Wireless Pers Commun
DOI 10.1007/s11277-007-9267-2

Survivability evaluation of SIGMA and mobile IP

Shaojian Fu · Mohammed Atiquzzaman

Received: 22 May 2006 / Accepted: 22 January 2007

Abstract Mobile IP has been developed by IETF to handle mobility of Internet hosts at the network layer. Mobile IP suffers from a number of drawbacks, including low survivability due to single-point failure of Home Agents. Recently, Seamless IP diversity based Generalized Mobility Architecture (SIGMA) was proposed to support low latency, low packet loss mobility of IP hosts. In this paper, we show that the location management scheme used in SIGMA enhances the survivability of the SIGMA-based mobile network. We develop an analytical model to evaluate and compare the survivability of SIGMA with that of Mobile IP. Numerical results show the improvement in system response time and service blocking probability of SIGMA over Mobile IP in the presence of hardware failures and Distributed Denial of Service (DDoS) attacks.

The research reported in this paper was funded by NASA Grants NAG3-2922 and NNX06AE44G

S. Fu
OPNET Technologies, 7255 Woodmont Avenue, Bethesda, MD 20814-7900, USA

M. Atiquzzaman (✉)
School of Computer Science, University of Oklahoma, Norman, OK 73019-6151, USA
e-mail: atiq@ou.edu

Keywords Mobility Management · Survivability · Mobile IP · Modeling

1 Introduction

Mobile IP (MIP) [13] is designed to handle mobility of Internet hosts at the network layer. MIP suffers from a number of drawbacks, one of which is low survivability due to single-point failure of Home Agents. MIP is based on the concept of Home Agent (HA) for recording the current location of the Mobile Host (MH), and forwarding packets to MH when it moves out of its home network. In MIP, the location database of the mobile nodes are distributed across all the HAs that are scattered at different locations (home networks). According to principles of distributed computing, this approach appears to have good survivability. However, MIP's location management scheme suffers from the following two major drawbacks, resulting in low survivability:

- Each user's location and account information is only accessible through its HA. The transparent replication of the HA, if not impossible, is not an easy task as it involves extra signaling support as proposed in [9].
- HAs have to reside in the home network of an MH in order to intercept the packets sent to the MH. For scenarios where the complete home

network is located in a hostile environment, the failure of the home network makes all the MHs of the home network inaccessible, regardless of whether a specific MH is physically attached to the home network.

As the amount of real-time traffic over wireless networks keeps growing, the deficiencies of the network layer based Mobile IP, in terms of high latency and packet loss, becomes more obvious. Since most of the applications in the Internet are end-to-end, a transport layer mobility solution would be a natural candidate as an alternative approach. A number of transport layer mobility protocols have been proposed, for example, MSOCKS [10] and connection migration solution [15] in the context of TCP, and M-SCTP [18] and mobile SCTP [8] in the context of SCTP [5]. In our previous study in [6], we proposed a new architecture for supporting low latency, low packet loss mobility, called Seamless IP diversity based Generalized Mobility Architecture (SIGMA), and evaluated its handover performance compared with MIP and its enhancements.

The location management and data traffic forwarding functions in SIGMA are decoupled, allowing it to overcome the drawbacks of MIP in terms of survivability. In SIGMA, location management can be achieved by DNS servers, which can be deployed anywhere in the Internet and in a highly secure location. Also, it would be fairly straightforward to duplicate the Location Managers (LMs) since they are not responsible for user data forwarding.

The location management of SIGMA does not require any manual configuration among the root servers. Only the Authorative Name Server (ANS) of DNS is periodically updated using the secure dynamic DNS update protocol [17] to reflect the new location of the mobile node. The ANS is the last server in the DNS hierarchy which can be updated without any scalability issues. For example, secure dynamic DNS update is currently used by Internet search companies like Yahoo and Google to balance the load among their different servers. SIGMA uses the well tested and widely used stable DNS system which has been shown to work reliably in the current Internet.

In the literature, two recent papers have addressed the problem of MIP survivability [19] and [7]. T. You et al. proposed allowing MH to register with multiple Mobility Anchor Points (MAPs) to avoid single point of failure [19]. Jan et al. [7] used a similar idea as SIGMA; the authors proposed a scheme to move HA (they call it Location Register) to a secure location, and duplicate HA through some translation servers or a Quorum Consensus algorithm borrowed from distributed database systems [7]. Lin and Arul [9] proposed using backup mobility agents to increase the survivability of MIP. They have shown analytically the improvement in MIP's ability to survive failures of mobility agents. Pack et al. [19] proposed using multiple Mobility Anchor Points to increase the faulty tolerance of Hierarchical Mobile IP. However, none of the above papers analytically modeled the survivability of MIP. The *objective* of this paper is to show, using analytical models, that the location management scheme used in SIGMA enhances the survivability of a mobile network. The *contributions* of this paper can be summarized as:

- Investigate reasons for higher survivability of SIGMA over MIP.
- Develop an analytical model based Markov Reward Process to determine the survivability of SIGMA.
- Compare the survivability of SIGMA and MIP in terms of system availability and user response time.

The rest of this paper is structured as follows: Section 2 reviews the basic idea of SIGMA and its location management scheme, Sect. 3 illustrates the basic reason for SIGMA achieving higher survivability than MIP. The analytical models for SIGMA and MIP survivability are described in Sect. 4, and followed by the numerical results in Sect. 5. Finally, concluding remarks are presented in Sect. 6.

2 A brief introduction to SIGMA and its Location Management

Seamless IP diversity based Generalized Mobility Architecture (SIGMA) [6] is a new scheme for supporting low latency, low packet loss mobility

for IP hosts. It can cooperate with normal IPv4 or IPv6 infrastructure without the support of Mobile IP. The basic idea of handover in SIGMA is to exploit IP diversity (multihoming) to keep the old path alive during the process of setting up the new path to achieve a seamless handover. SIGMA relies on the signaling message exchange between the MH, correspondent node (CN), and location manager (LM). For every handover, MH sends binding update and location update to CN and LM, respectively.

2.1 Handover process of SIGMA

A typical mobile handover in SIGMA using SCTP as an illustration is shown in Fig. 1, where the Mobile Host (MH) is multi-homed node connected through two wireless access networks. Correspondent node (CN) is a single-homed node sending traffic to MH.

The handover process of SIGMA can be described by the following five steps [6]: (1) obtain new IP address; (2) add IP addresses into the transport layer association (this requires the transport layer protocol supporting multihoming); (3) redirect data packets to new IP address; (4) Update location manager (LM); (5) Delete or deactivate obsolete IP address.

2.2 Location management of SIGMA

SIGMA needs to setup the LM for maintaining a database of the correspondence between MH's identity and its current IP address. Unlike MIP, the location manager in SIGMA is not restricted to the same subnet as MH's home network (in fact, SIGMA has no concept of home or foreign network). The location of the LM has no impact on the handover performance of SIGMA. This will make the deployment of SIGMA much more flexible than MIP.

The location management is done as shown in Fig. 2: (1) MH updates the location manager with the current primary IP address. (2) When CN wants to setup a new association with MH, CN sends a query to the location manager with MH's identity (home address, domain name, or public key, etc.) (3) Location manager replies to CN with the current primary IP address of MH. (4) CN sends a signaling message to MH's new primary IP address to setup the association.

If we use domain name as MH's identity, we can merge the location manager into a DNS server. The idea of using a DNS server to locate mobile users can be traced back to [18]. The advantage of this approach is its transparency to existing network applications that use domain name to IP address mapping. An Internet administrative domain can allocate one or more location servers for its registered mobile users. Compared to MIP's requirement that each subnet must have a location

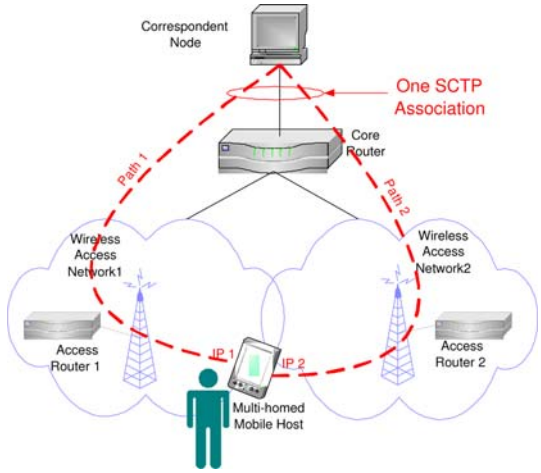

Fig. 1 An SCTP association with multi-homed mobile host

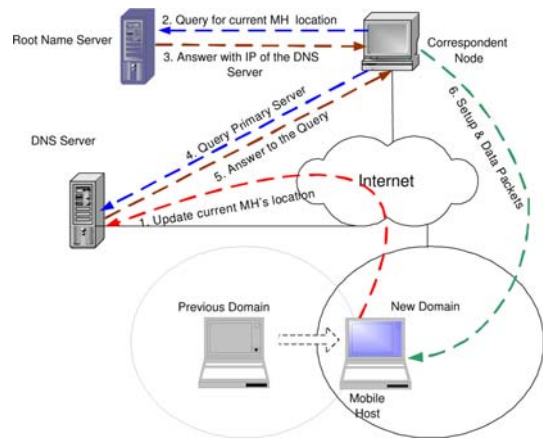

Fig. 2 Location management in SIGMA

management entity (which is HA), SIGMA significantly reduces system complexity and operating cost significantly by not having such a requirement. Moreover, the survivability of the whole system is also enhanced as discussed in Sect. 3. Note that In SIGMA, the location lookup operation is only required once at transport layer association setup time. After that, no location lookup required for currently connected correspondent nodes, even if mobile host changes location. Generally, users are much more tolerant to the latency incurred at association setup time, so the location lookup latency caused by DNS queries is acceptable. The more detailed discuss on SIGMA location management can be found in the other two papers of us [1,14].

3 Survivability comparison of SIGMA and MIP

In this section we discuss the survivability of MIP and SIGMA. We highlight the limitations of MIP in terms of survivability, and discuss how those limitations are avoided in SIGMA.

3.1 Survivability of MIP

In MIP, the location database of the mobile nodes are distributed across the HAs that are scattered at different locations (home networks). According to principles of distributed computing, this approach appears to have good survivability. However, MIP's location management scheme suffers from the following two major drawbacks as given below:

- If we examine the distribution of the mobile users' location information in the system, we observe that each user's location and account information can only be accessible through its HA; these information are not truly distributed to increase the survivability of the system. The transparent replication of the HA, if not impossible, is not an easy task as it involves extra signaling support as described in [9].
- Even if we replicate a HA to another agent, these HAs have to be located in the home network of an MH for intercepting packets sent to the MH. If the complete home network is located in a hostile environment, such as a battlefield, the possibility of all HAs being destroyed is relatively high. In the case of failure of a home network, all the MHs belonging to the home network would be inaccessible.

3.2 Centralized location management of SIGMA offers higher survivability

Referring to Fig. 2, SIGMA uses a centralized location management approach. As discussed in Sect. 2, the location management and data traffic forwarding functions in SIGMA are decoupled, allowing it to overcome many of the drawbacks of MIP in terms of survivability (see Sect. 3.1) as given below:

- The LMs can be based on a DNS-like structure, or can be combined with a DNS server. It is, therefore, easy to replicate the Location Manager of SIGMA at distributed secure locations to improve survivability.
- Only location updates/queries have to be directed to the LM. Data traffic do not pass through the LM. Thus, the LM does not have to be located in a specific network to intercept data packets destined to a particular MH. It is thus possible to avoid physically locating the LM in a hostile environment; it can be located in a secure environment, making it highly available.

Figure 3 illustrates the survivability of SIGMA's location management, implemented using DNS servers. Currently, 13 servers in the Internet [3] constitute the root of the DNS name space hierarchy. There are also several delegated name servers in the DNS zone [16], one of which is primary and the rest are for backup and they share a common location database. If an MH's domain name belongs to a DNS zone, the MH is managed by the name servers in that zone. When the CN wishes to establish a connection with the MH, it first sends a request to one of the root name servers, which directs the CN to query the intermediate name servers in the hierarchy. Eventually, CN obtains the IP addresses of the name servers in the DNS zone to which the MH belongs. The CN then tries to contact the primary name server to obtain MH's

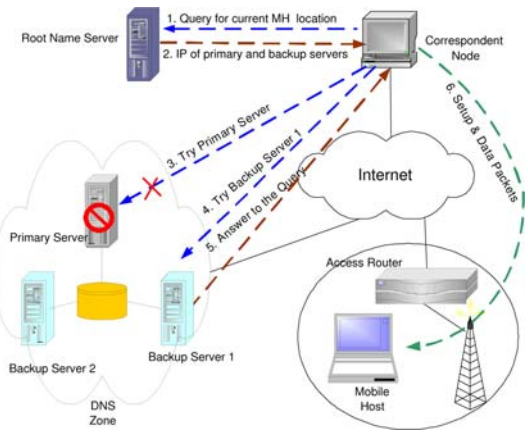

Fig. 3 Survivability of SIGMA's location management

current location. If the primary server is down, CN drops the previous request and retries backup name server 1, and so on. When a backup server replies with the MH's current location, the CN sends a connection setup message to MH. There is an important difference between the concept of MH's DNS zone in SIGMA and MH's home network in MIP. The former is a logical or soft boundary defined by domain names, while the latter is a hard boundary determined by IP routing infrastructure.

If special software is installed in the primary/backup name servers to constitute a high-availability cluster, the location lookup latency can be further reduced. During normal operation, heart beat signals are exchanged within the cluster. When the primary name server goes down, a backup name server automatically takes over the IP address of the primary server. A query request from a CN is thus transparently routed to the backup server without retransmission of the request from the CN.

Other benefits of SIGMA's centralized location management over MIP's location management can be summarized as follows:

- *Security*: Storing user location information in a central secure database is much more secure than being scattered over various Home Agents located at different sub-networks (in the case of Mobile IP).
- *Scalability*: SIGMA's location servers do not intervene with data forwarding task, which helps in adapting to the growth in the number of mobile users gracefully.
- *Manageability*: SIGMA's centralized location management provides a mechanism for an organization/service provider to control user accesses from a single server.

4 Analytical model

The aim of our model is to perform a combined analysis of system availability and performance evaluation. J. Meyer defined a new measure called *performability* [11,12], which will be used in this paper to measure the survivability of SIGMA and MIP. A performability model consists of an availability sub-model, a performance sub-model, and a glue model that combines these two sub-models. We choose *Markov Reward Model* as the glue model since it provides a natural framework for an integrated specification of state transitions due to server failures and system performance (equivalent to reward) under each system state.

4.1 Networking architecture

Our analytical model is based on the networking architecture shown in Fig. 4. The router forwards location updates from MHs, location queries from CNs, and Distributed Denial of Service (DDoS) [4] attack traffic to N location managers according to a round-robin policy. Each location manager has an independent queue of size K packets. After processing of a packet by a location manager, the acknowledgement/reply to the update/query/attack packets are transmitted back to their originators.

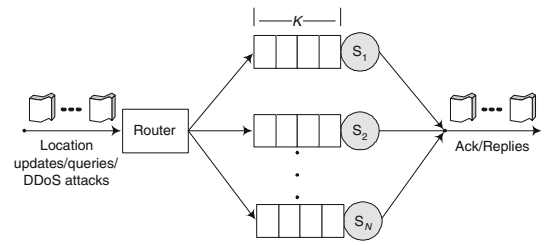

Fig. 4 Queuing model of N location managers

4.2 Assumptions and notations

We have made the following assumptions in our analytical model to make it computationally tractable:

- Arrival of location updates, queries, and DDoS attacks are *Poisson* processes.
- Location managers can not differentiate DDoS attack traffic from legitimate traffic.
- All location managers share common set of MH's mobility bindings.
- Processing time of location updates, queries, and DDoS attacks are exponential distributed and have same mean value. We assume DDoS attacks have same processing time as location updates or queries since these attacks will either emulate a update or a query packet to get around the firewall. We assume the location update and query have same processing time mainly to control the complexity of the underlying CTMC.
- Hardware failures can be perfectly covered[1], i.e. system can degrade gracefully when one of the working server fails.
- Hardware failures always occur on the servers with heaviest load.

Following are the notations that will be used in our analytical model:

N	total number of location managers.
$\lambda_u, \lambda_q, \lambda_a$	arrival rate of location updates, queries, and DDoS attacks, respectively.
λ	summation of $\lambda_u, \lambda_q, \lambda_a$.
μ	location manager processing rate.
K	queue size of each location manager (packets).
γ, δ	hardware failure rate and repair rate, respectively.
τ	Mean Time To Failure (MTTF)
ϕ	Mean Time To Repair (MTTR)

4.3 Combined system availability & performance model for SIGMA survivability

The objective of our model is to determine the average response time and blocking probability of SIGMA due to hardware failures and DDoS attacks. We use a two-dimensional Continuous Time Markov Chain (CTMC) to capture system characteristics. The state transition diagram is shown in Fig. 5, in which each state is labelled as (N_w, L), where N_w is the number of currently working servers and L is the total number of packets in the system. When N_w equals N, since each server has a queue size of K, the maximum value of L is $K'' = N \times K$. Similarly, When N_w equals $N-1$, the maximum value of L is $K' = (N-1) \times K$.

We illustrate the transition diagram through several transition types:

- Current state is (s,p) with $p < s \times K$, arrival of one update/query/attack packet will change the state to (s,$p+1$). Since router use a round-robin policy, each server has equal share of load. Therefore, the transition rate is λ/N.
- Current state is (s,p) $p \geq 1$, departure of one packet will change the state to (s,$p-1$). Since each server has equal processing rate of μ, therefore, the transition rate is μ.
- Current state is (s,0) with $s \geq 1$, the hardware failure of any one server (happens with a rate of $N\gamma$) will make the next state ($s-1$,p).
- Current state is (s,p) with $s, p \geq 1$ and, one hardware failure will make the next state ($s-1$,$p-1$). Since we assume the hardware failure always occurs on the servers with heaviest load (equals one in this case), the packets assigned to the failed server will be lost.
- Current state is (s,p) with $s < N$, the repair of the failed server will change the state of ($s+1$,p).

We can determine each element of infinitesimal generator matrix Q of CTMC shown in Fig. 5 as follows:

$$q_{i,j} = \begin{cases} \lambda/N_w & j = i+1, L_i \leq N_w K \quad \text{(arrival)} \\ \mu & j = i-1, L_i \geq 1 \quad \text{(departure)} \\ \gamma N_w & j = i - \left\lceil \frac{i-1}{N_w} \right\rceil - \frac{K(N_w-1)}{2} \quad \text{(failure)} \\ \delta & j = i + N_w K + 1 \quad \text{(repair)} \\ 0 & \text{other } j \neq i \\ -\sum_{k=1}^{m} q_{i,k} & j = i, k \neq i \end{cases} \tag{1}$$

[1] In an imperfect coverage system, some failures are impossible to be detected and the failure of one component will halt the whole system.

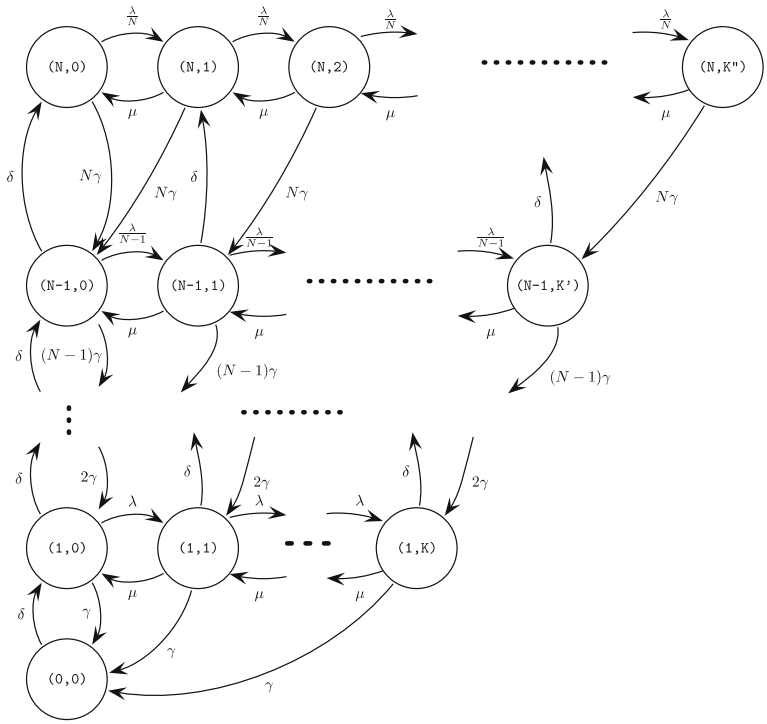

Fig. 5 State digram of N location managers

Where L_i is the total number of packets in system when current state is labelled as i, and m is the size of matrix, which is given by:

$$m = K\frac{N(N+1)}{2} + (N+1) \tag{2}$$

The j in arrival, departure, and repair cases of Eq. 1 are self-describing. Equation 3 shows how j is determined in the failure case of Eq. 1.

$$\begin{aligned} j = & \left(i - 1 - \sum_{x=0}^{N_w-1}\sum_{z=0}^{xK} 1\right) \\ & - \left\lceil \frac{\left(i - 1 - \sum_{x=0}^{N_w-1}\sum_{z=0}^{xK} 1\right)}{N_w} \right\rceil \\ & + \left(1 + \sum_{x=0}^{N_w-2}\sum_{z=0}^{xK} 1\right) \\ = & \left[i - (N_w - 1)K - 1\right] \\ & - \left\lceil \frac{\left(i - 1 - \sum_{x=0}^{N_w-1}\sum_{z=0}^{xK} 1\right)}{N_w} \right\rceil \\ = & \; i - \left\lceil \frac{i-1}{N_w} \right\rceil - \frac{K(N_w-1)}{2} \end{aligned} \tag{3}$$

Once we have determined the infinitesimal generator matrix Q, we can compute the stationary distribution of the CTMC π by:

$$\pi Q = \mathbf{0} \tag{4}$$

When a packet arrives, if the system is in state (0,0) or state (N_w,N_wK), the packet is dropped since no service is possible. Therefore, the blocking probability can be calculated by:

$$\begin{aligned} & P_b = \pi B^T \\ & \text{where } B = [1, B_1, \ldots B_j \ldots B_N], \\ & \text{and } B_j = [0, \ldots 0, 1]_{jK+1}, j = 1, \ldots, N \end{aligned} \tag{5}$$

The average number of packets in the whole system can be calculated by:

$$\begin{aligned} & E[n] = \pi v^T \\ & \text{where } v = [v_0, v_1, \ldots v_j \ldots v_N], \\ & \text{and } v_j = [0, 1, \ldots jK], j = 0, \ldots, N \end{aligned} \tag{6}$$

According to Little's law, the system response time can be determined by:

$$E[T] = \frac{E[n]}{\lambda_{accepted}} = \frac{E[n]}{\lambda(1 - P_b)} \tag{7}$$

4.4 Analytical model for MIP survivability

In this section, the survivability of MIP is analyzed. We use the same assumptions and notations as used for SIGMA in Sect. 4.2. Additionally, if λ_d is the arrival payload data traffic rate at HA, then $\lambda = \lambda_u + \lambda_q + \lambda_a + \lambda_d$. Two modes of MIP will be considered here:

- *Single server mode*: only one HA is available for a network. Once failure happens, all service requests are blocked until the server repaired.
- *Standby mode*: there are multiple HAs available, one of which is the primary HA. Once the primary HA fails, one of the backup HAs will be switched in within time T_{sw}. During T_{sw}, all service requests are blocked.

Both these two MIP modes can be modelled by a CMTC as shown in Fig. 6. At any time instants, at most one HA can be serving requests. Any hardware failure will move the state from $(1,L), (L = 1,2,\ldots,K)$ to (0,0). In the single server model, state (0,0) models the time for server repair, whereas in standby mode, state (0,0) models the time required for switching a standby server into a primary one. Therefore, the value of δ in Fig. 6 can be determined as follows:

$$\delta = \begin{cases} \frac{1}{MTTR} & \text{(single server mode)} \\ \frac{1}{T_{sw}} & \text{(standby mode)} \end{cases} \tag{8}$$

From now on, we will use the same technique as used in Sect. 4.3 to compute the average system response time and service blocking probability by setting $N = 1$, and δ to the value given in Eq. 8.

We can determine each element of infinitesimal generator matrix Q of MIP CTMC shown in Fig. 6 as follows:

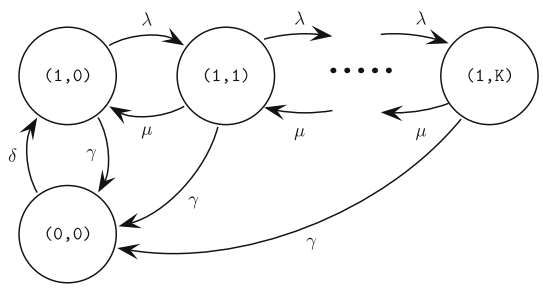

Fig. 6 State digram of MIP HA

$$q_{i,j} = \begin{cases} \lambda & j = i+1, L_i \le K \quad \text{(arrival)} \\ \mu & j = i-1, L_i \ge 1 \quad \text{(departure)} \\ \gamma & j = 1 \quad \text{(failure)} \\ \delta & i = 1, j = 2 \quad \text{(repair)} \\ 0 & \text{other } j \ne i \\ -\sum_{k=1}^{m} q_{i,k} j = i, k \ne i \end{cases} \tag{9}$$

We can follow the same procedure shown in Eqs. 4–7 to calculate the number of packets in system and the system response time in MIP CTMC.

5 Numerical Results

In this section, we evaluate the survivability of SIGMA using the analytical model developed in Sect. 4. The survivability of SIGMA is also compared with that of MIP. The survivability is measured by the combined performance index consisting of system response time and blocking probability.

5.1 SIGMA survivability

First, we look at the impact of DDoS attack strength (λ_a) on the system response time. We set $N = 3$, $\lambda_u = 0.2$, $\lambda_q = 0.4$, $\mu = 2$, $1/\delta = 24$ h, and $K = 10$ packets. As shown in Fig. 7, with increasing DDoS attack strength, the system response time increases dramatically compared to its normal values. Also, with more frequent hardware failures (smaller MTTF values), the system response time also increases due to less working server available to process client requests.

Next, we look at the impact of DDoS attack strength on the system blocking probability. As shown in Fig. 8, with increasing DDoS attack strength, the system blocking probability increases, due to fewer buffer space available to serve legitimate client requests. As expected, the impact of DDoS attack on blocking probability increases as K decreases. Therefore, increasing the value of K can decrease the sensitivity of system blocking probability to DDoS attack.

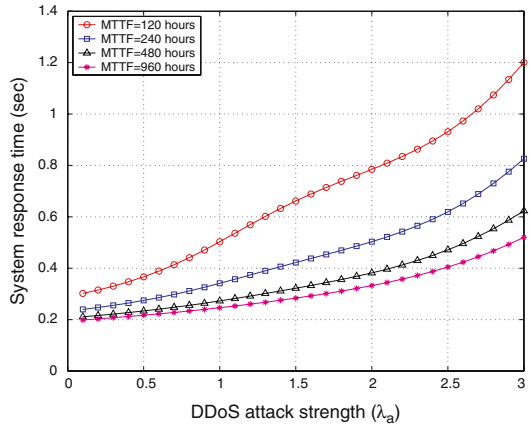

Fig. 7 Impact of DDoS attack strength on system response time

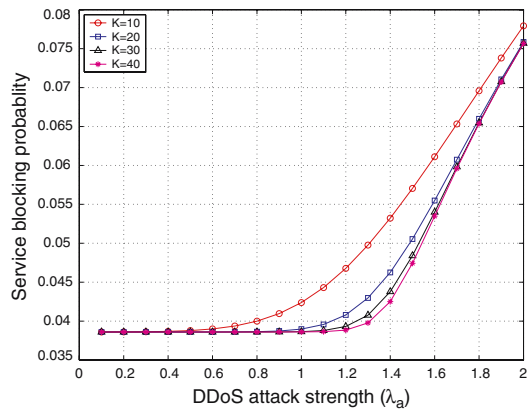

Fig. 8 Impact of DDoS attack strength on blocking probability

Figure 9 shows the impact of MTTR on system response time. We can observe the average response time increases with increasing repair time. This is because once a server fails, it needs longer time to repair. Thus fewer working server are available to process client requests when MTTR is high, resulting in a high response time.

Finally, Fig. 10 shows the impact of *Limiting Availability* on system response time. The limiting availability is defined as $\alpha = \frac{MTTF}{MTTF+MTTR}$, which denotes the long range average percentage of available time. As expected, when α increase, the system response time decrease.

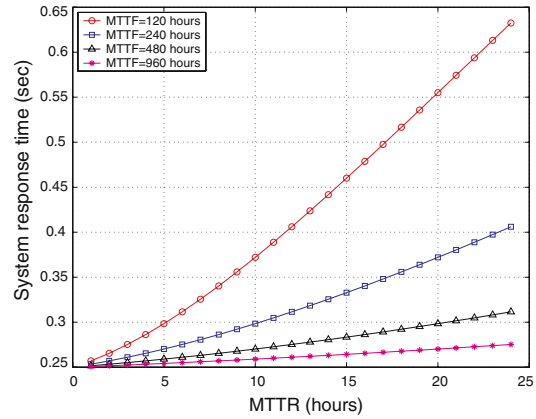

Fig. 9 Impact of MTTR on system response time

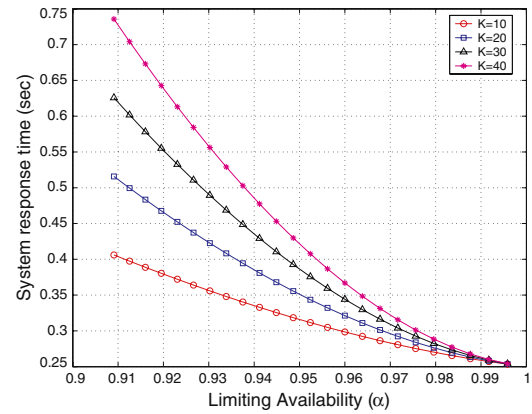

Fig. 10 Impact of hardware limiting availability on system response time

5.2 Survivability comparison of SIGMA and MIP

Now, we compare the survivability of SIGMA against MIP. First, we look at the impact of DDoS attack strength (λ_a) on the system response time, with $\lambda_d = 0$ and $T_{sw} = 10$ min, as shown in Fig. 11. The average response time for both modes of MIP is much higher than that of SIGMA, even with $\lambda_d = 0$. MTTF does not have an impact on the response time of MIP. This is because we only consider the response time for non-blocked requests. Higher MTTF will results in the system staying in the available state for longer time, at the expense of higher queueing delays. These two effects cancel out, leaving no effect on the overall response time.

Next, we compare the impact of DDoS attack strength on the service blocking probability of

SIGMA against MIP. As shown in Fig. 12, for increasing DDoS attack strength, all schemes incur a higher service blocking probability. However, SIGMA has a lower blocking probability than both modes of MIP. For MIP standby mode, MTTF does not have any obvious impact on the service blocking probability. This is because T_{sw} is 10 min, which is very small compared to MTTF. Once HA fails, it is deemed to be replaced by a new one immediately.

Figure 13 compares the impact of data traffic strength (λ_d) on the service blocking probability of SIGMA against MIP, with $\lambda_a = 1$. Since SIGMA decouples location management from data forwarding, the data traffic strength does not have impact on the service blocking probability. For MIP, the data traffic contends with location management traffic for the buffer slots, which increases the blocking probability. *This observation justifies our initial design of decoupling the location management from data forwarding function in SIGMA*.

Figure 14 compares the impact of hardware limiting availability on the response time of SIGMA against MIP. As in the case of MTTF in Fig. 11, the limiting availability does not affect the response time of MIP. Since MTTR is fixed, the limiting availability only depends on MTTF according to its definition. In comparison, higher α (which implies more reliable server hardware) results in a lower response time for SIGMA.

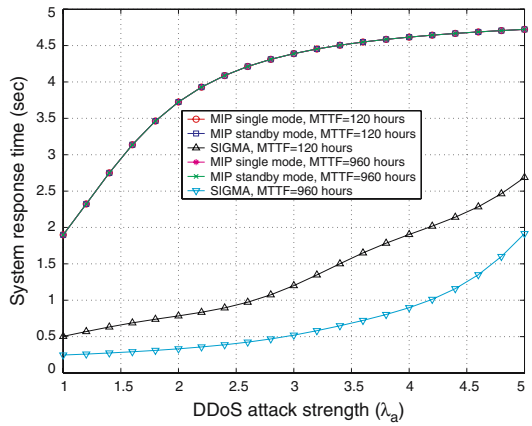

Fig. 11 Impact of DDoS attack strength on system response time for $\lambda_d = 0$

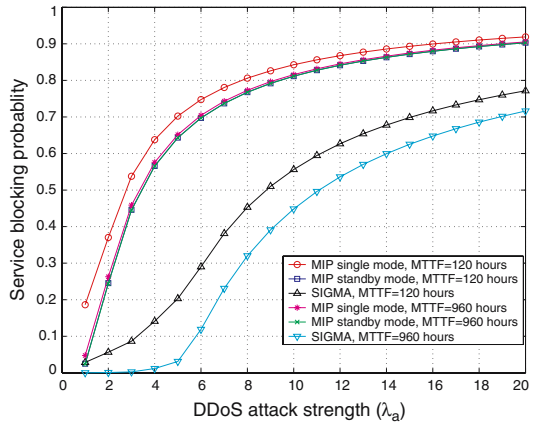

Fig. 12 Impact of DDoS attack strength on blocking probability for $\lambda_d = 0$

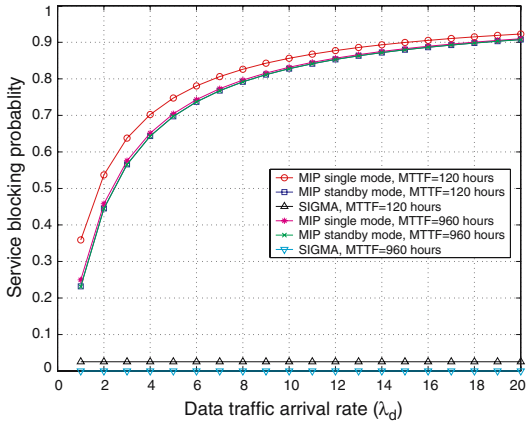

Fig. 13 Impact of data traffic strength on blocking probability

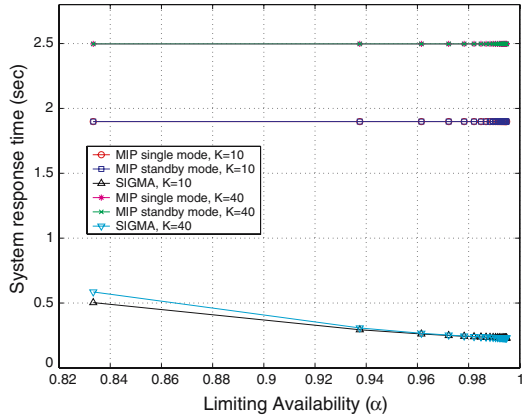

Fig. 14 Impact of hardware limiting availability on system response time

6 Conclusions

In this paper, we show that the location management scheme used in SIGMA enhances the survivability of the mobile network. We developed an analytical model based Markov Reward Process to evaluate the survivability of location management schemes of SIGMA and Mobile IP. Numerical results have shown the improvement in system response time and service blocking probability of SIGMA over Mobile IP in practical environments in the presence of the risk of hardware failures and Distributed Denial of Service attacks. The results also justified some choices we have made in designing SIGMA, such as, decoupling the location management from data forwarding function to improve the survivability of SIGMA.

References

1. Atiquzzaman, M., Reaz, A., Fu, S., & Ivancic, W. (2005). Location management of sigma. In *NASA earth science technology conference*. Maryland, June 2005.
2. Awerbuch, B., & Peleg, D. Concurrent online tracking of mobile users. In *ACM SIGCOMM symposium on communications, architectures and protocols* (pp. 221–233). September 1991.
3. Bush, R., Karrenberg, D., Kosters, M., & Plzak, R. (2000). Root name server operational requirements. IETF RFC 2870, June 2000.
4. Chang, R. K. C. (2002). Defending against flooding-based distributed denial-of-service attacks: A tutorial. *IEEE Communications Magazine, 40*(10), 42–51.
5. Fu, S., & Atiquzzaman, M. (2004). SCTP: State of the art in research, products, and technical challenges. *IEEE Communications Magazine, 42*(4), 64–76.
6. Fu, S., Atiquzzaman, M., Ma, L., & Lee, Y. (2005). Signaling cost and performance of SIGMA: A seamless handover scheme for data networks. *Journal of Wireless Communications and Mobile Computing, 5*(7), 825–845.
7. Jan, R., Raleigh, T., Yang, D., & Chang L. F. et al. Enhancing survivability of mobile Internet access using mobile IP with location registers. In *IEEE INFOCOM*, pp. 3–11, March 1999.
8. Koh, S. J., Lee, M. J., Ma, M. L., & Tuexen, M. (2004). *Mobile SCTP for Transport Layer Mobility*. draft-sjkoh-sctp-mobility-03.txt, February 2004.
9. Lin, J.W., & Arul, J. (2003). An efficient fault-tolerant approach for Mobile IP in wireless systems. *IEEE Transactions on Mobile Computing, 2*(3), 207–220.
10. Maltz, D. A., & Bhagwat, P. (1998). MSOCKS: An architecture for transport layer mobility. In *INFOCOM* (pp. 1037–1045). San Francisco, USA, March 1998.
11. Meyer, J. (1980). On evaluating the performability of degradable computing systems. *IEEE Transactions on Computers, 29*(8), 720–731.
12. Meyer, J. (1982). Closed-form solutions of performability. *IEEE Transactions on Computers, 31*(7), 648–657.
13. Perkins, C. E. (ed.) (2002). IP Mobility Support. IETF RFC 3344, August 2002.
14. Reaz, A., Fu, S., & Atiquzzaman, M. (2005). Lperformance of dns as a location manager for mobile networks. In *IEEE electro/information technology conference*, Lincoln, NE, May 2005.
15. Snoeren, A. C., & Balakrishnan, H. (2000). An end-to-end approach to host mobility. In *ACM MobiCom* (pp. 155–166). Boston, MA, August 2000
16. Stevens, W. R. (1994). *TCP/IP Illustrated, Vol 1 (The Protocols)*, Addison Wesley, November 1994.
17. Vixie, P., Thompson, S., Rekhtar, Y., & Bound, J. (1997). Dynamic updates in the domain name system (DNS update). IETF RFC 2136.
18. Xing, W., Karl, H., & Wolisz, A. (2002). M-SCTP: Design and prototypical implementation of an end-to-end mobility concept. In *5th international workshop on the internet challenge: Technology and applications*. Berlin, Germany, October 2002.
19. You, T., Pack, S., & Choi, Y. (2003). Robust hierarchical mobile IPv6 (RH-MIPv6): an enhancement for survivability and fault-tolerance in mobile IP systems. In *IEEE 58th vehicular technology conference* (pp. 2014–2018). October Fall 2003.

Shaojian Fu received a B.E. degree in transportation engineering in 1997 and an M.E. degree in systems engineering in 2000, both from Northern Jiaotong University, Beijing, P. R. China. During 2000–2001 he worked with Bell Labs China, Lucent Technologies in the area of network surveillance and performance management. He earned his Ph.D. degree at the School of Computer Science, University of Oklahoma, and currently works at OPNET. His research interests are in the areas of wireless communications, IP mobility, transport protocols, network simulation, and embedded reconfigurable computing.

Mohammed Atiquzzaman (atiq@ou.edu) received M.Sc. and Ph.D. degrees in electrical engineering from the University of Manchester, England. Currently he is a professor of Computer Science at the University of Oklahoma. He is Co-Editor-in-Chief of Computer Communications Journal, and serves on the editorial boards of IEEE Communications Magazine, Wireless and Optical Networks Journal, Real Time Imaging Journal, International Journal of Sensor Networks, and Telecommunication Systems. He was technical co-chair of HPSR 2003 and the SPIE Quality of Service over Next-Generation Data Networks Conference (2001, 2002, and 2003). He serves on the technical program committee of many national and international conferences, including IEEE INFOCOM and IEEE GLOBECOM. His current research interests are in wireless, satellite, and mobile networks, QoS for next-generation Internet, broadband networks, and multimedia over high speed networks. He is the c-chair of Next Generation Networks. Symposium at Globecom'06 and Wireless Communications Symposium at ICC'06. He is a coauthor of the book TCP/IP over ATM Networks. He has taught many short courses to industry in the area of computer and telecommunication networking. His research has been supported by state and federal agencies like NSF, NASA, U.S. Air Force, Ohio Board of Regents, and DITARD (Australia). He has over 150 refereed publications in the above areas, most of which can be accessed at http://www.cs.ou.edu/∼atiq.