IP Address Management with Fault-Tolerant Support in Mobile IP Networks

Chia-Ho Ou Kuo-Feng Ssu Hewijin Christine Jiau

Department of Electrical Engineering
National Cheng Kung University
Tainan, Taiwan 701

Contact:

Kuo-Feng Ssu
Department of Electrical Engineering
National Cheng Kung University
Tainan, Taiwan 701
ssu@ee.ncku.edu.tw
Phone: 886-6-2757575 ext. 62331
Fax: 886-6-2345482

Abstract

The Internet Protocol (IP) plays an important role of wireless mobile networks. As the need of connecting to the Internet increases enormously, the address starvation problem for the IP version 4 (IPv4) has appeared gradually. Many companies and institutes thus use private IP addresses to conquer the problem. However, private IP addresses are not currently supported in mobile IP networks. Several approaches were proposed to support private IP addresses using the Network Address Translator (NAT) function with mobile IP. The approaches may lead to erroneous routing if no available IP address exists in home network. This paper presents an mechanism that can help the home agent to obtain a global IP address from supported foreign agents when the home agent cannot provide a global IP address. The paper also describes fault-tolerant techniques to strengthen the operation of the vital agents in the mobile network. When agents fail, redundant agents can take over rapidly and resume normal operation.

Keywords: Internet protocol, private IP addresses, mobile IP, fault tolerance.

1 Introduction

Wireless mobile networks are currently toward the fully Internet Protocol (IP) based network architecture [1–4]. The IP thus plays an important role of mobile networks. The IP-based mobile network requires that every mobile node have its own address. The IP address space of IPv4 could be short in a few years since the need of using the Internet increases enormously. In order to solve the address starvation problem, the IP version 6 (IPv6) [5, 6] that increases in address size from 32 bits to 128 bits was introduced by the Internet Engineering Task Force (IETF). However, the IPv6 is barely exploited due to the cost and efforts required to migrate from IPv4 to IPv6 [7]. On the other hand, Private IP addresses and the Network Address Translator (NAT) [8] function are usually adopted to solve the problem in IPv4. The NAT function maintains a table that contains private IP addresses and its correspondent global IP addresses. Computers use private IP addresses in a closed personal network and utilize global IP addresses in the Internet. The NAT function can manage global IP addresses without changing original operations of routers.

Some approaches were proposed [9–11] to solve the starvation problem using private IP addresses. Mobile nodes can use their private IP addresses for communication within both the home network and visited networks. Integration of Domain Name System (DNS) server and NAT function converts global IP addresses for the mobile nodes. Hierarchical structure of foreign agents is used for reducing latency during handoff and registration. When a mobile node needs to communicate with others, the home agent with NAT function assigns a global IP address to mobile node. The mobile node uses the global IP address to connect to the Internet.

The previous approaches obtain global IP addresses only from the home agent. This paper introduces a global IP address management scheme to solve the starvation problem. If global IP addresses of the home agent are not enough, the home agent can ask a gateway foreign agent to provide global IP addresses. Mobile nodes are thus able to use the global IP addresses for communication. The main advantage of our approach include better utilization of global IP addresses and higher rate of successful routing.

Failure of vital agents (home agents, gateway foreign agents, and foreign agents) can discontinue the network connection of mobile nodes. Therefore, fault-tolerant capability is necessary to enhance mobile IP operations. In our mechanism, two or more redundant vital agents cooperate together in the mobile network. If a vital agent does not function correctly, the others can immediately resume normal operation.

2 Related Work

2.1 Private IP Addresses in Mobile IP

Several approaches were proposed to enable mobile IP [12] with private IP addresses in recent years. They integrated regional registration mobile IP, the NAT function, and a DNS server to support mobile nodes with private IP addresses. A mobile node is allowed to use the same private IP address as its home address for communication in both the home network and visited network. When a gateway foreign agent detects communication is required between the mobile node and a correspondent node, the gateway foreign agent will ask the home agent to provide a global IP address from the global IP addresses pool of the home agent.

2.2 Home Agent Redundancy Protocol

In mobile IP network, a home agent is a router or a host located on the border of the home network. Packets delivered to mobile nodes are first sent to the home agent. The home agent then forwards the packets to mobile nodes in visited network. If the home agent fails, no data will be delivered to the mobile nodes. The HARP (Home Agent Redundancy Protocol) [13] allows two or more home agents to cooperate and share registration information of mobile nodes. The design of redundant home agents prevents system crash due to a single point of failure.

All home agents share an identical IP address in the HARP. The mobile nodes do not know about the redundant home agents. When a mobile node needs to register, it just sends registration information to the IP address. When one home agent gets the packets, it will encapsulate registration packets and forward them to the other home agents. Two kinds of home subnet, the Non-partitioned Home Subnet and the Partitioned Home Subnet, are supported in this protocol. The home agents can connect directly one another in the non-partitioned home subnet; The home agents must use tunnels [14, 15] for communication in the partitioned home subnet.

2.3 Fault-Tolerant Mobile IP

Fault-Tolerant Mobile IP [16] proposed a mechanism to recover failure in the mobile IP system. Redundant home agents and foreign agents are utilized in the mobile networks. The redundant agents will resume execution when the failure occurs. Unlike HARP, Fault-Tolerant Mobile IP does not support home agents in the partitioned home subnet.

3 System Architecture Overview

3.1 System Requirements

The network system is based on the mobile IPv4 network with private IP addresses. The global IP addresses are used for communication over the Internet; private IP addresses can be used only in the local network. Nodes with private IP address cannot be located in the Internet.

Home agents and foreign agents support NAT function to assign global IP addresses to mobile nodes that use private IP addresses. Every mobile node during communication has its own global IP address assigned by a home agent or a foreign agent. When a mobile node communicates with others, gateway foreign agents with NAT function will convert the private IP address to the correspondent global IP address for the mobile node.

The correspondent node cannot communicate with the mobile node using a private IP address. The correspondent node has to know Fully Qualified Domain Name (FQDN) of the mobile node and then asks the DNS server in the home network for obtaining the global IP address of the mobile node. The DNS server maintains a mapping between the private IP address and the FQDN of mobile node.

The architecture of hierarchical foreign agents [17] is used in our mechanism. The gateway foreign agent controls several foreign agents and can request the foreign agents for global IP address assignment. An important advantage of the architecture is that handoff and registration overhead is reduced for mobile nodes. The mobile nodes simply perform a regional registration if they move from old foreign network to new foreign network that is controlled by the same gateway foreign agent.

3.2 Network Architecture

As shown in Figure 1, the network architecture based on hierarchical mobile IPv4 consists of Home Agents (HA), Foreign Agents (FA), and Gateway Foreign Agents (GFA).

- Home networks and foreign networks are consisted of closed networks with private IP addresses. Each mobile node (MN) has a home address that is a private IP address assigned by the HA. The home address of MN is not changed even though the MN moves to a foreign network.

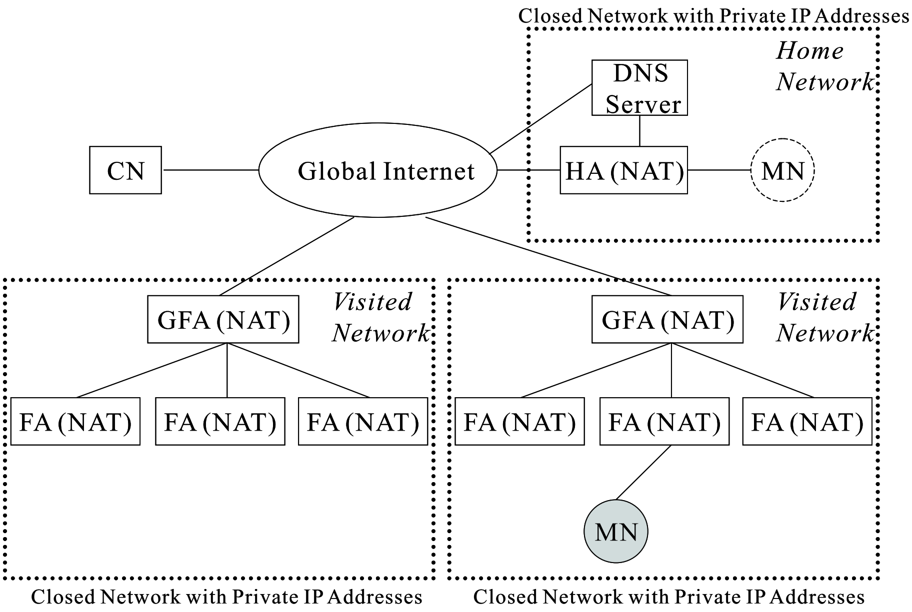

Figure 1: Network architecture.

- HAs and FAs have their own global IP addresses and provide the NAT function to manage shared global IP addresses. The NAT function supports nodes with private IP addresses for connecting to the Internet.

- The GFA has its own global IP address and the NAT function works as gateway of several FAs of the visited network. The MN uses FA's IP address as Local Care-Of Address (LCOA) registered at the GFA and also uses GFA's IP address as Global Care-Of Address (GCOA) registered at the HA.

- The lifetime of the global IP address will be extended when the GFA detects that the mobile node communicates with others through the Internet. The GFA sends the information of the lifetime to the agents (HA or FA) which provides the global IP address.

3.3 Global IP Address Management

3.3.1 Mobile Node Communicates with Correspondent Node

An MN cannot directly uses its private IP address to communicate with others. The HA and FA can assign a global IP address to the MN for exchanging data over the Internet.

Table 1: Global IP Addresses Mapping Table

FAID	Available global IP addresses	Total amount of global IP addresses	Percentage (%)
FA1	5	10	50%
FA2	4	5	80%
FA3	2	6	33%

When an MN delivers data packets to a correspondent node (CN) across the Internet, the GFA examines whether the MN has a global IP address. If no global IP address assigned to the MN, the GFA sends a Global IP Address reQuest (GAQ) message to the HA. The HA receives the message and then checks its managed global IP addresses. If there are available global IP addresses for the MN, the HA will send a Global IP Address Reply (GAR) message to the GFA. If the HA does not have global IP addresses left, it will send the GAQ message to the GFA. The GFA then checks its own usage of global IP addresses using an address mapping table (see Table 1). The GFA selects an FA that has the highest percentage of the available global IP addresses to provide a global IP address. The FA assigns a global IP address to the MN and sends a GAR message back to the GFA. The GFA relays the message to the HA. Finally, the GFA converts the source address of the delivered packet sent by MN and relays packets sent by the MN to CN using normal routing procedures.

3.3.2 Correspondent Node Communicates with Mobile Node

An CN is required to know FQDN of the MN to communicate the MN with a private IP address. To obtain the global IP address of the MN, the CN asks for the related DNS server using the FQDN of the MN. After the DNS server catches the message, it sends the GAR message to the HA if the MN does not have a global IP address. If the HA has available global IP addresses, it will assign one to the MN and sends a Global IP Address Informing (GAI) message to the GFA. If the HA does not have any available global IP address, it will send the GAQ message to the GFA. The GFA checks its global IP address mapping table (see Table 1). After the GFA selects an FA, it relays the GAQ message to the FA. The FA assigns a global IP address to MN and then sends the GAR message to the GFA. The GFA relays the message to the HA. The DNS server sends a DNS Answer message to the CN. Therefore, the CN knows the global IP address of the MN and starts to deliver data packets to the MN. If the global IP address is assigned by the FA, the packets will be directly delivered to the GFA; if the global IP address of MN assigned by HA, the packets will be transmitted to the GFA through the HA. The GFA converts the destination address of the packets to the corresponding private IP address of MN. The GFA relays the packets to the MN via the FA.

With route optimization [18] supported by the HA and the CN, the CN is able to cache the binding of the MN and tunnel packets to the GFA directly. The GFA receives the packets and relays the packets to the FA where the MN is located. The FA then forwards the packets to the MN.

3.3.3 Handoff Management

The CN is not aware that the mobile node moves to a new gateway foreign agent. Consequently, the CN still delivers data packets to the original GFA. The data packets are lost because the original GFA does not know where the MN is. Moreover, the global IP address of the MN is occupied and cannot be released for other nodes.

Our mechanism supports smooth handoff. The previous GFA maintains a binding for its former visited mobile nodes. The binding contains the current GCOA of the former visited mobile node. When data packets are sent to the previous GFA, they will be forwarded to the current GCOA of the MN. Therefore, the MN is able to receive data packets continuously even if the MN moves off the original GFA.

4 Fault-tolerant Support

The system architecture comprises home agents, foreign agents and gateway foreign agents. These essential agents are indispensable to operations in the system. The failure in our system can be divided into three parts:

- Failure of the home agents: The home agent forwards data packets for the mobile nodes and also receives registration information from the mobile nodes. If the home agent fails, the mobile nodes cannot receive data packets from the Internet.

- Failure of the gateway foreign agents: The gateway foreign agent works as gateway of several foreign agents of the visited network. It is the only connection of point of the visited network that can reach outside networks. Furthermore, it is responsible for conversion between private IP addresses and global IP addresses when mobile nodes are communicating. The failure of a gateway foreign agent causes the loss of connection of its visited network.

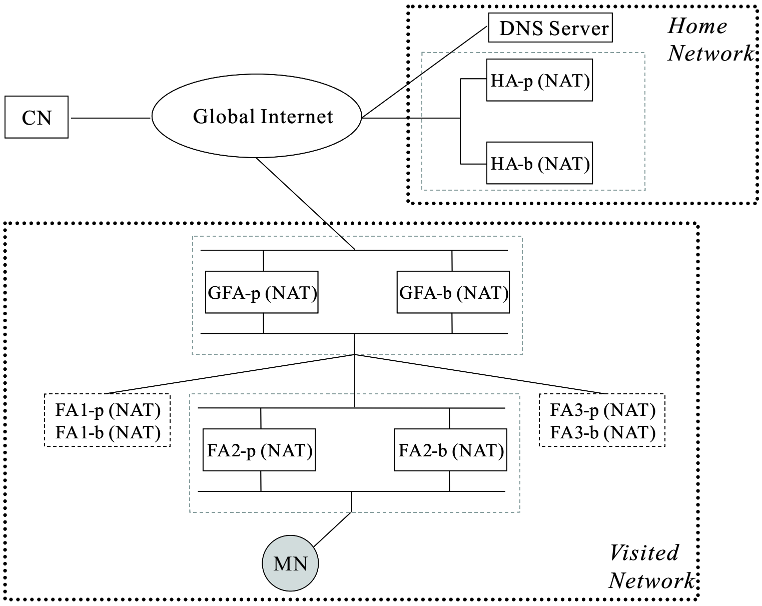

Figure 2: Integrated network architecture.

- Failure of the foreign agents: The foreign agent is in charge of supporting to assign global IP addresses when the home agent does not have enough global IP addresses. Failure of a foreign agent is not typically critical for global address assignment. The gateway foreign agent can choose another foreign agent to assign global IP addresses. The only impact of the failure of the foreign agent is the loss of network connection of all mobile nodes within its coverage.

4.1 Redundant Agents

Figure 2 shows the system integration with three kinds of the redundant agents collaborating together. In the integrated architecture, the messages or data packets of other agents or mobile nodes are always delivered to the primary agent. If the received messages are related to the primary agent, the primary agent will forward them to the backup agent. Otherwise, the primary agent just relays the messages or data packets. With the scheme, registration, global IP address assignment, and data transmission are completely supported with fault tolerance in the integrated mobile network. The detailed procedures will be presented latter.

Our approach assumes that the primary agent and the backup agent are in the non-partitioned home subnet. In Figure 2, redundant home agents that consists of the primary home agent (HA-p) and the backup home agent (HA-b). The redundant mechanism for foreign agents are the primary foreign agent (FA-p) and backup foreign agent (FA-b). Furthermore, replication of gateway foreign agents is essential

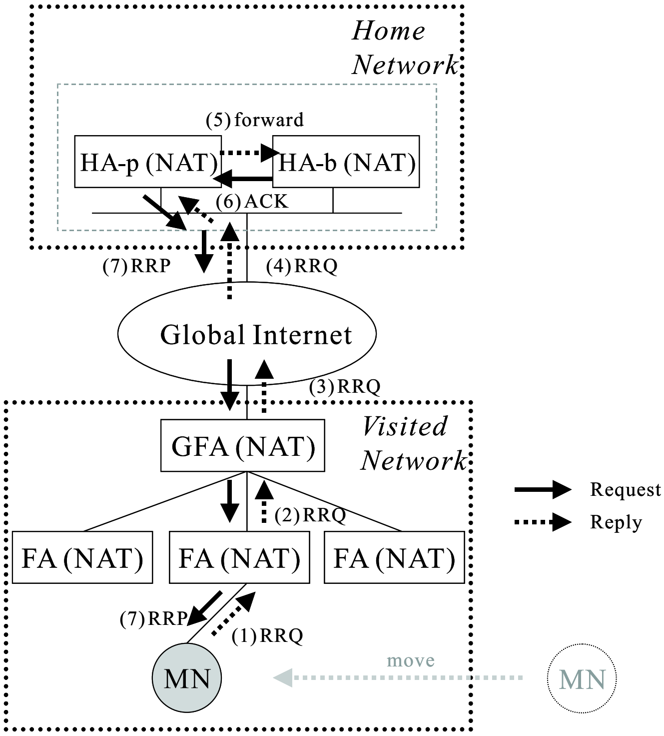

Figure 3: Home registration of redundant home agents.

because it can catch data packets of the mobile nodes and detect whether they communicate with other nodes or not. The redundant gateway foreign agents are the GFA-p and GFA-b.

4.1.1 Home Registration

In the hierarchical mobile IP, the mobile nodes will launch the home registration via the visited network. The detailed process of home registration is described below (see Figure 3).

1. When the MN moves from an old GFA to a new GFA, the MN sends the Registration ReQuest (RRQ) message to its current FA.

2. The FA relays the RRQ message to its GFA. The FA also registers its IP address to its GFA as the LCOA of the MN.

3. The GFA replays the RRQ message to the MN's HA for authentication.

4. The HA-p receives the RRQ message first.

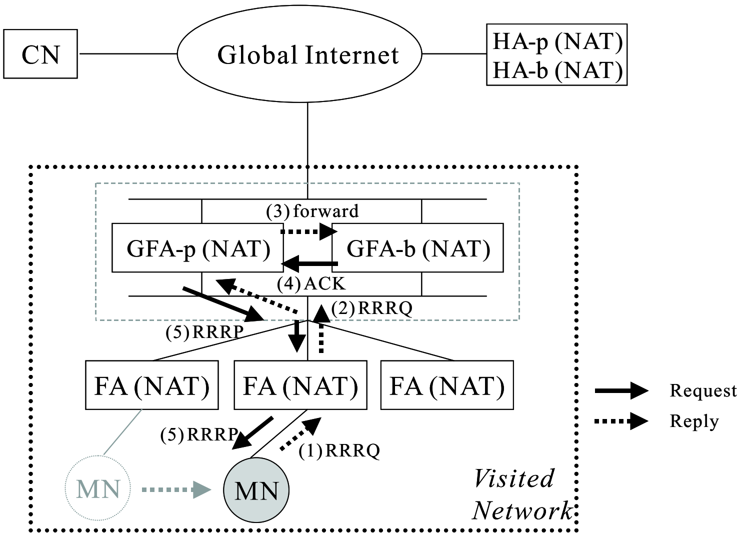

Figure 4: Regional registration of redundant gateway foreign agents.

5. The HA-p updates the mobility binding between the MN's home address and GCOA. After successful authentication, the HA-p forwards binding information to the HA-b.

6. The HA-p receives the ACK message that confirms that the HA-b received the binding information.

7. The HA-p sends the Registration RePly (RRP) message back to the MN.

4.1.2 Regional Registration

When the mobile nodes sends regional registration information to the primary gateway foreign agent, it will forward the information to the backup gateway foreign agent. The detailed process of regional registration is described below (see Figure 4).

1. When the MN moves from an old FA to a new FA in the same GFA, the MN sends the Regional Registration ReQuest (RRRQ) to the new FA first.

2. The FA relays the RRRQ message to the its GFA. Then the GFA-p receives the message.

3. The GFA updates the mobility binding between MN's home address, LCOA, and then forward them to the GFA-b.

4. The GFA-b returns the ACK message to the GFA-p.

5. The GFA-p sends the Regional Registration RePly (RRRP) message to the MN.

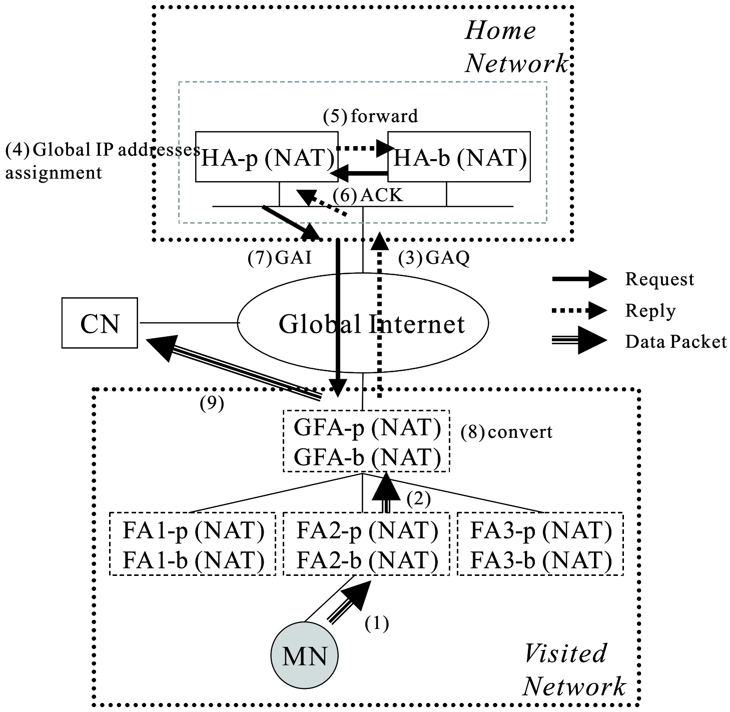

Figure 5: Global IP addresses assignment of redundant home agents.

4.1.3 Global IP Addresses Assigned by HA

When the mobile node communicates with other nodes, the home agent needs to assign a global IP address to the mobile node. After the primary home agent assigns a global IP address to the mobile nodes, it will forward the information, including IP addresses mapping and lifetime, to the backup home agent. Figure 5 shows the process of the global IP address assignment of redundant home agents.

1. The MN delivers data packets destined to the CN to the FA first.

2. The FA receives the packets and tunnels them to the GFA.

3. The GFA verifies whether the MN has a global IP address. If not, the GFA sends a Global IP Address reQuest (GAQ) message to the HA-p. Otherwise, the MN uses the global IP address for communication.

4. When the HA-p receives the message, it assigns a global IP address to the MN.

5. The HA-p forwards the lifetime and the mapping between the private IP address and the global IP address of the MN to the HA-b.

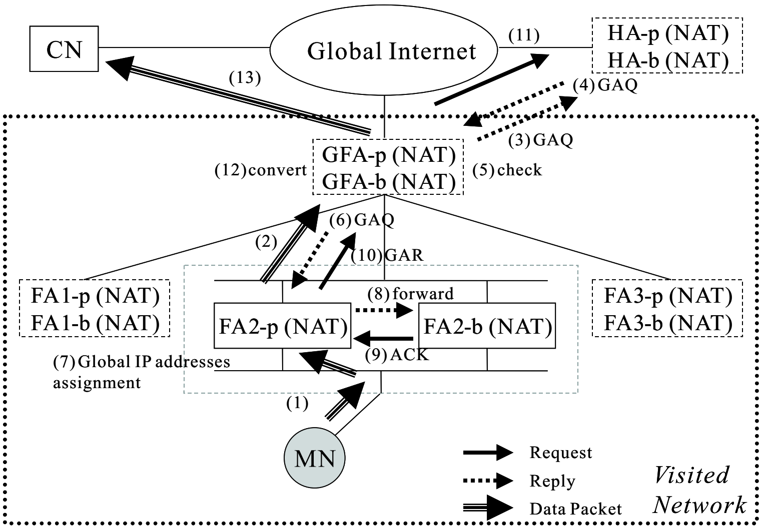

Figure 6: Global IP addresses assignment of redundant foreign agents.

6. The HA-b sends an ACK message to the HA-p.

7. The HA-p sends the Global IP Address Informing (GAI) to the GFA. The GFA updates the mapping of IP addresses.

8. The GFA converts the source address of the delivered packets to the global IP address of the MN.

9. The GFA relays data packets to the CN using normal routing procedures.

4.1.4 Global IP Addresses Assigned by FA

Assume global IP addresses of the home agent are unavailable for the mobile nodes. The GFA chooses a foreign agent with the highest percentage of the available global IP addresses within the coverage. The primary foreign agent assigns a global IP address to the mobile node and also forwards the assignment information to the backup foreign agent. The following describes detailed global IP address assignment by FA (see Figure 6).

1. The FA-p receives data packets destined to the CN form the MN.

2. The FA-p tunnels the received packets to the GFA.

3. The GFA verifies if there is a global IP addresses assigned to the MN. If the MN does not own a global IP address, the GFA sends a Global IP Address reQuest (GAQ) message to the HA.

4. The HA sends the GAQ message to the GFA due to that home agent has unavailable global IP addresses.

5. The GFA checks its global IP address mapping table. The GFA chooses an FA that has the highest percentage of the available global IP addresses to assign a global IP address to the MN.

6. The GFA relays the message to the FA. The message will be received by the FA-p.

7. The FA-p assigns a global IP address to the MN.

8. The FA-p forwards the address mapping and lifetime to the FA-b.

9. The FA-b sends an ACK message to the FA-p.

10. The FA-p sends a Global IP Address Reply (GAR) message back to the GFA. The GFA then updates the related address mapping and lifetime.

11. The GFA relays the message to the HA. Both the HA-p and the HA-b update the mapping information.

12. The GFA converts the source address to the global IP address of MN for the delivered packets.

13. The GFA relays data packets to the CN.

4.2 Failure Handling and Recovery

The fault-tolerant mechanism ensures that mobile nodes can still maintain the Internet connection when failure occurs in the network system. Redundant agents take over and resume operations transparently. When failed agents recover, they will synchronize with the operated redundant agents to obtain the latest system information.

4.2.1 Failure Recovery for Primary Agents

As illustrated in Figure 7, when the mobile nodes or other agents send messages to the primary agent and the primary agent does not respond in a predefined time, the primary agent will be considered faulty. The mobile nodes retransmit the messages to the backup agent for informing the failure of the primary agent. The backup agent thus takes control of the work of the primary agent. When the primary agent

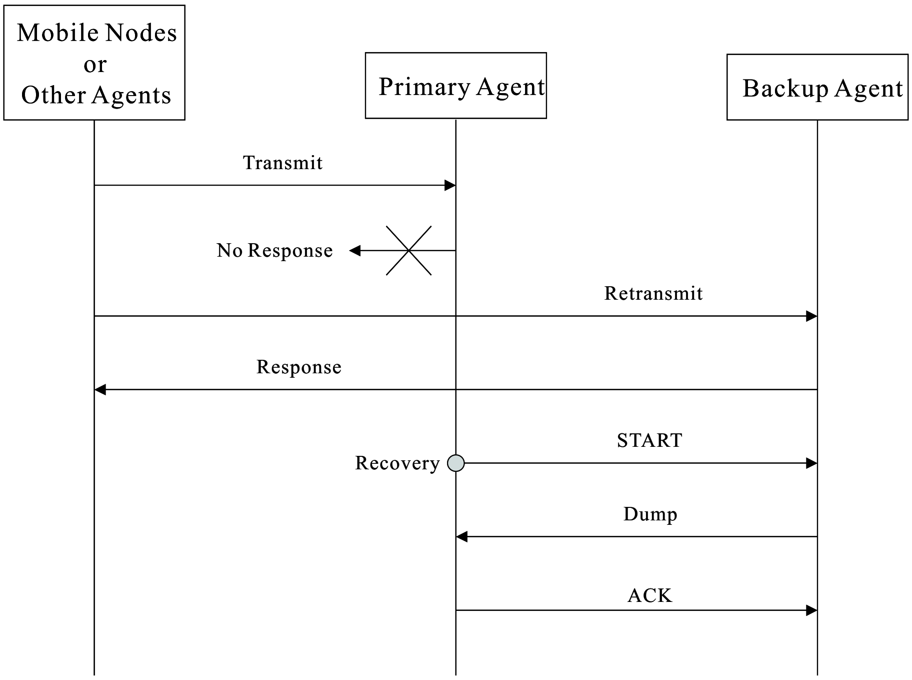

Figure 7: Failure recovery for the primary agents.

is recovered from the failure, it will send an START message to the backup agent. The backup agent transmits updated information to the primary agent. After the primary agent receives the information, it sends an ACK message to the backup agent.

4.2.2 Failure Recovery for Backup Agents

On the other hand, in Figure 8, when the backup agent fails, the primary agent will stop sending information to the backup. Once the backup agent restarts, it sends an START message to the primary agent. The primary agent then transmits needed states to the backup agent and also starts to synchronize with the backup agent.

5 Conclusion and Future Work

The mechanism described in the paper has three advantages: efficient usage of IP address, fault tolerance, and transparency. Mobile nodes can obtain global IP addresses from their HAs for wireless communication. Foreign agents can also provide global IP addresses if the home agents do not have available global addresses. The mechanism can tolerate the failure of the home agents, foreign agents and gateway foreign agents. The redundant agents will recover the network system and take control of

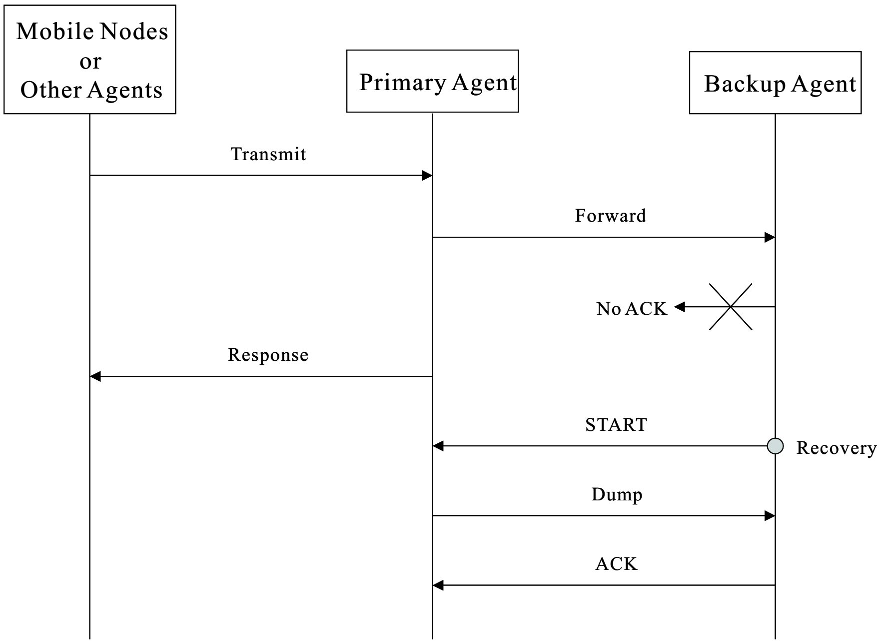

Figure 8: Failure recovery for the backup agents.

the operations if the failure occurs. Mobile nodes are not aware of existence of the redundant agents during normal operation or failure recovery.

The future work is to implement a prototype of the mobile network architecture with redundant home agents, foreign agents, and gateway foreign agents. Experiments, measurements, and performance evaluation will be included.

References

[1] S. Uskela, "All IP Architectures for Cellular Networks," *Proceedings of IEEE 3G Mobile Communication Technologies*, pp. 180–185, Mar. 2001.

[2] G. Patel and S. Dennett, "The 3GPP and 3GPP2 Movements Toward an All-IP Mobile Network," *Proceedings of IEEE Personal communications*, pp. 62–64, Aug. 2000.

[3] 3rd Generation Partnership Project (3GPP). URL http://www.3GPP.org.

[4] 3rd Generation Partnership Project 2 (3GPP2). URL http://www.3GPP2.org.

[5] S. Deering and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification," RFC 2460, Dec. 1998.

[6] D. Johnson and C. Perkins, "Mobility Support in IPv6," IETF Draft, Nov. 2000.

[7] G. Lawton, "Is IPv6 Finally Gaining Ground?," *IEEE Computer Magazine*, vol. 34, no. 8, pp. 11–15, Aug. 2001.

[8] K. Egevang and P. Francis, "The IP Network Address Translator (NAT)," RFC 1631, May. 1994.

[9] T. Kato, A. Idoue, and H. Yokota, "Mobile IP Using Private IP Addresses," *Proceedings of IEEE Computers and Communications*, pp. 491–497, July 2001.

[10] A. Idoue, H. Yokota, and T. Kato, "Mobile IP Network Supporting Private IP Addresses Utilizing Regional Registration and NAT Function," *Proceedings of IEEE Parallel and Distributed Systems*, pp. 141–146, June 2001.

[11] J. Malinen, "Using Private Addresses with Hierarchical Mobile IPv4," Helsinki University of Technology, Mar. 2000.

[12] C. Perkins, "IP Mobility Support," RFC 2002, Oct. 1996.

[13] "Home Agent Redundancy Protocol," Bjorn Chanbless Portland State University and Jim Binkley Oregon Graduate Institute, Internet Draft, Oct. 1997.

[14] C. Perkins, "IP Encapsulation within IP," RFC 2003, Oct. 1996.

[15] C. Perkins, "Minimal Encapsulation within IP," RFC 2004, Oct. 1996.

[16] R. Ghosh and G. Varghese, "Fault-Tolerant Mobile IP," Tech. Rep. WUCS-98-11, Washington University, Apr. 1998.

[17] E. Gustafsson, A. Jonsson, and C. Perkins, "Mobile IP Regional Registration," IETF Draft, Sept. 2001.

[18] C. Perkins and D. Johnson, "Route Optimization in Mobile IP," IETF Draft, Nov. 2000.