APCC 2012

The 18th Asia-Pacific Conference on Communications
October 15-17, 2012 / Ramada Plaza Jeju Hotel, Jeju Island, Korea
"Green and Smart Communications for IT Innovation"

APCC Asia-Pacific Conference on Communications

- About APCC
- Welcome Message
- Call for Papers
- Committees
- Paper Submission
- Information for Authors
- Program
- Registration
- Venue & Accommodation
- Travel Information

The 18th Asia-Pacific Conference on Communications (APCC 2012) will be held at Ramada Plaza Jeju Hotel in Jeju island, Korea, during October 15-17, 2012. Since 1993, APCC has been a technical forum for researchers and engineers to interact and disseminate information on the latest developments in advanced communication and information technologies. Prospective authors are invited to submit original technical papers for presentation at the conference and publication in the conference proceedings.

Important Dates

Paper submission deadline	~~May 15, 2012~~ May 31, 2012
Notification of acceptance	~~June 30, 2012~~ July 20, 2012
Camera ready submission	~~July 31, 2012~~ August 15, 2012
Tutorial proposals	June 30, 2012
Author Registration Deadline	August 15, 2012
Early Registration Deadline	August 31, 2012

What's New

- Final program is available. PDF
- The session assignment for accepted papers is available.
- All papers in the conference proceedings will be published in IEEE Xplore and indexed by EI.
- Prospective authors may submit a full paper or a short paper.
- Paper length should be five or six pages for a full paper and two pages for a short paper.
- The APCC 2012 will present the best paper awards to the selected outstanding full papers only.

Organizer

KICS
The Korean Institute of Communications and Information Sciences

Technically Co-sponsored by

IEICE Communications Society

中国通信学会
CHINA INSTITUTE OF COMMUNICATIONS

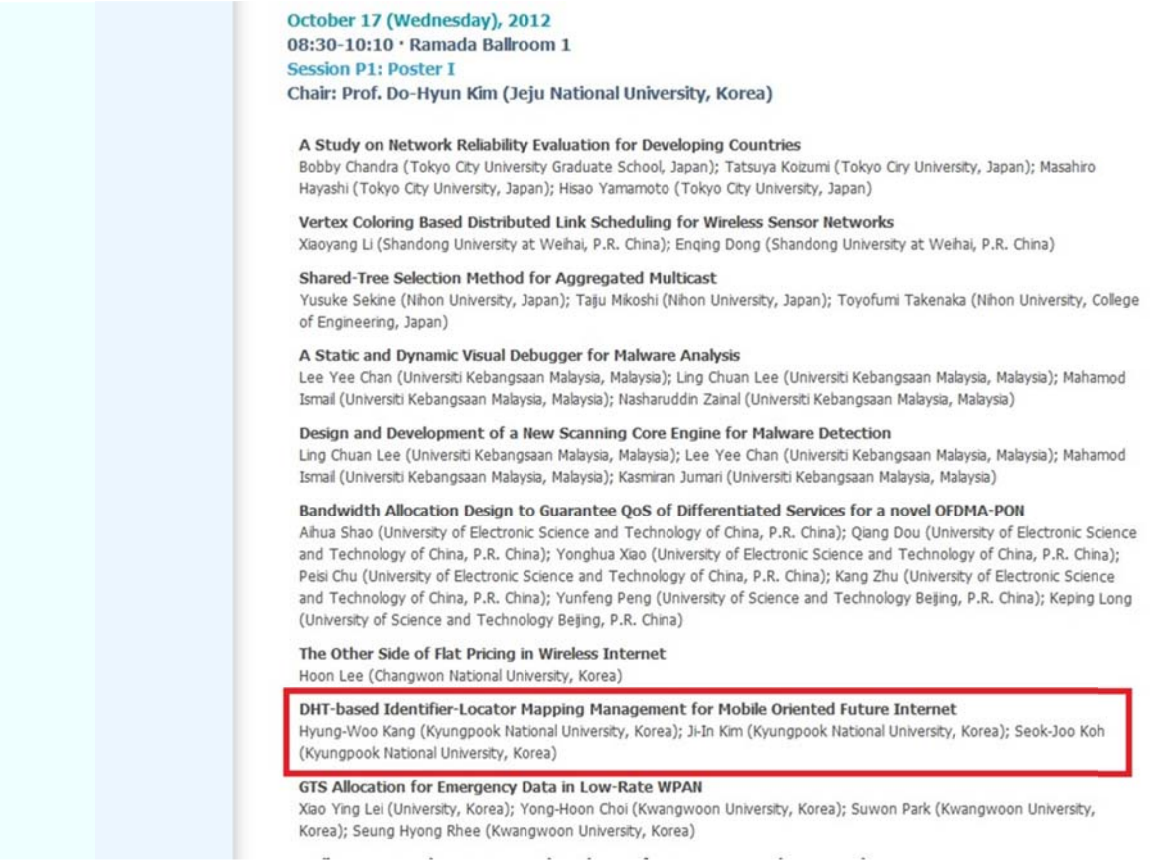
IEEE COMMUNICATIONS SOCIETY

GCC
IEEE ComSoc TSCGCC

Patrons

October 16 (Tuesday)					
8:30-10:10	**Session III-1:** MIMO I	**Session III-2:** Cognitive Radio	**Session III-3:** Sensor and Mesh Networks	**Session III-4:** Channel Modeling I	**Session III-5:** Optical Networks
10:10-10:30	Coffee Break				
10:30-12:00	**Plenary Session 2: Keynote Speeches** • "Rethinking about the Cellular Networks - A Novel Hyper-Cellular Architecture for Green and Smart ICT," Prof. Zhisheng Niu (Tsinghua Univ., China) • "Challenges in Today's Telco R&D," Dr. James W. Hong (Senior Executive Vice President, KT) • "Economic Trends and Limits in Communications and Computing," Prof. Bijan Jabbari (George Mason University, USA)				
12:00-13:30	Luncheon				
13:30-15:30	**Industrial Session 2:** Future Wireless Communications and Networking Technologies • "Future Wireless Communications Technologies", Min-Goo Kim (Vice President, Samsung Electronics) • "A Scalable ID-Based Communication Architecture for the Future Internet", Woojik Chun (Director, ETRI) • "A Global Standard Solution for Machine-to-Machine (M2M) Communications", Scarrone Enrico (ETSI TC M2M Chair, Telecom Italia)			**Tutorial 2:** "Human Mobility Patterns: Measurements, Models and Implications" (Prof. Song Chong, KAIST, Korea)	
15:30-15:50	Coffee Break				
15:50-17:30	**Session IV-1:** MIMO II	**Session IV-2:** Compressed Sensing	**Session IV-3:** Ad hoc Networks	**Session IV-4:** Channel Modeling II	**Session IV-5:** Green Optical Networks
18:30-20:30	Banquet				

October 17 (Wednesday)						
8:30-10:10	**Session V-1:** Signal Processing	**Session V-2:** DTN and VANET	**Session V-3:** Green Communication	**Session V-4:** Coding	**Session V-5:** Optical Communication	**Session P1:** Poster I
10:10-10:30	Coffee Break					
10:30-12:10	**Session VI-1:** OFDM(A)	**Session VI-2:** WLAN and WPAN	**Session VI-3:** Switching and Routing	**Session VI-4:** Short Range Communication	**Session VI-5:** Network Inform -ation Security	**Session P2:** Poster II



October 17 (Wednesday), 2012
08:30-10:10 · Ramada Ballroom 1
Session P1: Poster I
Chair: Prof. Do-Hyun Kim (Jeju National University, Korea)

A Study on Network Reliability Evaluation for Developing Countries
Bobby Chandra (Tokyo City University Graduate School, Japan); Tatsuya Koizumi (Tokyo Ciry University, Japan); Masahiro Hayashi (Tokyo City University, Japan); Hisao Yamamoto (Tokyo City University, Japan)

Vertex Coloring Based Distributed Link Scheduling for Wireless Sensor Networks
Xiaoyang Li (Shandong University at Weihai, P.R. China); Enqing Dong (Shandong University at Weihai, P.R. China)

Shared-Tree Selection Method for Aggregated Multicast
Yusuke Sekine (Nihon University, Japan); Taiju Mikoshi (Nihon University, Japan); Toyofumi Takenaka (Nihon University, College of Engineering, Japan)

A Static and Dynamic Visual Debugger for Malware Analysis
Lee Yee Chan (Universiti Kebangsaan Malaysia, Malaysia); Ling Chuan Lee (Universiti Kebangsaan Malaysia, Malaysia); Mahamod Ismail (Universiti Kebangsaan Malaysia, Malaysia); Nasharuddin Zainal (Universiti Kebangsaan Malaysia, Malaysia)

Design and Development of a New Scanning Core Engine for Malware Detection
Ling Chuan Lee (Universiti Kebangsaan Malaysia, Malaysia); Lee Yee Chan (Universiti Kebangsaan Malaysia, Malaysia); Mahamod Ismail (Universiti Kebangsaan Malaysia, Malaysia); Kasmiran Jumari (Universiti Kebangsaan Malaysia, Malaysia)

Bandwidth Allocation Design to Guarantee QoS of Differentiated Services for a novel OFDMA-PON
Aihua Shao (University of Electronic Science and Technology of China, P.R. China); Qiang Dou (University of Electronic Science and Technology of China, P.R. China); Yonghua Xiao (University of Electronic Science and Technology of China, P.R. China); Peisi Chu (University of Electronic Science and Technology of China, P.R. China); Kang Zhu (University of Electronic Science and Technology of China, P.R. China); Yunfeng Peng (University of Science and Technology Beijing, P.R. China); Keping Long (University of Science and Technology Beijing, P.R. China)

The Other Side of Flat Pricing in Wireless Internet
Hoon Lee (Changwon National University, Korea)

DHT-based Identifier-Locator Mapping Management for Mobile Oriented Future Internet
Hyung-Woo Kang (Kyungpook National University, Korea); Ji-In Kim (Kyungpook National University, Korea); Seok-Joo Koh (Kyungpook National University, Korea)

GTS Allocation for Emergency Data in Low-Rate WPAN
Xiao Ying Lei (University, Korea); Yong-Hoon Choi (Kwangwoon University, Korea); Suwon Park (Kwangwoon University, Korea); Seung Hyong Rhee (Kwangwoon University, Korea)

DHT-based Identifier-Locator Mapping Management for Mobile Oriented Future Internet

Hyung-Woo Kang
Kyungpook National University
Daegu, Korea
hwkang0621@gmail.com

Ji-In Kim
Kyungpook National University
Daegu, Korea
jiin16@gmail.com

Seok-Joo Koh
Kyungpook National University
Daegu, Korea
sjkoh@knu.ac.kr

Abstract—**In this paper, we discuss a new architecture of future Internet for mobile-oriented environments, named Mobile-Oriented Future Internet (MOFI). The MOFI architecture is designed with Host Identifier and Local Locator (HILL) for identifier and locator separation, and Query-First Data Delivery (QFDD). Based on HILL and QFDD functional blocks, this paper proposes a DHT-based Distributed Mapping System (DDMS) for identifier-locator mapping control. In DDMS, the mapping control function is distributed onto each access router in the domain, which is different from the centralized approach using a central anchor. For validation of the proposed MOFI-DDMS architecture, we implemented the data delivery and mapping control functions using Linux platform. From the testbed experimental results, we see that the DDMS architecture can give better performance than the existing Proxy Mobile IP (PMIP) protocol in terms of data transmission throughput.**

Keywords : MOFI, DHT, ID, LOC Mapping Control, Analysis

I. INTRODUCTION

With the popularity of smart phones, network environment has rapidly changed from fixed-based to mobile-based. This mobile trend is going to be much dominant and very common in the future. With this trend, the mobile environment is now a primary factor to be considered in the design of future Internet.

It is noted that the current Internet was historically designed for fixed network environment, rather than for the mobile network environment. This has enforced Internet to add a lot extensional features to satisfy the mobility requirements. As shown in the example of Mobile IP (MIP) [1, 2]. However, this patch-on approach seems to be just a temporal heuristic to the problems in mobile environment, rather than an optimization approach to substantially solve the mobile-related issue.

Based on these observations, a variety of research activities have been made to design the future Internet for mobile environment, which include eMobility [3], 4WARD [4], FIND [5], MobilityFirst [6], GENI [7], and AKARI [8]. It is also noted that many challenging works are in progress with the identifier-locator separation principle, as shown in Host Identity Protocol (HIP) [9], Locator-Identifier Separation Protocol (LISP) [10], and Identifier-Locator Network Protocol (ILNP) [11].

In this paper, we discuss the architectural design of Mobile Oriented Future Internet (MOFI) [12] to support the mobile environment of future Internet. The MOFI architecture is designed with the three functional blocks: Host Identifier and Local Locator (HILL), Query-First Data Delivery (QFDD), and DHT-based Distributed Mapping System (DDMS). In HILL, each host has a globally unique Host ID (HID) which is used for end-to-end communication, whereas an IP address of the network router is used as a Locator (LOC) by which the packet routing is performed 'locally' within a network. In QFDD, the signaling operation for LOC query is performed before data transmissions so as to obtain an optimal path. In DDMS, the HID-LOC mapping for hosts is managed in the distributed way.

This paper addresses a distributed HID-LOC mapping control scheme using the Distributed Hash Table (DHT) for MOFI. In particular, we describe the data delivery model and the HID-LOC mapping control operations, such as HID-LOC binding and LOC query for data transport. For verification, the proposed architecture is implemented over Linux platform.

This paper is organized as follows. In Section II, we give a brief overview of MOFI. Section III describes the proposed DDMS system for DHT-based HID-LOC mapping control. In Section IV, we discuss the implementations of MOFI over Linux platforms. The experimental analysis is given in Section V. Finally, Section VI concludes this paper.

II. MOFI OVERVIEW

A. *Host ID and Local Locator (HILL)*

HID is used to identify a host, which is a fixed-length secure format and it shall be globally unique in Internet. For scalable inter-domain mapping control, we assume that a HID contains the Autonomous System (AS) number of the domain that a host is subscribed to. At present, we consider the 128-bit (16-byte) format, which is designed for compatibility of IPv6 applications.

LOC is used to represent the location of a host in the network and also used for delivery of data packets. In addition, a LOC is a locally routable address that has only to be locally unique in the concerned network. As a LOC, we use the IP address of an access router and gateway those a host is attached to. These IP addresses may be local in the network.

It is noted that LOC is used for data delivery in the network, whereas HID is used for end-to-end communications between the two hosts. In mobile environments, a host with a single HID may change its LOC by movement. Moreover, the mappings between HIDs and LOCs will be updated and managed by DDMS in the dynamic and distributed manner.

B. Query-First Data Delivery (QFDD)

The current MIP mobility protocol is based on the 'data-driven packet delivery' model, which induce non-optimal routes. In MIP, a mobile node (MN) updates its LOC to the HA, when it is attached to a Foreign Agent (FA). The correspondent node (CN) sends the data packets to HA, and HA will forward these packets to MN via FA, which induces a non-optimal route.

In QFDD of MOFI, the LOC query operation will be performed before data transmission to find the optimal route. The HID and LOC of MN is registered with the DDMS agent. When CN sends a data packet to MN, the access router of CN will perform the LOC query operation with the DDMS agents to find the LOC of MN. After that, the data packet is delivered to MN by using the optimal route.

C. Data Delivery Model

In MOFI, each host has a globally unique HID, by with global communication is accomplished. In the meantime, one or more LOCs are used for packet routing in the network. Each LOC may be used locally in the transit networks, without any assumption on global uniqueness of LOC.

Fig. 1 shows the data delivery operations with global HID-based communication and local LOC-based routing in MOFI.

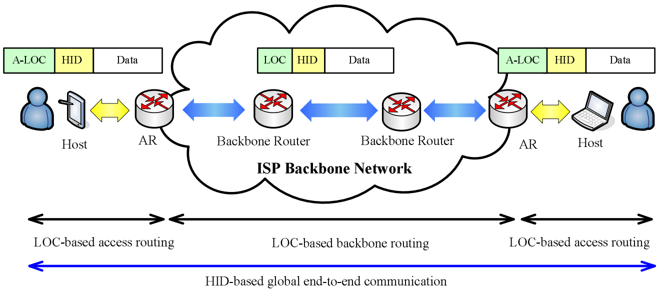
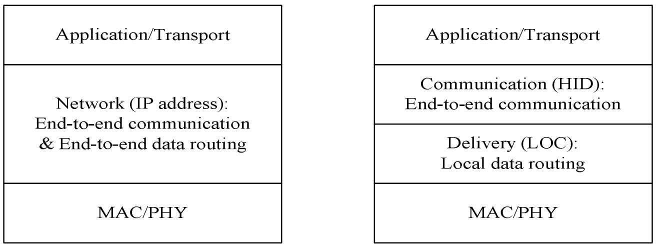


Fig. 1. HID-based communication and LOC-based routing

In the figure, communication between two hosts is performed with HIDs, whereas LOCs are used for packet delivery. For packet delivery, an A-LOC is used as LOC within access network, whereas IP address of ARs will be used as LOCs in the backbone network. The data packet routing is performed locally in the access and backbone network, in which AR performs the header (or LOC) translation between A-LOC and LOC.

In the viewpoint of protocol stack, MOFI takes a layered model similar to the TCP/IP architecture. Fig. 2 shows that MOFI considers a protocol stack for data transport. The current application layer, transport layer, and MAC/PHY protocols are re-used in MOFI.



(a) Current TCP/IP (b) MOFI

Fig. 2. Protocol stacks for data delivery

As for the network layer, the current IP protocol performs end-to-end communication (by using a socket interface with the upper layer application) and data delivery (or routing). That is, the network layer is divided into the following two sub-layers: communication and delivery.

The communication sub-layer is responsible for end-to-end communication between the two end hosts, which may be implemented as a shim layer protocol between transport and network layers. The delivery sub-layer is responsible for packet routing in the network, which is divided into Access Delivery Protocol (ADP) and Backbone Delivery Protocol (BDP). ADP is used to deliver data packets between host and AR, whereas BDP is used between ARs in the ISP backbone network. The current IPv4/IPv6 protocol is used as ADP and/or BDP.

Fig. 3 shows the protocol model for data delivery. In the figure, each AR performs the protocol (LOC) translation between ADP and BDP. During this process, the MOFI header (containing the source and destination HIDs) may be referred to by AR. Note that each of the intermediate backbone routers shall not be aware of HID.

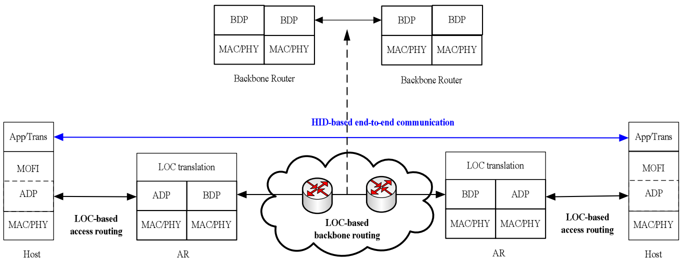


Fig. 3. Protocol model for data delivery

III. DHT-BASED DISTRIBUTED MAPPING SYSTEM

The network model for DDMS can be divided into intra-domain and inter-domain cases. The intra-domain mapping control (within a domain) is performed with the DHT-based mapping system, in which a specific LMC is determined for a given HID, as per the DHT hash function. The inter-domain mapping control (between different domains) is performed with the domain-based mapping system, in which HID is used to identify the home ISP domain of a host. This paper focuses on 'intra-domain' HID-LOC mapping control, whereas 'inter-domain' mapping control is not discussed in this paper.

A. DHT-based Mapping Control Model

Fig. 4 shows the DHT-based mapping control. In the figure, the control plane is separated from the data plane. In the data plane, an access router (AR) maintains a Local Binding Cache (LBC) that maintains the list of HID: A-LOC of the attached local hosts and a Data Forwarding Cache (DFC) that maintains the list of HID-LOC of the remote hosts for data packet forwarding.

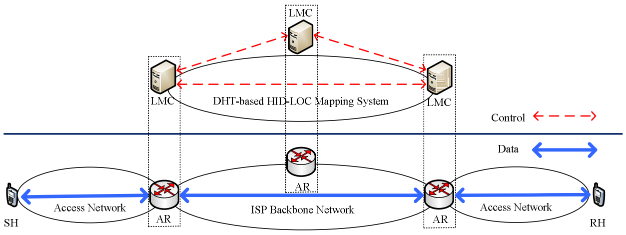


Fig. 4. Intra-domain mapping control

The DHT-based intra-domain mapping control operations are performed between LMCs. For mapping control, each LMC has a DHT table and a HID-LOC Register (HLR). For a given HID, the LMC who is responsible for the HID-LOC mapping control of the corresponding host will be determined by the DHT table. That is, the DHT table is used to find the LMC that is in charge of the mapping control from the HID of the host. The HLR maintains the list of the HID-LOC bindings for the associated hosts, in which LOC represents the IP address of the LMC that the host is bound to. In this way, the HLRs will be distributed onto every LMC in the domain. This HLR is updated and referred to by DDMS. In the HID-LOC binding operation, the binding (or mapping) information of HID-LOC for a host will be updated and maintained by the HLR of a specific LMC.

B. HID-LOC Binding Operations

With the network attachment of host, the HID-LOC operation is performed, in which HID and A-LOC of the host will be registered with AR attached to the host. AR will maintain and update its LBC cache that contains the information of bindings between HIDs and A-LOCs for all of the hosts attached to the AR. The LBC cache information will be referred to by AR for forwarding of data packets that are destined to the local hosts in the subnet.

In the HID-LOC binding, the HID Binding Request (HBR) and HID Binding ACK (HBA) messages are exchanged between host and AR, as shown Fig. 5.

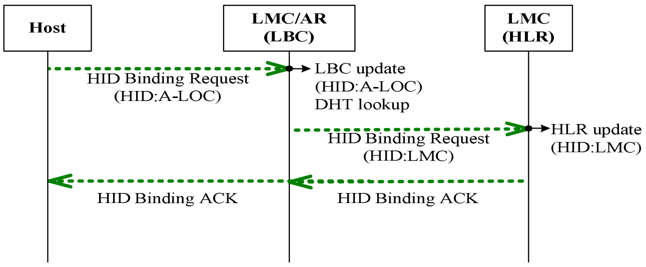


Fig. 5. HID-LOC binding between host and AR/LMC

After the HID-LOC binding between host and LMC/AR, the LMC/AR of the host may send a HBR message to another LMC that is in charge of the HID-LOC binding control for the host with HLR. This LMC is determined by the DHT lookup. The HBR message contains the HID of the host and the LOC (IP address of LMC that the host is attached to). Based on the received HBR, the LMC shall update its HLR and respond with a HBA message to LMC of the host, and further to the host.

C. LOC Query Operations for Data Delivery

In the LOC query operation, the HLR will be referred to by the DHT-based mapping system so as to find the LMC that the destination host is attached to. In this case, it is assumed that SH is attached to LMC-1 and RH is connected to LMC-3, and that LMC-2 is in charge of the HID-LOC binding for RH, based on the DHT-based mapping system.

Fig. 6 shows the data delivery with LOC query operations.

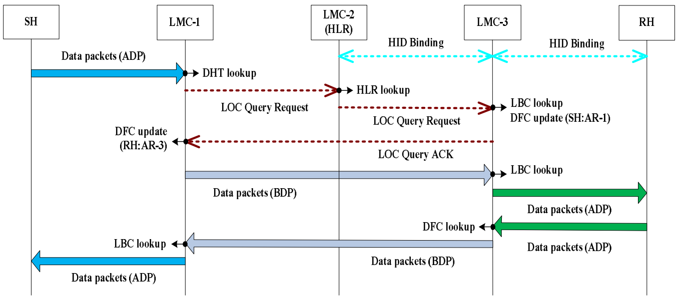


Fig. 6. Data delivery for intra-domain case

When a data packet arrives from SH, the LMC-1 sends a LOC Query Request (LQR) message to LMC-2 by the DHT lookup, since LMC-2 is in charge of the binding control for RH. On reception of a LQR message, LMC-2 looks up its HLR to find the corresponding LMC-3, and then sends the LQR message to LMC-3. LMC-3 now looks up its LBC, and its AR-3 updates its DFC with SH: AR-1. Then, LMC-3 responds with a LOC Query ACK (LQA) message to LMC-1 of SH. On reception of LQA message, AR of SH will update its DFC with RH: AR-3. AR of SH can now send the data packet directly to AR-RH by using BDP. When a data packet arrives at AR-3, it is now delivered to RH over ADP. The subsequent data delivery can be performed between SH, AR-1, AR-3, and RH by referring to the associated DFCs and LBCs along the path.

IV. IMPLEMENTATIONS

For validation of the proposed architecture/schemes, the host and LMC/AR have been implemented over Linux platforms.

A. Host

For host implementation, we use the *Ubuntu 10.04* and *Linux kernel 2.6.32.16 version*. The implementation of host is based on the well-known 6-to-4 tunneling [13]. In implementation, an IPv6 address for 6-to-4 tunneling is used as HID, whereas IPv4 address as LOC. The 128-bit HID includes 2-byte prefix (2002) for 6to4 tunneling, 4-byte AS number, and 10-byte Subscriber ID, as shown in Fig. 7.

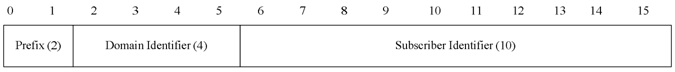


Fig. 7. HID format

B. *Access Router (AR)*

For implementation of AR, we also use the *Ubuntu 10.04* and *Linux kernel 2.6.32.16 version*. When a data packet arrives from a host, AR translates the ADP header to the BDP header for the data packet. For this header translation, we employ *netfilter* [14] and *iptables* [15].

Fig. 8 shows the protocol model of AR. It is assumed that each AR uses ADP for packet delivery between host and AR. It is noted that each AR performs the LOC query operation to find the LOC of the correspondent host before data transmission.

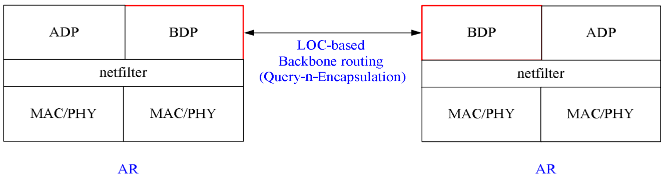


Fig. 8. Protocol model at AR

Fig. 9 shows the *netfilter* functions to support the protocol (header) translation at AR. In the figure, the modified function modules (*netfilter* hooking points) are indicated as shared boxes.

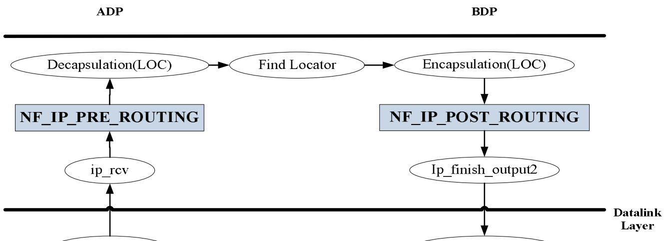


Fig. 9. *Netfilter* modules modified for AR

When a packet arrives from the host, *ip_rcv* function is invoked to process the packet at the network layer. Then, the *NF_IP_PRE_ROUTING* function of *netfilter* will hook the data packet. After that, the packet header is translated from ADP to BDP (or from BDP to ADP). To construct the BDP header, the LMC associated with AR performs the LOC query operations by using the DHT-based mapping system, so as to find the LOC of the mobile host. As the protocol (header) translation is completed, the *NF_IP_POST_ROUTING* function will forward the packet to the *ip_finish_output2* function for data forwarding. It is noted that *iptables* is used together with *netfilter*. In MOFI, *ipatbles* is used for packet forwarding to AR.

C. *Local Mapping Controller (LMC)*

For implementation of the DHT-based mapping control at LMC, we employed a simple hash function using a *modulo (%)* operator, instead of a complicated legacy DHT scheme. That is, for a given HID, so as to determine the LMC that is responsible for the concerned host, we calculate "*HID % number of LMCs in the domain.*"

For this purpose, the LMCs in the domain are numbered in sequence. Then, the LMC that will be responsible for a host is selected as the LMC that has the equal sequence number to the resulting value of the *modulo* hash function. If the LMC is determined for a host in this way, the HBR and LQR messages for mapping control of the host will be delivered the determined LMC. In implementations, the mapping control messages are exchanged between LMCs by using UDP.

V. EXPERIMENTAL ANALYSIS

A. *Testbed Network*

Fig. 10 shows the testbed network configuration, in which the two hosts (SH and RH) and three ARs with LMC (AR-1, AR-2, and AR-3) are employed.

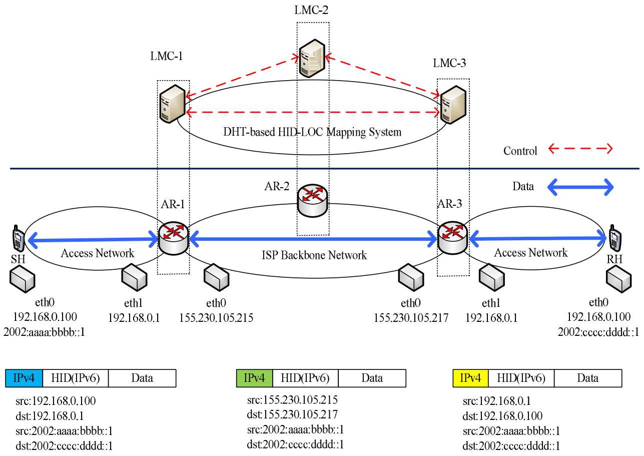


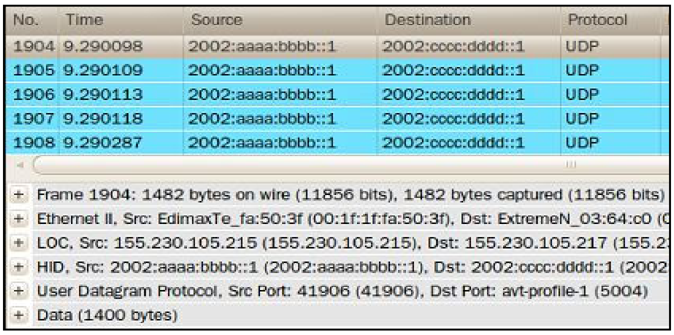
Fig. 10. Testbed network

In testbed network, SH acts as the packet sender (i.e., CN) and RH plays a role of the packet receiver (i.e, MN). SH uses the HID of 2002:aaaa:bbbb::1, and RH uses the HID of 2002:cccc:dddd::1. As for A-LOC and LOC, *private* IPv4 address (192.168.x.y) is used as A-LOC, and *public* IPv4 address (155.230.x.y) is used as LOC.

B. *Experimentations of Data Delivery*

For experimental analysis of data delivery, the following test scenario is applied. First, SH and RH are connected to AR-1 and AR-2, respectively. Then, SH sends the data packet to RH. In this experiment, it is assumed that the associated LOC query operation has already been completed. We have captured the data packets by using the *Wireshark* [16].

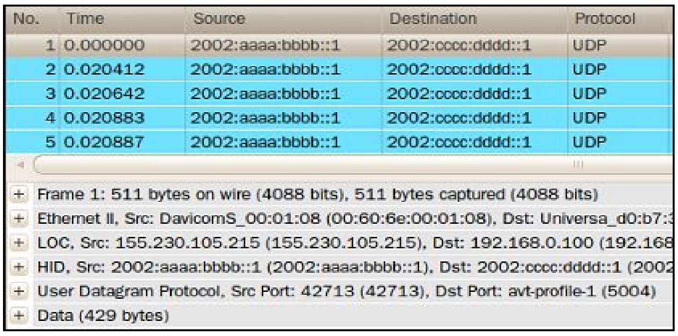
Fig. 11 shows the packet capturing results for the data packets transmitted from AR-1 to AR-2. Similarly, Figure 12 shows the data packet transmitted from AR-2 to RH.



```
No.  Time      Source              Destination         Protocol
1904 9.290098  2002:aaaa:bbbb::1   2002:cccc:dddd::1   UDP
1905 9.290109  2002:aaaa:bbbb::1   2002:cccc:dddd::1   UDP
1906 9.290113  2002:aaaa:bbbb::1   2002:cccc:dddd::1   UDP
1907 9.290118  2002:aaaa:bbbb::1   2002:cccc:dddd::1   UDP
1908 9.290287  2002:aaaa:bbbb::1   2002:cccc:dddd::1   UDP

+ Frame 1904: 1482 bytes on wire (11856 bits), 1482 bytes captured (11856 bits)
+ Ethernet II, Src: EdimaxTe_fa:50:3f (00:1f:1f:fa:50:3f), Dst: ExtremeN_03:64:c0 (
+ LOC, Src: 155.230.105.215 (155.230.105.215), Dst: 155.230.105.217 (155.2
+ HID, Src: 2002:aaaa:bbbb::1 (2002:aaaa:bbbb::1), Dst: 2002:cccc:dddd::1 (2002
+ User Datagram Protocol, Src Port: 41906 (41906), Dst Port: avt-profile-1 (5004)
+ Data (1400 bytes)
```

Fig. 11. Packet capture from AR-1 to AR-2



```
No.  Time      Source              Destination         Protocol
   1 0.000000  2002:aaaa:bbbb::1   2002:cccc:dddd::1   UDP
   2 0.020412  2002:aaaa:bbbb::1   2002:cccc:dddd::1   UDP
   3 0.020642  2002:aaaa:bbbb::1   2002:cccc:dddd::1   UDP
   4 0.020883  2002:aaaa:bbbb::1   2002:cccc:dddd::1   UDP
   5 0.020887  2002:aaaa:bbbb::1   2002:cccc:dddd::1   UDP

+ Frame 1: 511 bytes on wire (4088 bits), 511 bytes captured (4088 bits)
+ Ethernet II, Src: DavicomS_00:01:08 (00:60:6e:00:01:08), Dst: Universa_d0:b7:
+ LOC, Src: 155.230.105.215 (155.230.105.215), Dst: 192.168.0.100 (192.168
+ HID, Src: 2002:aaaa:bbbb::1 (2002:aaaa:bbbb::1), Dst: 2002:cccc:dddd::1 (2002
+ User Datagram Protocol, Src Port: 42713 (42713), Dst Port: avt-profile-1 (5004)
+ Data (429 bytes)
```

Fig. 12. Packet capture from AR-2 to RH

From the figures, we can also see that LOCs are translated along the path. In Fig. 11, AR-1 and AR-2 use 155.230.105.215 and 155.230.105.217 as LOCs (public IP addresses). In Fig. 12, the A-LOC of RH is used with 192.168.0.100 (private IP address). In the meantime, the HIDs of SH and RH are not changed during the data delivery.

C. *Experimentations of Distributed Mapping Control*

For experimentation of DDMS mapping control, we consider the three different cases for distributed mapping control. For each case, the LMC that is responsible for HID-LOC mapping control is selected differently, as per the *modulo* hash function.

In Case 1, as shown in Fig. 13, Sending Host (SH) is attached to AR-1, and Receiving Host (RH) is attached to AR-3. It is assumed that the HID of RH is registered with LMC-1, as per the hash function. Accordingly, there is no need of LOC query to RH, when a data packet of SH arrives at AR-1, since the HID-LOC mapping information is already maintained at LMC-1. The data packets are delivered from AR-1 to AR-3.

In Case 2, as shown in Fig. 14, SH and RH are attached to AR-1 and AR-3, respectively. However, the HID of RH is registered with LMC-2, as per the hash function. Accordingly, when a data packet of SH arrives at AR-1, LMC-1 will send the LQR message to LMC-2. Then, LMC-2 forwards this LQR message to LMC-3. LMC-3 responds with the LQA message to LMC-1. After that, AR-1 transmits the data packets to AR-3.

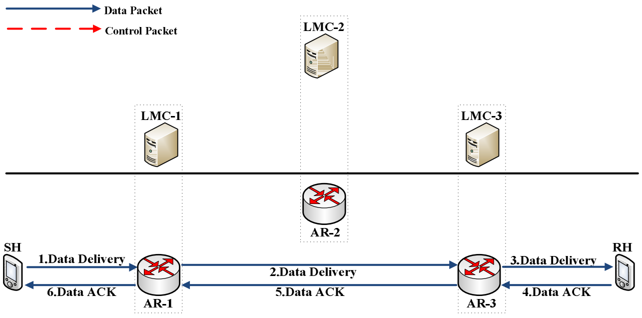


Fig. 13. Case 1: No need of LOC Query

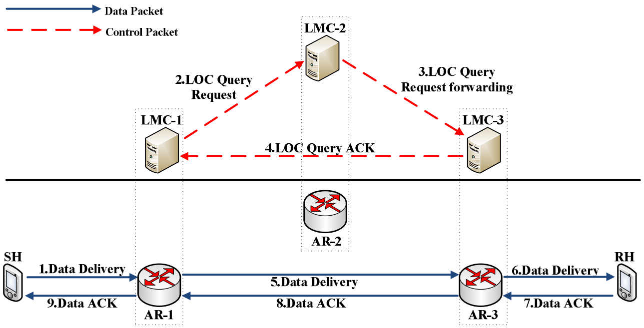


Fig. 14. Case 2: LOC query to LMC-2 and to LMC-3

In Case 3, as shown in Fig. 15, SH and RH are attached to AR-1 and AR-3, respectively. It is assumed that the HID of RH is registered with LMC-3, as per the hash function. Accordingly, when a data packet of SH arrives at AR-1, LMC-1 will send the LQR message to LMC-3. Then, LMC-3 responds with the LQA message to LMC-1. After that, AR-1 transmits the data packets to AR-3.

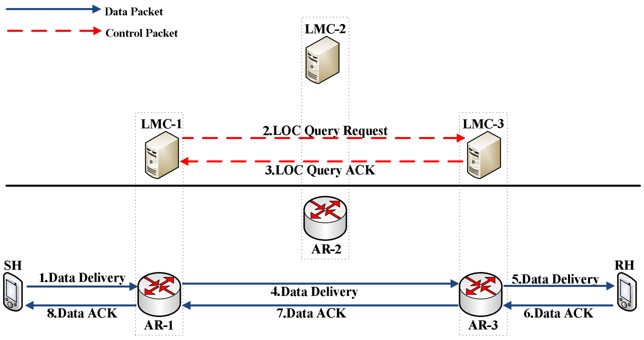


Fig. 15. Case 3: LOC query to LMC-3

For comparison, we also performed the Proxy MIP (PMIP) operations, in which LMC-2 plays a role of LMA and all the data packets of SH in AR-1will be delivered to RH in AR-3, by way of AR-2. In PMIP, the LOC query operations are not performed.

In the three test cases and the PMIP case, SH transmits 10 data packets to RH, and then we measure the packet delivery time including the LOC query operation and the data packet delivery.

Fig. 16 compares the packet delivery time for the candidate schemes, denoted by DDMS: Case 1, 2, 3 and PMIP. From the figure, the PMIP gives worse performance than the three DDMS schemes. This is because PMIP does not use the optimal routes, even though the LOC query operation is not required. Among the three DDMS cases, Case 1 provides the best performance. This is because the optimal route is used without using the LOC query operations in this case. In the meantime, Case 2 tends to give relatively worse performance than Case 1 and 3, since the LOC Query message is delivered from LMC-1 to LMC-3 via LMC-2.

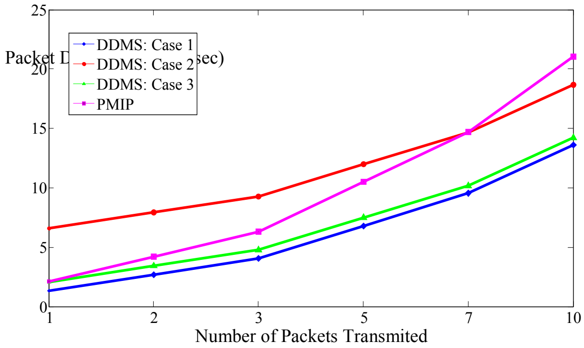


Fig. 16. Packet delivery time for DDMS and PMIP

Fig. 17 compares the packet delivery time for DDMS and PMIP, as the number of hosts in the domain increases. In DDMS, Case 2 is employed, since it gives the worst performance among the three cases. Form the figure, we can see that DDMS gives better performance than PMIP, and the performance gap gets larger, as the number of hosts increases in the domain.

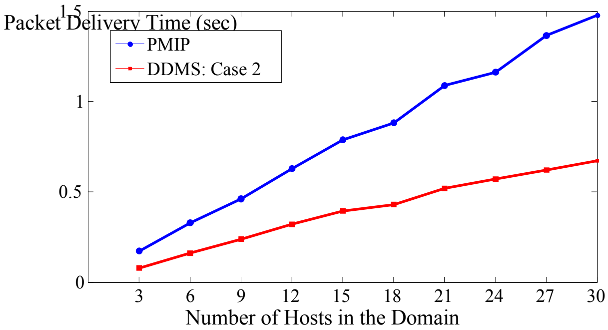


Fig. 17. Comparison of DDMS (Case 2) and PMIP

VI. CONCLUSIONS

In this paper, we presented a new architecture of future Internet for mobile environments, named MOFI. The proposed MOFI architecture provides a set of distinctive features: HILL and QFDD. Based on the MOFI architecture, we propose a DHT-based Distributed Mapping System (DDMS) for identifier-locator mapping control. In DDMS, the mapping control function is distributed onto each access router in the domain, which is different from the existing centralized scheme.

For verification of the proposed MOFI architecture, we implemented the data delivery and DDMS functions over the Linux platform. From the testbed experimental results, we see that the MOFI architecture can give better performance than the existing mobility protocol in terms of data transmission throughputs. Such the performance gain comes from the distinctive features of MOFI: HILL for HID-LOC separation, QFDD for route optimization using the LOC query, and DDMS for distributed mapping control.

ACKNOWLEDGMENT

This research was supported by Basic Science Research Program of NRF (2011-0026529), ITRC support program of NIPA (NIPA-2012-H0301-12-2004), and IT R&D support program of KCA (KCA-2011-10913-05004).

REFERENCES

[1] IEFT RFC 5944, IP Mobility Support for IPv4: Revised, November 2010
[2] IETF RFC 3775, Mobility Support in IPv6, June 2004
[3] eMobility Project, http://www.emobility.eu.org/
[4] 4WARD Project, http://www.4ward-project.eu/
[5] Future Internet Design (FIND), http://www.nets-find.net/
[6] Mobility First: Future Internet Architecture, http://mobilityfirst.winlab.rutgers.edu/
[7] Global Environment for Network Innovations (GENI), http://www.geni.net/
[8] AKARI, http://akari-project.nict.go.jp/eng/
[9] Host Identity Protocol (HIP), http://www.ieft.org/html.charters/hip-charter.html
[10] Locator Identifier Separation Protocol (LISP), http://www.ietf.org/html.charters/lisp-charter.html
[11] Identifier Locator Network Protocol (ILNP), http://ilnp.cs.st-andrews.ac.uk/
[12] Mobile Oriented Future Internet (MOFI), http://www.mofi.re.kr
[13] 6to4 tunneling, http://en.wikipedia.org/wiki/6to4
[14] Netfilter HOWTO, http://netfilter.org/documentation/HOWTO/netfilter-hacking-HOWTO.html
[15] IPtables HOWTO, https://help.ubuntu.com/community/IptablesHowTo
[16] Wireshark homepage, http://wireshark.org