAdv messages to get a new CoA. After receiving LGD (Link_Going_Down), MN sends a FBU to PAR and PAR sends a HI message with the Hop-by-Hop option header to start a pre-handover procedure. The HI message is received by PAR and then is forwarded to the next hop, i.e., CAP. When the HI message is passed to the CAP, it finds that it is located at the path between CN to PAR, i.e., it finds that it ever processed a flow from CN to MN. CAP then puts its IP address into the PFC option in the HI header and forwards the HI message to NAR. After NAR receives the HI message, NAR checks the PFC option and gets the IP address of CAP. NAR puts the CAP’s IP address into the CAP option and sends back the H Ack message with the Hop-by-Hop option header. The H Ack message is also received and checked by intermediate nodes, which locate at the path between PAR and NAR. Each intermediate node again checks the IP address embedded in the PFC option. If it finds that its IP address is different from the IP address embedded in the PFC option, it just forwards the H Ack message. Otherwise, the intermediate node identifies it as the CAP. Then the CAP will intercept packets destined to MN and then forward them to NAR. NAR sends the buffered packets to MN when it is appeared in NAR’s domain.

5. Performance analysis

In this Section, performance analysis results of the proposed PFC scheme are given.

5.1. Analysis of handover overhead

A handover delay ($T_{Ho}$) is the time period between the time that MN receives the last packet from PAR and the time that MN receives the first packet from NAR. The total handover delay includes the time of L2 handover ($T_{L2}$) and L3 handover. The L3 handover ($T_{L3}$) involves the time of movement detection ($T_{MD}$), CoA acquisition ($T_{CoA}$), duplicate address detection (DAD) of CoA ($T_{DAD}$), and registration ($T_{REG}$). Eq. (1) shows the handover latency caused by mobile IP.

\[
\begin{align*}
\{ T_{Ho} &= T_{L2} + T_{L3} \\
T_{L3} &= T_{MD} + T_{CoA} + T_{DAD} + T_{REG}
\end{align*}
\]

In the fast handover (FH) scheme and the proposed PFC scheme, the movement detection and CoA acquisition can be performed when MN exchanges RtSolPr/PrRtAdv messages with PAR; The DAD of CoA is checked during the HI/H Ack procedure. The movement detection, CoA acquisition, and DAD of CoA are then accomplished when MN is in the PAR domain. Finally, the registration is performed when MN sends F-NA to NAR. MN can receive tunnel packets between PAR and NAR before the registration is completed. The handover delay depends on the L2 handover and the time that MN sends FNA and receives the first packet from NAR ($T_{FNA}$). Eq. (2) depicts the handover delay caused by the FH and the proposed PFC scheme.

\[
T_{Ho} = T_{L2} + T_{FNA}
\]

$T_{L2}$ is the time of network reentry of 802.16e network. Handover modes of 802.16e can be Fast BS switching (FBSS), Macro diversity handover (MDHO), and three types association handover, which are level 0, 1, and 2 respectively. Both of the FBSS and MDHO handover have lower $T_{L2}$, but they require extra messages to be exchanged between BSs. $T_{L2}$ is about 0ms to 450 ms [3,5].

The packet transmission time ($T_{DT}$) is defined as the time period between the time that data center (DC) sends a packet and the time that MN receives it. $T_{DT}$ can be divided into three stages. Fig. 6 depicts the specified stages.

- Stage 1: Before handover, i.e., the time period before MN sends MOB_HO-IND. The packet transmission time $T_{DT}$ depends on the packet traversal route from DC to MN.
- Stage 2: During handover, i.e., the time period between MN sends MOB_HO-IND and F-NA. In this case, MN leaves PAR and connects to NAR. MN will then receive tunneled packets. Eq. (3) shows the $T_{DT}$ of the FH scheme and the proposed method respectively. The packet transmission time depends on the time of tunnel transmission and L2 handover delay. $T_{PAR-NAR}$ is the transmission time from PAR to NAR, $T_{PAR-CAP}$ and $T_{CAP-NAR}$ is the transmission time from PAR to CAP and CAP to NAR respectively.

\[
\begin{align*}
T_{DT} &= \max(T_{DC-CAP} + T_{CAP-PAR} + T_{PAR-NAR}, T_{Ho}), & \text{FH} \\
T_{DT} &= \max(T_{DC-CAP} + T_{CAP-NAR}, T_{Ho}), & \text{PFC}
\end{align*}
\]
Stage 3: Tunnel receiving, i.e., the time period after MN sends F-NA before the registration is completed. In this stage, MN starts to receive tunneled packets from NAR. The packet delivery time depends on the tunnel transmission path. Eq. (4) depicts the packet delivery time $T_{DL}$ of the FH scheme and the proposed PFC scheme respectively.

\[
\begin{align*}
T_{DL}^{\text{FH}} &= T_{\text{DC-CAP}} + T_{\text{CAP-PAR}} + T_{\text{PAR-NAR}}, \\
T_{DL}^{\text{PFC}} &= T_{\text{DC-CAP}} + T_{\text{CAP-NAR}},
\end{align*}
\]

5.2. Performance evaluation

For the measurement, we use the ns-2 simulator [31] and the ns-2 NIST add-on [32] to compare the performances of fast handover over 802.16e (Wimax) and our proposed PFC. The simulation topology is depicted in Fig. 7. The radios of PAR and NAR’s wireless coverage are 1 km and the overlapped area of PAR’s and NAR’s network domains is 200 m. Data center has a source agent which will establish an FTP connection with MN. MN is the sink agent of the FTP connection. MN initially stays in PAR’s network domain, and MN moves linearly toward NAR domain after 5 s passed. AR2 is the CAP of PAR and NAR. MN’s moving speed is 30 km/h. The ranging procedure delay is set to 50 ms. The scanning mode is set to level 0 (association), i.e., neighbor BS sends NBR-ADV messages to MN and provides contention-based ranging allocations.

Fig. 8 depicts the WiMax message timing with L2 trigger supported, i.e., MN can receive Link_Going_Down (LGD) message when the signal strength of currently connected link is decreased. MN receives the LGD message at the 15.164th second. Since the strength of the current link is still available, the probability of triggering LGD is 0. As MN is moving far away PAR, the strength is decreased and the probability of triggering LGD is increasing. When the probability approaches to 0.94, a LGD is triggered at the 17.632th second. MN starts scanning and stop scanning at the 17.836th second. At the 17.916th second, MN receives a Link_Down (LD) message due to disconnect from the PAR domain. MN then starts the synchronization processes with nearby BSs, i.e., MN receives DL-MAP sync., DCD sync., and UCD parameters from neighbor BSs respectively. After the synchronization process is finished, MN starts a ranging procedure with neighbor BSs.
for uplink synchronization and parameter adjustment. After all parameter adjustments are completed, a network reentry procedure is set to build a connection between MN and target BS, i.e., the registration procedure. Finally, a Link_Up (LU) message is received by MN at the 17.924th second. The L2 delay time is about 58 ms.

Fig. 9 depicts the WiMax message timing without L2 trigger supported, i.e., without LGD trigger supported. MN receives a LD message at the 18.376th second. MN then enters scanning, synchronization, ranging and network reentry procedures sequentially. MN receives a LU message at the 20.028th second. The L2 delay time is about 1.45 s. Therefore, without the trigger support of LGD, the L2 handover delay is significant.

As mentioned in Section 5.1, a handover can be classified into three time intervals, which are before handover, during handover and tunnel receiving. PFC and FH have almost the same packet transmission time in the time interval of before and during handover. Since the FH scheme has redundant tunnel delivery property, its packet transmission time is longer than our proposed PFC scheme in the time interval of tunnel receiving. Fig. 10 depicts the scenario of packet delivery time. The handover time is started at the 17.836th second in the fast handover (FH) and our proposed PFC scheme. Since FH and PFC can prepare for handover when MN enters the coverage of PAR and NAR’s domains, the handover time is started earlier than the mobile IP (MIP) handover scheme. Simulation results show that the FH scheme and our PFC scheme has the same packet transmission time before the 17.894th second, i.e., the time interval of before and during handover. After MN connecting to NAR and before the registration is completed, i.e., the tunnel receiving period, MN receives tunneled packets from PAR or CAP from FH and PFC.
respectively. PFC scheme spends less time (about 58 ms) than FH in the time interval of tunnel receiving.

Fig. 11 depicts the packet delivery time of FH and PFC schemes, in which the path from CAP to PAR and the path from CAP to NAR are 4 hops respectively. The layer 2 delay time is set to 100 ms in this scenario. When the hop counter is increasing, the tunnel receiving time period is also increasing. The reason is that the binding update message needs to be passed through more hops to reach HA. During the tunnel receiving time period, the packet delivery time of the FH scheme spends almost extra 100 ms than PFC’s. Therefore, the number of hops for forwarding packets to MN is an important factor that affects the packet delivery time before the binding update procedure is completed. The proposed PFC scheme can reduce the number of hops for forwarding packets to MN if there exists a common ahead point (CAP) which is located at the intersection of two packet transmission paths over the ITS network.

Fig. 12 depicts the packet delivery time of FH and PFC schemes, in which the path from CAP to PAR and the path from CAP to NAR are 4 hops respectively without layer 2 handover time. The handover latency totally depends on the packet transmission time. This is urgent data type in the 802.16 technology (MDHO is described in the above). Data center can transmit urgent messages such as safety related information to drivers. The real-time transmission can also be applied into MDHO. However, MDHO suffers from more exchanging messages between BSs. Our proposed PFC can reduce the redundant transmission and has a shorter handover latency than the FH scheme.

Fig. 13 depicts the packet transmission time of FH and PFC. When CN delivers packets to MN during handover, packets will arrive at PAR’s domain first and then be tunneled to NAR’s domain in the FH scheme. As the hop counts from CAP to PAR and CAP to NAR are increasing from 2 to 4, packets are sent through the redundant path between CAP and PAR. In our proposed PFC scheme,
In this paper, we have proposed a packet forwarding control (PFC) control scheme to select a suitable forwarding point for delivering packets through the tunnel. Advantages of the proposed PFC scheme include (1) a fast tunneled packet delivery and (2) a shorter bicasting path. Tunneled packets will be delivered to vehicles from the forwarding point instead of the original access router to reduce packet delivery time during handover.

References


[29] IEEE standard for local and metropolitan area networks-part 16: air interface for fixed and mobile broadband wireless access systems amendment 2: physical and medium access control layers for combined fixed and mobile operation in licensed bands and corrigendum 1, February 2006.

