ID/LOC Separation Network Architecture for Mobility Support in Future Internet

Nakjung Choi*, Taewan You*, Jungsoo Park†, Taekyoung Kwon* and Yanghee Choi*

*School of Computer Science and Engineering, Seoul National University, Korea
Email: {fomula, twyou, tk, yhchoi}@mmlab.snu.ac.kr

†, u-Infra Standards Research Team, Electronics and Telecommunications Research Institute, Korea
Email: pjs@etri.re.kr

***Abstract*—In this paper, we propose a novel network architecture for future Internet to solve both routing scalability and mobility. Our proposal is based on a LISP+ALT architecture to achieve routing scalability in a global Internet scale. We extend the LISP+ALT architecture to provide roaming for global mobility and take a network-based approach for seamless local mobility. Our network architecture for mobility support in future Internet is evaluated by simple analysis, in terms of handover latency and communication overhead.**

I. Introduction

Recently, Internet has been reconsidered in various parts of problems, which mainly parts are about fundamental architecture. Especially, BGP routing table scalable issues have been taken into account for Internet Engineering Task Force (IETF). Analysis of the routing tables in the default free zone (DFZ) reveals important problems for Internet routing. According to the report of Internet Architecture Board (IAB) Workshop on Routing and Addressing [1], there are some factors to mainly drive forces behind the rapid growth of the DFZ routing table sizes; multihoming, traffic engineering, and non-aggregatable address allocations. The IETF had been taking into account these problems early, after that the ROuing and Addressing Problem (ROAP) meeting was held at 68^{th} IETF meeting, March 2007.

Since 68^{th} IETF meeting, the ROAP had been taking by Routing Research Group (RRG) in Internet Research Task Force (IRTF), and lots discussions on mailing lists, such as ram@iab.org, and rrg@psg.com. Concretely, several concepts changing scalable routing architecture were proposed and there were discussions about more than 800 messages on Routing and addressing Mailing lists (RAM) and about more than 400 messages on RRG mailing lists. During these IRTF meetings, there were many presentations and lots discussions include variable solutions, such as Locator/ID Separation Protocol (LISP) [2] developed by Cisco, A Solution for Routing and Addressing in IPv6 (Six/One) [3], and Separating Routing and Forwarding (PFRI) [4] that is based on clean slate approaches as well as existing solutions, such as Site multihoming by IPv6 Intermediations (SHIM6) [5], Global, site, and end system (GSE) [6], and Host Identity Protocol (HIP) [7].

Regarding mobility support, mainly mobility support protocol trends were moving toward a network-based approach. Conventional host-based mobility solutions such as mobile IP were not deployed globally, because a mobile host has serious overheads which are additional signaling process in a wireless part and installing extra programs to take part in mobility support procedures. Therefore, the network-based approach summarized that complicated procedures handled by a mobile host were taken charge in a network side, whereas a mobile host is not modified anymore. The representative of the network-based mobility support protocols is a Proxy Mobile IPv6 (PMIPv6) protocol [9] proposed in IETF.

The remainder of this paper is organized as follows. In Section II, we propose a novel network architecture for future Internet to solve both *routing scalability* and *mobility* by coupling two representative concepts, *identifier/locator separation* and *network-based mobility support*. A LISP+ALT (Alternative Logical Topology) architecture [8] for routing scalability is extended to enable global LISP-based mobility and local network-based mobility. Then, we evaluate our network architecture for mobility support in future Internet in Section III by simple analysis. Finally, we conclude our work in Section IV.

II. Mobility Support Network Architecture

Prior to proposing global and local mobility support network architecture with the concept of identifier/locator separation, we have the following assumptions;

- A list of representative authentication mechanisms which are supported in a global Internet scale is pre-defined, and a fixed or mobile host is able to select and use one among them.
- AAA (Authentication, Authorization, and Accounting) information can be shared among ISPs for global mobility support, depending on their arrangements.
- In Internet where there coexist various wired/wireless technologies and ISPs, seamless connectivity support is hardly possible, so the objective of global mobility is to keep the same identifier anywhere[1] (regardless of

[1]In this sense, global mobility means *roaming*.

locator). On the contrary, local mobility in a single domain aims to provide seamless connectivity for end-to-end sessions.

A. Network Architecture Overview

We propose global and local mobility support network architecture for future Internet, which is depicted in Fig. 1. In the proposed network architecture, a new entity termed *MATP* (Mobility Anchor Tunnel Point) is introduced, which has two types: *global* and *local*. G-MATP (Global-MATP) plays a role as ITR/ETR to support LISP [2] proposed in IRTF, and also performs management for home EIDs and mobility-related signaling for foreign EIDs to provide global mobility in a LISP+ALT architecture. In addition, it maintains bidirectional tunnels with L-MATPs (Local-MATP) to provide local mobility in a single domain. L-MATP is responsible for detecting a mobile host which moves into its managed area and performing an authentication process, and it also dynamically creates and deletes a tunnel with a G-MATP in a single domain. Lastly, all domains have one or more AAA home and cache servers. The former stores AAA information for home EIDs while the latter makes a cache of AAA information for foreign EIDs temporarily with a soft state to provide seamless local mobility even for foreign EIDs.

B. Signaling for Mobility

When a mobile host is connected in a home domain, mobility-related signaling is described in Fig. 2. After the layer-2 attachment of the mobile host, it sends an *authentication request* message which includes its EID (*MH-EID*). L-MATP receiving the *Auth. Req.* message sends a *proxy binding update* message with *MH-EID* to G-MATP. After receiving the *PBU* message, the G-MATP determines which authentication mechanism will be used and initiates an AAA process with its AAA home server because the *MH-EID* belongs to an home EID prefix managed by the G-MATP. During the process, the G-MATP acquires a profile of the *MH-EID*, which may involve an EID of an authentication server responsible for the *MH-EID*. Then, the G-MATP sends a *proxy binding acknowledgement* message to the L-MATP. As a result, a bidirectional tunnel is created between the L-MATP and the G-MATP, and the L-MATP sends an *authentication reply* message to the mobile host. Afterwards, if a mobile host moves locally in its home domain, a new tunnel between a currently attached L-MATP and the G-MATP is created, and the previous tunnel is deleted[2]. When a mobile host opens an EID-based session with a correspondent host, G-MATP at the mobile host side conducts an EID-to-RLOC mapping resolution over ALT and then a LISP tunnel is created between the mobile host's G-MATP and the correspondent host's G-MATP, according to a LISP+ALT principle. Although any local network architecture without L-MATPs is possible, it cannot serve as a foreign domain for global and local mobility.

[2]In case that a mobile host exists in its home domain, operations except an EID instead of an IPv6 address are similar to a PMIPv6 mechanism.

When a mobile host moves from a home domain to a foreign domain, or from a foreign domain to another foreign domain, mobility-related signaling is described in Fig. 3. From the mobile host's view, there is nothing different from a home domain scenario. After the layer-2 attachment, it sends an *Auth. Req.* message with *MH-EID*. L-MATP$_{foreign}$ receiving the *Auth. Req.* message also sends a *PBU* message with *MH-EID* to G-MATP$_{foreign}$. The G-MATP$_{foreign}$ determines which authentication mechanism will be used according to the *PBU* message, and initiates an AAA process over ALT because the *MH-EID* does not belong to an home EID prefix managed by the G-MATP$_{foreign}$. After the AAA process over ALT, the G-MATP$_{foreign}$ acquires a profile (AAA information) of the *MH-EID*, which is stored at a local AAA cache server temporarily to provide seamless local mobility even for foreign EIDs. Then, the G-MATP$_{foreign}$ sends a *PBA* message to the L-MATP$_{foreign}$, and a bidirectional tunnel is created between the L-MATP$_{foreign}$ and the G-MATP$_{foreign}$. Finally, the L-MATP$_{foreign}$ sends an *Auth. Rep.* message to the mobile host with the foreign EID (*MH-EID*). It is noted that the G-MATP$_{foreign}$ should also register a new EID-to-RLOC mapping information at G-MATP$_{home}$ for correspondent hosts' EID-to-RLOC resolutions, which involves *MH-EID* and G-MATP$_{foreign}$'s locator as EID and RLOC, respectively.

C. Communication Example

Fig. 4 describes a communication procedure when a corresponding host initiates sending data packets to a mobile host currently staying at a foreign domain. The corresponding host first sends data packets destined for the mobile host's EID (*MH-EID*) to its L-MATP$_{ch}$. Then, the L-MATP$_{ch}$ transfers the data packets to its G-MATP$_{ch}$ through a local tunnel between the L-MATP$_{ch}$ and the G-MATP$_{ch}$. The G-MATP$_{ch}$ receiving the data packets performs an EID-to-RLOC mapping resolution for *MH-EID* over ALT. During the EID-to-RLOC mapping resolution, G-MATP$_{ch}$ creates a new global LISP tunnel with G-MATP$_{foreign}$ for the mobile host with *MH-EID*. After the EID-to-RLOC mapping resolution is completed, the data packets sent by the corresponding host traverse G-MATP$_{ch}$, G-MATP$_{foreign}$, and L-MATP$_{foreign}$ sequentially Then, they are finally transported to the mobile host.

III. Analysis

We evaluate our network architecture for mobility support in future Internet by analysis. For this purpose, we write a simple C program. In our analysis, two performance indices, handover latency and communication overhead are measured in various scenarios. Global or local handover latency is calculated as a duration between the completion of layer-2 connection setup and the reception of an *Auth. Req.* message. Kinds of communication overhead is defined as follows.

- Initial latency - the sum of all signaling times required for the exchange of data packets, e.g., control overhead, authentication time.
- Control overhead - the time required for an EID-to-RLOC mapping resolution over ALT.

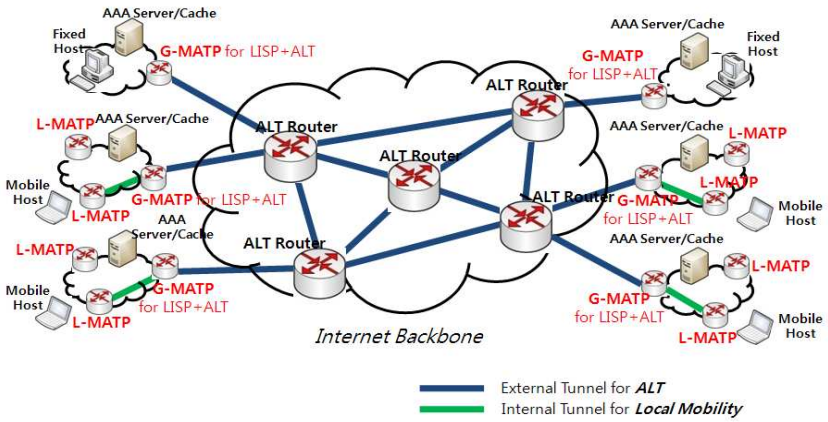

Fig. 1. Proposed Mobility Support Network Architecture

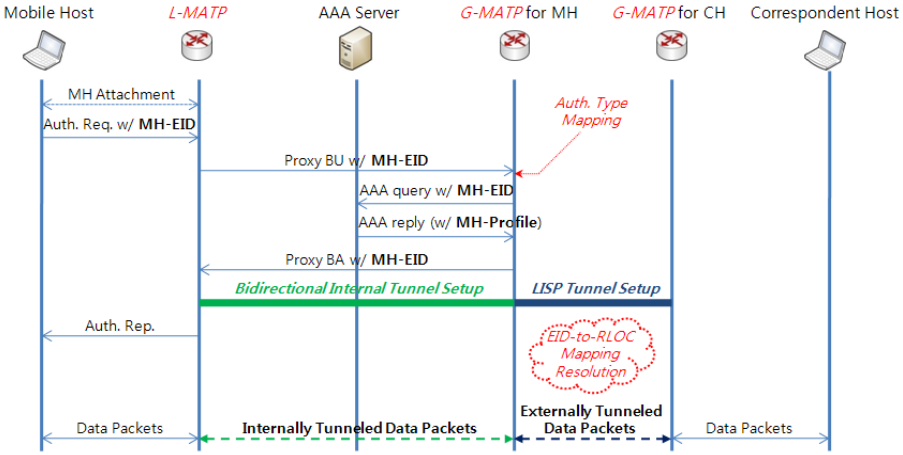

Fig. 2. Mobility Signaling in a Home Domain

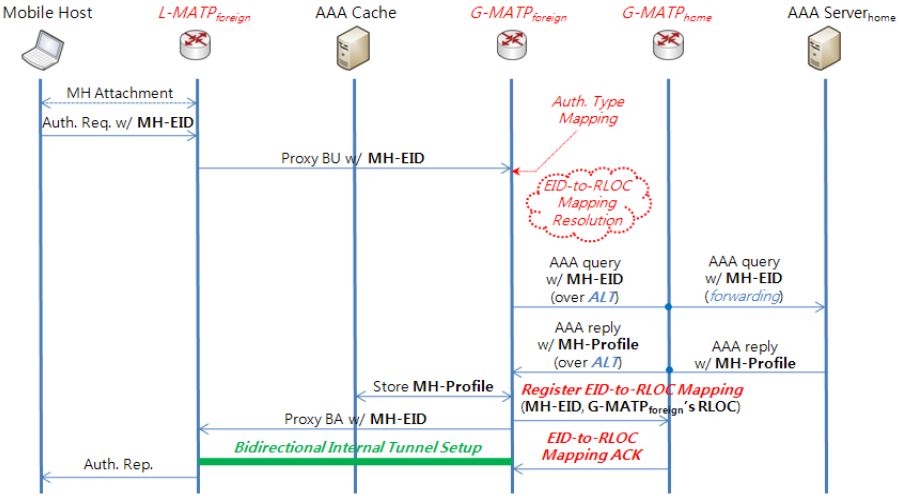

Fig. 3. Mobility Signaling in a Foreign Domain

- Transmission delay - the transmission time required for end-to-end communication.
- Tunnel overhead - the additional transmission time spent by IPv4 or IPv6 tunnels.

Table I and II show handover latency in intra- and inter-domain handover scenarios. In case of intra-domain handover,

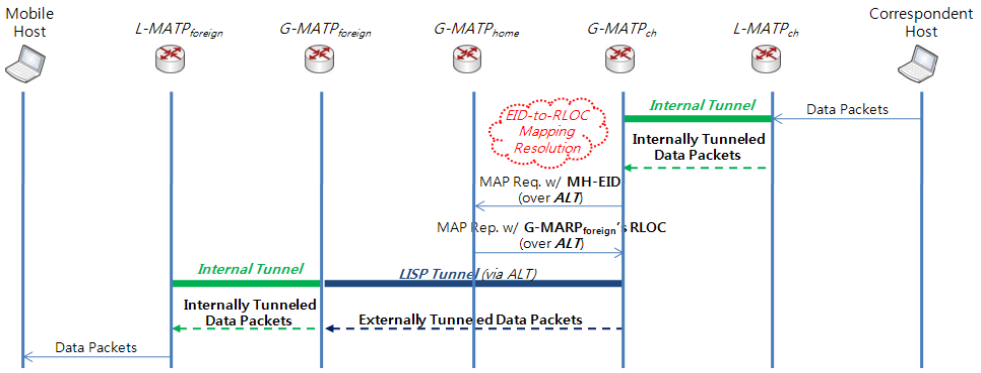

Fig. 4. Communication Procedure between MH and CN

TABLE I
LOCAL MOBILITY: INTRA-DOMAIN HANDOVER

Scenario	Handover Latency
In Home	245(ms)
In Foreign	245(ms)

TABLE II
GLOBAL MOBILITY: INTER-DOMAIN HANDOVER

Scenario	Handover Latency
Home → Foreign	655(ms)
Foreign → Foreign	655(ms)
Foreign → Home	249(ms)

there is no difference between handover latency in a home domain scenario and handover latency in a foreign domain scenario because local mobility is handled by only local entities, e.g., G-MATP, L-MATP, and AAA home (or cache) server. It is noted that a mobile host moving around within a foreign domain can be authenticated by local AAA cache server(s) in the foreign domain. On the other hand, in case of inter-domain handover, handover to a foreign domain takes a little more time than handover to a home domain because it requires a little more time to register a new EID-to-RLOC mapping information at G-MATP$_{home}$.

TABLE III
COMMUNICATION OVERHEAD (MH IN HOME)

Performance Index	CH → MH	MH → CH
Initial Latency	402(ms)	623(ms)
Control Overhead	402(ms)	399(ms)
Transmission Delay	416(ms)	420(ms)
Tunnel Overhead in IPv4	12.672(us)	12.672(us)
Tunnel Overhead in IPv6	22.528(us)	22.528(us)

Table III and IV show kinds of overhead on each one-way communication between a mobile host and a corresponding host. Analysis results reveal that the communication's direction between the mobile host and the corresponding host has more effect on various communication overhead than where the mobile host exists (in a home or foreign domain) does.

TABLE IV
COMMUNICATION OVERHEAD (MH IN FOREIGN)

Performance Index	CH → MH	MH → CH
Initial Latency	401(ms)	616(ms)
Control Overhead	401(ms)	396(ms)
Transmission Delay	416(ms)	422(ms)
Tunnel Overhead in IPv4	12.672(us)	12.672(us)
Tunnel Overhead in IPv6	22.528(us)	22.528(us)

IV. CONCLUSION

In this paper, we extended a LISP+ALT architecture for future Internet to provide global and local mobility effectively. Our proposed network architecture can solve both *routing scalability* and *mobility* which are the most challenging issues when a future Internet architecture is designed. Simple analysis results support our argument. Future works involve how to provide seamless global handover within our network architecture when a mobile host has several ongoing sessions.

ACKNOWLEDGMENT

This research was supported in part by Electronics and Telecommunications Research Institute and in part by the Ministry of Knowledge Economy under the Information Technology Research Center support program supervised by the Institute of Information Technology Advancement (grant number IITA-2008-C1090-0803-0004), 2008, Korea.

REFERENCES

[1] D. Meyer, L. Zhang, and K. Fall, "Report from the IAB Workshop on Routing and Addressing," RFC 4984, September 2007.
[2] D. Farinacci, V. Fuller, D. Oran, and S. Brim, "Locator/ID Separation Protocol (LISP)," draft-farinacci-lisp-09.txt (work in progress), October 2008.
[3] C. Vogt, "Six/One: A Solution for Routing and Addressing in IPv6," draft-vogt-rrg-six-one-00.txt, March 2008.
[4] K.L. Calvert, J. Griffioen, and L. Poutievski, "Separating routing and forwarding: A clean-slate network layer design," IEEE BROADNETS 2007, September 2007.
[5] E. Nordmark and M. Bagnulo, "Shim6: Level 3 Multihoming Shim Protocol for IPv6," draft-ietf-shim6-proto-09.txt, October 2007.
[6] M. O'Dell, "GSE - An Alternate Addressing Architecture for IPv6," draft-ietf-ipngwg-gseaddr-00.txt, February 1997.
[7] R. Moskowitz and P. Nikander, "Host Identity Protocol (HIP) Architecture," RFC 4423, May 2006.

[8] D. Farinacci, V. Fuller, and D. Meyer, "LISP Alternative Topology (LISP+ALT)," draft-fuller-lisp-alt-03.txt (work in progress), October 2008.
[9] S. Gundavelli, K. Leung, V. Devarapalli, K. Chowdhury, and B. Patil, "Proxy Mobile IPv6," RFC 5213, August 2008.