Hindawi
Mobile Information Systems
Volume 2017, Article ID 2867127, 13 pages
https://doi.org/10.1155/2017/2867127

Research Article

Design of Optimized Multimedia Data Streaming Management Using OMDSM over Mobile Networks

Byungjoo Park,[1] Ankyu Hwang,[2] and Haniph Latchman[3]

[1] *Department of Multimedia Engineering, Hannam University, 133 Ojeong-Dong, Daejeok-Gu, Daejeon 306-791, Republic of Korea*
[2] *Technical R&D Center JVG, 53, Neungwolro No. 10-Gil, Yongin-Si, Gyeonggi-Do, Republic of Korea*
[3] *Department of Electrical and Computer Engineering, University of Florida, Gainesville, FL 32603, USA*

Correspondence should be addressed to Byungjoo Park; bjpark@hnu.kr

Received 28 October 2016; Revised 15 February 2017; Accepted 28 February 2017; Published 20 March 2017

Academic Editor: Jaegeol Yim

Mobility management is an essential challenge for supporting reliable multimedia data streaming over wireless and mobile networks in the Internet of Things (IoT) for location-based mobile marketing applications. The communications among mobile nodes for IoT need to have a seamless handover for delivering high quality multimedia services. The Internet Engineering Task Force (IETF) mobility management schemes are the proposals for handling the routing of IPv6 packets to mobile nodes that have moved away from their home network. However, the standard mobility management scheme cannot prevent packet losses due to longer handover latency. In this article, a new enhanced data streaming route optimization scheme is introduced that uses an optimized Transmission Control Protocol (TCP) realignment algorithm in order to prevent the packet disordering problem whenever the nodes in the IoT environment are communicating with each other. With the proposed scheme, data packets sequence realignment can be prevented, the packet traffic speed can be controlled, and the TCP performance can be improved. The experimental results show that managing the packet order in proposed new scheme remarkably increases the overall TCP performance over mobile networks within the IoT environment thus ensuring the high quality of service (QoS) for multimedia data streaming in location-based mobile marketing applications.

1. Introduction

The Internet of Things (IoT) has been rapidly evolving which has changed our way of living allowing us to innovate new designs and services. IoT provides network architecture for physical objects such as devices, equipment, vehicles, homes, or buildings that are embedded with sensors and actuators. It allows the different objects to interact and communicate with each other and enables them to collect and exchange data. The emerging location-based mobile marketing applications for IoT demand mobility management to ensure the quality of service for multimedia data streaming management over wireless/mobile networks, whereas an important challenge for supporting location-based mobile marketing applications in the Internet of Things is the data packet streaming management over wireless and mobile networks.

Location-based mobile marketing applications are consisting of wireless communication networks, mobile devices (such as personal digital assistants (PDAs), smartphones, and navigation devices), geo-information systems, and location or positioning identification. These applications require the support for seamless mobility management among mobile devices to ensure the high degree of accuracy for location requirements.

The mobility management plays a vital role in achieving a high quality of service (QoS) in multimedia data streaming management in an IoT environment for location-based mobile marketing applications. Therefore, IoT convergence networks and mobility management will be essentially important in transmitting multimedia data packets. With the evolution of IoT environments, mobile devices will be moving frequently to foreign networks. A huge amount of multimedia traffic will be developed due to these frequent movements of mobile devices. Thus, the possibility of packet losses and packet ordering problems would likely happen. In order to provide seamless mobile network which meets the routing requirements of the location-based mobile marketing applications in IoT, the research community has proposed mobility management schemes [1–3].

In this regard, the need to support mobile nodes in IPv6-based networks has been rapidly evolving. Mobile IPv6 is a standard that provides the mobile nodes (MNs) with mobility management across IP-based wireless networks [4] in an IoT environment.

However, in a TCP error control, the occurrence of temporal time delays caused by handovers cannot be determined for its focus is merely on packet losses due to congestions. Unnecessary measures to prevent congestion are provided by the TCP since these packet losses are considered as congestion indication within handovers on wireless networks [5–7].

A mobile node in the standard Mobile Internet Protocol version 6 (MIPv6) maintains two addresses, that is, a home address (HoA) which is a permanent identification address, and a Care-of Address (CoA) which is a temporary address used for redirecting information in order to perform the packet transmission continuously without disconnection of the network layer. The MN must disconnect with the access router where it is currently connected and attach to the new access router (NAR) whenever it moves to another subnet. A new temporal address defined as the Care-of Address (COA) must be obtained by the MN. This new CoA (NCoA) as well as the HoA needs to be registered by the MN to its home agent (HA) and the correspondent nodes (CNs) it is communicating with. The delay incurred during the movement detection known as the handover latency, the configuration time of the NCoA, and the time consumed for a binding update in order to start the Internet services from the new subnet are essential characteristics that must be analyzed in MIPv6. That is, since the packets that are transmitted from the HA or the CN may be lost during the handover, the improvement of the handover performance of MIPv6 has been aimed by the latest works in order to provide real-time support and prevent delays on traffic flows.

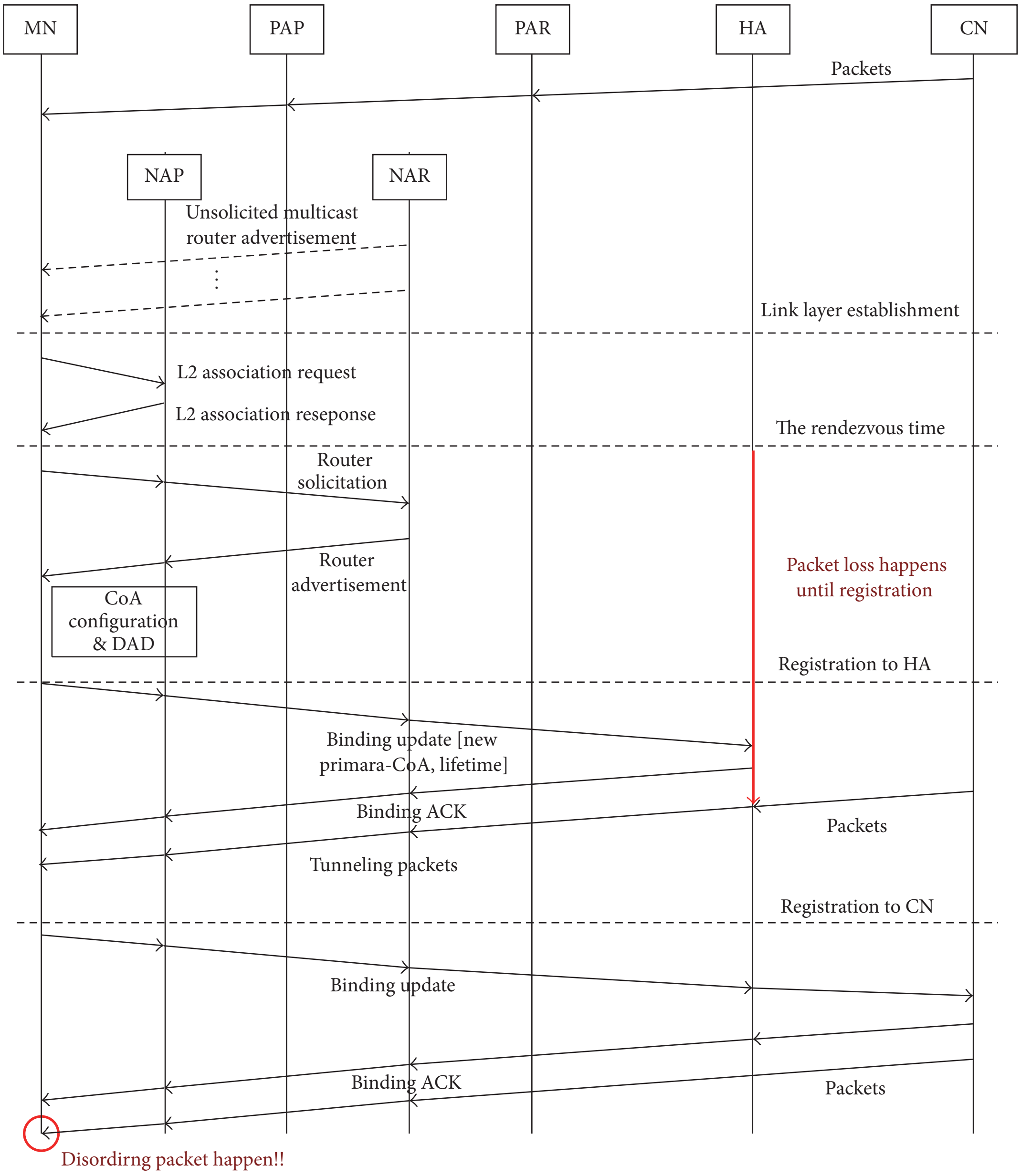
Through the newly defined messages in Fast Mobile Internet Protocol version 6 (FMIPv6) [8], *Router Solicitation for Proxy* and *Proxy Router Advertisement*, the MN can obtain the NCoA before its actual movement to a new subnet. This NCoA is also registered by the MN to its previous AR (PAR) in order to indicate that packets can be forwarded to its NCoA. Thus, it can immediately receive the forwarded packets from its PAR as soon as it moves to the new subnet and connect with a new link. In order to prevent packet losses, buffers may exist in PAR and NAR. Thus, packet losses as well as the handover latency will be reduced with this proposal. However, the disordering packet problem between the packets that are tunneled from the home agent (HA) and the previous access router (PAR) and on the packets that are directly delivered by the CN can be caused by the various features in FMIPv6. The congestion control by the TCP causes the duplicate ACKs (DACKs) as a result of the disordering packets degrading the TCP performance on the transport layer. In addition, useless packet retransmissions from the CN can be induced by disordering packets. An efficient disordering packets solution is difficult to provide in wireless/mobile service applications. Some proposals have been analyzed in order to provide solutions to these problems [9–12]

This paper proposes an optimized multimedia data streaming management algorithm to prevent the packet ordering problem during the handover of mobiles nodes for location-based mobile marketing applications within the IoT environment. This is achieved by applying a new route optimization scheme to the modified access router which can support L2 snoop functions and through the additional of an adapted TCP header format at the HA and CN as the source devices. The remainder of this paper is organized as follows. Section 2 explains the previous works and problems in conventional protocols. Section 3 introduces the proposed realignment algorithm called "OMDSM" in order to increase the TCP performance. This section also discusses the comparison of the data packets sequence in the modified access router (MAR) and the final packet arrival indication from the previous access router (PAR) that requires these modifications. The performance evaluations are shown in Section 4. Finally, the conclusions are presented in Section 5.

2. Related Works

2.1. IETF Standard MIPv6. The basic idea of the standard Mobile IPv6 is to provide a mobile node (MN) with a stationary proxy in the form of a home agent (HA) [4]. The standard handover procedure for Mobile IPv6 (MIPv6) is depicted in Figure 1. The home agent intercepts the packets destined to a mobile node whenever it is away from home and forwards these packets directly to the New Care-of Address (NCoA) of the mobile node through tunneling. The home address is being used as the stationary identifier for the mobile node by the transport layer [13]. Tunneling through the home agent is required as a basic solution resulting to a longer path that leads to a degraded performance. Thereby, a route optimization [1] is included in order to improve its performance. Within the route optimization, in order to modify the handling of the outgoing packets between the mobile node's fixed home address and its NCoA, a binding needs to be discovered by the CN. The mobile node then sends its NCoA to the CN when the route optimization is used through the binding update (BU) messages. The packets that are sent by the CN are then routed to the MN's NCoA once the BU message has been received. However, the CN continues to route the packets to the mobile nodes NCoA through the HA until the BU has been received. Thus, the NAR will disorderly receive these two types of packets.

2.2. IETF Fast Handover for MIPv6 (FMIPv6). The MIPv6 movement detection algorithm and CoA configuration procedure have been replaced by a protocol provided by the proposed FMIPv6 in order to reduce its handover latency. The basic operation of the FMIPv6 [8] is shown in Figure 2. The MN is required by the FMIPv6 to acquire a new CoA at the NAR while still connected in the PAR whenever it attempts to move from its PAR going to the NAR. In addition, a BU message needs to be sent by the MN to its PAR in order that



MN: mobile node
PAP: previous access point
PAR: previous access router
NAR: new access router
NAP: new access point
HA: home agent
CN: correspondent node

Figure 1: The IETF MIPv6 handover procedure.

its binding cache will be updated with the MN's new CoA. Then, the packets that are originally destined for the MN will be forwarded by the PAR to the NAR. The Fast Handover procedure can be initiated by either the MN or the PAR by using the L2 trigger. The link-layer information indicates the movement of the mobile node (MN) between access routers. An L3 handover will be initiated by the MN by sending a "*Router Solicitation for Proxy* message" to the previous access router (PAR) whenever the MN is receiving an L2 trigger (i.e., mobile-initiated handover). However, when the PAR is the one that received the L2 trigger (Network-controlled handover), a *"Proxy Router Advertisement"* (PrRtAdv) message will be transmitted by the PAR to the suitable MN. An NCoA is obtained by the MN through the network information contained from router advertisements that are broadcasted from the NAR while the MN is still connected to the PAR. The MN's new CoA is validated by the PAR and through the delivery of an HI message to the new access router (NAR); a bidirectional tunnel is formed between the previous access router (PAR) and new access router (NAR). Moreover, a

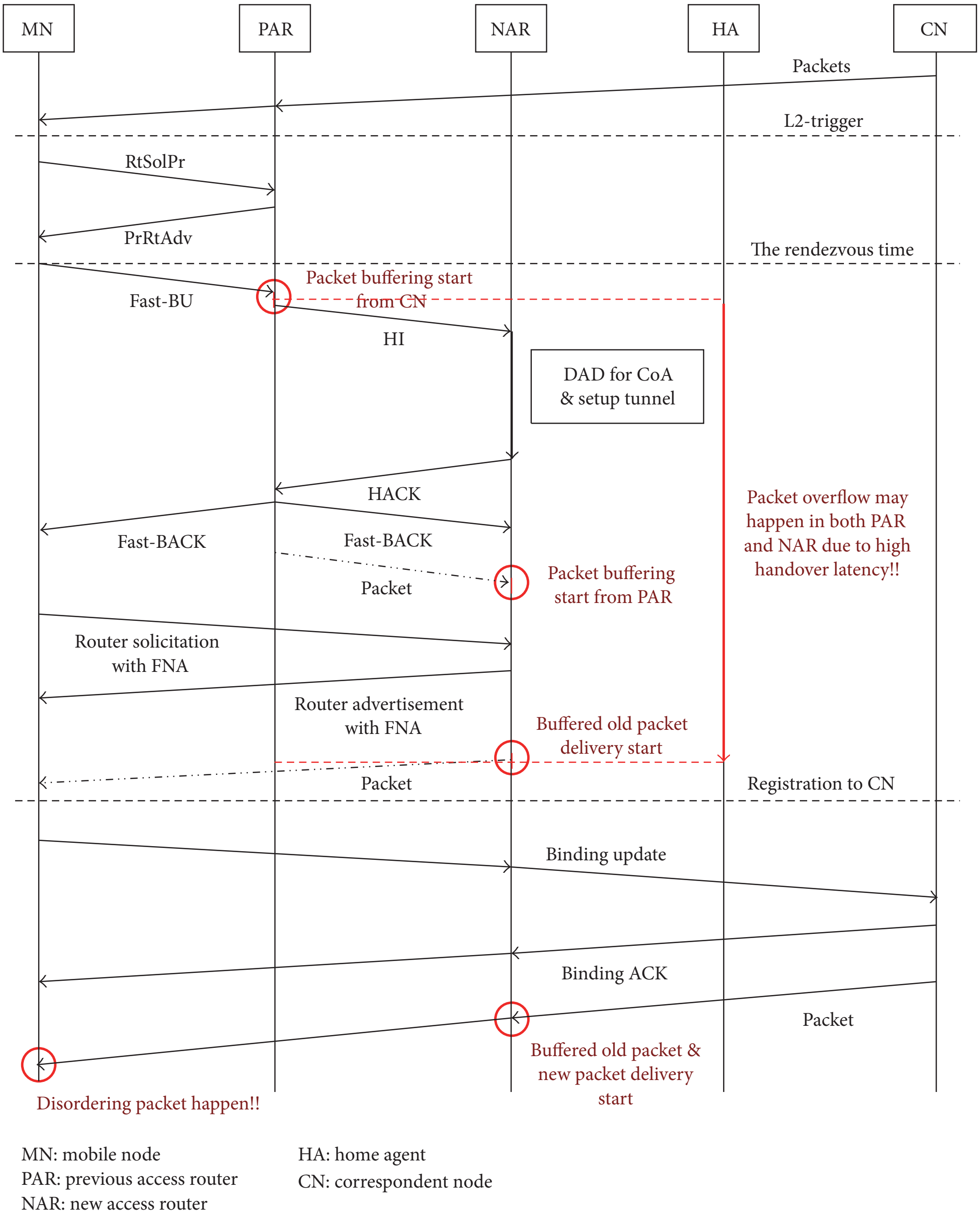
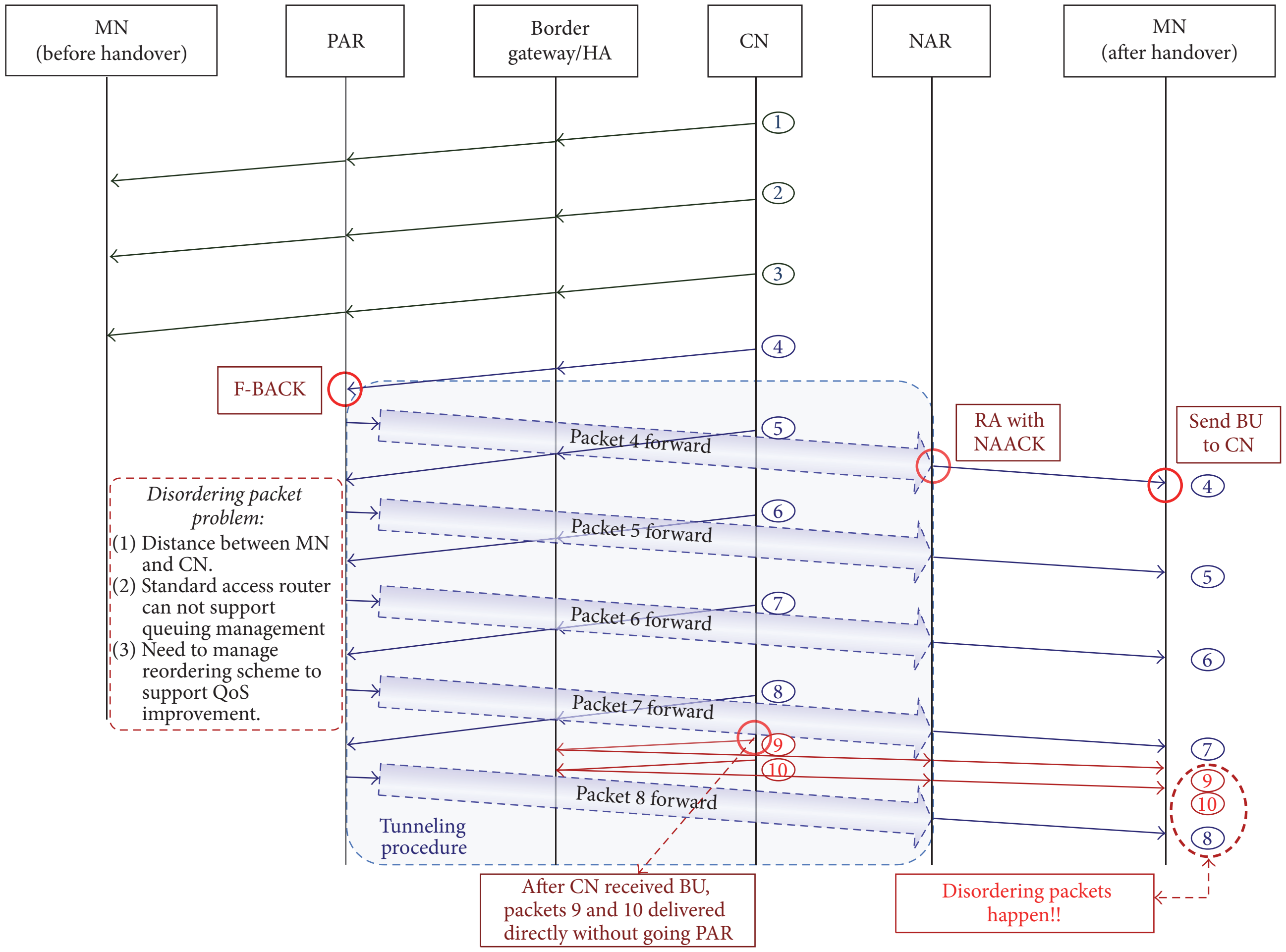

MN
PAR
NAR
HA
CN
Packets
L2-trigger
RtSolPr
PrRtAdv
The rendezvous time
Packet buffering start from CN
Fast-BU
HI
DAD for CoA & setup tunnel
Packet overflow may happen in both PAR and NAR due to high handover latency!!
HACK
Fast-BACK
Fast-BACK
Packet
Packet buffering start from PAR
Router solicitation with FNA
Router advertisement with FNA
Buffered old packet delivery start
Packet
Registration to CN
Binding update
Binding ACK
Packet
Buffered old packet & new packet delivery start
Disordering packet happen!!
MN: mobile node
PAR: previous access router
NAR: new access router
HA: home agent
CN: correspondent node

Figure 2: The IETF FMIPv6 handover procedure.

host route is being set up by the new access router (NAR) for the previous Care-of Address (PCoA) of the MN in response to the HA message and a Handover Acknowledge (HACK) message is sent as a reply. A Fast Binding Update (F-BU) should be sent by the MN preferably prior to its disconnection on its link whenever a PrRtAdv message is received. If the FBU message is received by the PAR, wherein the status code in the HACK message indicates, it is required to check if the new access router (NAR) has accepted the handover request. Then, the packets destined to the PCoA on the NAR will be forwarded by the PAR and a Fast Binding Acknowledgement (F-BACK) will be sent to the MN. The MN will then include a Fast Neighbor Advertisement (FNA) option to the Router Solicitation (RS) message that is sent to the new access router (NAR). On the other hand, the NAR includes a Neighbor Advertisement Acknowledgement (NAACK) option to the Router Advertisement (RA) message to be sent to the mobile node (MN). These two messages are exchanged after the link connectivity with the NAR has been changed. The NAR starts to deliver the buffered packets as soon as the NAR sends an RA message with the NAACK option. These buffered packets are delivered through the



Disordering packet problem:
(1) Distance between MN and CN.
(2) Standard access router can not support queuing management
(3) Need to manage reordering scheme to support QoS improvement.

After CN received BU, packets 9 and 10 delivered directly without going PAR

MN: mobile node
NAR: new access router
CN: correspondent node

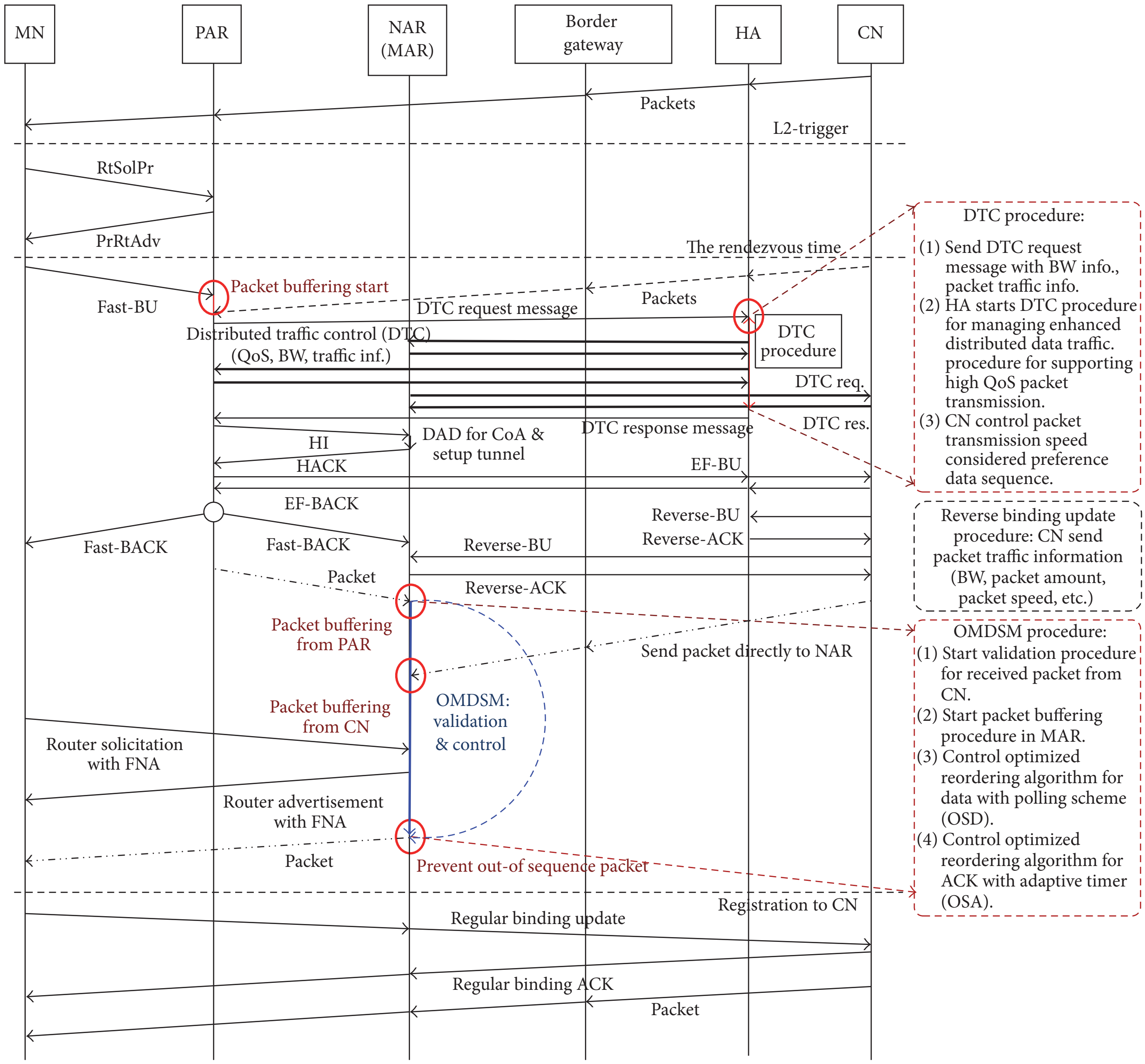
PAR: previous access router
HA: home agent

FIGURE 3: Disordering packet problem in FMIPv6.

bidirectional tunnel from the previous access router (PAR). The packets coming from the correspondent node (CN) are transmitted from the previous access router (PAR) to the new access router (NAR) through a bidirectional tunnel as soon as a binding update (BU) message is received by the CN [14, 15].

The CN can then forward the packets directly to the MN as soon as a BU message is received by the CN. Consequently, the disordered packets may be received by the MN, in the condition that the tunneled distance from the correspondent node (CN) to the new access router (NAR) through the previous access router (PAR) is farther compared to the distance from the correspondent node (CN) to the new access router (NAR). A disordered packet problem example is shown in Figure 3 [16, 17]. Based on the figure, packets four (4) through eight (8) are tunneled from the previous access router (PAR) to the new access router (NAR), wherein it is buffered until a router solicitation (RS) message with a fast neighbor advertisement (FNA) is delivered by the MN to the NAR as soon as an F-BU message is received by the PAR.

The packets nine (9) to ten (10) are sent by the CN to the NAR directly when a BU message from the MN is received by the CN. The new access router (NAR) buffers these packets until the mobile node (MN) receives a router advertisement (RA) with a NAACK option. The new access router (NAR) buffered packets will become disordered because of the packet delay time incurred by the tunneling, that is, whenever it utilizes a tunneling mechanism from the correspondent node (CN) going to the new access router (NAR) through the previous access router (PAR) which is measured to be farther as compared to the transmission from the correspondent node (CN) going to the new access router (NAR) without tunneling. Hence, duplicate ACK (DACK) occurs in the mobile node (MN) for packets seven (7) and eight (8) when an MN receives the disordered packets [18, 19].


MN
PAR
NAR (MAR)
Border gateway
HA
CN
Packets
L2-trigger
RtSolPr
PrRtAdv
The rendezvous time
Fast-BU
Packet buffering start
Packets
DTC request message
Distributed traffic control (DTC)
(QoS, BW, traffic inf.)
DTC procedure
DTC req.
DTC res.
DTC response message
HI
HACK
DAD for CoA & setup tunnel
EF-BU
EF-BACK
Reverse-BU
Reverse-ACK
Fast-BACK
Fast-BACK
Reverse-BU
Packet
Reverse-ACK
Packet buffering from PAR
Send packet directly to NAR
OMDSM: validation & control
Packet buffering from CN
Router solicitation with FNA
Router advertisement with FNA
Packet
Prevent out-of sequence packet
Registration to CN
Regular binding update
Regular binding ACK
Packet
DTC procedure:
(1) Send DTC request message with BW info., packet traffic info.
(2) HA starts DTC procedure for managing enhanced distributed data traffic. procedure for supporting high QoS packet transmission.
(3) CN control packet transmission speed considered preference data sequence.
Reverse binding update procedure: CN send packet traffic information (BW, packet amount, packet speed, etc.)
OMDSM procedure:
(1) Start validation procedure for received packet from CN.
(2) Start packet buffering procedure in MAR.
(3) Control optimized reordering algorithm for data with polling scheme (OSD).
(4) Control optimized reordering algorithm for ACK with adaptive timer (OSA).

MN: mobile node
PAR: previous access router
NAR: new access router/modified AR
HA: home agent
CN: correspondent node

Figure 4: OMDSM handover procedure.

3. OMDSM: Optimized Multimedia Data Streaming Management Algorithm with Traffic Distribution

The performance of TCP in both wired and wireless networks suffers from drawbacks of packet losses caused by bit-errors. This problem was assumed by the TCP sender to be caused by the congestion of the network traffic. Hence, the transmission window of the sender of the TCP is dropped and frequent timeouts occur resulting to a degraded throughput. In order to improve the performance of the TCP, the snoop protocol has been proposed while recovering the wireless errors locally in a wireless LAN environment [12, 20].

In this section, a new data traffic controller scheme is proposed to manage a packet flow which can support a reliable traffic QoS and multimedia packet realignment scheme to enhance the performance of TCP in IP-based wireless networks through the disordered packets elimination throughout the handover process. The proposed OMDSM handover procedure is shown in Figure 4. The model is

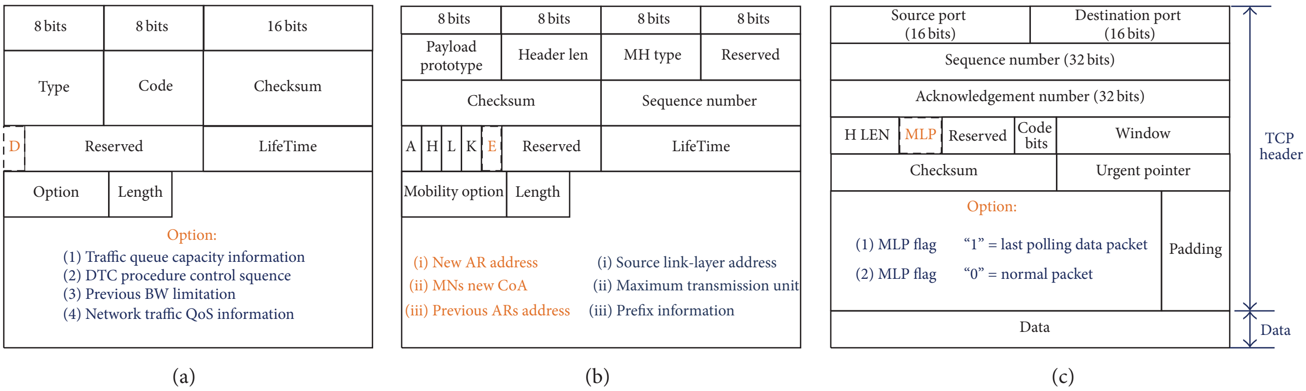


Figure 5: The DTC, EFBU, and MLP message formats: (a) DTC, (b) EFBU, and (c) MLP.

similar to the snoop protocol wherein a duplicate ACK (DACK) is prevented and the sequence of TCP data packets is controlled in the access point (AP).

However, link level snoop functions are only applied into the modified integrated access router. Also, the TCP packet transmission time structure is considered between the data packets and ACK packets which can prevent the disordering of packets using adaptive timer in the modified integrated access router called "MAR." The MAR with snoop agents consists of a controller, a buffer, traffic manager, and a sequence checker. In this article, a snoop agent is implemented with link level buffers in the modified access router (MAR) as specified by the snoop protocol causing the packets that are flowing through the wireless link to be cached. Thus, the unacknowledged packets retransmission can be avoided; hence, the unnecessary timeouts can be prevented. The duplicated packets can also be prevented through the filtering of acknowledgements that are copied. There are two main routines that allow these functions to be performed: the optimized snoop for data (OSD) and snoop for ACK (OSA).

3.1. Data Traffic Control (DTC) Reverse BU Control and Route Optimization.

During the movement detection, due to channel maintenance or L3 handover, the handover is performed by the mobile node (MN) to another access point (AP). The list of AP's L2 information will be the result of scanning performed by the MN. The MN sends the association request message with NAP's MAC address as soon as the comparison of previous AP (PAP) L2 power with new AP (NAP) L2 power is done. A scan will then be performed by the MN in order to see the APs through probes. The PAR immediately send a data traffic control (DTC) request message to HA and CN as soon as it receives the Fast-BU message from the MN. The HA broadcasts a DTC message which can support seamless traffic control to all neighboring access routers. In order to support a reliable data traffic distribution without packet interruption, an optional DTC traffic control procedure has been optimized. This can take place through the utilization of a 1-bit D-flag in the reserved field and notifying the node that follows the proposed scheme.

Table 1: The E-Flag of EF-BU message.

E-Flag	Mean
00	EF-BU message does not apply in the case of IEEE 802.
01	The MN's new CoA will be used.
10	Data packets must be sent to the MN's old CoA.
11	The standard BU message needs to be used.

This bit is named as "DTC Request bit (D bit)" wherein it contains four options, namely, "Traffic Capacity Option," "DTC Procedure Option," "Previous BW Limitation," and the "Network Traffic QoS address." Upon receiving a DTC message, ARs and CN can share traffic information with abutting ARs and save a certain period of time to its own buffer. Figure 5(a) shows the formats of the DTC message. The PAR sends a handover initiation (HI) message to the NAR in order to set up the tunnel as soon as the DTC message has been sent. In the proposed scheme, as soon as the establishment process of the bidirectional tunnel from the PAR to the NAR is done, a new enhanced fast binding update (EF-BU) [16] message will be sent by the PAR to the CN. This is done as soon as the MN starts moving in order to decrease the number of packets that are needed to be forwarded from PAR to the NAR. That is, the PAR sends quickly an EF-BU to the CN as soon as the tunnel between the PAR and NAR is setting up. This EF-BU message can be modified by adding a 2-bit E-flag to the reserved flag that includes the "New AR address" and "MNs New CoA" as options in the option field. The formats of the EF-BU message are shown in Figure 5(b) and the E-bits definitions are depicted in Table 1 [16]. The CN has to be operated by the E-bits whenever it receives and EF-BU message. As soon as the EF-BACK message was sent, the CN sends a reverse binding update (reverse-BU) message that include the CN's packet speed, BW, and packet processing priority information.

Each of the message exchanges in the OMDSM scheme is defined as follows:

(1) After receiving a Fast-BU, the PAR sends a DTC request message to HA. The HA starts the DTC procedure and the PAR buffers the packet addressed to PCoA.

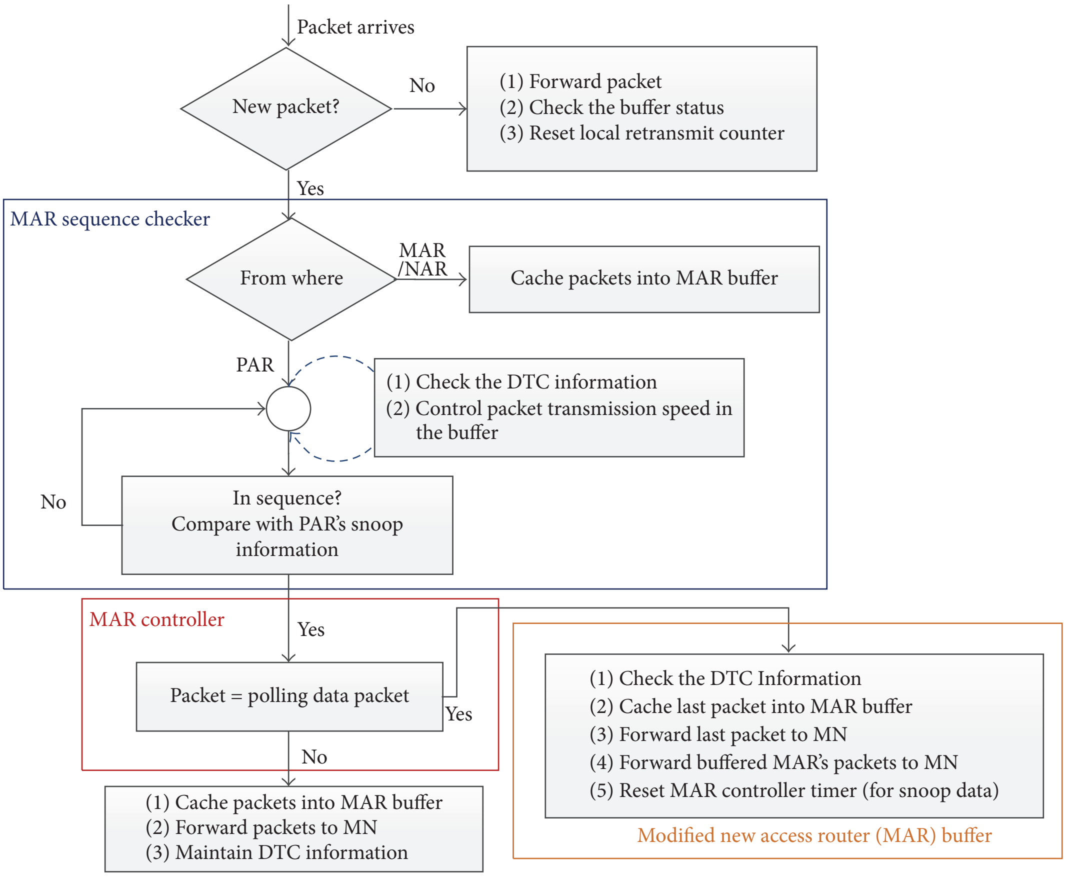

Packet arrives
New packet?
No
(1) Forward packet
(2) Check the buffer status
(3) Reset local retransmit counter
Yes
MAR sequence checker
From where
MAR /NAR
Cache packets into MAR buffer
PAR
(1) Check the DTC information
(2) Control packet transmission speed in the buffer
No
In sequence? Compare with PAR's snoop information
MAR controller
Yes
Packet = polling data packet
Yes
No
(1) Check the DTC Information
(2) Cache last packet into MAR buffer
(3) Forward last packet to MN
(4) Forward buffered MAR's packets to MN
(5) Reset MAR controller timer (for snoop data)
Modified new access router (MAR) buffer
(1) Cache packets into MAR buffer
(2) Forward packets to MN
(3) Maintain DTC information

FIGURE 6: The flow chart of optimized MAR snoop function for data (OSD).

(2) The HA sends the DTC information to all neighboring access routers (ARs).

(3) The PAR sends an EF-BU message after finishing the tunneling-path between PAR and NAR.

(4) The CN sends an EF-BACK message to the PAR. The CN then sends a modified TCP data packet after setting the MLP flag to "1."

(5) At the same time, the CN sends a reverse binding update message to HA and MAR. After the HA received the reverse binding update, it replies with a reverse binding acknowledgement to the CN.

(6) An F-BACK message is then sent by the PAR to the MN and NAR.

(7) The PAR starts to forward the buffered packets to the NAR with an adequate packet transmission speed using the DTC information.

(8) The NAR starts to check the received TCP data packet MLP flag. The MAR starts the OMDSM packet managing procedure which can supply the ordering sequence.

(9) The MN sends a router solicitation message to the NAR.

(10) The NAR sends back a router advertisement message to the MN.

(11) The CN send packets to the MN addressed to the NCoA.

(12) The NAR buffers the packets addressed to NCoA until getting the tunneled packet with an MLP flag "1."

(13) After receiving the last tunneled packet with MLP flag "1," the NAR deliver the buffered packets which came directly from the CN.

3.2. Optimized Realignment Algorithm for Data with Polling Scheme. The realignment algorithm flowchart for data to perform the proposed scheme is shown in Figure 6. Initially, during a handover, a handover initiation (HI) message that includes a snoop information of the previous access router (PAR) is sent in order for the sequence of the TCP packets to be controlled after the PAR has received an F-BU message. The remaining packets are directly sent by the correspondent node (CN) to the new access router (NAR) whenever it receives an EF-BU message. In addition, the CN also sends the last packet with a modified header to the PAR. The buffered packets are directed by the previous access router (PAR) to the new access router. It happens as soon as an F-BACK message is delivered by the previous access router (PAR) going to both the new access router (NAR) and the mobile node (MN). The format of the TCP packet with MLP flag is depicted in Figure 5(c). An MLP flag bit can be added

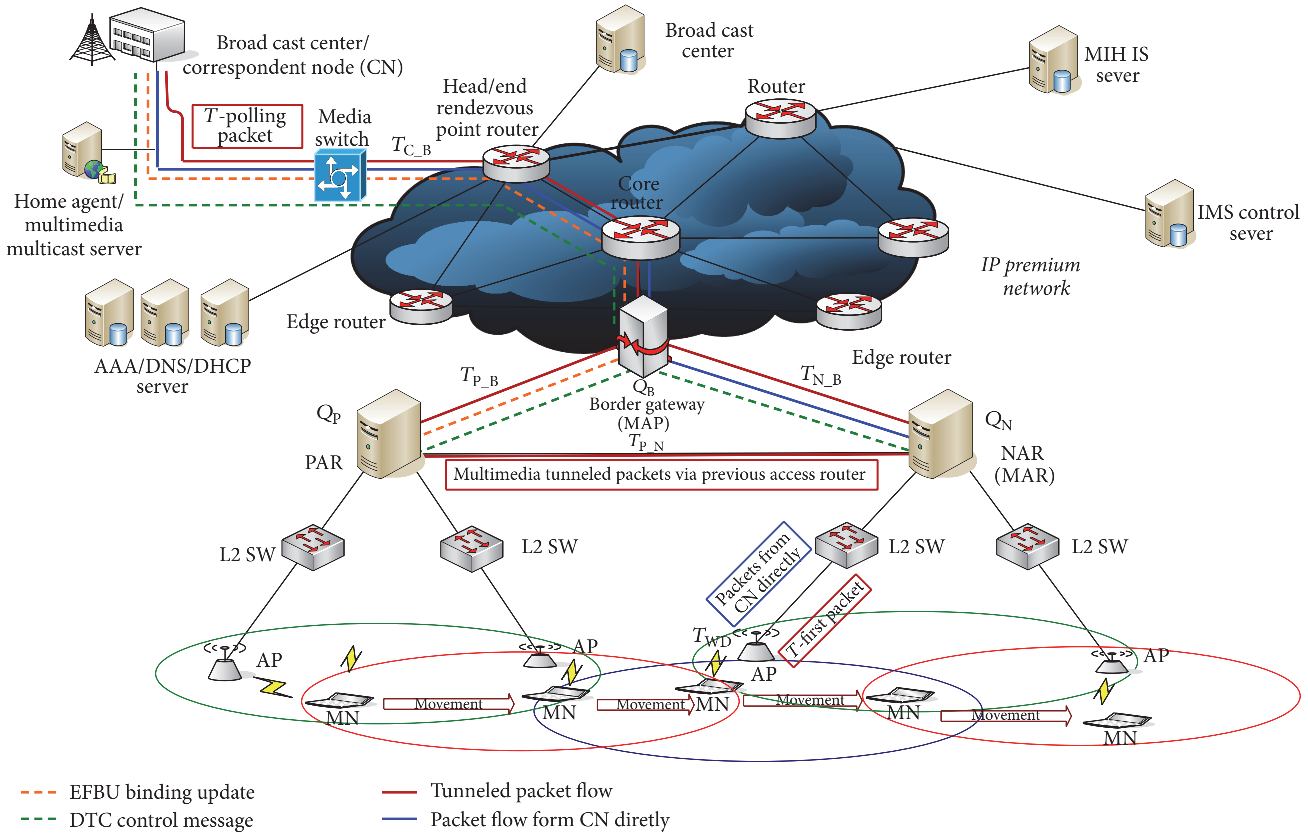


Figure 7: The packet transmission during handover in OMDSM.

to modify the TCP packet reserve field in the TCP header in order for the last packet to be distinguished from all of the TCP packets coming from the new access router (NAR). The last packet that is modified is called the MLP.

Thus, the option field in the TCP packet will be utilized. If the MLP flag is set to "0," then the packet acts as a normal packet. On the other hand, if the MLP flag is set to "1," then the packet is acting as the polling data packet that originates from the previous access router (PAR). Whenever the CN receives an EF-BU message from the PAR, the last data packet as well as a polling data packet is simultaneously sent to the NAR. The polling data packet acts as a control message to the MN signaling where no more tunneled packets exist. The PAR can then remove the MN's information as soon as it receives this polling message. A new data packet can be sent without the tunneling process by the correspondent node (CN) going to the new access router (NAR) after it has sent a polling data packet. At first, the PAR's snoop information that is included in the HI message will be used by the MAR sequence checker for determining whether the packet that is received comes from either of the previous access routers (PAR) of the new access router (NAR). That is, the snoop information about the PAR is included in the HI message whenever it is sent by the PAR to the NAR. Then, the MAR controller starts checking for the MLP flag, that is, to check whether the arriving packets are received in a correct sequence. The MLP flag is essentially important in distinguishing between packets delivered through tunneling from the PAR and those packets that are directly delivered from the CN without tunneling. The MAR buffers the packets that are directly transmitted by the CN until the NAR receives the MLP with the flag bit that is set to "1." The packet transmission network architecture during a handover in OMDSM scheme is shown in Figure 7. As depicted in Figure 7, the packets that are sent directly from the CN to NAR are cached in the MAR's buffer after the CN has received the EF-BU message from the PAR. Thus, the data packet buffering time T_{PBT} is the time required for the previous access router (PAR) to finish the transfer of packets to the new access router (NAR) [17]. T_{PBT} is represented by

$$T_{\mathrm{PBT}} = \left| T_{\text{First-packet}} - T_{\text{polling-data-packet}} \right|, \qquad (1)$$

where $T_{\text{First-packet}}$ indicates the time of the delivery of the first packet and $T_{\text{polling-data-packet}}$ defines the time for the delivery of the polling data packet through tunneling between the previous access router (PAR) going to the new access router (NAR). During T_{PBT}, only the received packets through tunneling mechanism by the previous access router (PAR) are then directed to the mobile node (MN). During this process, the waiting time, T_{PBT}, is calculated by the MAR controller until the polling data packet has arrived. It is assumed in this article that, during T_{PBT}, the modified access router (MAR) buffer size is enough for buffering packets that are directly received from the correspondent node (CN). As soon as T_{PBT} expires, the buffered packets will be delivered continuously

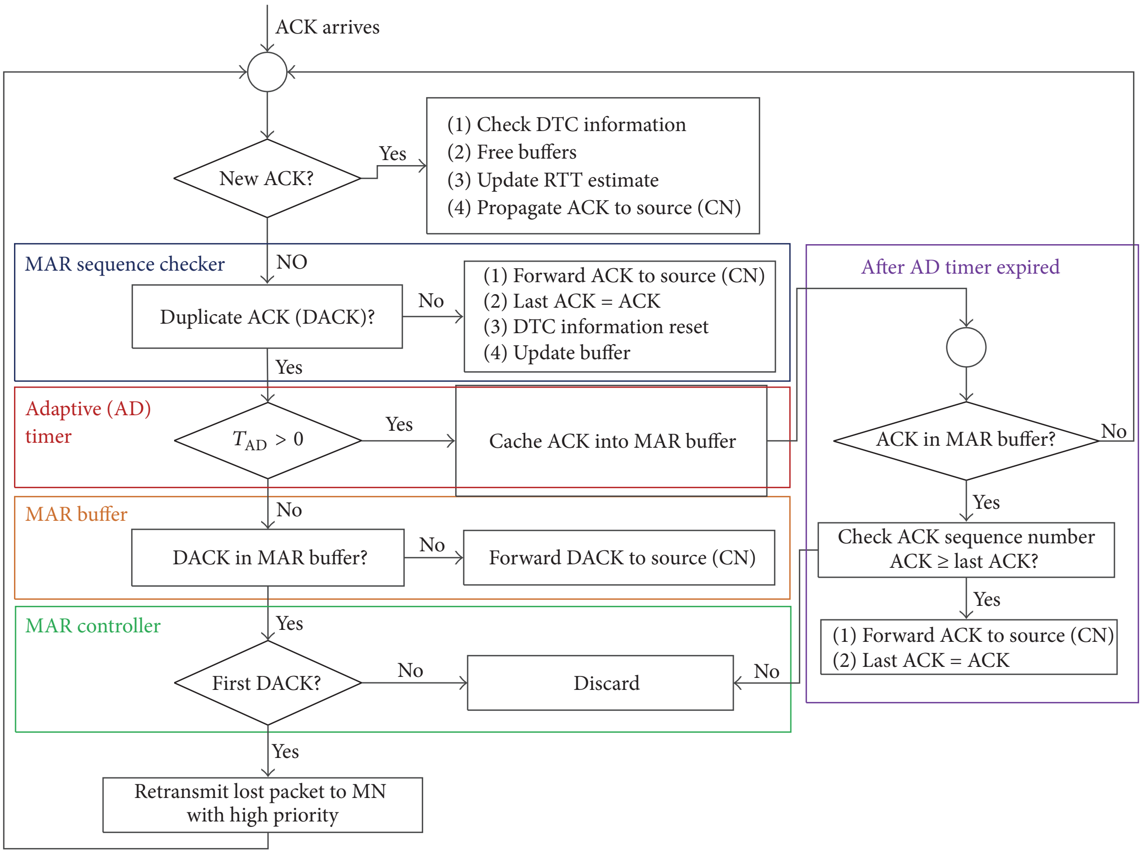


FIGURE 8: The flow chart of optimized MAR snoop function for ACK.

by the MAR buffer to the MN. Moreover, the NAR can periodically send control messages for notifying the buffer states to the CN or HA in order to prevent packet overflow in the MAR buffer. The CN or the MN can then control the data traffic by utilizing these messages. The NAR buffer is constructed with nonpriority First-In-First-Out.

3.3. Optimized Realignment Algorithm for ACK with Adaptive Timer. The realignment algorithm flowchart for ACK to achieve the proposed scheme is depicted in Figure 8. The MN sends ACKs whenever it received data packets from the NAR. These ACKs are processed by the MAR sequence checker in order to see whether the received ACKs are duplicates or not. The ACK is forwarded to the CN if there is no occurrence of duplication of an ACK. That is, this ACK acts as the final ACK. On the other hand, if duplication has occurred, the optimized snoop for ACK (OSA) algorithm will be processed by a snoop agent for the ACK in order to accommodate the disordered packets through delaying the ACK segment processing. An adaptive timer (AD) to delay the ACKs will be used to prevent TCP performance degradation due to DACK. The adaptive delay is denoted by T_{AD}, which is defined as the time required postponing ACKs during the schedule time. T_{AD} is derived by

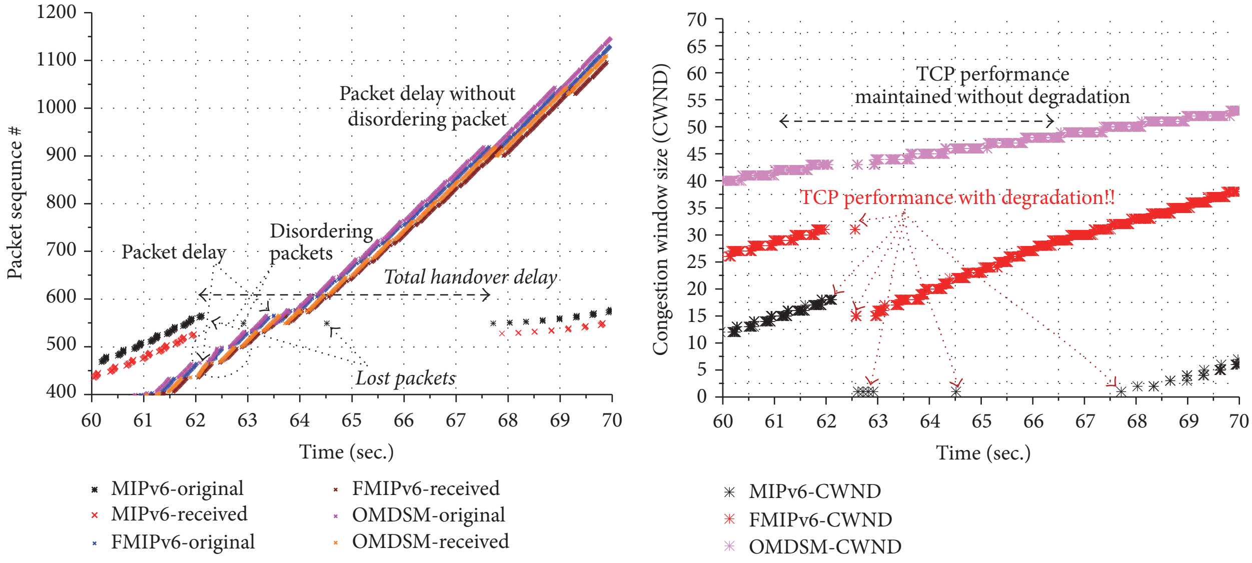
$$T_{\mathrm{AD}} = \max\left(T_{\mathrm{S\_PN}} \;\&\; T_{\mathrm{OSP}}\right), \qquad (2)$$

where $T_{\mathrm{S\_PN}}$ is the snoop information transmission delay between the PAR and NAR via the border gateway (BG). The time period in which disordered packets can arrive during a handover is defined by T_{OSP}. As shown in Figure 7, the packet transmission delay between a CN and a BG is denoted by $T_{\mathrm{C\_B}}$. $T_{\mathrm{P\_B}}$ and $T_{\mathrm{N\_B}}$ denote the packet transmission delay between the BG and the PAR and NAR. T_{WD} denotes the wireless transmission delay. Q_{B} is the queuing delay in the BG whereas Q_{P} and Q_{N} are the queuing delay in the PAR and NAR, respectively. The packet transmission delay between the PAR and NAR is denoted by $T_{\mathrm{P\_N}}$ where tunneling is used. Thus, $T_{\mathrm{P\_N}}$ is denoted by

$$T_{\mathrm{P\_N}} = T_{\mathrm{P\_B}} + T_{\mathrm{N\_B}} + Q_{\mathrm{B}}. \qquad (3)$$

T_{OSP} denotes the difference between the delay times of a normal packet that is directly transmitted by the correspondent node (CN) to the new access router through the BG and a polling packet transmitted by the CN via tunneling from the PAR to the NAR via the BG. Thus, the distance between the BG and the PAR affects T_{OSP}. The polling packet transmission delay through the previous access router (PAR), that is, from the correspondent node (CN) going to the new access router (NAR), is denoted as $T_{\text{D-Tunneling}}$ in order to calculate T_{OSP}. Thus, $T_{\text{D-Tunneling}}$ is derived by

$$T_{\text{D-Tunneling}} = T_{\mathrm{C\_B}} + Q_{\mathrm{B}} + T_{\mathrm{P\_B}} + Q_{\mathrm{P}} + T_{\mathrm{P\_N}}. \qquad (4)$$



(a)

(b)

Figure 9: The packet transmission performance comparisons: (a) handover latency comparisons; (b) TCP performance comparisons.

Also, the packet transmission delay from the CN to the NAR directly via the BG is denoted as $T_{\text{D-Direct}}$. $T_{\text{D-Direct}}$ is represented by

$$T_{\text{D-Direct}} = T_{\text{C\_B}} + Q_{\text{B}} + T_{\text{N\_B}}. \tag{5}$$

Thus, T_{OSP} can be described as follows:

$$\begin{aligned} T_{\text{OSP}} &= T_{\text{D-Tunneling}} - T_{\text{D-Direct}} \\ &= \left(T_{\text{C\_B}} + Q_{\text{B}} + T_{\text{P\_B}} + Q_{\text{P}} + T_{\text{P\_N}}\right) \\ &\quad - \left(T_{\text{C\_B}} + Q_{\text{B}} + T_{\text{N\_B}}\right) \\ &= \left(T_{\text{P\_B}} + Q_{\text{P}} + T_{\text{P\_N}} - T_{\text{N\_B}}\right). \end{aligned} \tag{6}$$

Therefore, the duplicated ACK problem can be solved through delaying the ACKs during T_{AD}. The delayed ACKs of the content in the temporary buffer are transmitted by the MAR to the CN after T_{AD}. That is, the NAR sends the stored ACKs to the CN by arranging the ACK packets with respect to the transmission order after the NAR waits a maximum time between $T_{\text{S\_PN}}$ and T_{OSP}, if the adaptive timer has expired.

A snoop agent tries to find a duplicated ACK (DACK) in the MAR buffer if the adaptive timer has a value of less than 0. As soon as the DACK has been found, the MAR controller then determines whether it is the first DACK or not. Consequently, in order to prevent the retransmission of packets from the CN that would be detrimental to the performance of TCP in Mobile IPv6 networks, the proposed OMDSM algorithm keeps the data transmission and ACK transmission in sequence.

4. Performance Evaluation and Comparisons

In this section, the performance of the proposed scheme is evaluated using the Network Simulator (NS). The experiments are performed utilizing the simulation code that is created through the INRIA/Motorola MIPv6 code which is based on the standard Network Simulator distribution version. Two main modules have been extended with these codes: first, a data realignment algorithm and an ACK realignment algorithm that utilizes an optimized snoop protocol. It is assumed that, during the L2 handover, the DTC procedure, EF-BU, and reverse-BU procedures would be processed. That is, the DTC and BU processing time during total handover latency can be neglected. The OSDSM packet management processing requires a very short period, so, it can be ignored in the total handover latency. That is because the packet management algorithm in the router is very fast which is about 120 ηsec in the worst case [21, 22]. The original release of the code has been extended to enable it to work with two or more mobile nodes. Wired links with available bandwidths and link delays were used for the simulation network. The binding between the correspondent node and the mobile node allows the bulk data transfer, that is, by file transfer protocol. In the simulation, it is required that the size of the buffer needs to be predetermined in order to know if it is enough to cache the packets that are received directly from the correspondent node, thus, packet overflow can be prevented. The sequence number of the TCP data that are received considering its simulation time within the MIPv6, FMIPv6, and OMDSM are shown in Figure 9. It is depicted in Figure 9(a) that, during the handover between access routers, before the MN can send a binding update to the home agent (HA), some packets may have been dropped caused by route disconnection wherein it requires packet retransmission in Mobile IPv6. The congestion window size (CWND) in MIPv6 between ARs is shown in Figure 9(b). Continuous data packet losses abruptly reduce the CWND after the handover between ARs. Therefore, multiple TCP timeouts can occur if the handover latency is excessively high which causes the TCP performance degradation in MIPv6.

In FMIPv6, the figure shows the packet transmission during the handover that includes the buffering of packets between the new access router (NAR) and the previous access router (PAR). The received packets through tunneling mechanism and those that are directly sent from the correspondent node cause the disordering of packets that can be received by the mobile node even though packet loss does not happen. Thus, sending a DACK message to the CN resulted from the disordering of packets problem which leads to decrease in TCP performance. In FMIPv6's CWND between ARs, packet disruption did not occur during the handover between ARs. Nevertheless, due to the tunneling mechanism between the previous access router and the new access router, the sender is required to retransmit the packets that are delayed right after the same ACK was received three times coming from the mobile node. The CWND has been reduced by these packet retransmissions which have caused a lot of data packets to wait for a higher CWND. This is caused by the FMIPv6 handover procedure since tunneling of packets causes longer time delays leading to packet retransmissions. In OMDSM scheme, it is shown that the receiver accepts the packets normally although there is an occurrence of packet delay that is caused by traffic management in MAR; thus, the disordering of packets problem as well as packet losses can be avoided and will not require for retransmission. Therefore, the OMDSM scheme can improve the packet transmission QoS despite a slight packet transmission delay that might happen. A minor packet delay can be allowed by the OMDSM scheme which manages the data streaming in total transmission time. Thus, the congestion window size value of the sender is sustained; hence, it enhances the TCP performance. Accordingly, as compared to alternative approaches, the OMDSM scheme has achieved prominent results which can support a remarkable data streaming management without packet losses, long time packet transmission delay, and disordering of packets.

5. Conclusions

This paper introduced an optimized multimedia data streaming management algorithm in IP-based wireless/mobile networks during handover for multimedia data streaming for location-based mobile marketing applications within the Internet of Things (IoT) environment. The impact of handovers between access routers (ARs) has been analyzed for disordering of packets under the MIPv6 in a fast handover environment. The proposed OMDSM scheme shows that it can improve the TCP performance and prevent the packet disordering problem in the existing IP-based mobility management protocols. The simulation results show that the OMDSM scheme has a better performance as compared with the conventional protocols. Also, it is found out to be working satisfactorily in fast handover situations in IoT applications. In addition, a seamless multimedia streaming can be supported with the right sequence of packets with the integration of the OMDSM scheme for location-based mobile marketing applications in an IoT environment.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This research was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Science, ICT, and future Planning (2015R1A2A2A03002851).

References

[1] V. Tsaotissidis, "Open issues on TCP for mobile computing," *Journal of Wireless Communication and Mobile Computing*, vol. 1, no. 2, 2002.

[2] S. J. Vaughan-Nichols, "Mobile IPv6 and the future of wireless Internet access," *IEEE Computer*, vol. 36, no. 2, pp. 18–20, 2003.

[3] G. Al-Gadi, A. Babiker, and N. Mustafa, "Comparison between IPv4 and IPv6 using OPNET simulator," *IOSR Journal of Engineering*, vol. 4, no. 8, pp. 44–50, 2014.

[4] D. B. Johnson, C. E. Perkins, and J. Arkko, "Mobility support in IPv6," RFC 3775, IETF, 2004.

[5] A. J. Jabir, S. Shamala, Z. Zuriati, and N. Hamid, "A comprehensive survey of the current trends and extensions for the proxy mobile IPv6 protocol," *IEEE Systems Journal*, pp. 1–17, 2015.

[6] A. Moravejosharieh and H. Modares, "A proxy MIPv6 handover scheme for vehicular ad-hoc networks," *Wireless Personal Communications*, vol. 75, no. 1, pp. 609–626, 2014.

[7] F. Li, X. Wang, T. Pan, and J. Yang, "Packet delay, loss and reordering in IPv6 world: a case study," in *Proceedings of the International Conference on Computing, Networking and Communications (ICNC '16)*, pp. 1–6, February 2016.

[8] R. Koodli, "Fast handovers for mobile IPv6," RFC 4068, 2005.

[9] D. Lee, C. Oh, S. Lee, J. Park, and K. Kim, "Design and analysis of the mobile agent preventing out-of-sequence," in *Proceedings of the International Conference on Information Networking (ICOIN '99)*, Tokyo, Japan, January 1999.

[10] D. S. Eom, M. Sugano, M. Murata, and H. Miyahara, "Performance improvement by packet buffering in mobile IP based networks," *IEICE Transactions on Communications*, vol. 83, no. 11, pp. 2501–2512, 2000.

[11] D. Lee, G. Hwang, and O. Changhwan, "Performance enhancement of mobile IP by reducing out-of-sequence packets using priority scheduling," in *Proceedings of the APCC*, pp. 513–516, November 2001.

[12] H. Balakrishnan, V. N. Padmanabhan, S. Seshan, and R. H. Katz, "A comparison of mechanisms for improving TCP performance over wireless links," *IEEE/ACM Transactions on Networking*, vol. 5, no. 6, pp. 756–769, 1997.

[13] J. Gu, "The adaptive header compression algorithm of mobile IPv6 Network," *Lecture Notes in Electrical Engineering*, vol. 238, pp. 1603–1610, 2014.

[14] A. K. Barbudhe, V. K. Barbudhe, and C. Dhawale, "Comparative analysis of security mechanism of mobile IPv6 threats against binding update, Route Optimization and Tunneling," in *Proceedings of the 6th IEEE International Conference on Adaptive Science and Technology (ICAST '14)*, 7, 1 pages, October 2014.

[15] A. Dhamdhere, M. Luckie, B. Huffaker, K. Claffy, A. Elmokashfi, and E. Aben, "Measuring the deployment of IPv6: topology, routing and performance," in *Proceedings of the ACM Internet Measurement Conference (IMC '12)*, pp. 537–550, Boston, Mass, USA, November 2012.

[16] B. J. Park, H. In, and H. A. Latchman, "An approach to efficient and reliable media streaming scheme," in *Proceedings*

of the IEEE International Symposium on Broadband Multimedia Systems and Broadcasting (IEEE ISBMSB '06), April 2006.

[17] B. J. Park and H. A. Latchman, "Performance enhancement of fast handover for MIPv6 by reducing out-of-sequence packets," *Wireless Personal Communications*, vol. 47, no. 2, pp. 207–217, 2008.

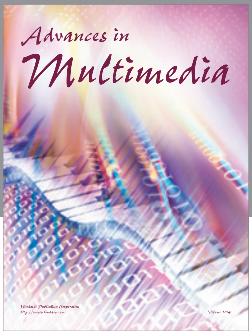
[18] A. K. Quoc, D. S. Kim, and H. Choo, "A novel scheme for preventing out-of-order packets in fast handover for Proxy Mobile IPv6," in *Proceedings of the 28th International Conference on Information Networking (ICOIN '14)*, pp. 422–427, February 2014.

[19] N. Kwon, H. Kim, S. Oh, and H. Choo, "Fast handover scheme based on mobility management of head MAG in PMIPv6," in *Computational Science and Its Applications—ICCSA 2011*, vol. 6786 of *Lecture Notes in Computer Science*, pp. 181–193, Springer, 2011.

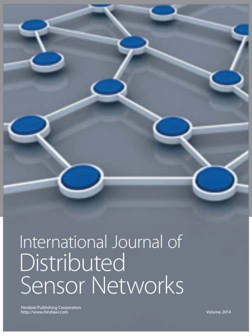
[20] I. Al-Surmi, M. Othman, N. A. W. A. Hamid, and B. M. Ali, "Latency low handover mechanism considering data traffic lost preventing for proxy mobile IPv6 over WLAN," *Wireless Personal Communications*, vol. 70, no. 1, pp. 459–499, 2013.

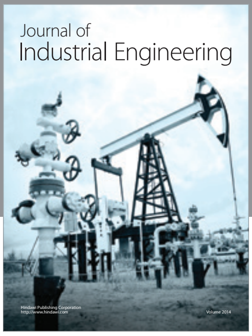
[21] V. Srinivasan and G. Varghese, "Fast address lookups using controlled prefix expansion," *ACM Transactions on Computer Systems*, vol. 17, no. 1, pp. 1–40, 1999.

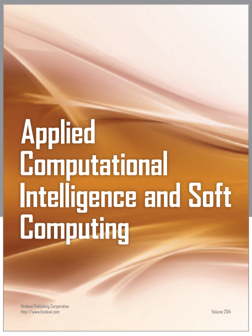
[22] R. Kawabe, S. Ata, M. Murata, M. Uga, K. Shiomoto, and N. Yamanaka, "On performance prediction of address lookup algorithms of IP routers through simulation and analysis techniques," in *Proceedings of the International Conference on Communications (ICC '02)*, pp. 2146–2151, May 2002.

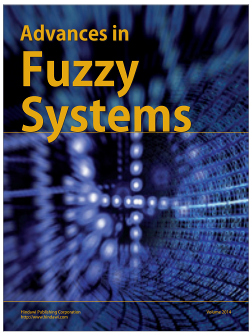

Advances in
Multimedia

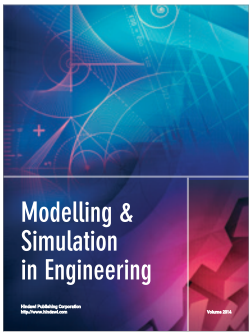
The Scientific
World Journal

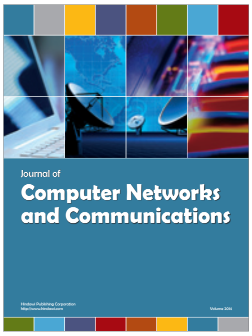

International Journal of
Distributed
Sensor Networks

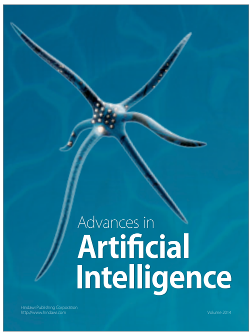

Journal of
Industrial Engineering

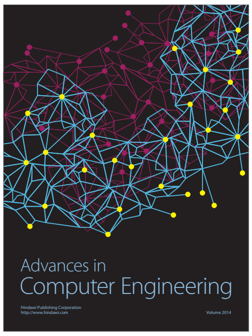

Applied
Computational
Intelligence and Soft
Computing


Advances in
Fuzzy
Systems

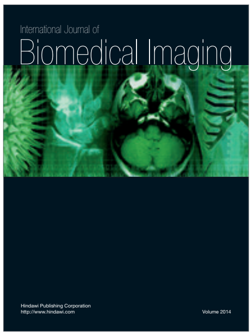

Modelling &
Simulation
in Engineering

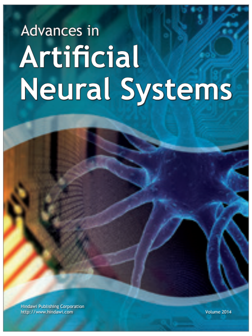

Journal of
Computer Networks
and Communications

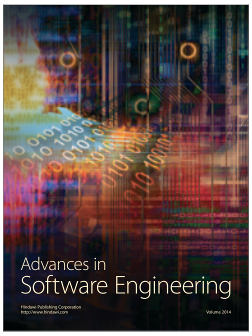

Advances in
Artificial
Intelligence


Advances in
Computer Engineering

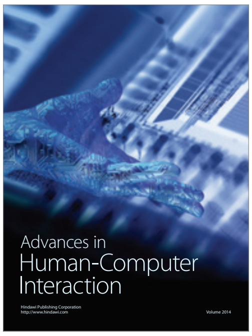
International Journal of
Computer Games
Technology

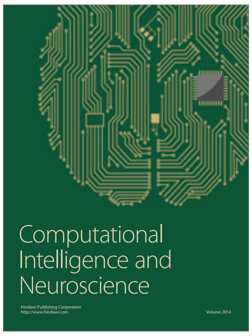

International Journal of
Biomedical Imaging


Advances in
Artificial
Neural Systems


Advances in
Software Engineering

Journal of
Robotics


Advances in
Human-Computer
Interaction


Computational
Intelligence and
Neuroscience

International Journal of
Reconfigurable
Computing

Journal of
Electrical and Computer
Engineering