IEICE TRANS. COMMUN., VOL.E87–B, NO.5 MAY 2004

PAPER Special Section on Mobile Multimedia Communications

Performance Analysis of Robust Hierarchical Mobile IPv6 for Fault-Tolerant Mobile Services

Sangheon PACK[†a)], ***Student Member***, **Taewan YOU**[†b)], ***and*** **Yanghee CHOI**[†c)], ***Nonmembers***

SUMMARY In mobile multimedia environment, it is very important to minimize handoff latency due to mobility. In terms of reducing handoff latency, Hierarchical Mobile IPv6 (HMIPv6) can be an efficient approach, which uses a mobility agent called Mobility Anchor Point (MAP) in order to localize registration process. However, MAP can be a single point of failure or performance bottleneck. In order to provide mobile users with satisfactory quality of service and fault-tolerant service, it is required to cope with the failure of mobility agents. In [1], we proposed Robust Hierarchical Mobile IPv6 (RH-MIPv6), which is an enhanced HMIPv6 for fault-tolerant mobile services. In RH-MIPv6, an MN configures two regional CoA and registers them to two MAPs during binding update procedures. When a MAP fails, MNs serviced by the faulty MAP (i.e., primary MAP) can be served by a failure-free MAP (i.e., secondary MAP) by failure detection/recovery schemes in the case of the RH-MIPv6. In this paper, we investigate the comparative study of RH-MIPv6 and HMIPv6 under several performance factors such as MAP unavailability, MAP reliability, packet loss rate, and MAP blocking probability. To do this, we utilize a semi-Markov chain and a $M/G/C/C$ queuing model. Numerical results indicate that RH-MIPv6 outperforms HMIPv6 for all performance factors, especially when failure rate is high.

key words: *Hierarchical Mobile IPv6 (HMIPv6), Robust HMIPv6 (RH-MIPv6), fault-tolerant mobile service, performance analysis, semi-Markov chain*

1. Introduction

In wireless/mobile networks, system survivability is one of the most important issues for providing a certain quality of service (QoS) with users. Survivability is used to describe the available performance after a failure. Originally, Mobile IP systems do not consider system survivability and fault tolerance. However, when Mobile IP systems are deployed in wireless/mobile networks, survivability and fault tolerance should be taken into consideration as important performance factors. To do this, a few protocols and systems were proposed in [3]–[5], and [6].

However, these schemes are based on Mobile IPv4 or require redundant mobility agents, which result in a higher cost. To overcome these drawbacks and to provide fault tolerance with Mobile IP systems, we proposed an enhanced Hierarchical Mobile IPv6 (HMIPv6) for system survivability in the distributed Mobility Anchor Point (MAP) environment, called *Robust Hierarchical Mobile IPv6 (RH-MIPv6)*, in [1]. We adopted HMIPv6 as a location management scheme because it is able to reduce registration overhead and handoff latency by using a local agent (i.e., MAP). In HMIPv6, MAP and HA can be two points of failures, but RH-MIPv6 is designed mainly to cope with MAP failures. This is because mobile users perform more local registrations rather than home registration in general. Also, since HA contains very important mobility information, it is necessary to guarantee the highest reliability to HA although it requires a higher cost. So, in the case of HA failures, the existing primary-backup approaches can be applied.

In this paper, we investigate performance analysis of RH-MIPv6 and HMIPv6. We compare RH-MIPv6 with HMIPv6 in terms of a variety of performance factors such as MAP unavailability, reliability, blocking probability, and packet loss rate. To do this, we use a semi-Markov chain representing the state of a MAP. In addition, a M/G/C/C queuing model is used to obtain MAP blocking probability caused by a MAP failure.

The remainder of this paper is organized as follows. Section 2 describes main characteristics of RH-MIPv6. Section 3 proposes a semi-Markov chain to obtain MAP unavailability and reliability, and packet loss rate. Section 4 shows various numerical results and MAP blocking probability based on the M/G/C/C model. Section 5 concludes this paper.

2. Robust Hierarchical Mobile IPv6

In this section, we briefly describe main characteristics and key schemes of RH-MIPv6. More detailed specification can be found in [1].

2.1 Primary and Secondary Binding Update

In RH-MIPv6, an MN chooses two serving MAPs (i.e., primary MAP (P-MAP) and secondary MAP (S-MAP)) during MAP selection procedure. Also, the MN configures primary RCoA (P-RCoA) and secondary RCoA (S-RCoA) in a P-MAP domain and S-MAP domain, respectively. P-RCoA refers to an RCoA which is valid in the P-MAP domain and S-RCoA is a valid RCoA in the S-MAP domain. The MN performs a binding update using both P-RCoA and S-RCoA. Since P-MAP and S-MAP have flexible relationships in the case of RH-MIPv6, it is distinguishable from the existing primary-backup schemes [4], where one or more backup agents are pre-assigned to a primary agent. Namely, if there is no failure event, P-MAP and S-MAP act as independent local agents without any interactions. The S-MAP

Manuscript received August 25, 2003.
Manuscript revised October 23, 2003.

[†]The authors are with Seoul National University, Seoul, Korea.
a) E-mail: shpack@mmlab.snu.ac.kr
b) E-mail: twyou@mmlab.snu.ac.kr
c) E-mail: yhchoi@snu.ac.kr

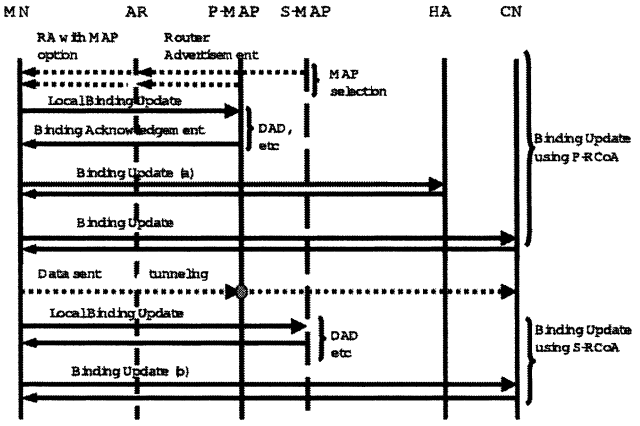


Fig. 1 Binding update procedure in RH-MIPv6.

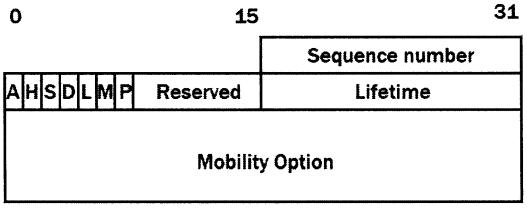


Fig. 2 The extended binding update message.

temporarily takes the role instead of the P-MAP only when the P-MAP fails. In addition, since the S-MAP is selected as a result of MAP selection by MNs, the load resulting from the P-MAP's failure can be efficiently distributed to multiple S-MAPs if it is assumed that MNs are evenly distributed. Furthermore, S-MAPs are optimal agents except P-MAP in view of MNs. Figure 1 depicts primary and secondary binding update procedures.

First of all, an MN collects all RA messages from MAPs that can be reachable from the MN in a foreign network. Then, the MN selects a P-MAP and a S-MAP using an MAP selection algorithm (e.g., the furthest MAP selection, preference-based selection, or other schemes [7]). After selecting a P-MAP and configuring a P-RCoA, the MN should perform a local binding update (BU) procedure to the selected P-MAP, HA, and CNs using the configured P-RCoA. In RH-MIPv6, since an MN registers both P-RCoA (i.e., primary BU) and S-RCoA (i.e., secondary BU), we extend the BU message in order to separate a primary BU from a secondary BU. Figure 2 shows the extended BU message. Unlike the original BU message, the message contains a *P flag* in the option field. The new flag indicates whether the specified RCoA is P-RCoA or S-RCoA. Namely, when an MN registers its P-RCoA to the P-MAP, HA and CNs, *P flag* is set to 1. Otherwise, the *P flag* is unset for the secondary BU procedure.

In RH-MIPv6, secondary BU procedure begins only after the completion of the primary BU procedure, so that the secondary BU procedure does not effect the latency of the primary BU procedure. In addition, the secondary BU procedure can be performed in concert with data transmission through P-MAP as shown in Fig. 1. Namely, RH-MIPv6 has no affect on the failure-free behavior of HMIPv6, except one more binding update message. As shown in Fig. 1, note that the MN doesn't send a BU message to the HA in the case of a secondary BU procedure. There are two reasons for not sending a BU message to the HA in the secondary BU procedure. First reason is to minimize the modification from the existing HMIPv6 protocol. RH-MIPv6 can be supported only by the simple modification in end systems (e.g., MNs and CNs). Second, although the secondary BU message is not sent to the HA, only new sessions, which have a lower priority than on-going sessions, are influenced. This is because RH-MIPv6 supports the route optimization and packets of only new sessions transit to the HA. Therefore, RH-MIPv6 does not perform secondary BU to the HA to minimize binding update overhead. However, since an MN immediately performs a binding update to the HA when a P-MAP fails and a S-MAP takes over it, RH-MIPv6 can provide new sessions with fault tolerance after some latency.

2.2 Failure Detection and Recovery Schemes

In HMIPv6, a MAP failure event can be detected by checking a MAP option, which contains an invalid lifetime for the broadcasted Router Advertisement (RA) message. However, it takes too much time for an MN to detect the failure by this passive method because the interval of the RA message is set to a few seconds[†]. Thus, the failure recovery mechanism of the HMIPv6 results in high packet losses, especially when the MN is communicating with multiple CNs. On the other hand, RH-MIPv6 detects a MAP failure during packet transmission by utilizing Internet Control Management Protocol (ICMP) [9]. Therefore, fast failure detection can be achieved in the case of active sessions without waiting for an RA message with a coarse grained broadcasting interval. Of course, CNs or MNs, that aren't currently sending or receiving any packets, can detect a MAP failure by RA messages. However, in this case, since there are no active sessions, fast failure detection may not be a critical problem. In this section, we divide the failure detection and recovery mechanisms into two cases: those detected by MN and by CN.

2.2.1 Failure Detection and Recovery by MN

In RH-MIPv6, if an MN is actively sending data to CNs, the MN can detect a MAP failure after receiving ICMP error messages [9]. Or, if the MN is receiving some packets from CNs, the MN will receive the encapsulated packets from the S-MAP instead of the P-MAP. Then, the MN considers that the P-MAP has failed. If the MN does not communicate with any other nodes, the MN can detect the failure by the

[†]Recently, router advertisement interval in ARs is recommended to be set to about 50 ms for fast movement detection. However, in terms of reduction of signaling load, a few seconds is more reasonable value because router advertisement from the MAP is not related to the movement detection.

reception of RA messages. Therefore, failure detection time by MN can be expressed as follows:

$$T_{detection} = \min\{t_{RA}, t_{CN}, t_{ICMP}\}$$

where t_{RA}, t_{CN}, and t_{ICMP} are the time until an MN receives RA messages, encapsulated packets from S-MAP, and ICMP error messages, respectively.

After the detection of a P-MAP failure, the MN changes its serving MAP into S-MAP from P-MAP. Then, the MN resumes data transmission, if the MN was sending some packets to CNs. In this case, S-MAP receives some packets from a MN listed in the backup mapping table and the S-MAP moves the binding information of the MN from backup mapping table to the serving mapping table. In RH-MIP, MAP maintains two types of mapping table: serving and backup mapping tables. Serving and backup mapping tables have binding information of MNs having performed primary and secondary BU procedures, respectively. With data transmission, the MN sends BU messages to the HA and CNs with S-RCoA as soon as possible. When the BU message arrive at the HA, the HA updates a CoA of the MN into S-RCoA from P-RCoA. On the other hand, CNs eliminate primary binding information and set the P field of the secondary binding entry to 1.

2.2.2 Failure Detection and Recovery by CN

Let's assume that a CN is currently sending some data to an MN via a P-MAP, which is a serving MAP containing binding information between RCoA and LCoA. If the P-MAP fails, the CN receives ICMP error messages (i.e., Host Unreachable) for the sent packets. Then, the CN decides that the P-MAP has failed and rerouting through an S-MAP is then required. Typically, the link loss rate in a wired link is extremely low. Therefore, if the CN determines a MAP failure after receiving a few successive ICMP error messages, a wrong determination can be minimized.

Failure recovery by CN is as follows. The CN regards multiple receptions of ICMP error messages as a MAP failure. Then, the CN finds out a binding entry with an unset P field in its binding cache, which is updated by the secondary BU procedure. If there is such an entry, the CN eliminates the binding entry with a set P field and the P field of the found binding entry (i.e., secondary binding entry) is newly set to 1. After updating the binding cache, the CN resumes data transmission through the S-MAP and the S-MAP updates its mapping tables. Namely, the S-MAP looks for a corresponding entry from the backup mapping table and moves the entry to the serving mapping table. After completion of the mapping table update, the S-MAP tunnels the received packets to the destination MN. Since the MN receives some tunneled packets from its S-MAP not P-MAP, the MN believes its P-MAP does not work any more for some reasons, so that the MN sets S-MAP as its serving MAP. If the MN detects a MAP failure, the MN sends a BU message with S-RCoA, which is configured in the MAP selection procedure in advance, to the HA as soon as possible. After re-BU procedure, the MN can communicate with new CNs, which try to connect the MN using binding information in the HA, through the S-MAP.

3. Semi-Markov Chain Model for Performance Analysis

To investigate the effectiveness of RH-MIPv6 over HMIPv6, we compare RH-MIPv6 with HMIPv6 using an analytic model based on the Markovian Process. Figure 3 shows a state diagram for MAP operation in view of a source node†. In *Normal* state (or state 0), a MAP correctly performs its functions as a local mobility agent. *Undetected* state (or state 1) refers to a state where a failure occurs at the MAP, but the failure is still not detected by MNs or CNs. On the other hand, *Detected* state (or state 2) represents a state where the MAP failure is detected.

In general, since the residence time in each state does not follow an exponential distribution, this state diagram is analyzed as a semi-Markov chain [8]. Let $P_{0,1}$, $P_{1,2}$, and $P_{2,0}$ be the transition probability from state 0 to state 1, from state 1 to state 2, and from state 2 to state 0. As shown in Fig. 3, since there is only one transition available between two states, $P_{0,1}$, $P_{1,2}$, and $P_{2,0}$ are 1. Let the steady state probability for each state in an imbedded Markov chain be π_i. Then, balance equations are as follows:

$$\pi_0 P_{0,1} = \pi_1 P_{1,2} = \pi_2 P_{2,0}$$

$$\sum_{i=0}^{2} \pi_i = 1$$

Therefore, π_i $(i = 0, 1, 2)$ is equal to $1/3$.

Figure 4 shows a timing diagram when a MAP failure occurs during a MAP RA interval denoted by T_A. Let t_{FA} be the time period from the failure event to the next MAP RA reception time. If we assume that a MAP failure randomly occurs in a MAP RA interval, t_{FA} follows an uniform distribution with a mean of $T_A/2$. In addition, it is assumed that the time (t_F) between two MAP failure events follows an exponential distribution with a mean of $1/\lambda_F$. T_I is a random variable representing the latency required for ICMP error messages to get to the source node (i.e., CNs or MNs).

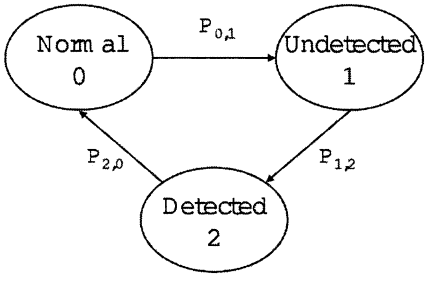


Fig. 3 State diagram for MAP operation.

†In terms of failure detection in RH-MIPv6, the source node always detect more earlier than the destination node does. Therefore, we analyze the MAP state in view of the source node.

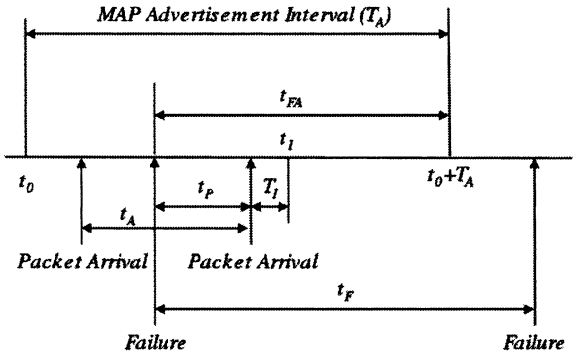


Fig. 4 Timing diagram in MAP failure event.

3.1 Hierarchical Mobile IPv6 (HMIPv6)

First, the steady state probability in each state is derived in HMIPv6. A MAP in the normal state transits to the undetected state when a MAP failure event occurs. Thus, the average residence time in the normal state is as follows:

$$E(T_0) = \int_0^\infty t \cdot \lambda_F e^{-\lambda_F t} dt = \frac{1}{\lambda_F} \tag{1}$$

According to the specification of HMIPv6 [2], an MN can detect a MAP failure only after the reception of the advertised MAP RA message with a lifetime of 0. Therefore, the residence time in the undetected state is dependent on the MAP RA interval, which is fixed to T_A. Then, the residence time in the undetected state follows a uniform distribution at [0, T_A] and the average residence time is as follows:

$$E(T_1) = \int_0^{T_A} t \cdot \frac{1}{T_A} dt = \frac{1}{T_A} \cdot \frac{{T_A}^2}{2} = \frac{T_A}{2} \tag{2}$$

The transition from the detected state to the normal state can be done only when all procedures (e.g., new MAP selection, address configuration, DAD procedure, and BU procedure, etc.) have been completed. We assume that the time required for these procedures is a constant value (R_{HMIPv6}). Then, the average residence time in the detected state is

$$E(T_2) = R_{HMIPv6} \tag{3}$$

Using these average residence times, we can calculate the steady state probability in each state in the semi-Markov chain as shown in Eq. (4).

$$v_i = \frac{E(T_i) \cdot \pi_i}{\sum\limits_{all\ j} E(T_j) \cdot \pi_j} \tag{4}$$

3.2 Robust Hierarchical Mobile IPv6 (RH-MIPv6)

In RH-MIPv6, the average residence time in the normal state is same as that of HMIPv6. However, in the RH-MIPv6, a MAP failure can be detected by MN's (or CN's) packet transmission as well as by a MAP RA message. In other words, if an MN (CN) sends some packets to a faulty MAP and the MN receives ICMP error messages after some latency (i.e., T_I), the MN concludes that the MAP is broken down. Of course, if there is no packet transmission during a MAP RA interval, the MN can detect the MAP failure after receiving a MAP RA message. Thus, the average residence time in the undetected state in RH-MIPv6 can be obtained from Eqs. (5) and (6). $E(T_1|t_{FA})$ denotes the average residence time in the undetected state when t_{FA} is given. In this paper, we assume that the inter-arrival time (t_A) between one packet arrived just before the MAP failure event and another packet arrived just after the MAP failure event follows an exponential distribution with a mean of $1/\lambda_A$. Then, by the random observer property, t_P also follows an exponential distribution and its the probability density function (pdf) is $\lambda_A e^{-\lambda_A t}$. Since t_{FA} follows a uniform distribution in [0, T_A], the average residence time ($E(T_1)$) is calculated as Eq. (6) using the conditional average residence time ($E(T_1|t_{FA})$) in Eq. (5). As shown in Fig. 4, if the t_P is in the period of [0, t_{FA}-T_I] within a MAP advertisement interval, the MAP failure is detected at the time of t_1. Therefore the failure detection time is $t_P + T_I$. Otherwise, the failure can be detected only after receiving the next advertisement message at the time of $t_0 + T_A$ and the failure detection time is equal to t_{FA}.

$$E(T_1|t_{FA}) = \int_0^{t_{FA}-T_I} (t + T_I) \cdot \lambda_A e^{-\lambda_A t} dt + \int_{t_{FA}-T_I}^{\infty} t_{FA} \cdot \lambda_A e^{-\lambda_A t} dt \tag{5}$$

$$E(T_1) = \int_0^{T_A} E(T_1|t_{FA}) \cdot f_{t_{FA}}(t) dt = \int_0^{T_A} E(T_1|t_{FA}) \cdot \frac{1}{T_A} dt \tag{6}$$

In terms of state transition from state 2 to state 0, RH-MIPv6 requires only binding cache or mapping table update procedures when a MAP failure is detected. This is because RH-MIPv6 performs several functions such as address configuration and DAD procedure during secondary binding procedure in advance. Therefore, we assume that the failure recovery time of RH-MIPv6 is another constant value ($R_{RHMIPv6}$), which is less than R_{HMIPv6}.

$$E(T_2) = R_{RHMIPv6} \tag{7}$$

The steady state probabilities in the semi-Markov chain can be also obtained by using Eq. (4).

4. Numerical Results

To compare the performance of RH-MIPv6 with that of HMIPv6, we have defined four performance factors: MAP unavailability (U), MAP reliability (R), MAP blocking probability (B), and packet loss rate (L). MAP unavailability is defined as the mean recovery time to the mean time between failure events [10]. This factor represents the availability of the HMIPv6 and RH-MIPv6. On the other hand, MAP reliability refers to the probability that an MAP is in

the failure-free state (i.e., normal state) in the equilibrium state. Thus, if the MAP reliability is high, the reliability of the protocol is also high. MAP blocking probability refers to a blocking probability of S-MAP caused by the transferred load from P-MAP due to a P-MAP failure [6]. Packet loss rate refers to the average packet loss rate occurred by a MAP failure. For numerical analysis, R_{HMIPv6}, $R_{RHMIPv6}$ and T_I are set to 3 sec, 1 sec, and 100 ms, respectively [11].

4.1 MAP Unavailability Probability

As mentioned before, MAP unavailability (U) is defined as Eq. (8). Since it is assumed that inter-failure time follows an exponential distribution with a mean of $1/\lambda_F$, the mean time between two consecutive failures is $1/\lambda_F$. In addition, the mean recovery time is the time period from the occurrence of a MAP failure to the recovery of the failure, so that the mean recovery time is the sum of average residence times in state 1 and 2.

$$U = \frac{Mean\ \ recovery\ \ time}{Mean\ \ time\ \ between\ \ failures} = \frac{E(T_1) + E(T_2)}{1/\lambda_F} = \lambda_F(E(T_1) + E(T_2)) \quad (8)$$

Figure 5 shows MAP unavailability as a function of the MAP failure rate. Since failure detection of RH-MIPv6 depends on the packet arrival pattern, the unavailability in RH-MIPv6 is varied as the packet arrival rate is changed. Therefore, MAP unavailability of RH-MIPv6 is calculated when packet arrival rates (λ_A) are 0.1, 1, and 10. As failure rate increases, MAP unavailability also increases. Comparing RH-MIPv6 with HMIPv6, the slope of the RH-MIPv6 is much less than that of HMIPv6. Specifically, the increasing slope of HMIPv6 is 3.5, whereas the increasing slopes of RH-MIPv6 are 1.49, 1.4, and 1.117 when λ_A is 0.1, 1, and 10, respectively. In addition, MAP unavailability of RH-MIPv6 decreases as the packet arrival rate increases. However, the differences are not high. In short, MAP unavailability can be reduced to 42.5% when RH-MIPv6 is used instead of HMIPv6.

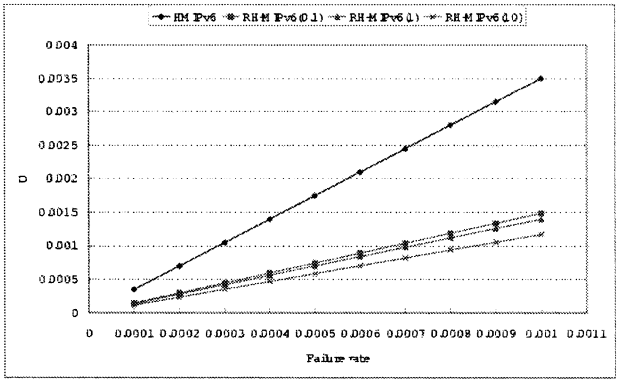


Fig. 5 Unavailability vs. failure rate.

4.2 MAP Reliability

The MAP reliability (R), the probability that the MAP state remains in the normal state at the equilibrium state, is defined as follows:

$$R = v_0 \quad (9)$$

Figure 6 shows MAP reliability as a function of the MAP failure rate. Unlike unavailability probability, the MAP reliability decreases as failure rate increases. Namely, as more MAP failures occur, MAP becomes more unstable and unreliable. As shown in Fig. 6, MAP reliability in HMIPv6 drastically decreases as the failure rate increases. In contrast, MAP reliability in RH-MIPv6 is not affected by the failure rate so much. The decreasing slope of HMIPv6 is −3.4963, whereas the decreasing slopes are −1.4874, −1.4008, and −1.1724 when λ_A is 0.1, 1, and 10, respectively. This result indicates that MAP reliability in RH-MIPv6 is higher than that of HMIPv6. Also, although failure rate increases, if RH-MIPv6 is used, MAP remains in a more stable and reliable state.

4.3 MAP Blocking Probability

To investigate S-MAP blocking probability caused by a P-MAP failure, we utilize a $M/G/C/C$ queuing model [8]. Figure 7 shows the $M/G/C/C$ queuing model. In Fig. 7, state i represents the number of MNs serviced by a MAP (A). Blocking probability of MAP (A), which is one of secondary MAPs in RH-MIPv6 or backup MAPs in typical primary-backup schemes, can be obtained as follows. Let λ_{MAP} and μ_{MAP} be the MN arrival rate and MN departure rate in MAP (A) domain, respectively. It is assumed that

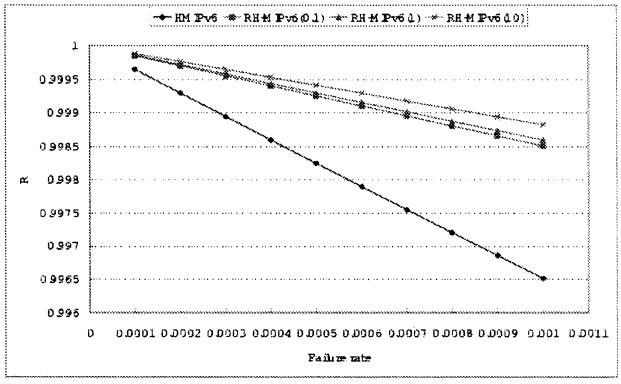


Fig. 6 Reliability vs. failure rate.

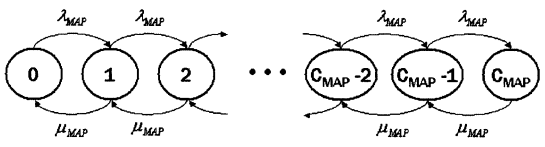
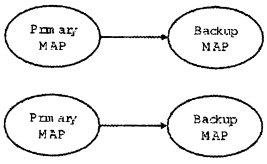
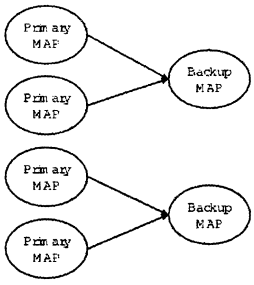


Fig. 7 $M/G/C/C$ queuing model.



(a) $N' = 1$.



(b) $N' = 2$.

Fig. 8 Primary-backup relationship in HMIPv6.

λ_{MAP} follows a poisson distribution and λ_{MAP} for each MAP is independently and identically distributed. On the other hand, μ_{MAP} does not assume to obey a specific distribution. Let λ_{over} be the arrival rate transferred to MAP (A) by the P-MAP failure. Then, λ_{over} is as follows:

$$\lambda_{over} = \lambda_F \times N \times M \times \omega$$

where N is the number P-MAPs which use MAP (A) as its S-MAP and λ_F is the failure rate. M denotes the total number of MNs to be served by the faulty P-MAP. ω is the ratio of the redirected MNs from the faulty P-MAP to MAP (A) to the total number of MNs of the P-MAP (M).

On the other hand, λ_{over} in HMIPv6 using a typical primary-backup scheme is as follows:

$$\lambda_{over} = \lambda_F \times N' \times M$$

where N' is the number of MAPs using MAP (A) as its backup MAP. The typical primary-backup approach refers to all MNs located in the primary MAP domain are serviced by a backup MAP after the primary MAP failure. Figure 8 shows primary-backup relationships in HMIPv6 when N' is 1 and 2. In contrast, Fig. 9 shows primary-secondary relationship in RH-MIPv6 when N is 2.

Based on these assumptions, MAP blocking probability can be obtained as Eq. (10) by *Erlang's loss formula* [8].

$$B = \frac{\frac{((\lambda_{MAP}+\lambda_{over})/\mu_{MAP})^{C_{MAP}}}{C_{MAP}!}}{\sum_{i=0}^{C_{MAP}} \frac{((\lambda_{MAP}+\lambda_{over})/\mu_{MAP})^{i}}{i!}} \tag{10}$$

where C_{MAP} is the capacity of a MAP, which is represented by the number of MNs.

Figure 10 shows MAP blocking probability as the failure rate increases. In this result, λ_{MAP} and μ_{MAP} are 50 and 1, respectively. In addition, C_{MAP}, M and N are set to 50, 20, and 3, respectively. The utilization ratio (ρ_{MAP}) of a MAP, which is defined as λ_{MAP}/μ_{MAP}, is 50. In Fig. 10, MAP

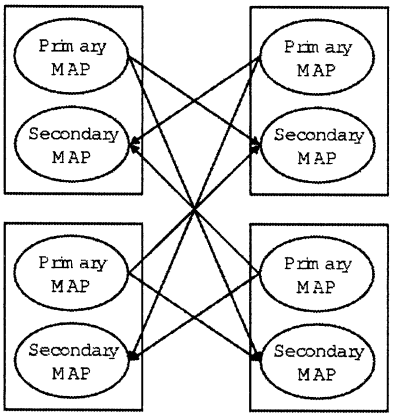


Fig. 9 Primary-secondary relationship in RH-MIPv6.

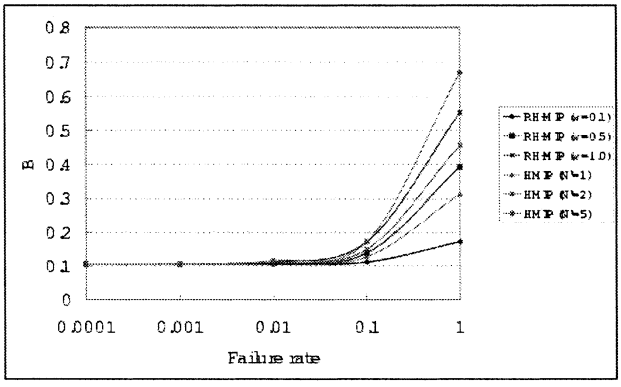


Fig. 10 MAP blocking probability (utilization ratio = 50).

blocking probabilities in RH-MIPv6 are shown when ω is 0.1, 0.5, and 1.0. Also, Fig. 10 shows MAP blocking probabilities of HMIPv6 using a typical primary-backup scheme when N' is 1, 2, and 5. As shown in Fig. 10, MAP blocking probability is proportional to MAP failure rate. Its increasing rate also increases as the failure rate increases. When ω is 0.1, RH-MIPv6 shows the lowest MAP blocking probability. In contrast, in the case where ω is 0.5 or 1.0, the MAP blocking probability of RH-MIP is higher than that of HMIPv6 with N' of 1. However, this result does not indicate that HMIPv6 outperforms RH-MIP in terms of MAP blocking probability. In HMIPv6, N' of 1 means that a MAP is exclusively used as a backup agent for a primary agent (refer Fig. 8). Therefore, it requires more redundant agents and it results in a higher cost. In practical networks, a MAP may act as a backup agent for multiple MAPs due to limited network resources, so that N' will be larger than 1. As shown in Fig. 10, when N' is larger than 1, the MAP blocking probability of HMIPv6 is larger than that of RH-MIPv6 with ω of 0.5. Of course, when ω is 1.0, MAP blocking probability of RH-MIPv6 is larger than that of HMIPv6 with N' of 2. However, ω of 1.0 represents the worst case, where all MNs serviced by the faulty P-MAP configure MAP (A) as their S-MAP. Since ω is equal to $1/N$ in the average case, it is more reasonable to compare RH-MIPv6 of ω of 0.3 or 0.4

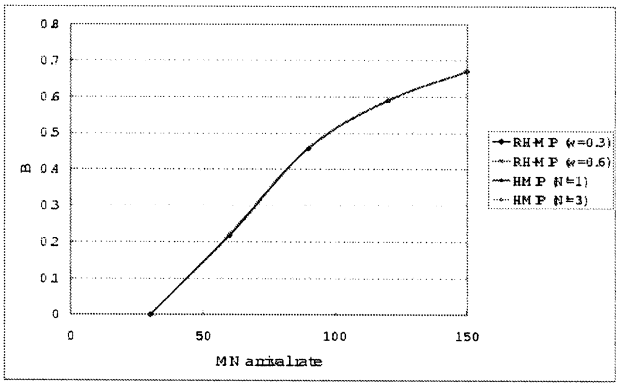


Fig. 11 MAP blocking probability vs. MN arrival rate.

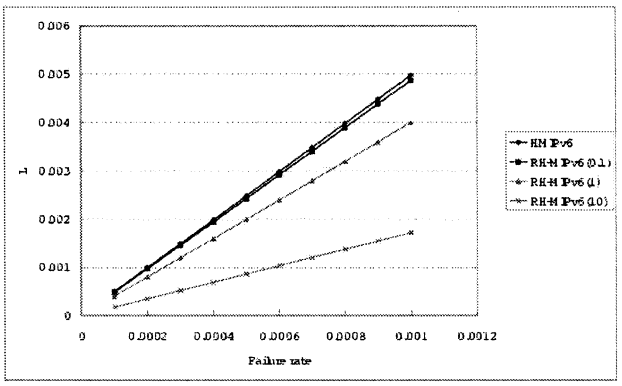


Fig. 13 Packet loss rate vs. failure rate.

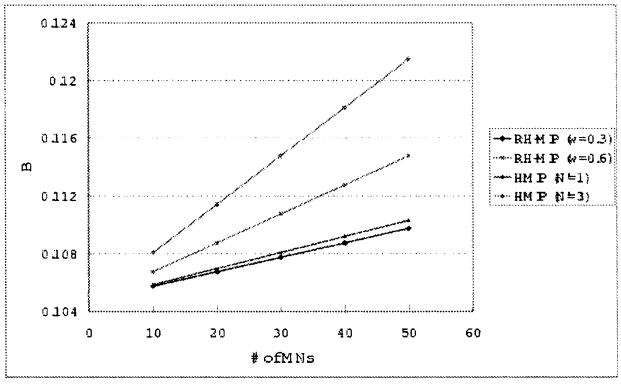


Fig. 12 MAP blocking probability vs. number of MNs serviced by faulty MAP.

with HMIPv6.

Figure 11 shows MAP blocking probability as λ_{MAP} increases whereas μ_{MAP} is fixed to 1. As shown in Fig. 11, The MAP blocking probability is proportional to the MN arrival rate. However, there are no apparent differences between HMIPv6 and RH-MIPv6. On the other hand, Fig. 12 shows the MAP blocking probability when M is varied. Figure 12 indicates that blocking probability is proportional to the number of MNs serviced by the faulty P-MAP. Also, it represents that the MAP blocking probability can be reduced when the MNs are evenly distributed to several S-MAPs. Comparing Fig. 12 with Fig. 11, in terms of MAP blocking probability, the performance of RH-MIPv6 is more sensitive to the number of MNs redirected from the faulty P-MAP rather than the original MN arrival rate. Therefore, an efficient MAP selection is required.

4.4 Packet Loss Rate

At last, the average packet loss rate due to MAP failure can be expressed as Eq. (11).

$$L = \lambda_p \times v_1 \tag{11}$$

where λ_p is the average packet arrival rate.

Figure 13 shows packet loss rate as failure rate increases. In Fig. 13, three packet arrival rates (i.e., 0.1, 1, and 10) are evaluated. Intuitively, packet loss rate increases as failure rate increases. In addition, RH-MIPv6 has a shorter fault time, so that it provides less packet loss rate than HMIPv6. However, when packet arrival rate is small (i.e., λ_A is 1), RH-MIPv6 shows almost the same packet loss rate as HMIPv6, as shown in Fig. 13. This is because failure detection time in RH-MIPv6 is highly dependent on packet arrival rate in most cases, but failure detection time is determined by the RA interval in the case of low packet arrival rate.

5. Conclusion

Fault-tolerance and reliability are critical issues for successful deployment and operation of mobile multimedia systems because they are closely related to QoS degradation of mobile users. To provide fault-tolerance with HMIPv6, we proposed the use of an enhanced HMIPv6, called RH-MIPv6, in the distributed MAP environment. The key ideas are to allow multiple binding updates using primary and secondary RCoAs by the MN and to change the serving MAP from the primary MAP to the secondary MAP in the case of a MAP failure. By these mechanisms, it is possible to reduce the failure detection and recovery time. In this paper, we presented comparative study results between RH-MIPv6 and HMIPv6 under various performance factors. To do this, we utilized the semi-Markov chain and the $M/G/C/C$ queuing model. As a result, RH-MIPv6 shows a lower MAP unavailability and a higher MAP reliability than HMIPv6. In addition, RH-MIPv6 shows a lower blocking probability and packet loss rate than HMIPv6.

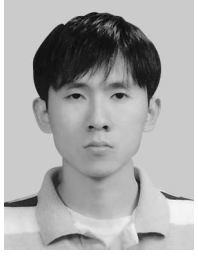
Acknowledgement

This work was supported in part by the Brain Korea 21 project of the Ministry of Education and in part by the National Research Laboratory project of the Ministry of Science and Technology, 2003, Korea.

References

[1] T.W. You, S.H. Pack, and Y.H. Choi, “Robust hierarchical mo-

bile IPv6 (RH-MIPv6)—An enhancement for survivability & fault-tolerance in mobile IP systems," Proc. IEEE VTC 2003 Fall, Oct. 2003.
[2] H. Soliman, C. Castelluccia, K. El-Malki, and L. Bellier, "Hierarchical Mobile IPv6 mobility management (HMIPv6)," Internet Draft, draft-ietf-mipshop-hmipv6-00.txt, Work in Progress, June 2003.
[3] H. Omar, T. Saadawi, and M. Lee, "Supporting reduced location management overhead and fault tolerance in Mobile-IP systems," Proc. IEEE ISCC 1999, July 1999.
[4] R. Ghosh and G. Varghese, "Fault-tolerant mobile IP," Washington Univ. Technical Report WUCS-98-11, 1998.
[5] J.H. Ahn, S.G. Min, and C.S. Hwang, "Scalable and efficient fault-tolerant protocol for mobility agents in mobile IP-based systems," Future Generation Computer Systems, vol.18, no.5, pp.613–625, April 2002.
[6] J. Lin, J. Tsai, and C. Huang, "A dynamical redirection approach to enhancing mobile IP with fault tolerance in cellular systems," Proc. IEEE GLOBECOM 2002, Nov. 2002.
[7] Y. Xu, H.C.J. Lee, and V.L.L. Thing, "A local mobility agent selection algorithm for mobile networks," Proc. IEEE ICC 2003, May 2003.
[8] L. Kleinrock, Queuing Systems, vol.I, Theory, John Wiley & Sons, New York, 1976.
[9] A. Conta and S. Deering, "Internet control message protocol (ICMPv6) for the Internet protocol version 6 (IPv6) specification," IETF RFC 2463, Dec. 1998.
[10] R. Ramjee, L. Li, T. La Porta, and S. Kasera, "IP paging service for mobile hosts," ACM Wireless Networks, vol.8, no.5, pp.427–441, Sept. 2002.
[11] N. Montavont and T. Noel, "Handover management for mobile nodes in IPv6 networks," IEEE Commun. Mag., vol.40, no.8, pp.38–43, Aug. 2002.



Sangheon Pack received B.S. (2000, magna cum laude) and M.S. (2002) degrees from Seoul National University, both in computer engineering. He is currently working toward a Ph.D. degree in the School of Computer Science and Engineering at the Seoul National University, Korea. He is a student member of the IEEE. Since 2002, he has been a recipient of the Korea Foundation for Advanced Studies (KFAS) Computer Science and Information Technology Scholarship. He has been also a member of Samsung Frontier Membership (SFM) from 1999. He received a student travel grant award for the IFIP Personal Wireless Conference (PWC) 2003. He was a visiting researcher to Fraunhofer FOKUS, German in 2003. His research interests include mobility management, multimedia transmission, and QoS provision issues in the next-generation wireless/mobile networks.

Taewan You received B.S. in the Department of Computer Science from Chonbuk National University, Chonbuk, Korea, and M.S. degree in the School of Computer Science and Engineering from Seoul National University, Seoul, Korea, in 2001 and 2004, respectively. His research interests include multimedia communication in wireless and mobile networks, multimedia system design based on IPv6, mobility management, and survivability issues in mobile systems.

Yanghee Choi received B.S. in electronics engineering from Seoul National University, M.S. in electrical engineering from Korea Advanced Institute of Science, and Doctor of Engineering in Computer Science from Ecole Nationale Superieure des Telecommunications (ENST) in Paris, in 1975, 1977 and 1984 respectively. Before joining the School of Computer Engineering, Seoul National University in 1991, he has been with Electronics and Telecommunications Research Institute (ETRI) during 1977–1991, where he served as director of Data Communication Section, and Protocol Engineering Center. He was research student at Centre National d'Etude des Telecommunications (CNET), Issy-les-Moulineaux, during 1981–1984. He was also Visiting Scientist to IBM T.J. Watson Research Center for the year 1988–1989. He is now leading the Multimedia Communications Laboratory in Seoul National University. He is also director of Computer Network Research Center in Institute of Computer Technology (ICT). He was editor-in-chief of Korea Information Science Society journals. He was chairman of the Special Interest Group on Information Networking. He has been associate dean of research affairs at Seoul National University. He was president of Open Systems and Internet Association of Korea. His research interest lies in the field of multimedia systems and high-speed networking.