Fault-Tolerant Cellular IP with Multiple Gateways

Chia-Ho Ou[1,*], Kuo-Feng Ssu[2], and Wen-Jia Zhang[3]

[1] Department of Computer Science and Information Engineering,
National Pingtung Institute of Commerce,
Pingtung 900, Taiwan, ROC
cho@npic.edu.tw

[2] Department of Electrical Engineering,
National Cheng Kung University,
Tainan 701, Taiwan, ROC
ssu@ee.ncku.edu.tw

[3] Research and Development Department,
Skymedi Corporation,
Hsinchu 300, Taiwan, ROC
aga_chang@skymedi.com.tw

Received 27 February 2009; Revised 11 August 2009; Accepted 17 October 2009

Abstract. The Cellular IP protocol utilizes a gateway architecture to achieve better handoff performance. However, the gateway may become a single point of failure in the network. If the gateway fails, the domain network serviced by the gateway will be disconnected. This issue is not addressed in the original Cellular IP design. This paper introduces the concept of multiple gateways for tolerating failures on the gateways, the base stations, and the communication links. The gateways coordinate with each other for serving the mobile nodes. When failures occur, an available gateway will take over the operations. The fault-tolerant Cellular IP protocol was evaluated using the network simulator ns-2. The results show that the protocol not only improved the disconnection time but had little impact on the transmission performance.

Keywords: Cellular IP, fault tolerance, multiple gateways, micro-mobility

1 Introduction

With wireless communication and mobility management, the portable devices can continuously access the Internet services when they are moving. Two designs were developed for the mobility management. One is macro-mobility design, Mobile IP [1, 2, 3], and the other is micro-mobility development [1, 4, 5]. With the Mobile IP protocol, each mobile node (MN) has a permanent home address wherever it moves in the Internet. While away from its home network, the MN needs to inform its home agent (HA) of its latest location, i.e., care-of address (CoA). If a correspondent node (CN) delivers packets to the MN, the HA will intercept packets and tunnel them to the foreign agent (FA) that the MN is visiting. The FA then forwards packets to the MN. Note that tunneling is a packet encapsulated within the payload portion of another packet [2]. With the route optimization [2], the CN can cache the current location of the MN and tunnel packets to the MN directly bypassing the route for each packet through the MN's HA. However, when the MN changes its network location frequently, the Mobile IP mechanism introduces significant network overhead in terms of increased delay and packet loss. This delay is incurred as the registration request is sent to the HA and the response sent back to the FA. On the contrary, micro-mobility protocols are designed for handling local movement (i.e., within a domain network) of MNs. With micro-mobility, the MN notifies its nearby gateways for reducing delay and packet loss during handoff and eliminating registration between itself and the HA when it remains inside its domain network. Therefore, the micro-mobility development achieves a better handoff performance.

Cellular IP is one of the micro-mobility protocols [6, 7]. A Cellular IP network consists of several domain networks and each domain network attaches to the Internet through a gateway (see Fig. 1). A domain network is composed of several nodes, such as switches and base stations. The gateway periodically broadcasts the gateway broadcast packet to its domain network so the nodes receiving the packet can establish their up-link paths. The

* Correspondence author

MNs also periodically send the route-update and/or the paging-update packets to the gateway. Each intermediate node obtaining the packets updates its routing and/or paging cache and then forwards the packets to its up-link. The gateway uses the reverse path to transmit data packets to the MN. Cellular IP also provides a power saving mechanism. If an MN does not send or receive any packets during a time interval, the MN will enter an idle mode. Each node maintains the paging-cache for the idle MNs for the passive connection.

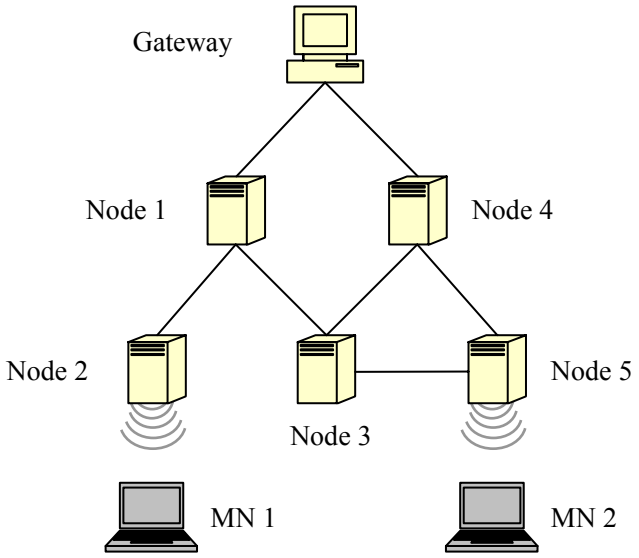

Fig. 1. A Cellular IP network

The gateway is a single point of failure in the Cellular IP Network. If the gateway crashes, its domain network cannot communicate with other domains. The original Cellular IP protocol did not address the issue. In addition, the previous fault-tolerant protocol, Hot Standby Router Protocol (HSRP) [8], cannot work correctly when the protocol are applied to Cellular IP. In the wired networks, most hosts typically use only one default router for delivering data. If the selected router fails, the host cannot communicate with Internet. HSRP developed by Cisco uses duplicated routers, called an HSRP group, to service the hosts in the subnet. An active-router performs as a virtual router for all hosts. Another router, called standby-router, is selected for failure detection and replacement. HSRP did not mention load balancing or network partition in the current implementation. Additionally, HSRP was essentially designed for the wired environments so mobility issues were not considered. This paper uses multiple gateways with fault-tolerant schemes to achieve fault detection and recovery. Multiple gateways cooperate with each other in a domain network. The gateways can balance service load during the failure-free operation. When one gateway fails or the network partition occurs, available gateways will recover the communication service rapidly so the MNs will not be aware of the failures.

Three mechanisms, including single gateway, multiple gateways, and multiple gateways with fault-tolerant support in Cellular IP, have been implemented and evaluated using the network simulator ns-2 [9, 10]. The simulation results show that our fault tolerant mechanism can recover from failures and also improve up to 50% of the disconnection time compared to multiple gateways mechanism. Moreover, our approach had competitive throughput and transmission delay in the failure-free execution scenarios.

2 Cellular IP with Multiple Gateways

As shown in Fig. 2, multiple gateways are deployed in a Cellular IP network. The gateways periodically propagate gateway broadcast packets to their domains for announcing their existence and information (e.g., current load). Each node has a watchdog timer for detecting available gateways in the network. The nodes broadcast beacons with the gateway information periodically so visiting MNs are able to locate the available gateways. If the node does not receive any gateway broadcast packet from a gateway in a predefined time interval repetitively, the gateway will be considered failed.

After an MN enters the Cellular IP network, the MN will select a gateway for registration. The base stations broadcast beacons that contain load information (i.e., the number of MNs serviced by a gateway) so the MN can make their decisions on gateway selection accordingly. The MN inserts the IP address of the selected gateway in its route-update packet and then sends the packet to the gateway periodically. The nodes receiving the packet

maintain the position of the MN and the gateway's information in their route caches. Thus, the nodes learn how to forward packets for the MN. For example, in Fig. 2, MN1 selects the Gateway1 for registration. Therefore, Gateway1, Node1, and Node2 have the caches for MN1. Packets sent by MN1 can be transmitted to the Internet; in addition, packets destined to MN1 are routed in the reverse path. Similarly, MN2 chooses the GatewaybN for the Internet connection. Based on the load information, the MNs can register with the gateway with the lightest load. Consequently, load balancing can be supported in the Cellular IP with multiple gateways.

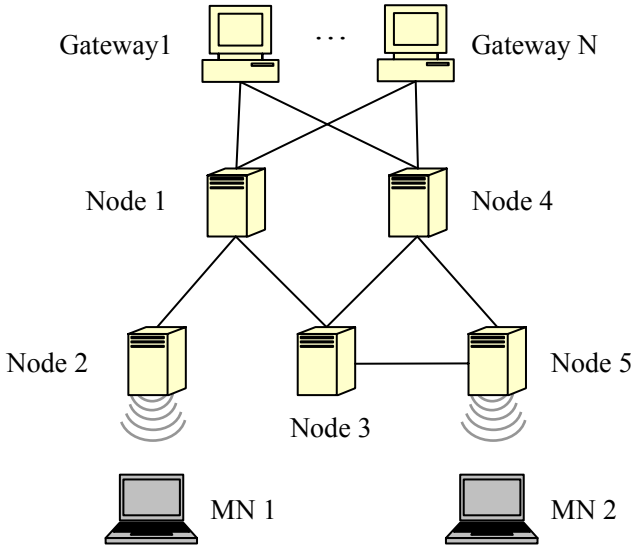

Fig. 2. A Cellular IP network with multiple gateways

3 Fault-Tolerance Support

In Cellular IP with multiple gateways, all MNs will be disconnected and try to select other gateway for re-registration when the service gateway fails. For reducing the disconnection latency, the failure detection and recovery mechanisms are developed for Cellular IP with multiple gateways.

3.1 Failure Detection and Recovery

Consider a set of gateways (**P** = {P_i | i = 1, 2, …, n}) in a Cellular IP network. Each gateway (primary gateway) P_i picks a set of backup gateways (**B** = {$B_{i,j} \neq P_i$ | j = 1, 2,…, m < n}, where **B** $\subset$ **P**) for detecting the occurrence of the failure. The gateway failure is due to the domain network partition (i.e., backup gateways are disconnected with their primary gateways within the domain network) or the gateway crash (i.e., software or hardware failure on gateways). Consider that the network partition is between the primary gateway and its backup gateways within the domain network and the gateways are reachable from outside of the network via the Internet. With the design of Cellular IP, P_i periodically sends gateway broadcast packets so **B** can monitor whether P_i is alive or not. If the backup gateway $B_{i,j}$, where j = 1, 2,…, m-1, does not receive the broadcast packet from P_i before the gateway broadcast timeout, P_i is assumed failed. At first, because no receiving the broadcast packet of P_i, $B_{i,j}$ exploits the ping/ping-ack interaction to detect whether the failure is the domain network partition or not. $B_{i,j}$ sends the ping packet to P_i and the backup gateway $B_{i,j+1}$. Note that $B_{i,j+1}$ has to verify whether $B_{i,j}$ could takeover the operations or not. If no receiving ping packets from $B_{i,j}$ before the ping timeout, $B_{i,j+1}$ will start the ping/pink-ack interaction to takeover and so on. On the other hand, if P_i is still alive, it will obtain the ping packet and then reply a ping-ack packet to $B_{i,j}$. When $B_{i,j}$ gets a ping-ack packet sent by P_i, $B_{i,j}$ can conclude the existence of the network partition in the domain network. The domain network partition typically includes two scenarios:

- If the MNs are in the same partition with their primary gateways, the Internet connection will be remained.
- Otherwise, each MN can communicate with its primary gateway through the backup gateway located in the same network partition. $B_{i,j}$ replaces P_i by broadcasting gateway broadcast packets. After the MNs receive the packets, they will send the update packets to $B_{i,j}$ and establish new routing paths to $B_{i,j}$. $B_{i,j}$ then forwards the

update packets to P_i through the Internet so P_i can locate the MNs. When the packets destined to MNs arrive at the domain, P_i will tunneled the packets to $B_{i,j}$. $B_{i,j}$ thus forwards the packets to MNs. The problem of maximum transmission unit (MTU) change during tunneling can be solved by tunnel MTU discovery mechanism [3]. The detailed timing diagram is shown in Fig. 3.

If $B_{i,j}$ does not receive any ping-ack messages from P_i before the ping timeout, $B_{i,j}$ will consider that P_i has crash failure. $B_{i,j}$ thus sends address resolution protocol (ARP) packets and broadcasts the gateway broadcast packet with the IP address of P_i to the domain network. $B_{i,j}$ handles ARP packets for P_i and intercepts all packets sent to P_i. However, the nodes and the MNs are not aware of the takeover procedure. The Fig. 4 displays the process of detection and takeover for crash failure.

When a Cellular IP node fails, the routing paths for the MNs can be recovered automatically due to the gateway broadcast packets sent by the gateways. The route-update packets sent by the MNs are routed via the paths to the gateway. Thus, the MNs can create the alternative routes for transmission without suffering from the node failure.

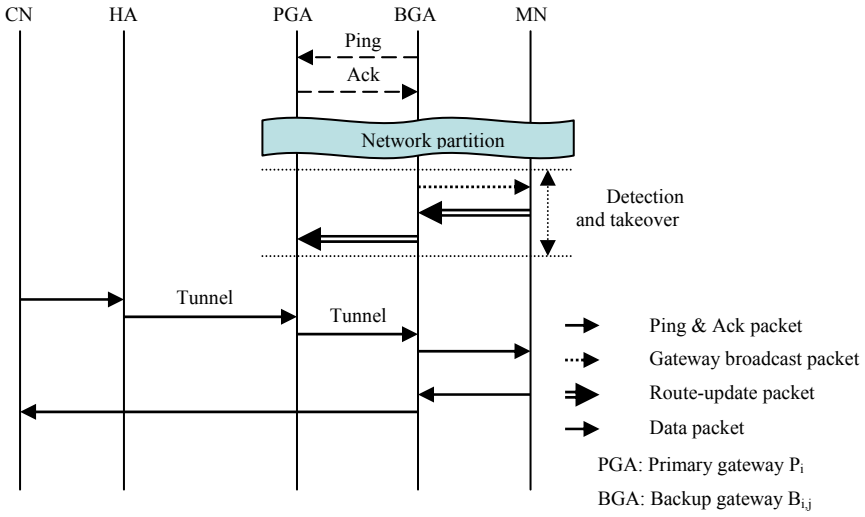

Fig. 3. Network partition

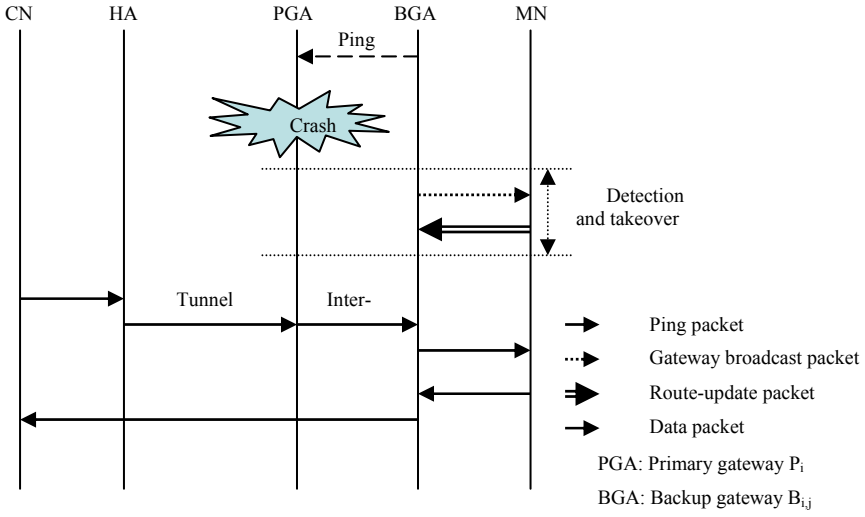

Fig. 4. Crash failure

3.2 Reintegration

When P_i has been fixed or the network partition is recovered, P_i and its backup gateway $B_{i,j}$ will be able to communicate. If $B_{i,j}$ receives the gateway broadcast packets from the recovered P_i, the reintegration procedure will be initiated. $B_{i,j}$ sends the registration data with related security information about the MNs to P_i. After obtaining

the data, P_i resumes the service. At the same time, $B_{i,j}$ stops both ARP function and broadcasting gateway broadcast packets for P_i (see Fig. 5).

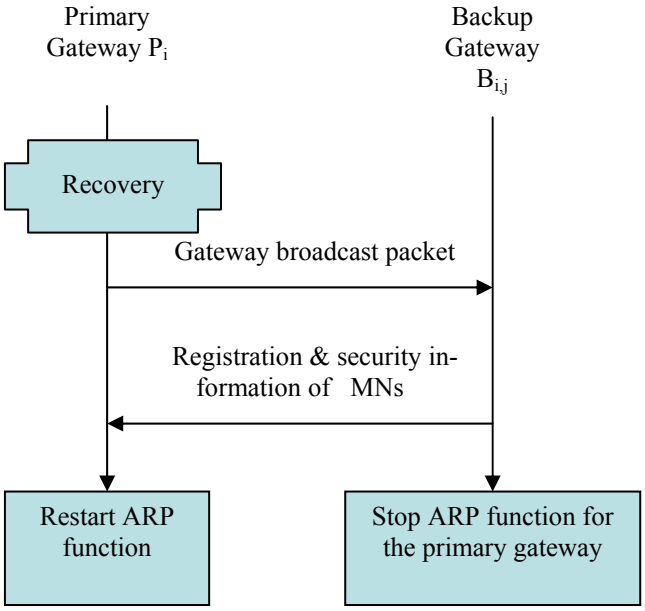

Fig. 5. Reintegration procedure

3.3 Security Considerations

The MNs connect to a Cellular IP network via wireless links which are vulnerable to security attacks. Accordingly, the authentication between the MN and the Cellular IP network are necessary. When a MN joins to the Cellular IP network, the gateway must authenticate the MN. The authentication process can be used by any known symmetric or asymmetric method [11]. With our scheme, the primary gateway (P_i) will share the authentication information with its backup gateways **B**. Besides, the connections between P_i and its backup gateways are established by the similar authentication mechanism. If P_i fails, the backup gateways **B** can take over the operations without influencing the Cellular IP security mechanisms. With the Cellular IP network, all control messages are authenticated to prevent the malicious node impersonating another node, creating denial-of-service attacks, and capturing traffic destined for MNs [12].

4 Analysis

The performance analysis is divided into two parts. The first one is to investigate the MNs' disconnection time for the primary gateway's failure. The second one is to investigate the control overhead for all gateways.

4.1 Disconnection Time

Multiple Gateways without Fault-Tolerance Support. In the multiple gateways protocol, the MNs treat the gateway failure as the gateway handoff. The MN selects another alive gateway for communication service. The disconnection time is shown as

$$T_{gateway\_timeout} + T_{node\_timeout} + T_{registration}. \quad (1)$$

When a node cannot receive the gateway broadcast packet for a particular period ($T_{gateway\_timeout}$), the node considers that the gateway failed. Furthermore, if the MN loses the beacon packet of its registered gateway in $T_{node\_timeout}$, the procedure of the handoff will be activated. After selecting a new gateway, the MN re-registers with its HA. The registration time, $T_{registration}$, is counted from the time when the MN sends the registration request packet to the MN receives the registration reply packet.

With the route optimization, the disconnection latency will be longer because there is no mechanism to notify the correspondent nodes of the failure of the gateway. The disconnection time is presented in the following equation where $T_{CN\_timeout}$ is the registration lifetime of the MN stored in the HA.

$$T_{gateway\_timeout} + T_{node\_timeout} + T_{registration} + T_{CN\_timeout}. \quad (2)$$

Multiple Gateways with Fault-Tolerance Support. The protocol uses the gateway broadcast packets for failure detection. Consider that the jth backup gateway takeovers the operations. The disconnection latency in the fault tolerant protocol under the domain network partition is displayed as

$$T_{gateway\_timeout} + (j - 1) \cdot T_{ping\_timeout} + T_{takeover}. \quad (3)$$

When the backup gateway cannot receive the gateway broadcast packet before $T_{gateway\_timeout}$, it considers that the gateway failed and transmits the ping packet to the primary gateway. $T_{ping\_timeout}$ is the timeout of waiting for ping or ping-ack packets. With network partition, the primary gateway replies the pink-ack packet to the backup gateway. $T_{takeover}$ is the needed time for the backup gateway for taking over the network service.

The disconnection latency in the fault tolerant protocol under the gateway crash is displayed as

$$T_{gateway\_timeout} + j \cdot T_{ping\_timeout} + T_{takeover}. \quad (4)$$

If no receiving the ping-ack packet before $T_{ping\_timeout}$, it regards that the primary gateway has the crash failure. Consider that the detection and recovery process can be completed before starting the handoff.

$$T_{gateway\_timeout} + j \cdot T_{ping\_timeout} + T_{takeover} < T_{gateway\_timeout} + T_{node\_timeout}. \quad (5)$$

Based on equation 5, the disconnection time with fault tolerant protocol is less than equation 1 and equation 2.

$$\begin{aligned} & T_{gateway\_timeout} + j \cdot T_{ping\_timeout} + T_{takeover} \\ & < T_{gateway\_timeout} + T_{node\_timeout} + T_{registration} \\ & < T_{gateway\_timeout} + T_{node\_timeout} + T_{registration} + T_{CN\_timeout}. \end{aligned} \quad (6)$$

4.2 Control Message Overhead

Single Gateway (Cellular IP). The control message overhead for the Cellular IP protocol includes the gateway broadcast packets, the route/paging-update packets, and the registration packets. The total control messages for Cellular IP can be represented as

$$M_{gateway\_broadcast} + M_{route-update} + M_{paging-update} + M_{registration}. \quad (7)$$

Multiple Gateways without Fault-Tolerance Support. The Cellular IP with multiple gateways requires all gateways broadcast gateway broadcast packet to the domain networks. Each MN selects one of the gateways for registration. Assume that there are n gateways in a Cellular IP network so the total control message is shown in equation 6.

$$n \cdot M_{gateway\_broadcast} + M_{route-update} + M_{paging-update} + M_{registration}. \quad (8)$$

Multiple Gateways with Fault-Tolerance Support. Our fault-tolerance protocol exploits the ping and the ping-ack packets for determining the domain network partition. Typically, our mechanism requires more control message overhead than the Cellular IP and the Multiple gateways protocol. Equation 9 presents the total control messages for the fault-tolerance mechanism. Suppose that the Cellular IP network has n primary gateways and the jth backup gateway can takeover the network service.

$$n \cdot M_{gateway\_broadcast} + M_{route-update} + M_{paging-update} + M_{registration} + M_{ping} (+ M_{ping-ack}). \quad (9)$$

5 Performance Evaluation

System performance was evaluated using the network simulator (ns-2) with the Monarch Project wireless and mobile extensions. In the simulations, Cellular IP with a single gateway (CIP), Cellular IP with multiple gateways (MG), Cellular IP with multiple gateways and fault tolerance (MGFT) were compared.

5.1 Environment

The network topology for the simulations is shown in Fig. 6. We assume that there were two primary gateways and one backup gateway in the network. The domain network included two gateways (GA1 and GA2), five switch nodes (N1 to N5), and nine base stations (BS1 to BS9). The network attached to the Internet via the gateways. All the wired links were 100 Mbps and their delay time was 5 milliseconds. The round trip time (RTT) from the Cellular IP domain network to all home networks was 110 milliseconds. The radio model was based on the Lucent WaveLAN IEEE 802.11 product. The bandwidth of the wireless channels was 11 Mbps and the delay time was 10 milliseconds. The radio range for each base station was 170 meters. Fig. 7 illustrates the location for each base station. The MNs moved in the area of 660×660 meters. The varying numbers of the MNs were simulated in our measurements, including 20, 40, 60, 80, and 100. The total simulation time was 100 seconds. The movement model for the MNs was based on Random Waypoint model. The maximum moving speed of each MN was 5 m/sec and no pause time for continuous movement. Lazy Cell Switching (LCS) [2] was implemented for detecting movement. If an MN moves away from its current base station and approaches to another one, the handoff will be initiated.

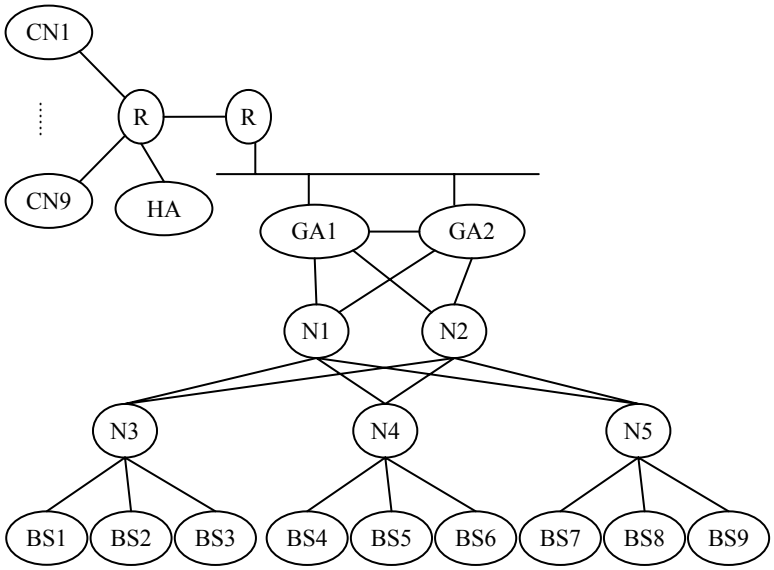

Fig. 6. The topology of simulations

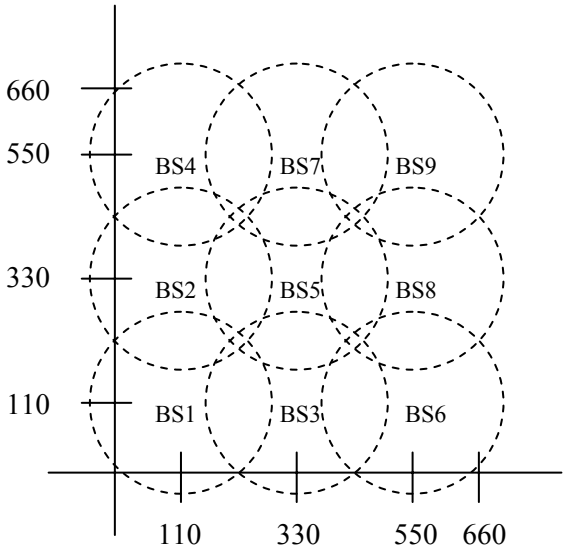

Fig. 7. Deployment for base stations

5.2 Parameters for Simulation

The routing-update packets were sent every second and the paging-update packets were sent every three seconds. The expiration time for both the route cache and the paging cache was three times of the update interval. The MN utilizes a handoff timer for detecting the cell change. When the MN registers with a base station, the handoff timer starts. The handoff timeout will be reset if the MN receives other packets from the registered base station. If the handoff timeout is expired, the MN will start the handoff procedure. The values for the needed parameters are displayed in Table 1.

Table 1. The Parameters for Simulation (Time unit: second)

Parameter	Value	Parameter	Value
Gateway broadcast interval	1	Gateway broadcast timeout	3
Route-update interval	1	Route-cache timeout	3
Paging-update interval	3	Paging-cache timeout	9
beacon interval	1	Handoff timeout	3
Registration interval	30	Registration timeout	30
Ping interval	0.5	Ping timeout	1
Ping-ack timeout	1	Active-state-timeout	3

5.3 Simulation Results

There are two sets of the simulations. First, we present the control overhead for three mechanisms, CIP, MG, and MGFT, in the failure-free execution. Second, the disconnection time for network partition, gateway failure, and node failure are described.

Failure-Free Execution

Without Traffic Connections. Fig. 8 compares the number of control packets used in CIP, MG, and MGFT protocols. The control packets included the route (and paging) update packets, the registration packets, and the gateway broadcast packets. The control overhead increased with larger numbers of MNs. MG and MGFT did not modify the original registration mechanism so the numbers of registration packets for the three protocols were similar. CIP required less control packets than MG and MGFT because one more gateway in MG and MGFT had to send the gateway broadcast packets for route construction. No ping and ping-ack messages appeared in the failure-free execution so the control overheads for MG and MGFT were identical. The simulation results confirmed the analysis of the control overhead in Section 4.2.

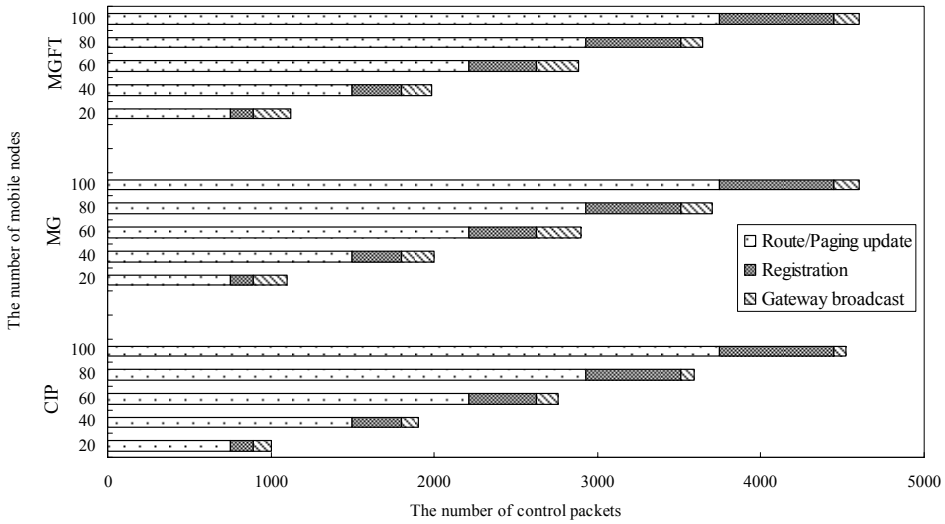

Fig. 8. The number of control packets without data traffic

With Traffic Connections. In this simulation, the correspondent nodes were the sources and the MNs were the destinations. It is obvious that the number of route update packets with data traffic was higher than that without

data traffic (see Fig. 9). Traffic congestions occurred and led to the loss of registration packets. The MNs needed to send more packets for registrations.

As shown in Fig. 10, the larger numbers of the MNs caused more end-to-end delay with all protocols. When the number of MNs was 100, the end-to-end delay was up to about 0.9 second. Fig. 11 demonstrates that all three protocols had similar throughput for varying numbers of the MNs. The above results show that the design of the MGFT did not affect the transmission delay or the system throughput.

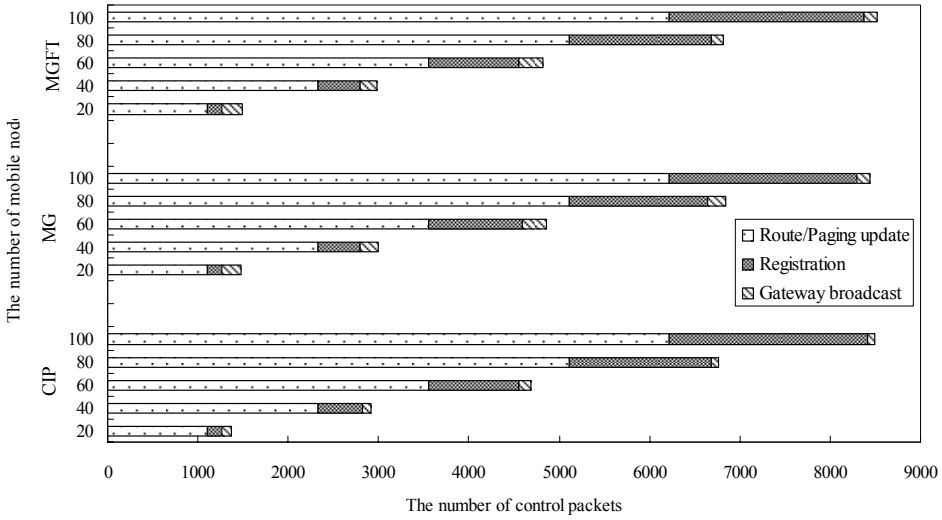

Fig. 9. The number of control packets with data traffic

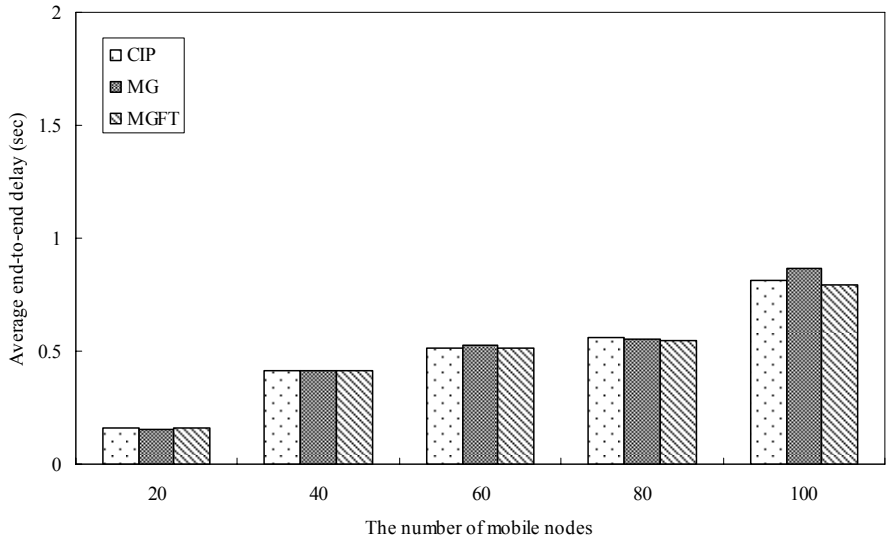

Fig. 10. Average end-to-end delay of data packets

Disconnection Time due to Failures

Network Partition. It is assumed that all MNs registered with GA1 initially (see Fig. 6) and then both physical links of "GA1 to N1" and "GA1 to N2" were crashed at the 50th second. Therefore, the network partitions occurred and all MNs were disconnected with GA1. Fig. 12 illustrates the disconnection time for each protocol. As analyzed in Sec. 4.1, MG took three seconds for the BSs to detect the gateway failure. The MNs spent another three seconds to recognize the failure from the BS and started to handoff and register with GA2. Thus, the total disconnection time was about six seconds. With MGFT, GA2 detected the network partition based on the ping and ping-ack interaction and then took over the operations and continued to serve the MNs. The takeover procedure was completed about three seconds.

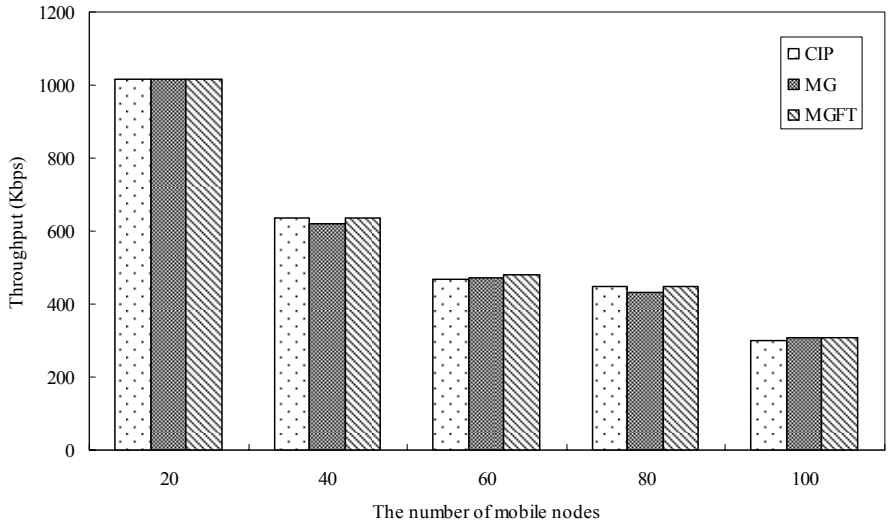

Fig. 11. Throughput

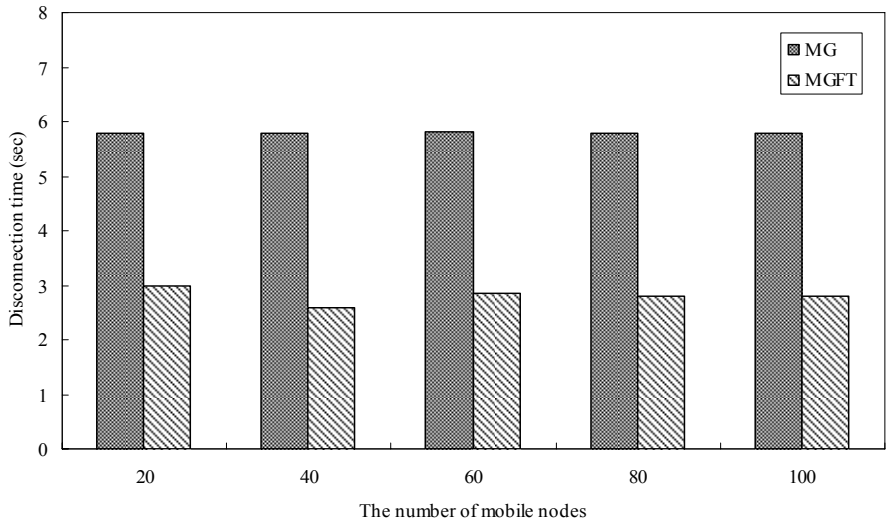

Fig. 12. Disconnection time on network partition

Failure on Primary Gateway. GA1 failed at the 50th second and the disconnection time is displayed in Fig. 13. Similar to the network partition, MG needed about six seconds to recover the failure. With MGFT, when GA2 discovered no gateway broadcast packets arrived from GA1, GA2 then sent the ping packet to GA1 for checking whether the domain network was partitioned or not. Because no ping-ack packet arrived before the timeout, GA2 took over the service. The total disconnection time was about four seconds.

Failure on a Cellular IP Node. All MNs registered with GA1 initially and all routing paths were routed via a Cellular IP node (N1). N1 crashed at the 50th second during the simulation. The gateways periodically broadcasted gateway broadcast packets with one-second interval so the routing paths will be re-established. The failure on N1 could be recovered automatically within one second. The data packets sent by the MNs were passed through N2 to GA1. Fig. 14 shows that the network recovery time was less than one second for both MG and MGFT.

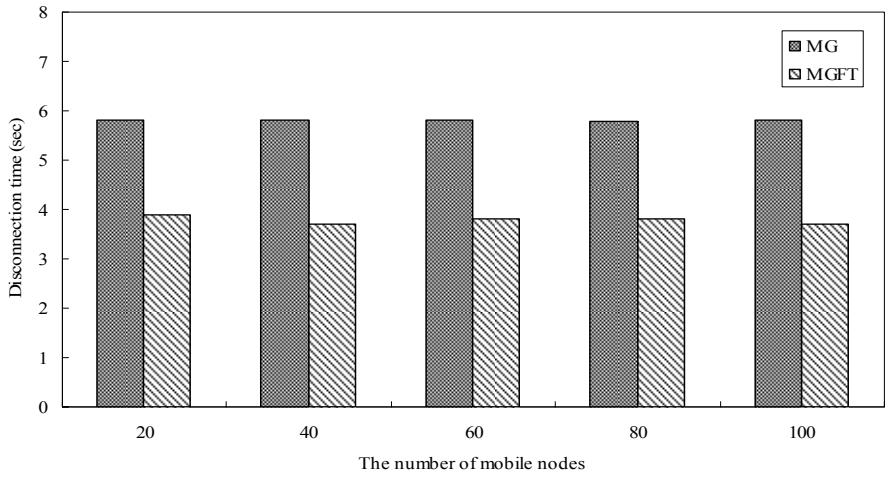

Fig. 13. Disconnection time on gateway failure

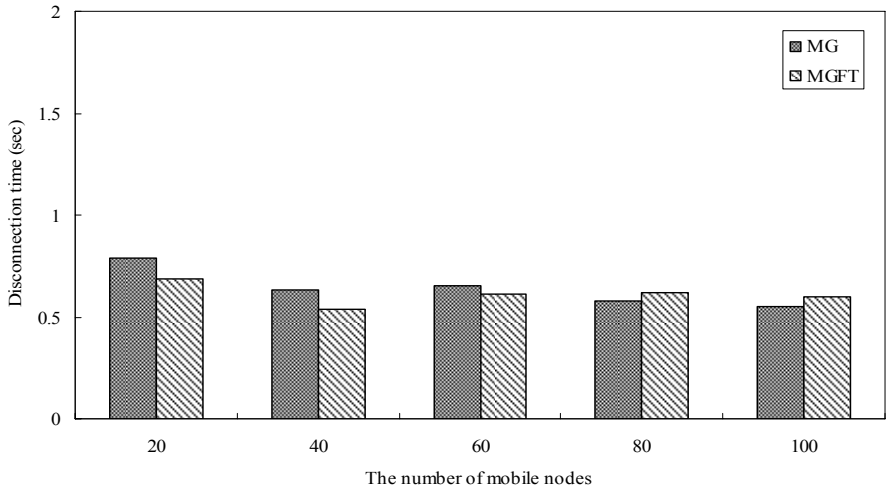

Fig. 14. Disconnection time on node failure

6 Conclusion

The paper has developed a fault-tolerant protocol with multiple gateways in a Cellular IP network. If a primary gateway fails, one available backup gateway will continue the service. The protocol can also detect the network partitions and maintain the network connections by tunneling. The design enables the transparent recovery so MNs can resume data transmissions without suffering from the failures. Besides, the load balancing can be supported in our mechanism. Based on the features of Cellular IP, the built-in gateway broadcast packets are used for gateway failure detection and recovery. In addition, two control packets, ping and ping-ack, are designed for detecting the presence of the network partition. The simulation results indicated that our mechanism not only recovered the failures automatically but improved the disconnection latency. The future work will investigate the performance of the load balancing in our scheme.

7 Acknowledgement

We would like to thank the anonymous reviewers for their valuable suggestions for improving this paper. This research was supported in part by the Taiwan National Science Council (NSC) under contracts NSC 97-2221-E-251-002, 97-2221-E-006-176-MY3, and 97-2628-E-006-093-MY3.

References

[1] D. Saha, A. Mukherjee, I. S. Misra, M. Chakraborty, N. Subhash, "Mobility Support in IP: A Survey of Related Protocols," *IEEE Network*, Vol. 18, No. 6, pp. 34-40, 2004.

[2] C.E. Perkins, IP Mobility Support for IPv4. RFC 3220, 2002.

[3] C.E. Perkins, "Mobile IP," *IEEE Communications Magazine*, Vol. 40, No. 5, pp. 66-82, 2002.

[4] A.T. Campbell and J. Gomez, "IP Micro-Mobility Protocols," *Mobile Computer and Communication Review*, Vol. 4, No. 4, pp. 45-54, 2001.

[5] A.T. Campbell, J. Gomez, S. Kim, C.Y. Wan, Z.R. Turanyi, A.G. Valko, "Comparison of IP Micro-mobility Protocols," *IEEE Wireless Communications*, Vol. 9, No. 1, pp. 72-82, 2002.

[6] A.T. Campbell, J. Gomez, S. Kim, A.G. Valko, C.Y. Wan, Z.R. Turanyi, "Design, Implementation, and Evaluation of Cellular IP," *IEEE Personal Communications*, Vol. 7, No. 4, pp. 42-49, 2000.

[7] H. I. Vicente and M. E. E. Quiroz, "Performance Analysis of the Cellular IP Mobility Protocol," *Proceedings of Electronics, Robotics and Automotive Mechanics Conference*, pp.43-48, 2006.

[8] T. Li, B. Cole, P. Morton, D. Li, Cisco Hot Standby Router Protocol (HSRP). RFC 2281, 1998.

[9] *The Network Simulator - ns-2*. Http://www.isi.edu/nsnam/ns/.

[10] *The ns Manual.* Http://www.isi.edu/nsnam/ns/doc/index.html.

[11] P. Metzger and W. Simpson, IP Authentication using Keyed MD5. RFC 1828, 1995.

[12] B. Xie, A. Kumar, D. P. Agrawal, S. Srinivasan, "Secured Macro/micro-mobility Protocol for Multi-hop Cellular IP ," *Pervasive and Mobile Computing*, Vol. 2, No. 2, pp. 111-136, 2006.