Mobility management and implementation of node addresses in NTMobile

Takuya Nishio, Katsuhiro Naito, Kazuo Mori, and Hideo Kobayashi Department of Electrical and Electronic Engineering, Mie University,
1577 Kurimamachiya-cho, Tsu-shi, 514-8507
Email: nishio@com.elec.mie-u.ac.jp, naito, kmori, koba@elec.mie-u.ac.jp
Hidekazu Suzuki, Akira Watanabe Graduate School of Science and Technology, Meijo University
1-501 Shiogamaguchi, Tenpaku, Nagoya-shi, 468-8502
Email: hsuzuki, wtnbakr@meijo-u.ac.jp

***Abstract*—IP mobility of wireless nodes is an important function in recent years. In conventional networks, Network Address Translation (NAT) is usually used to reduce the consumption of IPv4 global addresses. Therefore, IP mobility have to support not only global IP addresses but also private IP addresses under NATs. NTMobile (Network Traversal with Mobility) is the IP mobility scheme that achieves IP mobility in both global IP addresses and private IP addresses by employing virtual IP addresses and tunnel technologies. In this paper, we propose a management scheme for virtual IP addresses and physical IP addresses in NTMobile. In the proposed scheme, we have implemented a new DNS record for NTMobile in order to manage IP addresses. Therefore, NTMobile nodes can register and update their IP addresses by using dynamic DNS schemes. In the implementation, we have extended BIND to support our record for NTMobile, and implemented the proposed scheme on Linux.**

I. Introduction

With the development of wireless communication technologies in recent years, demands for Internet access from mobile devices are increasing. Also, the mobile devices in recent years have some wireless interfaces. Therefore, mobile devices can switch wireless interfaces connecting to different networks [1]. Network addresses are generally dependent on the connecting networks. Each network has its own network address. As the result, an IP address is changed when a connecting network is switched. On the other hand, higher-layer protocols such as TCP and UDP use an IP address as a connection identifier. Therefore, change of the IP address causes the disconnection of transport layer connection [2].

The technologies, which hide the change of IP address when switching networks, are called IP mobility, and a lot of technologies have been proposed in recent years [3]. However, almost all studies are intended to consider IPv6 networks [4], [5]. On the contrary, there are a little studies about IP mobility in IPv4 networks [6]. In addition, conventional studies have not solved some significant problems. First one is about a NAT traversal problem. Generally, most users use NAT routers in IPv4 networks to reduce the consumption of IP addresses. NAT routers cause some problems in IP mobility due to changing IP addresses in packets. Second one is redundant routes by using the relay device. Redundant routes make a large overhead for communication. [7], [8], [9].

In this paper, we propose IP address management mechanisms for NTMobile (Network Traversal with Mobility) that can achieve a seamless IP mobility. In the proposed mechanisms, we employ DNS (Domain Name System) to store the node information and extend it for the management of a special information about nodes. Our mechanisms are scalable because DNS is a distributed management scheme by nature. We have implemented our mechanisms in BIND, which is well known DNS software.

II. Overview of NTMobile

Main objective of NTMobile is to realize the mobility with low overhead even if end-nodes exist under NAT routers in IPv4 networks. Figure 1 shows the NTMobile network. The system is composed of Direction Coordinator (DC), Relay Server (RS) and NTMobile nodes. It is assumed that DCs and RSs have trust relationships by exchanging authentication keys beforehand. Also, DC and its NTMobile nodes have trust relationships. NTMobile can work with general NATs that may implement SPI (Stateful Packet Inspection), and does not require changing of NAT implementation. Therefore, NTMobile can be used in every IPv4 networks. Furthermore, NTMobile is a scalable system because we can multiply DSs and RSs according to demands.

DC distributes a virtual IP address, which is unique in a NTMobile network, to an NTMobile node. Applications in the node use the virtual IP address to make connections. NTMobile nodes create the tunnel to communicate with each

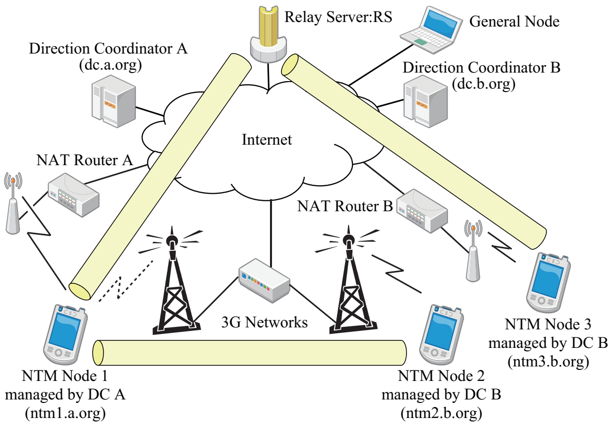

Fig. 1. NTMobile network.

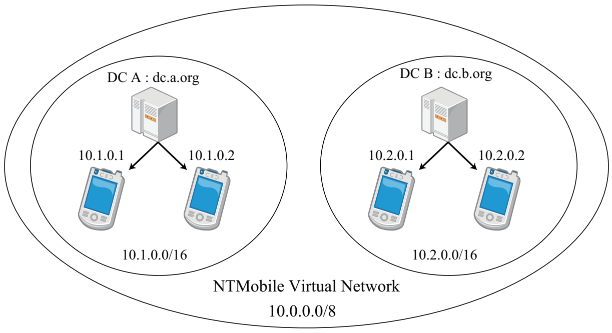

Fig. 2. NTMobile virtual networks.

other. They begin to build the tunnel just after the DNS A query.

In actual communication, applications generate IP packets by using the virtual IP addresses. Then, the kernel module in the node encapsulates the IP packets with the real IP addresses. As the results, applications can use the same virtual IP addresses even if the real IP addresses are changed due to switching networks.

NTMobile nodes create a tunnel directly between end nodes when only one of nodes have a private IP address. Meanwhile, both NTMobile nodes create tunnels with RS when both nodes have private addresses. In this way, NTMobile can achieve seamless mobility both in a global IP address space and a private IP address space.

III. Address and Location Management of NTMobile

A. Address management scheme

In NTMobile, applications communicate by using virtual IP addresses in order to achieve mobility. Each DC is allocated unique IP address ranges beforehand by administrators of the NTMobile network. Then, each DC distributes an unique virtual IP address from the allocated IP address range to an NTMobile node.

Figure 2 shows an overview of the virtual network of NTMobile. In Fig. 2, the address range of 10.0.0.0 / 8 is assumed. In addition, the administrator assigns a part of address range as

TABLE I
DNS Resource record for NTMobile

Record Name	Record Type
Node ID	128 bit
Real IP Address of NTMobile node	32 bit
Real IP Address of NAT router	32 bit
Real IP Address of Direction Coordinator	32 bit
Virtual IP Address of NTMobile node	32 bit

10.1.0.0/16 address for DC A, so DC A manages the assigned address range for its NTMobile nodes. Specifically, DC A assigns a virtual IP address from the assigned address range for its NTMobile node. As the results, NTMobile can achieve simple and scalable management mechanisms for virtual IP addresses because each DC manages its own address range and the number of DC can be increased according to the demand.

B. Location management scheme

In NTMobile, DCs manage the special location information of each NTMobile node. NTMobile employs DNS mechanisms to manage special location information about NTMobile nodes. In the proposal system, we extend DNS mechanisms to support new DNS records for NTMobile. According to RFC 3597, DNS server has to transfer unknown records [10]. Therefore, NTMobile nodes can use a primary DNS server as it is in its network.

Table I shows the elements of the new DNS records for NTMobile. The elements are Node ID for identifying the NTMobile node, Real IP address of NTMobile node, Real IP address of NAT router if NTMobile node exists under a NAT router, Real IP address of DC that manages the NTMobile node, and Virtual IP address of NTMobile node. Real IP address of NAT router is registered by DC by checking the source address.

C. Location registration processing at start up

Figure 3 shows the location registration process when an NTMobile node starts up. The NTMobile node registers its own location information to its DC according to the following procedures.

- Searching procedure for DC's IP address
  NTMobile nodes have to get the IP address of its own DC to inform its location information. In NTMobile, the special DNS record includes DC's address. Therefore, the NTMobile node can find the DC's address from its own FQDN. For example, DC's IP address is RIP_{DC} in Fig. 3.
- Registration procedure for location information
  NTMobile node registers its own location information to its DC by transmitting the Registration Request Message. Registration Request contains information about the node

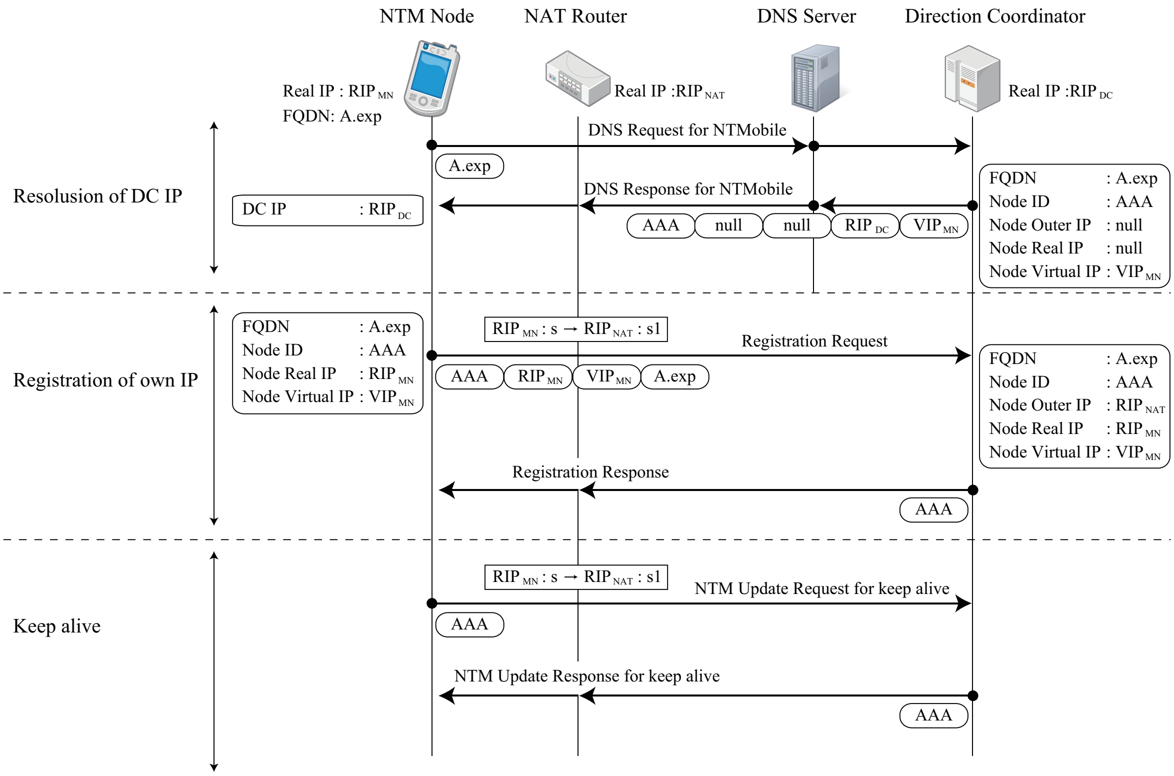

Fig. 3. Registration Process.

ID AAA, the physical IP address RIPMN, the FQDN A.exp. DC can recognize NAT router's IP address by checking the source IP address of Registration Request when the NTMobile node exists under the NAT router. These information is registered in the special record of NTMobile. After the registration process, DC replies Registration Response to the NTMobile node.

- Keep alive procedure for the connection with DC
  NTMobile node have to keep a connection with its DC when it exists under a NAT router because DC cannot initiate a connection with the NTMobile node. Therefore, the NTMobile node transmits Update Request to its DC periodically, and DC replies Update Response to the NTMobile node.

D. Location update procedure for moving to another networks

Figure 4 shows the location update procedures when an NTMobile node moves to another network. The main different point between Fig. 3 and Fig. 4 is to perform the update procedure of location information immediately when the NTMobile node detects a new network, because the NTMobile node has the information about its DC.

- Updating procedure for location information
  NTMobile node updates its own location information to its DC by transmitting the Registration Request Message. After the registration process, DC replies Registration Response to the NTMobile node.
- Keep alive procedure for the connection with DC
  NTMobile node transmits Update Request to its DC periodically and DC replies Update Response to the NTMobile node.

IV. Implementation

A. Implementation of DC

Figure 5 shows the system model of DC in NTMobile. The function of DC is implemented in a user space of Linux, and is classified into the DNS server function and the location management function for NTMobile nodes.

- DNS server function
  DC manages location information of NTMobile nodes as the special DNS records for NTMobile. Therefore, we extend Bind-9.7.1 to support the special DNS records. This modification is required at DC and NTMobile nodes. Therefore, NTMobile can use conventional DNS server in conventional networks. In order to update location information, NTMobile employs Dynamic DNS mechanisms.
- Location Management of NTMobile nodes
  NTMobile nodes inform their own location information to their DC by transmitting Registration Request. DC registers or updates their location information by using Dynamic DNS mechanisms when it receives Registration Request.

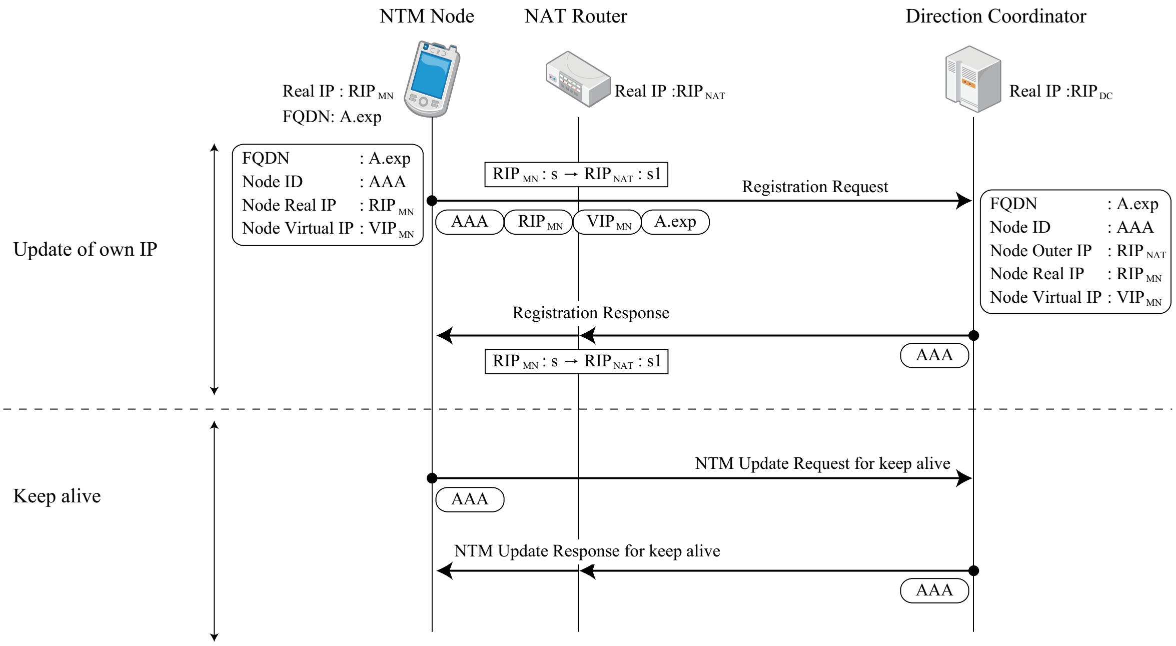

Fig. 4. Update Process.

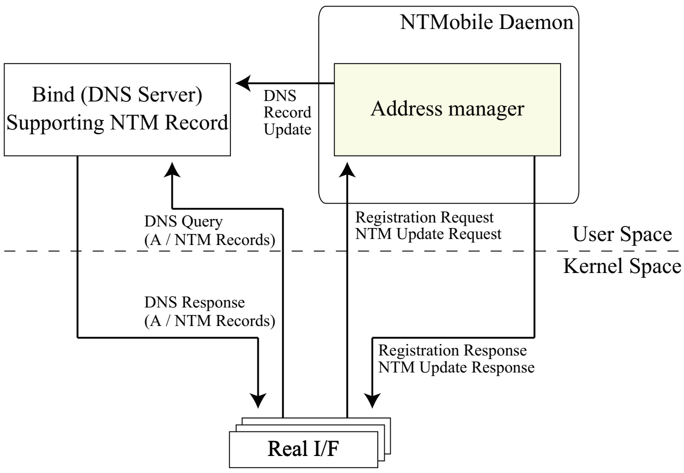

Fig. 5. System model of direction coordinator.

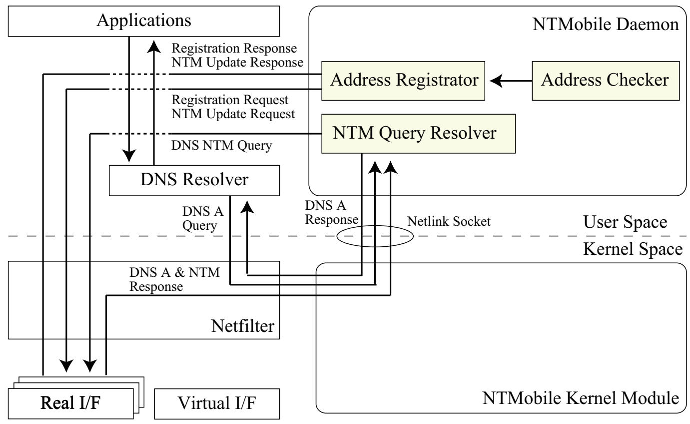

Fig. 6. System model of NTMobile node.

B. Implementation of the NTMobile node

Figure 6 shows the system model of the NTMobile node. The implementation of NTMobile nodes is divided into a user space and a kernel space to achieve high throughput performance. The location management function is implemented in the user space. NTMobile nodes transmit Registration Request when it receives a notification for an address change through Netlink socket of Linux.

- Detection of IP address change
  Linux OS has a notification mechanism for IP address change through Netlink socket. Therefore, NTMobile daemon can receive a notification when an IP address is changed. It obtains the interface information include IPv4 and IPv6 addresses when it receives the notification through Netlink socket.
- Acquisition of DC and a virtual IP address
  NTMobile nodes require their DC's IP address to register their own IP address. Additionally, they need to obtain a virtual IP address for their virtual interface. Therefore, NTMobile Daemon checks a special DNS record of NTMobile with their own FQDN, and obtain the DC's IP address and the virtual IP address.
- Registration of a real IP address
  NTMobile Daemon creates Registration Request and transmits it to its own DC to inform the real IP address when the notification about IP address changes arrives.
- Keep alive for connection to DC
  NTMobile Daemon creates Update Request and transmits it to its own DC periodically to keep the connection to its DC.

TABLE II
EVALUATION PARAMETERS.

OS	Linux
Distribution	Ubuntu 10.04
Kernel version	linux-2.6.32-24-generic
CPU	Intel Pentium 4 2.40GHz
Memory	512 MBytes
BIND	bind-9.7.1

C. Operation check

In order to check the operation of mobility management in NTMobile, we perform laboratory experiments with the developed software. We have verified the operation of the following procedures in making check the operation of implementation technology.

- Acquisition of DC and a virtual IP address
- Registration of a real IP address
- Updating of a real IP address
- Keep alive for connection to DC

DC receives Registration Request and Updating Request from many NTMobile nodes. Therefore, processing time in DC is important. In the experiment, we measured the processing time about a special DNS record of NTMobile. The processing starts when DC receives a Registration Request, and ends when the updating process of DNS completes. The results are obtained by 10 times measurements. The average processing time was about 5.55 [ms]. We also measured the processing time about A record in the same situation. The average processing time was about 5.51 [ms]. Therefore, the processing time in DC is not big overhead.

V. CONCLUSIONS

This paper has proposed a mobility management scheme for an NTMobile network. The feature of our scheme is to manage the mobility information as special DNS records. Therefore, the proposed mechanism can employ some Direction Coordinators to manage a lot of NTMobile nodes similar to DNS. Additionally, we can confirm that the processing time in DC is not big overhead according to the measurement results. As the results, our mechanism has enough scalability to support large number of nodes and achieve mobility management for the NTMobile network.

REFERENCES

[1] M. Buddhikot, G. Chandranmenon, S. Han, Y. W. Lee, S. Miller and L. Salgarelli, "Integration of 802.11 and third generation wireless data networks," Proceedings of the IEEE INFOCOM 2003, Vol. 1, Page(s): 503-512, 2003.

[2] L. A. Magagula and H. A. Chan, "IEEE802.21-Assisted Cross- Layer Design and PMIPv6 Mobility Management Framework for Next Generation Wireless Networks," Proc. IEEE WIMOB f08, pp. 159-164, Oct. 2008.

[3] D. Le, X. Fu and D. Hogrefe, "A Review of Mobility Support Paradigms for the Internet," IEEE Communications Surveys & Tutorials, Vol.8, No.1, pp.38-51, 2006.

[4] N. Seta, H. Miyajima, L. Zhang, H. Hayashi and T. Fujii, "All-SIP Mobility: Session Continuity on Handover in Heterogeneous Access Environment," in Proc. of IEEE VTC2007-Spring, pp.1121-1126, 2007.

[5] H. Miyajima, L. Zhang, H. Hayashi and T. Fujii, "An Implementation of Enhanced All-SIP Mobility," in Proc. of IEEE PIMRC2008, 2008.

[6] H. Suzuki, K. Terazawa and A. Watanabe, "Implementation of NAT Traversal for Mobile PPC with the Principle of Hole Punching," in Proc. of the IEEE International Region 10 Conference 2009 (TENCON2009)CNov.2009.

[7] C. Perkins, "IP Mobility Support for IPv4, Revised," RFC 5944, IETF (2010).

[8] M. Bonola, S. Salsano and A. Polidoro, "UPMT: universal per-application mobility management using tunnels," In Proc. of the 28th IEEE conference on Global telecommunications (GLOBECOM'09) 2009.

[9] M. Bonola and S. Salsano, "S-UPMT: a secure Vertical Handover solution based on IP in UDP tunneling and IPsec," GTTI Riunione Annuale 2010, (online), http://www.gtti.it/GTTI10/papers/gtti10 submission 29.pdf, 2010.

[10] A. Gustafsson, "Handling of Unknown DNS Resource Record (RR) Types," RFC 3597, September 2003.