Survivability Evaluation of SIGMA and Mobile IP

Shaojian Fu, **Mohammed Atiquzzaman**

TR-OU-TNRL-05-109
April 2005

Telecommunication & Network Research Lab

School of Computer Science

THE UNIVERSITY OF OKLAHOMA

200 Felgar Street, Room 159, Norman, Oklahoma 73019-6151
(405)-325-4042, atiq@ou.edu, www.cs.ou.edu/~atiq

Survivability Evaluation of SIGMA and Mobile IP

Shaojian Fu, **Mohammed Atiquzzaman**

Telecommunications and Networks Research Lab

School of Computer Science, University of Oklahoma,

Norman, OK 73019-6151, USA.

Email: {sfu,atiq}@ou.edu

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, one of which is low survivability due to single-point failure of Home Agents. In our previous study, Seamless IP diversity based Generalized Mobility Architecture (SIGMA) was proposed to support low latency, low packet loss IP mobility. In this paper, we show that the location management scheme used in SIGMA can enhance the survivability of the mobile network. We develop an analytical model to evaluate the survivability of SIGMA as compared to that of Mobile IP. Numerical results have shown the improvement in system response time and service blocking probability of SIGMA over Mobile IP in practical environments under the risk of hardware failures and distributed DoS attacks.

I. Introduction

Mobile IP (MIP) [1] is designed to handle mobility of Internet hosts at the network layer. Several drawbacks exist when using MIP in a mobile computing environment, one of which is low survivability due to single-point failure of Home Agents. Mobile IP 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 all 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, there are two major drawbacks to this location management scheme as given below:

- Each user's location and account information can only be 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 [2].
- HAs have to be located in the home network of an MH in order to intercept the packets sent to the MH. The complete home network could be located in a hostile environment, in the case of failure of the home networks, all the MHs belonging to the home network would no longer be accessible.

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 for an alternative approach. A number of transport layer mobility protocols have been proposed, for example, MSOCKS [3] and connection migration solution [4] in the context of TCP, and M-SCTP [5] and mobile SCTP [6] in the context of SCTP [7]. In our previous study in [8], we proposed an 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 MIPv6 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 Managers (LM) can be combined with 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 LMs since they are not responsible for user data forwarding.

In the literature, two recent papers that have addressed the problem of MIP survivability are [9] and [10]. Ref [9] proposed a procedure to let MH register with multiple MAPs to avoid single point failure. Ref [10] used a similar idea as SIGMA, and the authors proposed a way 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. But none of the papers analytically models the survivability of MIP. Through analytical models, the *objective* of this paper is to show that the location management scheme used in SIGMA can enhance the survivability of the mobile network. The *contributions* of the current study can be summarized as:

- Illustrate the reason of SIGMA can achieve better survivability than MIP.
- Develop a analytical model based Markov Reward Process to determine the survivability of location management schemes.
- 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: Sec. II reviews the location management scheme used by SIGMA, Sec. III illustrates the basic reason of SIGMA being able to achieve better survivability than MIP. The analytical model is described in Sec. IV and the numerical results are shown in Sec. V. Finally, the concluding remarks are presented in Sec. VI.

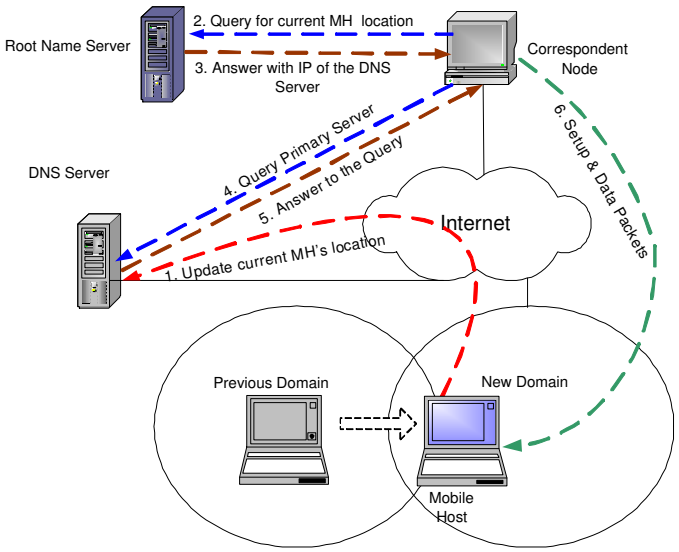

Fig. 1. Location management in SIGMA

II. Location Management of SIGMA

SIGMA needs to setup a location manager for maintaining a database of the correspondence between MH's identity and its current primary 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 does not have impact on the handover performance of SIGMA. This will make the deployment of SIGMA much more flexible than MIP.

The location management can be done in the following sequence as shown in Fig. 1: (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 an SCTP INIT chunk to MH's new primary IP address to setup the association.

If we use the 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 [11]. 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 management entity (HA), SIGMA can reduce system complexity and operating cost significantly by not having such a requirement. Moreover, the survivability of the whole system will also be enhanced as discussed in Sec. III.

III. Survivability comparison of SIGMA and MIP

In this section we discuss the survivability of MIP and SIGMA. We highlight the disadvantages of MIP in terms of survivability, and then discuss how those issues are taken care of in SIGMA.

A. Survivability of MIP

In MIP, the location database of all 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, there are two major drawbacks to this distributed nature of location management as given below:

- If we examine the actual distribution of the mobile users' location information in the system, we can see 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 proposed in [2].
- Even if we replicate HA to another agent, these HAs have to be located in the home network of an MH in order to intercept the packets sent to the MH. The complete home network could be located in a hostile environment, such as a battlefield, where the possibility of all HAs being destroyed is still relatively high. In the case of failure of the home networks, all the MHs belonging to the home network would no longer be accessible.

B. Centralized Location Management of SIGMA offers Higher Survivability

Referring to Fig. 1, SIGMA uses a centralized location management approach. As discussed in Sec. II, 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 Sec. III-A) as given below:

- The LM uses a structure which is similar to a DNS server, or can be directly 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 need to be directed to the LM. Data traffic do not need to be intercepted and forwarded by the LM to the MH. Thus, the LM does not have to be located in a specific network to intercept data packets destined to a particular MH. It is possible to avoid physically locating the LM in a hostile environment; it can be located in a secure environment, making it highly available in the network.

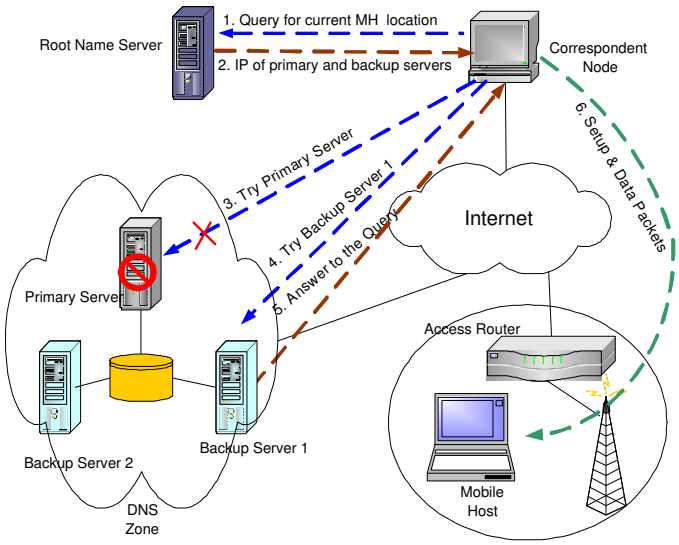

Fig. 2. Survivability of SIGMA's location management.

Fig. 2 illustrates the survivability of SIGMA's location management, implemented using DNS servers as location servers. Currently, there are 13 servers in the Internet [12] which constitute the root of the DNS name space hierarchy. There are also several delegated name servers in the DNS zone [13], one of which is primary and the others are for backup and they share a common location database. If an MH's domain name belongs to this 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 will direct the CN to query the intermediate name servers in the hierarchy. At last, 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 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 requests from a CN is thus transparently routed to the backup server without any need for retransmission of the request from the CN.

Other benefits 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*: Location servers do not intervene with data forwarding task, which helps in adapting to the growth in the number of mobile users gracefully.
- *Manageability*: Centralized location management provides a mechanism for an organization/service provider to control user accesses from a single server.

IV. Analytical Model

The aim of our model is to perform a combined analysis of system availability and performance evaluation. J. Meyer created a new measure called *performability* in [14], [15], which will be used in this paper to measure the survivability of a system. A performability model consists of a availability sub-model, a performance sub-model, and a glue model that combine 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 the system performance (equivalent to reward) under each system state.

A. Networking Architecture

The networking architecture been considered in the analytical model is shown in Fig. 3. The router in Fig. 3 forwards location updates from MHs, location queries from CNs, and DDoS attack traffic to N location managers according to a round-robin policy. Each location manager has an independent queue of size K packets. After being processed by one of location managers, the acknowledgement/reply to the update/query/attack packets are transmitted back to their originators.

B. 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.

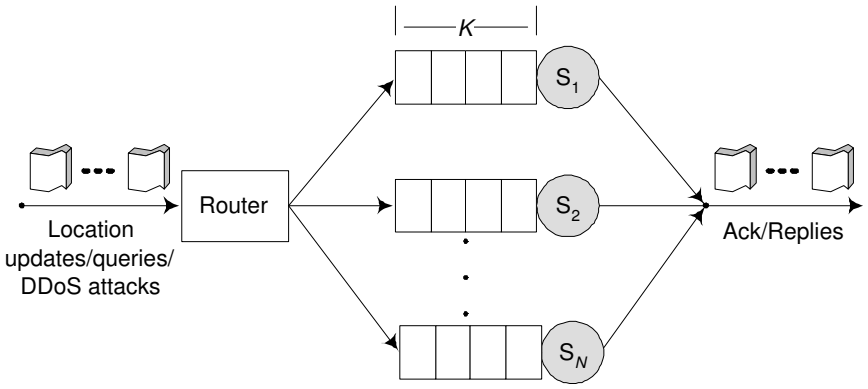

Fig. 3. Queuing model of N location managers

- Hardware failures can be perfectly covered[1], i.e. system can degrade gracefully when one of the working server fails.
- Hardware failures always occurs on the servers with heaviest load.

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

N	total number of location managers.
λ_u, λ_q, λ_a	arrival rate of location updates, queries, and DDoS attack, respectively.
λ	summation of λ_u, λ_q, λ_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)

C. 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 under the impact of 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. 4, 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 examples:

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

- current state is (N,0), the hardware failure of any one server (happens with a rate of $N\gamma$) will make the next state ($N-1$,0).
- current state is (N,1), arrival of one update/query/attack packet will change the state to (N,2). Since router use a round-robin policy, each server has equal share of load. Therefore, the transition rate is λ/N.
- current state is (N,2), departure of one packet will change the state to (N,1). Since each server has equal processing rate of μ, therefore, the transition rate is μ/N.
- current state is (N,2), one hardware failure will make the next state ($N-1$,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 ($N-1$,1), the repair of the failed server will change the state of (N,1).

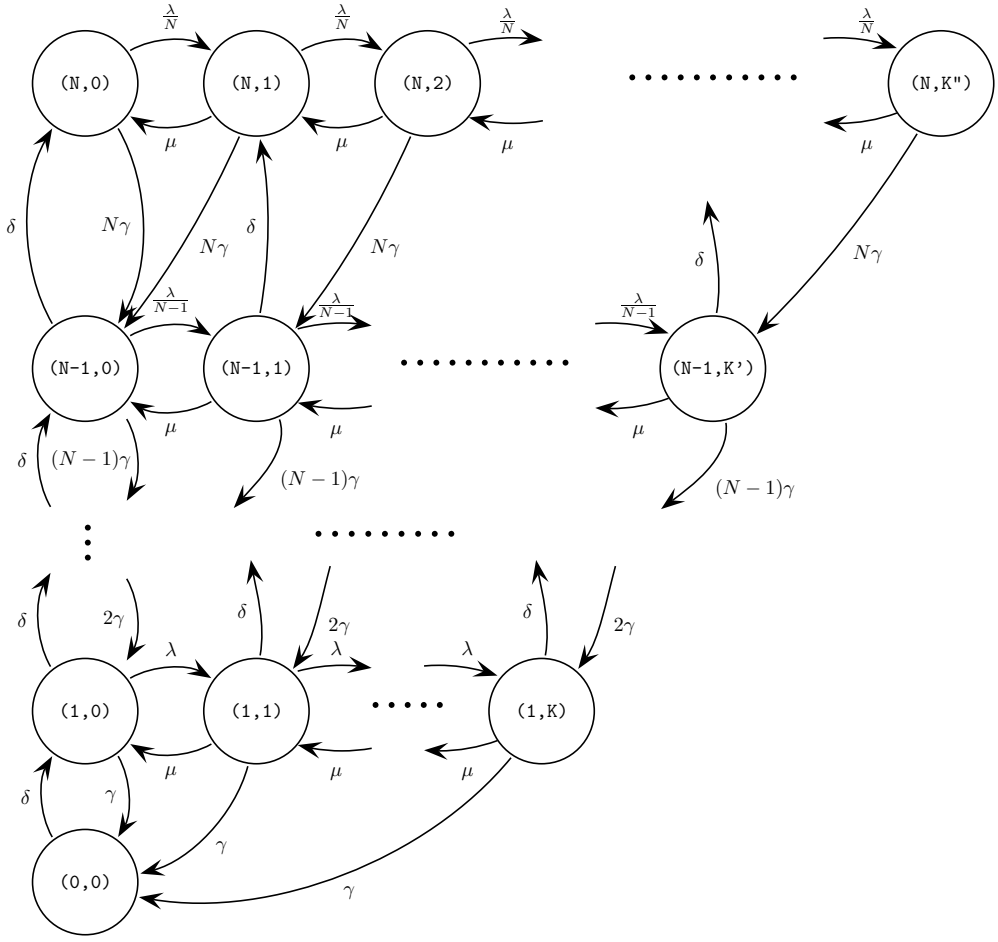

Fig. 4. State digram of N location managers

We can determine each element of infinitesimal generator matrix Q of CTMC shown in Fig. 4 as

follows:

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

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:

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

In the failure case in Eqn. 1, j is determined by:

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

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 a state where (N_w,$N_w K$), the packet is dropped since no service is possible. Therefore, the blocking probability can be calculated by:

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

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

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

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

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

D. 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 Sec. IV-B. In addition to the notations in Sec. IV-B, let λ_d be 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 available for one 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. 5. At any time, there can only be at most one HA serving requests. Any hardware failure will move the state from (1,L) ($L = 1, 2, \cdots, K$) to (0,0). In 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 primary one. Therefore, the value of δ in Fig. 5 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 can use the same technique as used in Sec. IV-C to compute the average system response time and service blocking probability by setting $N = 1$, and δ to the value given in Eqn. 8.

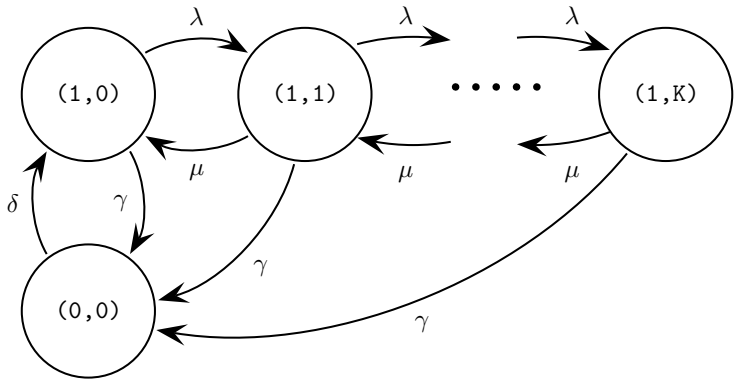

Fig. 5. State digram of MIP HA

V. Numerical Results

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

A. SIGMA survivability

First, we look at the impact of DDoS attack strength (λ_a) on the system response time. We set $N = 3$, $\lambda_u = 0.2$, $\lambda_q = 0.4$, $\mu = 2$, $1/\delta = 24$ hours, and $K = 10$ packets. As shown in Fig. 6, when DDoS attack has a higher strength, the system response time increases dramatically to as high as four times of normal values. Also, when the hardware failure is more frequent (smaller MTTF values), the system response time also increases due to less working server available to process client requests.

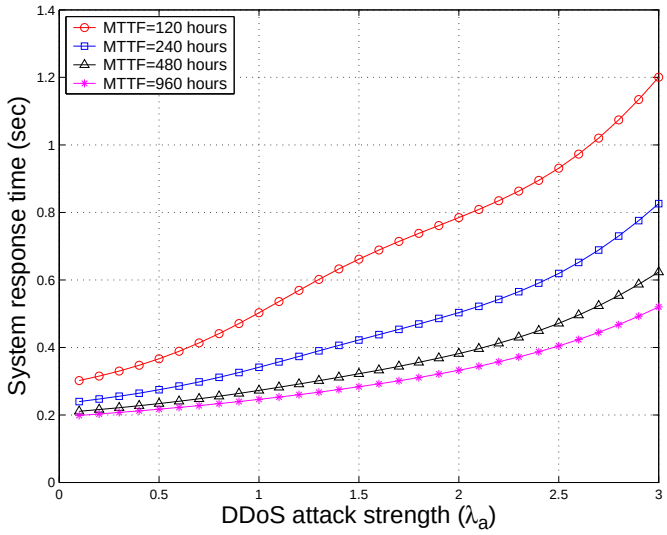

Fig. 6. Impact of DDoS attack strength on system response time

Next, we look at the impact of DDoS attack strength on the system blocking probability. As shown in Fig. 7, when DDoS attack has a higher strength, the system blocking probability increases as well, due to less buffer space available to serve legitimate client requests. As expected, the smaller K is, the larger the impact of DDoS attack on blocking probability. Therefore, increase the value of K can decrease the sensitivity of system blocking probability to DDoS attack.

Fig. 8 shows the impact of MTTR on system response time. We can observe that the longer time repairing requires, the higher the average response time. This is because once a server fails, it needs longer time to repair it. Thus less working server is available to process client requests when MTTR is higher, which results in a higher response time.

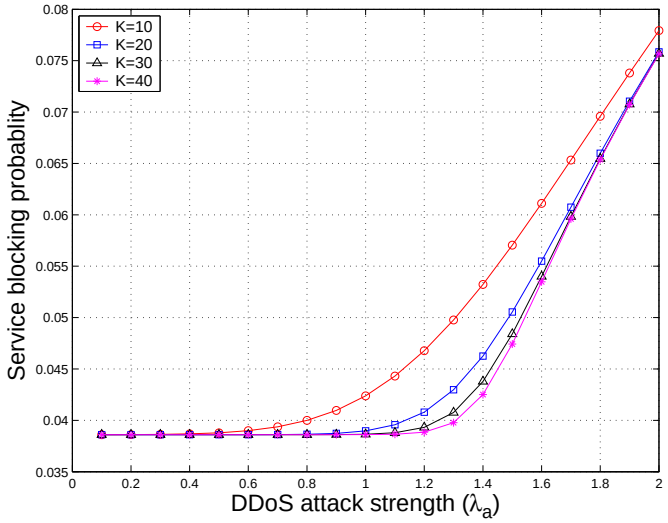

Fig. 7. Impact of DDoS attack strength on blocking probability

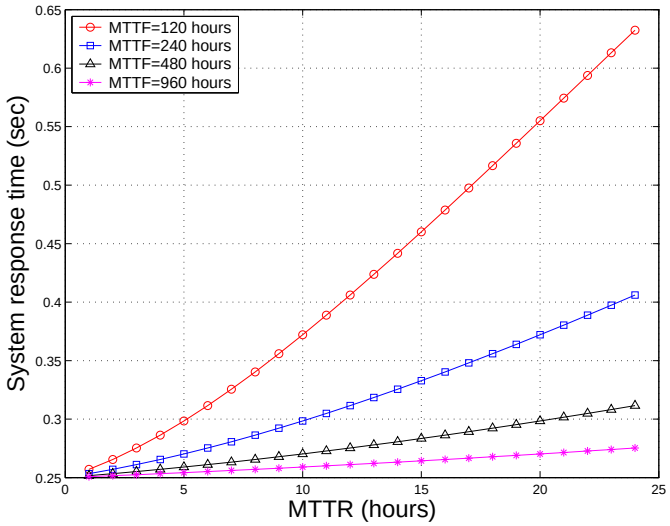

Fig. 8. Impact of MTTR on system response time

Finally, Fig. 9 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.

B. 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 $T_{sw} = 10$ minutes, as shown in Fig. 10. We can observe that the average response time in both modes of MIP is much higher than that of SIGMA, even with $\lambda_d = 0$. The value of MTTF does not have an impact on the response time for MIP. This is because we only consider the response time for non-blocked requests. Higher MTTF will results in

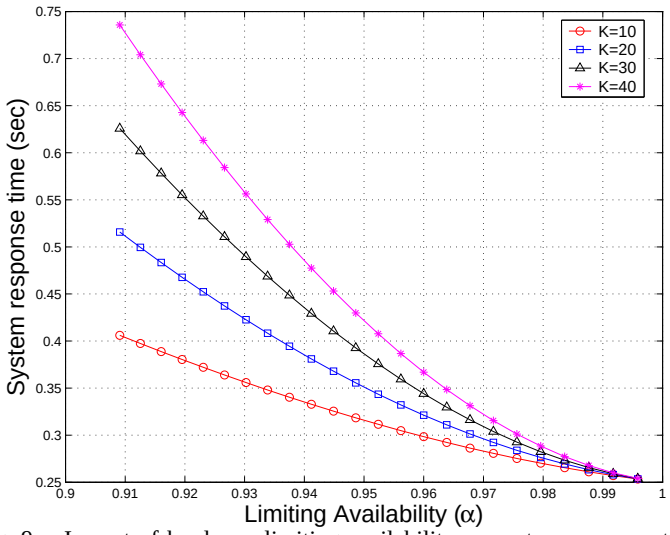

Fig. 9. Impact of hardware limiting availability on system response time

system staying in available state more time, but more queueing delays will be incurred, these two effects are cancelled out, leaving no effect on the overall response time.

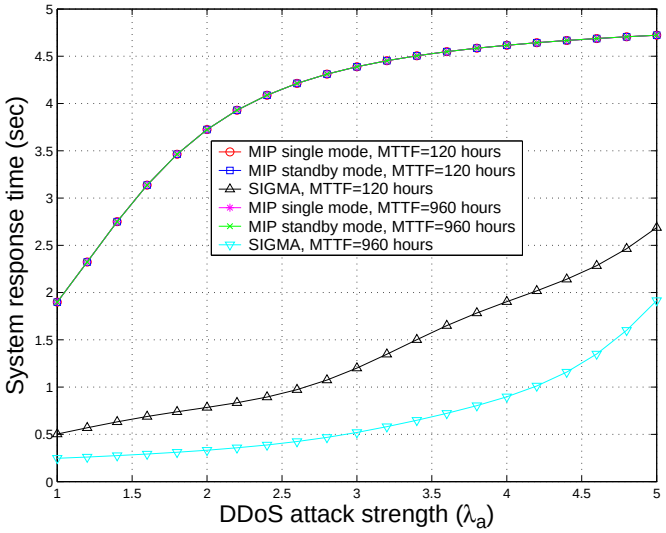

Fig. 10. Impact of DDoS attack strength on system response time zero λ_d

Next, we compare the impact of DDoS attack strength on the service blocking probability of SIGMA against MIP. As shown in Fig. 11, when DDoS attack has a higher 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 obvious impact on service blocking probability. This is because that T_{sw} is 10 minutes, which is so small compared to MTTF. Once HA fails, it can be deemed as to be replaced by a new one immediately.

Fig. 11 compare the impact of data traffic strength on the service blocking probability of SIGMA

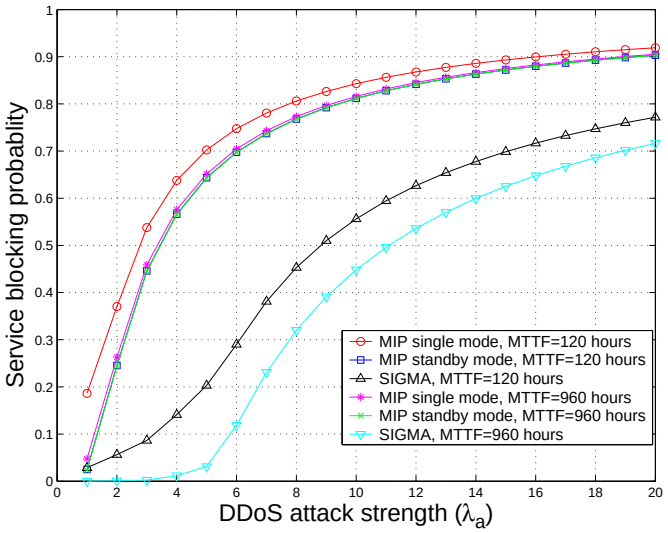

Fig. 11. Impact of DDoS attack strength on blocking probability with zero λ_d

against MIP, with $\lambda_a = 1$. Since SIGMA decouples the location management from data forwarding, the data traffic strength does not have impact on the service blocking probability. For MIP, the data traffic will contend with location management traffic for the buffer slots, which will increase the blocking probability. This observation justifies our initial design of decoupling the location management from data forwarding function in SIGMA.

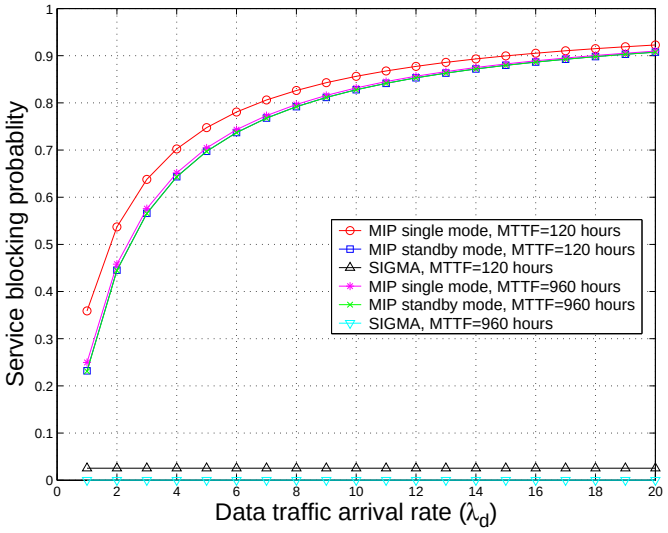

Fig. 12. Impact of data traffic strength on blocking probability

Fig. 13 compare the impact of hardware limiting availability on the response time of SIGMA against MIP. As in the case of MTTF in Fig. 10, 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 means server hardware is more reliable) will results a lower response time for SIGMA.

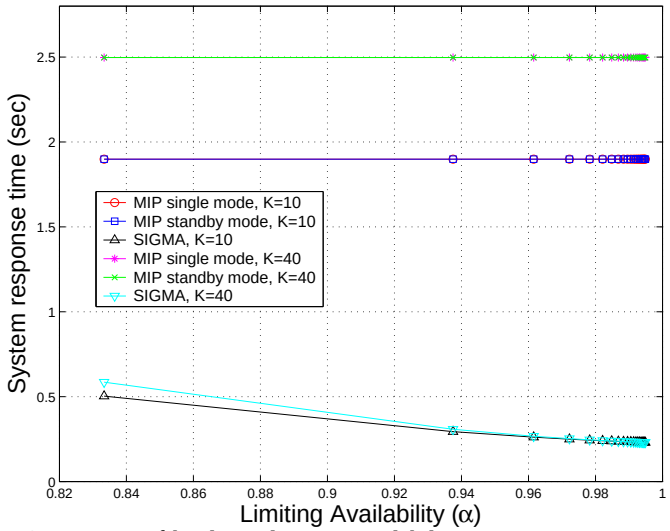

Fig. 13. Impact of hardware limiting availability on system response time

VI. Conclusions

In this paper, we show that the location management scheme used in SIGMA can enhance the survivability of the mobile network. We developed an analytical model based Markov Reward Process to evaluate the survivability of location management schemes. Through the model, the survivability of SIGMA as compared to that of Mobile IP. Numerical results have shown the improvement system response time and service blocking probability of SIGMA over Mobile IP in practical environments under the risk of hardware failures and distributed DoS attacks.

References

[1] C.E. Perkins (editor), "IP Mobility Support," IETF RFC 3344, August 2002.

[2] J.W. Lin and J. Arul, "An efficient fault-tolerant approach for Mobile IP in wireless systems," *IEEE Transactions on Mobile Computing*, vol. 2, no. 3, pp. 207–220, July-Sept 2003.

[3] D. A. Maltz and P. Bhagwat, "MSOCKS: An architecture for transport layer mobility," in *INFOCOM*, San Francisco, USA, March 1998, pp. 1037–1045.

[4] A. C. Snoeren and H. Balakrishnan, "An end-to-end approach to host mobility," in *ACM MobiCom*, Boston, MA, August 2000, pp. 155–166.

[5] W. Xing, H. Karl, and A. Wolisz, "M-SCTP: Design and prototypical implementation of an end-to-end mobility concept," in *5th Intl. Workshop on the Internet Challenge: Technology and Applications*, Berlin, Germany, October 2002.

[6] S. J. Koh, M. J. Lee, M. L. Ma, and M. Tuexen, *Mobile SCTP for Transport Layer Mobility*, draft-sjkoh-sctp-mobility-03.txt, February 2004.

[7] S. Fu and M. Atiquzzaman, "SCTP: State of the art in research, products, and technical challenges," *IEEE Communication Magazine*, vol. 42, no. 4, pp. 64–76, April 2004.

[8] S. Fu, L. Ma, M. Atiquzzaman, and Y. Lee, "Architecture and performance of SIGMA: Seamless IP diversity based Generalized Mobility Architecture," in *Accepted for publication by ICC*, Seoul, Korea, May 2005.

[9] T. You, S. Pack, and Y. Choi, "Robust hierarchical mobile IPv6 (RH-MIPv6): an enhancement for survivability and fault-tolerance in mobile IP systems," in *IEEE 58th Vehicular Technology Conference*, October Fall 2003, pp. 2014–2018.

[10] R. Jan, T. Raleigh, D. Yang, and L.F. Chang et. al., "Enhancing survivability of mobile Internet access using mobile IP with location registers," in *IEEE INFOCOM*, March 1999, pp. 3 – 11.

[11] B. Awerbuch and D. Peleg, "Concurrent online tracking of mobile users," in *ACM SIGCOMM Symposium on Communications, Architectures and Protocols*, September 1991, pp. 221–233.

[12] R.Bush, D. Karrenberg, M. Kosters, and R. Plzak, "Root name server operational requirements," IETF RFC 2870, June 2000.

[13] W. R. Stevens, *TCP/IP Illustrated, Volume 1 (The Protocols)*, Addison Wesley, November 1994.

[14] J. Meyer, "On evaluating the performability of degradable computing systems," *IEEE Transactions on Computers*, vol. 29, no. 8, pp. 720–731, August 1980.

[15] J. Meyer, "Closed-form solutions of performability," *IEEE Transactions on Computers*, vol. 31, no. 7, pp. 648–657, July 1982.