

New Mobility Management Mechanism for Delivering Packets with Non-Encapsulation

Myoung Ju Yu * and Seong Gon Choi *

*College of Electrical & Computer Engineering, Chungbuk National University, 410 Seongbong-ro, Heungdeok-gu, Cheongju, Chungbuk 361-763, South Korea

mjyu@cbnu.ac.kr, sgchoi@cbnu.ac.kr

Abstract— This paper proposes a new mobility management mechanism delivering packets without any encapsulation as well as supporting session continuity. In the proposed scheme, each communicating node performs address translation which changes the destination address of IP packets for packet delivery with non-encapsulation. The proposed scheme can decrease the delay and increase the speed of packet transmission.

Keywords—Mobility Management, Packet Delivery, Non-Encapsulation, Address Translation

I. INTRODUCTION

Nowadays, a variety of studies for mobility support have been progressed with the increasing demand for seamless service in Next Generation Network (NGN) [1].

The IETF has studied various mobility solutions including Mobile IP (MIP). The MIP is a well-known IP mobility protocol. However, it has several problems such as long handover latency, high packet loss and signaling overhead.

The MIP uses the encapsulation approach to the indirect routing. The encapsulation process itself will increase the transmission delay, and the process of encapsulation of the sending packet will enlarge its size, and then the speed of communication process will be decreased based on the enlarged size of the new packet sent from the Home Agent (HA). In addition, the de-encapsulation process will need a time to return the new packet to its original structure in which this process will also increase the delay of the communication process [2]. So, it needs more study to solve the above-mentioned problem.

Therefore, we propose a new mobility management mechanism which delivers packets without any encapsulation as well as supports session continuity to solve the problems caused by the encapsulation process.

II. RELATED WORKS

This section describes the related works regarding packet transmission mechanism with non-encapsulation. We introduce each procedure for packet delivery in [3]-[6].

A. IP Mobility with High Speed Access and Network Intelligence [3]

[3] proposes an architecture for network layer mobility support, using a network-based mobility manager, termed as

network server or gateway. There are three basic features in the proposed architecture. There is a network server/gateway (GW) for location update and IP mobility support. For simplicity, it is assumed that the server functionality is integrated in the GW. The GW has all the intelligence needed for the mobility management, including address translation and mapping. All the APs are pre-provisioned with the server in the network before the operation. The GW knows the list of IP addresses of all APs for a given service provider's network. The GW will maintain a table for location management and routing, where each entry is identified by the tuple: <permanent MN address, home AP address, new AP address, association life time>. The server can consult a database, connected via the high speed backbone network, for any address resolution or any other needs such as authentication, security and billing.

Compared to the MIP tunnelling, the proposed architecture has straight forward routing and reduced payload size without any IP-in-IP, unlike MIP. It is also envisioned that the network based solution operates at multi-gigabit speeds and the packet re-directional functionality is implemented with the server's traffic discrimination capability.

When the MN moves to the new AP while it is connected to the network, it initiates the handover by sending a route update message. The GW updates the routing table reflecting the move for MN. The GW may inform the home AP about the move. All packets from now on are sent to the new AP which in turn forwards these packets to the MN. The GW updates the routing table when the association time has expired for the visiting MN.

B. Indirect Routing of Mobile IP: A Non-Encapsulation Approach [4]

[4] proposes the non-encapsulation approach to the indirect routing. Using the proposed approach, when the MN moves from its own network to another network, MN receives an ICMP advertisement message that contains a CoA and new field which called flags.

MN after receiving its new address (CoA) must register CoA in its home agent. It sends a registration request message to the foreign agent, FA binds mobile permanent address to the new CoA which already given to MN in its own table.

Then FA forwards a registration request message to the HA which has the original MN. The HA receives a registration request message, then updates its own addressing table by binding the CoA to mobile permanent address (MA) of a particular MS. The HA sends a registration response message to the FA, and then the FA forwards a registration response message to the MN. In this registration process, the encapsulation format is ignored in all steps. This approach will save the time of registration process and decrease the processing delay in all parties of the registration process.

When the MN is currently located in a foreign network, the correspondent node sends a packet to the HA where the destination IP address of the sent packet is a MA. The HA receives the packet and checks its addressing table to identify the current temporary IP address (CoA) of the MN. Furthermore, the HA perform a header processing by coping all fields along with the data as it is except the destination IP address filed which must be change to be the CoA instead of MA.

The HA forwards the processed packet to the FA. When the FA received the packet, it will forward it directly to the MN since no need to any further header translation. The MN receives the packet which has the CoA as its destination address, and it will recognize that this packet is sent to its attention. If it is required, the MN will send a reply message to the CN, the source IP address of the reply message is MA and the destination IP address is CN.

C. AMP-A Indirect Routing of Mobile IP: A Non-Encapsulation Approach [5]

The key distinguishing features of AMP include an agent-based hierarchical architecture, the absence of encapsulation and tunnelling, direct-mode of packet delivery without re-routing, application-layer transparency, buffering of packets to mitigate packet loss, and a network-centric tracking mechanism for movement detection.

The mechanism for IP-based delivery to a MN located in a visited access network is described. In this case, it is assumed that a MN has been successfully registered in a visited access network and another host located in another domain initiates correspondence to the MN. In order to facilitate packet delivery from the CN to the MN, the access network needs to ascertain the current valid IP address of the MN.

A CN sends a datagram to the MN using the using IP as the destination address and this datagram is received at its AR-CN. Before delivering the datagram to MN's IP address, however, the registrar agent of the CN sends a location request query message to MN's home registrar agent. This is done based on the IP address of the MN. The MN's home registrar receives the query message, and does an address lookup in its database, and finds an entry. A location response message is sent by the MN's home registrar to the CN's registrar, with the required mapping. The MN's home registrar also enters the CN's registrar into its database as a CN to MN. The CN's registrar makes an entry for the current location of MN in its database, and creates a new IP header datagram with source address IP-CN, and destination address IP-CoA, but with the same

payload for MN. This datagram and subsequent datagrams destined for MN will be sent using IP-CoA as the destination address. Unlike MIP, AMP does not use any encapsulation, and for security reasons, CN never knows the location of MN.

D. Non-Encapsulation Mobile IP [6]

A method is provided of directing and IP packet to a MN. The MN has a home addressing in a home network and is temporarily connectable in foreign network having a FA. The IP packet has a header portion including the destination address to which the IP packet is to be sent. The method comprises the steps of: receiving, in the home network, the IP packet including a destination address corresponding to the HoA of the MN; modifying the IP packet by removing the HoA of the MN from the header portion of the IP packet and replacing it with the FA CoA, and appending a MN identifier to the IP packet, and transmitting the modified IP packet.

Thus [6] provides a method of directing an IP packet to a MN, the MN having a HoA is a home network and being temporarily connectable in a foreign network having a FA, the IP packet having a header portion including the destination address to which the IP packet is to be sent, the method comprising the steps of; receiving, in the home network, the IP packet including a destination address corresponding to the HoA of the MN; modifying the IP packet by; removing the HoA of the MN from the header portion of the IP packet and replacing it with the FA CoA; appending a MN identifier to the IP packet; and transmitting the modified IP packet.

The technique maintains the necessary routing information to enable IP packets addressed to a MN in a home network to be forwarded to the current CoA of the MN in a foreign network, but at the same time maintains the flow identification information requested by the originator of the IP packet visible to all routing switches between home network and the foreign network, as well as between the originator and the home network.

Advantageously, [6] provides a tunnelling technique where the simplicity of the header of the original IP packet is maintained, and the length of the new IP packet is minimised. This contrasts favourably with prior techniques where the length of the IP packet is significantly extended. [6] thus provides a simpler and shorter processing overhead than conventional techniques.

The non-encapsulation MIP technique of [6] also increases transmission efficiency. This is particularly important in real-time multi-media applications, such as audio and video, which usually feature short but fast data packets. As a result it dramatically reduces the concern of using MIP to support wireless/mobile multimedia services.

III. NEW MOBILITY MANAGEMENT WITH NON-ENCAPSULATION

In this section, we introduce the proposed mobility management mechanism supporting packet transmission with non-encapsulation. Fig. 1 shows the network configuration of the proposed scheme.

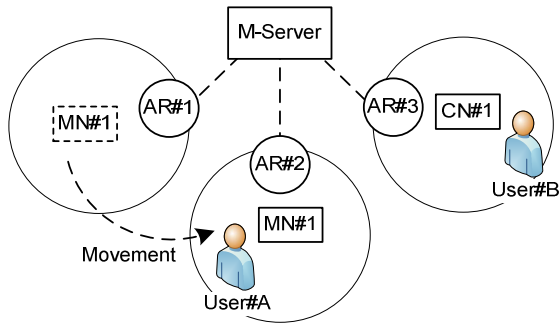


Figure 1. Network Configuration of the Proposed Scheme

The M-server manages all related binding information on an MN to support mobility. For this, the M-server has Mobility Server Binding Information Table (MSBIT), and manages an ID (i.e. physical ID and service ID), Permanent Address, Temporary Address (TA) and the mapping relation with its Corresponding Node (CN). Also, the M-server can function as Domain Name Server (DNS). So, it may inform an MN of the current location of a CN according to the request from the MN.

The AR is a network entity connected with a MN initially. It does not need to perform the encapsulation process as this way does not use tunneling for packet transmission.

The MN performs address translation to deliver packet without any encapsulation. For this, the MN has Terminal Binding Information Table (TBIT), and manages new address (i.e. TA) of MN or CN changed by handover after session connection as well as original session information between MN and CN. When the MN delivers packets to the CN which is located in new area by handover, the MN translates destination address of packets, from the CN's PA to TA, and sends the packets to the CN. And then the CN translates the destination address as the CN's PA again and receives the packets.

Fig. 1 illustrates location registration operation. The operations are explained in the following steps:

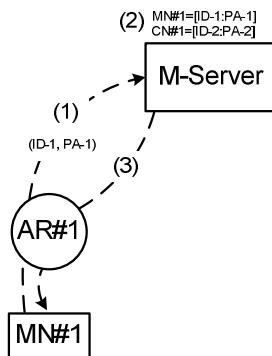


Figure 2. Location Registration Operation

- **Step 1:** MN#1 sends a registration request message to M-server. The request message contains the MN#1's ID and

PA (ID-1, PA-1). At this time, the MN#1's ID can be considered as MAC address.

- **Step 2:** The M-server receives the registration request message. A binding entry for the MN#1 in the MSBIT is created in the form of (MN#1=[ID-1:PA-1]).
- **Step 3:** The M-server sends a registration response message to MN#1 via AR#1.

Fig. 3 presents packet delivery operation. In this figure, the MN#1 is located in home network and the CN#1 initially delivers data packets to the MN#1. The steps for packet delivery are as detailed below:

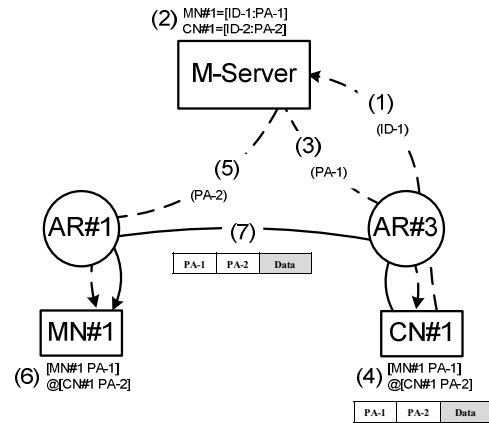


Figure 3. Packet Delivery Operation

- **Step 1:** The CN#1 sends a location query message with MN#1's ID (ID-1) to M-server. The M-server serves as DNS and the CN#1 uses the MN#1's ID for getting the MN#1's address (PA-1). At this time, the MN#1's ID can be considered as service ID (i.e. e-mail address, telephone number).
- **Step 2:** The M-server receives the query message, and does an address lookup in its MSBIT, and finds the entry for the MN#1 (MN#1=[ID-1:PA-1]).
- **Step 3:** The M-server sends a location query response message to CN#1 with the MN#1's PA (PA-1).
- **Step 4:** The CN#1 makes an entry for the mapping of MN#1 and CN#1 ([MN#1 PA-1]@[CN#1 PA-2]) in its TBIT.
- **Step 5:** The M-server sends a location information message to MN#1 with CN#1's PA (PA-2). This step occurred with Step 3 at the same time.
- **Step 6:** The MN#1 makes an entry for the mapping of MN#1 ([MN#1 PA-1]@[CN#1 PA-2]) in its TBIT.
- **Step 7:** The CN#1 creates IP header datagram with source address PA-2 and destination address PA-1. And then the CN#1 sends the datagram to MN#1.

Fig. 4 demonstrates handover operation. In this figure, the MN#1 moves from AR#1 to AR#2. The operations are described in the following steps:

- **Step 1:** MN#1 obtains new IP address (TA-1) by using auto-configuration or DHCP process, and updates its TBIT

such as the entry for the mapping of MN#1 and CN#1 ([MN#1 PA-1:TA-1]@[CN#1 PA-2]).

- *Step 2:* MN#1 sends a location update request message M-server. The request message contains the MN#1's ID and TA (ID-1, TA-1).
- *Step 3:* The M-server receives the location update request message, and updates the binding entry for the MN#1 in the MSBIT in the form of (MN#1=[ID-1:PA-1:TA-1]).
- *Step 4:* The M-server sends a location update response message to MN#1 via AR#2.
- *Step 5:* The M-server sends a location information message to CN#1 with MN#1's ID and TA (ID-1, TA-1). This step occurred with Step 4 at the same time.
- *Step 6:* The CN#1 updates the entry for the mapping of MN#1 and CN#1 ([MN#1 PA-1:TA-1]@[CN#1 PA-2]).
- *Step 7:* The CN#1 creates IP header datagram with source address PA-2 and destination address PA-1. Referring to the CN#1's TBIT, the CN#1 changes the destination address of the datagram from PA-1 to TA-1.
- *Step 8:* The CN#1 sends the datagram which have the MN#1's new IP address (TA-1) as the destination address, to MN#1 without any encapsulation.
- *Step 9:* The MN#1 checks the IP header datagram delivered with source address PA-2 and destination address TA-1. Referring to the MN#1's TBIT, the MN#1 changes the destination address of the datagram from TA-1 to PA-1.

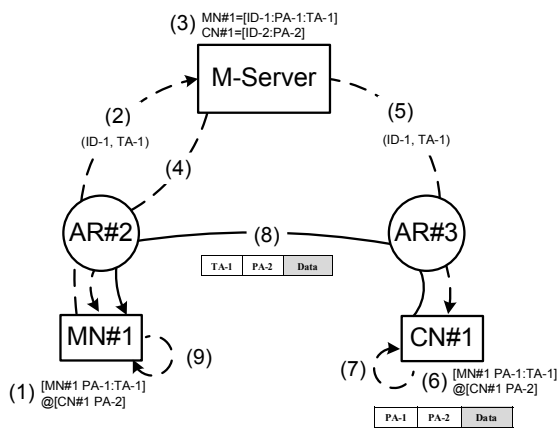


Figure 4. Handover Operation

IV. PERFORMANCE ANALYSIS AND RESULTS

This section presents a comparative analysis among the existing encapsulation method and the proposed non-encapsulation for IP packet transmission. TABLE 1 represents each header size of IP packet with or without encapsulation.

TABLE 1. THE SIZE OF IP HEADER IN PACKETS WITH OR WITHOUT ENCAPSULATION

Classification	Header Size [bytes]
IP packet with encapsulation	16
IP packet without encapsulation	8

In the following TABLE 2, the main symbols utilized in the performance analysis are reported.

TABLE 2. SYMBOLS UTILIZED IN PERFORMANCE ANALYSIS

Symbol	Meaning
fs	Source bit rate
fr	Source frame rate
T	Frame period
P	Payload
H	Encapsulated headers length in bytes for packet unit, until the network layer
N	Non-encapsulated headers length in bytes for packet unit, until the network layer
B _{ToT-encap.}	Bandwidth required from the service, with encapsulation
B _{ToT-non-encap.}	Bandwidth required from the service, with non-encapsulation

A. Overhead vs. Payload Length

Overhead is defined by the ratio between header size and header plus data size for a generic packet:

$$\text{OVERHEAD} = H/(H+P); \text{OVERHEAD}\% = 100 * H/(H+P) \quad (1)$$

Overhead is a measure of the line efficiency, because it represents also the scaled value of the bandwidth required from the transmission of the header alone.

$$\text{OVERHEAD}\% = 100 * H * fr / [(H+P) * fr] \\ = 100 * B_{\text{Header}} / B_{\text{ToT-encap.}} \quad (2)$$

The scale factor is the whole bandwidth required from the generic service, so that, the more higher is overhead, the more higher is the bandwidth required for the headers transmission respect to that required from the whole service.

With the proposed non-encapsulation scheme, overhead has the expression (1) with $H=N$.

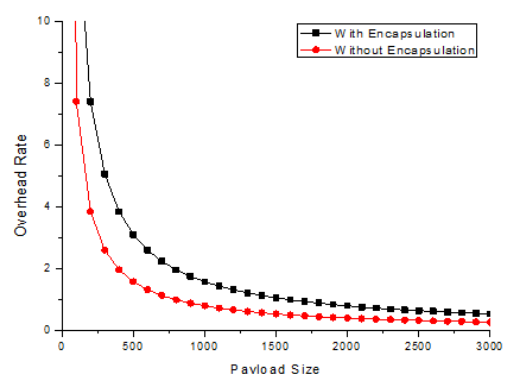


Figure 5. Overhead vs. payload size for a TCP/IPv4 stream

In our analysis we consider also the effect of the packet fragmentation on the overhead due to the limited SDU(Service Data Unit is the maximum size of a packet that can be accepted as input of the “interface driver to the radio channel”) and MRRL(Maximum Reconstructed Reception Unit is the maximum size, in the proposed scheme, of a non-encapsulated packet that can be accepted as input of the header encapsulated).

So that, if we name $SDU_MAX = \min\{SDU, MRRL\}$, the packet fragmentation is necessary when $P > SDU_MAX - H$. in this case for the transmission of the whole payload are necessary N_p packets, where $N_p = \text{INT}\{P/(SDU_MAX - H)\} + 1$, with a worsening of the overhead that assumes the following expression

$$\text{OVERHEAD\%} = 100 * (H * N_p) / (H * N_p + P) \quad (3)$$

Figure 5 and 6 illustrate the comparisons of the overhead performance in the case of a TCP/IPv4 stream($SDU = 1500B$, $MRRL > 1500B$). The proposed scheme benefits are more evident with low TCP payload size.

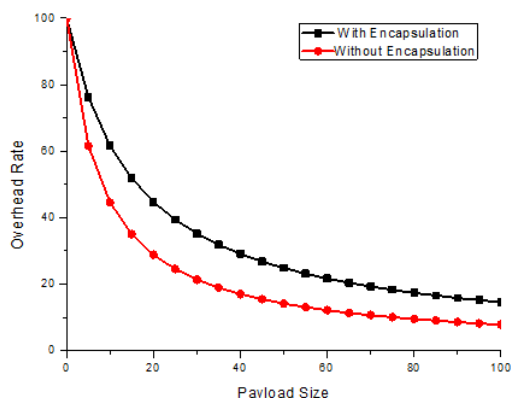


Figure 6. Overhead vs. payload size for a TCP/IPv4 stream

V. CONCLUSIONS

This paper proposes a new mobility management mechanism delivering packets without any encapsulation as well as supporting session continuity. In the proposed scheme, each communicating node performs address translation which changes the destination address of IP packets for packet delivery with non-encapsulation. The proposed scheme can decrease the delay and increase the speed of packet transmission. For the performance comparison, we calculated overhead for TCP/IPv4 stream. As a result, we verified the proposed method shows lower overhead than the existing one.

In the future, we will consider the performance evaluation regarding various factors except to overhead and define more correct parameter values.

ACKNOWLEDGMENT

This work was supported by the research grant of Chungbuk National University in 2012.

CORRESPONDING AUTHOR

Seong Gon Choi (sgchoi@cbbu.ac.kr)

REFERENCES

- [1] M. J. Yu, S. G. Choi, “New Mechanism for Global Mobility Management based MPLS LSP in NGN,” FGCN2010, 2010.
- [2] C. Perkins, “IP Mobility Support for IPv4,” RFC3344, IETF, 2002.
- [3] Moshir Rahman, Fotios C. Harmantzis, “IP Mobility with High Speed Access and Network Intelligence,” Wireless Communications and Networking Conference (WCNC), Vol. 4, pp. 2159-2164, 2004.
- [4] Basil M. Al-Kasasbeh, Rafa E. Al-Qutash and Khalid T. Al-Sarayreh, “Indirect Routing of Mobile IP: A Non-Encapsulation Approach,” International Journal of Computer Science and Network Security (IJCSNS), Vol. 8, No. 7, pp. 124-131, 2008.
- [5] Wan H Hassan, Aisha-Hassan A. Hashim, Ahmed Mustafa and Norsheila Faisal, “AMP-A Novel Architecture for IP-based Mobility Management,” International Journal of Computer Science and Network Security (IJCSNS), Vol. 8, No. 12, pp. 91-98, 2008.
- [6] Xiaobao Chen, Ioannis Kriaras, Andrea Paparella, “Non-Encapsulation Mobile IP,” United States Patent, No. US 6,842,456B1, 2000.
- [7] G. Boggia, P. Camarda and V.G. Squeo, “ROHC+: A New Header Compression Scheme for TCP Streams in 3G Wireless Systems,” in Proceedings of the IEEE International Conference on Communications (ICC), Vol. 5, pp. 3271-3278, 2002.



energy measurement in network.

Myoung Ju Yu received B.S. and M.S. degree in School of Electrical & Computer Engineering, Chungbuk National University, Korea in 2005 and 2007, respectively. She is currently a PhD. Candidate in School of Electrical & Computer Engineering, Chungbuk National University. Her research interests include mobile communication, user mobility and



Seong Gon Choi received B.S. degree in Electronics Engineering from Kyeongbuk National University in 1990, and M.S. and Ph.D. Degrees from Information Communications University, Korea in 1999 and 2004, respectively. He is currently a professor in School of Electrical & Computer Engineering, Chungbuk National University. His research interests include mobile communication, mobility, energy saving & measurement in network.