Yao *et al. EURASIP Journal on Wireless Communications and Networking* (2016) 2016:234
DOI 10.1186/s13638-016-0719-9

EURASIP Journal on Wireless Communications and Networking

RESEARCH Open Access

Survivable strategy set design for malicious attack propagation in NEMO scenario

Su Yao[1,2], Jianfeng Guan[3*] and Hongke Zhang[1]

Abstract

Large-scale failures triggered by undesirable events such as natural disasters, massive power malfunction, and malicious attacks are attracting serious concerns in communication network infrastructure perspective. However, there have been few survivability strategy analyses in network mobility (NEMO) scenarios. To properly address this issue, this paper proposes two novel survivability strategies to handle malicious attack propagation in NEMO scenario. We use fraction of active users (FAU) to illustrate the NEMO survivability performance based on continuous-time Markov chain (CTMC) and find the relationship between survivability performance and survivable strategy when facing malicious attack in NEMO scenario. The performance analysis is helpful for us to choose the right survivable strategy in the proper time.

Keywords: Survivability, NEMO, Strategy, Malicious attack, Continuous-time Markov chain

1 Introduction

In the previous years, the Internet has a significant impact on all aspects of modern life. It is essential to continuously provide the required data when facing natural disasters (e.g., typhoon, floods, earthquake) and intentional attacks (Distributed Denial-of-Service (DDoS) attack, power outages, worm virus) [1], especially in mobile scenarios [2]. As a consequence, the network survivability has become a significant element for network design and performance evaluation of network systems. In recent years, the survivability has greatly threatened by the network attack. According to the 2015 DDoS threat report [3], compiled by network security firm NSFOCUS, which has stated trends and methodologies of network attack in the last year, the number of DDoS attack is 179,298 in China. And the total flows of network attack go to 276,531,562 TB. Moreover, the propagation of network attack has increased significantly in mobile network communication.

The network survivability has been a critical research area of network security in the past years [4]. The term refers to the ability of a network to continue to provide services even in the presence of a failure [5]. Most studies regarding network survivability in the past primarily focus on natural disasters and massive power failures [6, 7]. In the papers [8] and [9], a continuous-time Markov chain (CTMC) model is proposed to characterize the network survivability performance in the presence of static disastrous failures and repairs, which is considered as a static disastrous event that destroys network. Authors of [10] analyzed several interesting characteristic of traffic flows in a fixed network. However, there has been little work on network survivability evaluation of network mobility.

The situations are quite different in mobile networks. Mobile networks consisted with mobile Internet devices such as smartphones, notebooks, and sensors are widely deployed in moving vehicles (buses, trains, airplanes, etc.). In order to manage continuous connectivity of an entire network as it changes its point of attachment to the Internet, network mobility basic support protocol (NEMO BSP) [11] is proposed by the Internet Engineering Task Force (IETF) to standardize the relevant procedure in this area.

In the NEMO basic protocol, there are four kinds of communication entities, namely mobile routers (MR), mobile network nodes (MNN), access routers (AR), and home agent (HA), respectively. The MR plays the role as gateways for all the MNN in the network. Besides, these MRs will be the gateway to connect MNN with the core network through AR and forwards the data traffic for

* Correspondence: jfguan@bupt.edu.cn
[3]Beijing University of Posts and Telecommunications, Beijing 100876, China
Full list of author information is available at the end of the article

the entire mobile network. More specifically, the MR and HA exchange the mobility management signaling messages once the mobile network changes its points of attachment. Due to signaling management and packets delivery, the mobile router may become the performance bottleneck and single point failure by the malicious attack.

The malicious attack propagation in a mobile network is quite different. When a malicious attack happens, the mobile network can go to the immunized state after repairing. To fill this important gap, we establish different math models of survivability in this paper and propose two different survivable strategies: delayed repair strategy and immediate repair strategy. And according to the simulation results, the right choice of survivable strategy sets has been given.

The main work and contributions of this article can be stated as follows:

1. The mathematical model of NEMO survivability for malicious attack propagation has been proposed.
2. Two different survivable strategies have been proposed to improve the outage performance of survivability in an effective way when malicious attack propagation is initiated.
3. The relationship between survivability performance and survivable strategy has been proposed which is helpful for making the right choice.

The rest of this paper is organized as follows: Section 2 describes the system model for malicious attack propagation. Section 3 describes the proposed strategies. Simulation results are obtained and analyzed in Section 4. Finally, conclusions are summarized in Section 5.

2 System model

In this paper, our objective is to quantify the survivability performance of malicious attack propagation in network mobility scenario; thus, the definition of survivability framework presented by ANSI T1A1.2 committee has been adopted [12]. As shown in Fig. 1, the survivability performance is illustrated in the y-axis while the x-axis indicates the time. In addition, we give several attributes to illustrate the behavior of survivability. The measure of interest M is supposed as the performance metrics of the loss probability in our paper. Before an attack occurs, the measure of interest M has the value m_0; m_a is the value of M just after the attack arrives; m_u is the maximum difference between the value of M and m_a after the attack arrives; m_r is the recovery value of M after the time t_r; and t_R is the relaxation time for the network to recover the value of $m_{0.}$

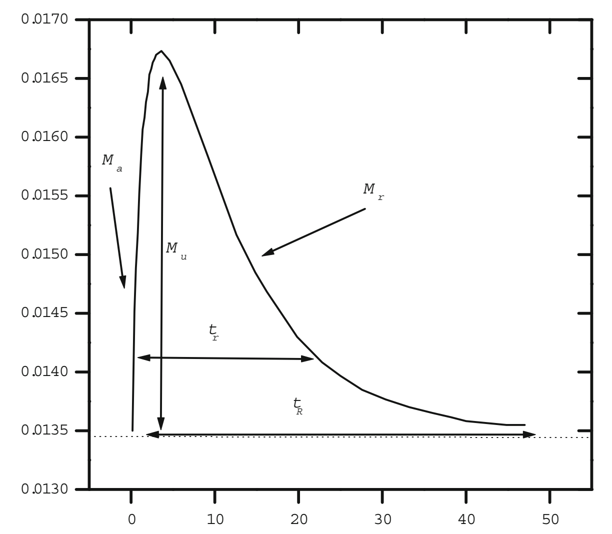

Fig. 1 Illustration of survivability (adapted from [7])

In our paper, it is assumed that a certain network infrastructure consists of several core network and access network. Take the access network as an example, its topology can be easily derived according to network architecture. In our analysis, the node in the topology is represented as a mobile subnet. At time t, there are three different states. When the subnet has been attacked, it is infected, which is called as *infected state* (*IN* for short). We classify the healthy state into two different kinds: one is susceptible state (*SP* for short) which is the initial state of a subnet and the other is the immunized state (*IM* for short) which means it cannot be attacked using the same approach.

Let a random variable $Y_j(t)$ denote a state of node j at the discrete time t. Then, we have

$$Y_j(t) = \begin{cases} \text{IN, Infected} \\ \text{HY, Healthy}\begin{cases} \text{SP, Susceptible,} \\ \text{IM, Immunizied.} \end{cases} \end{cases} \qquad (1)$$

Figure 2 illustrates the state transition diagram of node j. When node j starts at *SP* state, it can either transmit to *IM* state with the attack repair rate (*ARR*) $\mu(t)$ or *IN* state with the attack arrive rate (*AAR*) $\lambda(t)$. Thus, if the state of the node is *IN*, it can just transfer to *IM* state with the *ARR* $\mu(t)$. Once the node is repaired, it will stay at *IM* state. Furthermore, no matter which kind of state the node stay at, it may transfer to *IM* state finally.

We use a directed graph to model the malicious propagation procedure. This directed graph includes nodes, which represent mobile subnets (MoSN for short), and directed edges, which represent the possible propagation directions among different MoSNs. Using a mathematical model, we evaluate the network

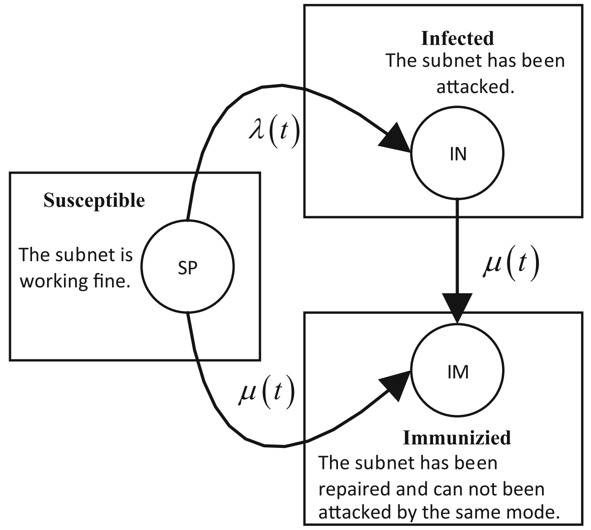
Infected
The subnet has been attacked.
IN
$\lambda(t)$
$\mu(t)$
Susceptible
The subnet is working fine.
SP
IM
$\mu(t)$
Immunizied
The subnet has been repaired and can not been attacked by the same mode.

Fig. 2 State transition diagram of one node

survivability performance of MoSN from attack arriving, attack propagation, and through to the process of repairment finished.

It is assumed that the process of attack propagation can be described as a continuous-time stochastic process. The state of the network system can be totally illustrated by the collection of the state of each MoSN. At any time t, the state $Y(t)$ can be denoted by a n-dimensional vector as follows:

$$Y(t) = (Y_1(t), Y_2(t), \ldots Y_m(t), \ldots Y_n(t)), t{\geq}0, 1{\leq}m{\leq}n, \tag{2}$$

where for each MoSN $1 \leq m \leq n$, $Y_m(t)$ describes the level of mth MoSN state at time t. There are three different states that the mth MoSN could remain at. $Y_m(t) = 1$ represents that the state of mth MoSN is in the *SP* state at time t and the attack has not arrived at time t; $Y_m(t) = 0$ indicates that the mth MoSN is in the *IN* state at time t and the attack has arrived. $Y_m(t) = 1'$ means that the mth MoSN has been restored to the *IM* state at time t. Furthermore, the last state is an absorbing state of all three ones. Based on the above assumption, Y_m(t) can be described as follows:

$$Y_m(t) = \begin{cases} 1, \text{ if the node is in the SP state} \\ 0, \text{ if the node is in the IN state} \\ 1', \text{ if the node is in the IM state} \end{cases}. \tag{3}$$

Generally, the attack is assumed initially to occur on the first MoSN. In addition, the attack and repair transition is only determined by the current state of MoSN and has nothing to do with the path to the current state. It is assumed that the time of attack is exponentially distributed. Since *AAR* and *ARR* are temporarily independent, it can be modeled using Poisson distribution.

According to the above assumptions, the transition process of all the MoSN can be completely modeled as a temporally CTMC on the state space S. The state space S is composed of a total of $N = 3^n$ states as below:

$$S = \{(Y_1, Y_2, \ldots, Y_n), Y_1, Y_2, \ldots, Y_n {\in} (0, 1, 1')\}. \tag{4}$$

For each time $t \geq 0$, the probability $F_k(t)$ that the MoSN is in state k of transient process S can be defined as follows:

$$F_k(t) = P_r\{Y(t) = k\}, k{\in}S. \tag{5}$$

Let

$$f(t) = [f_1(t), f_2(t), \ldots, f_N(t)] \tag{6}$$

denote a row vector of transient state probability of $Y(t)$. When the network system is in state $k \in S$, a reward rate $\gamma(k)$ can be assigned, where γ is defined as a reward function. The vector of reward rates associated with the state can be denoted as follows:

$$\Upsilon = [\Upsilon_1, \Upsilon_2, \ldots, \Upsilon_N]. \tag{7}$$

Suppose the probability of propagation from state i to state j is denoted by p_{ij}, the transition rate matrix of the process S could be expressed in matrix form as

$$P = \begin{pmatrix} p_{11} & \cdots & p_{1k} & \cdots & p_{1N} \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ p_{k1} & \cdots & p_{kk} & \cdots & p_{kN} \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ p_{N1} & \cdots & p_{Nk} & \cdots & p_{NN} \end{pmatrix}. \tag{8}$$

Table 1 summarizes the general rules for constructing the infinitesimal generator matrix of mode for a network with a general number of MoSN.

For the sake of calculating $f(t)$, the Kolmogorov differential equation written in the matrix form should meet as follows:

$$\frac{df(t)}{dt} = f(t)P. \tag{9}$$

After that, we can get the probability vector of the state

Table 1 The rules for constructing the generation matrix

Transition state	Condition	P_{ij}	State *i* to state *j*
Attack phase	$i[0] = 1; j[0] = 0$	λ_1	$(1,1, \ldots,1) \rightarrow (0,1, \ldots,1)$
	$\{1'\} \notin i$	λ_2	$(0,1, \ldots,1) \rightarrow (0,0, \ldots,1)$
	$\{1'\} \notin j$	…	……
	$L(i) = L(j) + 1$	λ_n	$(0,0, \ldots,1) \rightarrow (0,0, \ldots,0)$
Repair phase	$i[0] = 0; j[0] = 1'$	μ_1	$(0,0, \ldots,0) \rightarrow (1',0, \ldots,0)$
	$\{1\} \notin i$	μ_2	$(1',0, \ldots,0) \rightarrow (1',1', \ldots,0)$
	$\{1\} \notin j$	…	……
	$L'(j) = L(i) + 1$	μ_n	$(1',1', \ldots,0) \rightarrow (1',1', \ldots,1')$

L is the function to calculate the number of "1" in the state; *L'* is the function to calculate the number of "1'" in the state; state (1',…,1') ≠ state (1,…,1)

$$f(t) = f(0)e^{Pt}. \tag{10}$$

In this paper, it is assumed that the survivability performance is regarded as equal to the network connectivity, which is the fraction of active MoSN in the network system. Thus, the expected instantaneous reward rate $E[H(t)]$ gives the average connectivity of the system at time t as follows:

$$E[H(t)] = \sum_{j \in S} \gamma_j f_j(t). \tag{11}$$

However, different to fixed network, the most significant aspect of the mobile network is that it should consider the mobility factor. Therefore, we define the dwell time of subnet k as t_k to represent the mobility. Due to its memoryless property, the dwell time of subnet $k + 1$ has no relationship with the dwell time of subnet k.

We assume t_k follows exponentially distributed with mean value $1/\alpha$

$$f(t) \begin{cases} \alpha e^{-\alpha t} (t > 0) \\ 0 (t \leq 0) \end{cases}. \tag{12}$$

The parameter α represents the moving speed of the subnet. When $\alpha = 0$, it represents the fixed subnet. With the increase of α, the mobility becomes higher and more dynamic.

In our paper, we analyze two different strategies to repair the infected subnet. One is *delayed repair strategy* (DRS) and the other is *immediate repair strategy* (IRS). In DRS, the repairing action will start only after that all the subnets has been infected. While in IRS, the repairing action will start immediately as soon as the subnet has been infected. The following will be described in details.

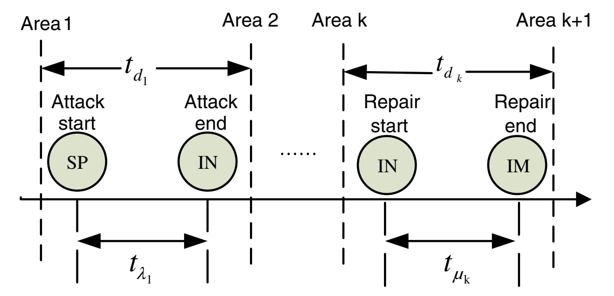

Fig. 3 The timing diagram for DRS

As shown in Fig. 3, in DRS, the subnet starts to enter area 1 and stays for the dwell time t_{d1}, then leaves for the area 2. Assuming that the attack will occur during this time period, the time interval between the attack start time and the attack end time is $t_{\lambda 1}$. Only if $t_{\lambda 1}$ is less than t_{d1} could the subnet be attacked. Otherwise, the subnet will leave area 1 and it therefore cannot be attacked.

So the probability of mobile subnet attack can be defined as

$$p_{10} = p(t_d > t_\lambda) = \int_{t_\lambda}^{+\infty} \alpha e^{-\alpha t} dt = e^{-\alpha t_\lambda}. \tag{13}$$

After all the subnets have been attacked, they can be repaired during the dwell time t_{d_k}. Assume that the time interval between the repair start time and the repair end time is t_{μ_k}. Only if t_{μ_k} is less than t_{d_k} could the subnet be repaired in area k. Otherwise, it cannot be repaired successfully in area k. So the probability of mobile subnets repair can be defined as

$$p_{10'} = p(t_d > t_\mu) = \int_{t_\mu}^{+\infty} \alpha e^{-\alpha t} dt = e^{-\alpha t_\mu}. \tag{14}$$

The timing diagram for IRS is depicted by Fig. 4. The IRS model is quite different from the DRS model. Once the subnet attack happens, it will start to repair this subnet. Only if the sum of t_λ and t_μ is less than t_d will the subnet be repaired successfully in the area. Otherwise, it cannot be repaired successfully in the area. As a result,

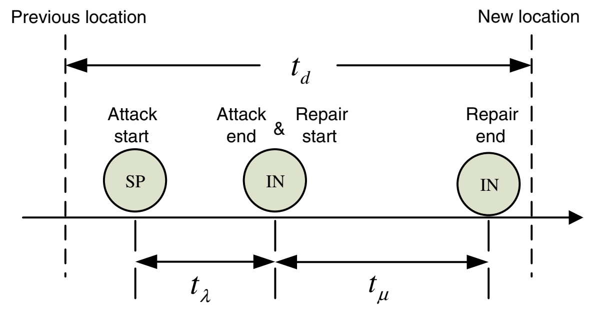

Fig. 4 The timing diagram for IRS

the probability of mobile subnet attack is the same as the DRS model. However, the probability of mobile subnet repair is different, and it can be defined as follows:

$$p_{10'} = p\left(t_d > t_{\lambda+\mu}\right) = \int_{t_{\lambda+\mu}}^{+\infty} \alpha e^{-\alpha t} dt = e^{-\alpha t_{\lambda+\mu}}. \qquad (15)$$

3 Attack scenario evaluation

As shown in Fig. 5, there is an infrastructure of network system deployed in a certain geographical area, which can be divided into two parts: the core network and the access network. The access network is composed by a set of MoSN, and it can forward the packets to the core network using multiple access routers (AR).

There can be three different types of nodes in MoSN: one is local fixed nodes (LFNs), and the other two are local mobile nodes (LMNs) and visiting mobile nodes (VMNs). With respect to MN, LFN does not move to other networks, while LMN can move to other networks and usually reside in MoSN. VMN is from another network and attaches to MN. VMNs and LMNs are referred as mobile nodes, and they are MIPv6 capable. The MR attaches MoSN to the core network through AR.

For simplicity, the network system which consists of $n = 2$ MoSN is considered in this paper. It is assumed that the propagation of attack occurred from the first MoSN to the second MoSN in successive steps.

According to the above assumption, the transient state can be described as double as (*Y1*, *Y2*), where $Y_j \in \{0, 1, 1\,'\}, j = 1, 2$. Then, the set of the state space *S* can be denoted as follows: S_0 = (11), S_1 = (01), S_2 = (10), S_3 = (1 ′ 1), S_4 = (00), S_5 = (11 ′), S_6 = (1 ′ 0), S_7 = (01 ′), S_8 = (1 ′ 1 ′).

In our survivability model, the rate of the initial event is out of consideration. Suppose the *AAR* of *i*th MoSN is λ'_i, the *ARR* is μ_i' and the initial state of the network system is (11).

When the attack arrives at the first MoSN, all the terminals in MoSN will disconnect from the core network. With the *AAR* λ'_1, the initial state can be transferred to state (01). It is the same for the second MoSN. With the *AAR* λ'_2, the initial state can be transferred to state (10). To demonstrate our proposed model, two strategies are considered:

3.1 Delayed repair strategy

In this strategy, only if all of the subnets have been infected, it will go into repair mode. When the state of subnet is staying at (01) or (10), the state can be transferred to state (00) and the impact of the network attack propagation from the first MoSN to the second MoSN should be taken into account.

As depicted in Fig. 6, if the state of the subnet stays at (01), the network attack arrives at the second MoSN,

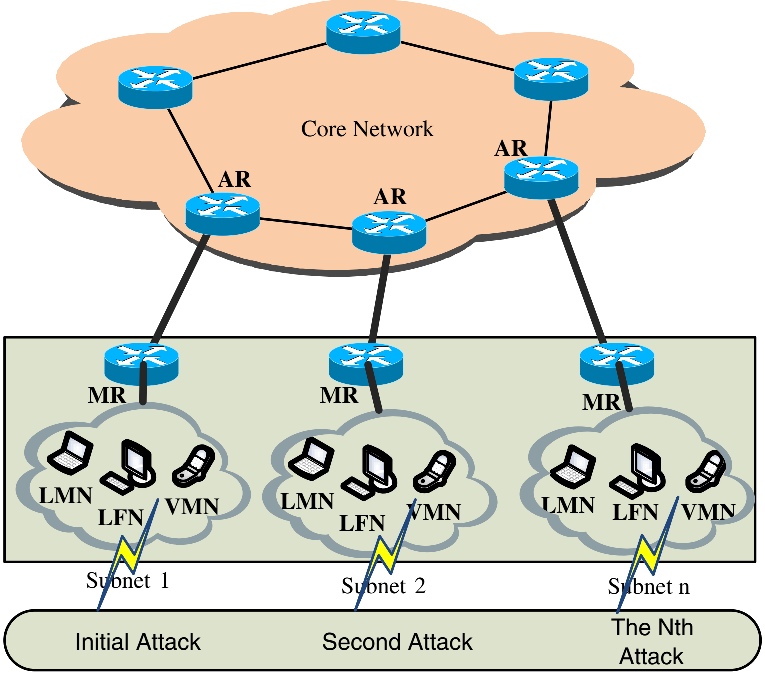

Fig. 5 Attack scenario in the NEMO scenario

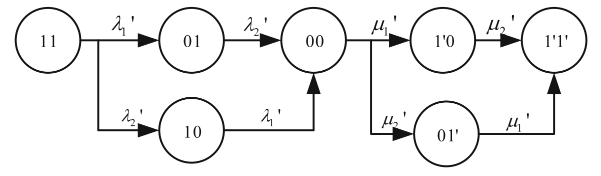

Fig. 6 State-transition rate diagram of DRS

and then all of the users in the second MoSN will disconnect to the core network. The state will go to state (00) with the *AAR* λ'_2. If the state of the subnet stays at (10), the network attack arrives at the first MoSN, and then all of the users in the first MoSN will disconnect to the core network. The state will transfer to state (00) with *AAR* λ'_1.

When all the subnets have been transferred to the state (00), the system could start its repair model. There are two kinds of possible states the system can choose. With the *ARR* $\mu_{1'}$, it may transit to state (1′0) which represents that the first MoSN is repaired. However, if the second MoSN is repaired, it may transit to state (01′) with the *ARR* $\mu_{2'}$. Finally, once all of the subnets in the network system have been repaired, they will transfer to the immunized state (1′1′).

When the subnet is in the NEMO scenario, the probability of mobile subnet attack or repair should be taken into the consideration.

In the DRS model, once the mobile subnet has been attacked successfully, the damage rate should multiply by the probability of mobile subnet attack; if the MN has been repaired successfully, the repair rate should multiply by the probability of mobile subnet repair as follows:

$$\begin{aligned}
&{\lambda_1}' = \lambda_1 p_{10} = \lambda_1 e^{-\alpha t_{\lambda_1}}\\
&{\lambda_2}' = \lambda_2 p_{10} = \lambda_2 e^{-\alpha t_{\lambda_2}}\\
&{\mu_1}' = \mu_1 p_{01'} = \mu_1 e^{-\alpha t_{\mu_1}}\\
&{\mu_2}' = \mu_2 p_{01'} = \mu_2 e^{-\alpha t_{\mu_2}}.
\end{aligned} \tag{16}$$

Based on Eqs. 8 and 16, the matrix *P* is defined as the infinitesimal generator matrix of the CTMC. Thus, we can describe the dynamic behavior using the Kolmogorov differential-difference equation in matrix form as follows:

$$P = \begin{pmatrix}
-{\lambda_1}'-{\lambda_2}' & {\lambda_1}' & {\lambda_2}' & 0 & 0 & 0 & 0 & 0 & 0\\
0 & -{\lambda_2}' & 0 & 0 & {\lambda_2}' & 0 & 0 & 0 & 0\\
0 & 0 & -{\lambda_1}' & 0 & {\lambda_1}' & 0 & 0 & 0 & 0\\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\
0 & 0 & 0 & 0 & -{\mu_1}'-{\mu_2}' & 0 & {\mu_1}' & {\mu_2}' & 0\\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\
0 & 0 & 0 & 0 & 0 & 0 & -{\mu_2}' & 0 & {\mu_2}'\\
0 & 0 & 0 & 0 & 0 & 0 & 0 & -{\mu_1}' & {\mu_1}'\\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0
\end{pmatrix}.$$

Based on the convolution approach, we can obtain the transient probability $f_j(t), j = 0, \ldots, 8$ in a closed-form as follows:

$$\frac{df_1(t)}{dt} = -({\lambda_1}' + {\lambda_2}')f_1(t) \tag{17}$$

$$\frac{df_2(t)}{dt} = {\lambda_1}'f_1(t) - {\lambda_2}'f_2(t) \tag{18}$$

$$\frac{df_3(t)}{dt} = {\lambda_2}'f_1(t) - {\lambda_1}'f_3(t) \tag{19}$$

$$\frac{df_5(t)}{dt} = {\lambda_2}'f_2(t) + {\lambda_1}'f_3(t) - ({\mu_1}' + {\mu_2}')f_5(t) \tag{20}$$

$$\frac{df_7(t)}{dt} = {\mu_1}'f_5(t) - {\mu_2}'f_7(t) \tag{21}$$

$$\frac{df_8(t)}{dt} = {\mu_2}'f_5(t) - {\mu_1}'f_8(t) \tag{22}$$

$$\frac{df_0(t)}{dt} = {\mu_2}'f_7(t) + {\mu_1}'f_8(t) \tag{23}$$

3.2 Immediate repair strategy

In this strategy, once one of the subnets has been infected, it will switch to repair model. As shown in Fig. 7, once one of the subnets has been transferred into the state 0, it will start to repair the subnet, until the subnet changed into the immunized state. Suppose the first attack arrives at the first MoSN, and the state of subnets goes into (01). In this case, the network system starts to repair the model immediately. As the result, it can be transited into the state (1′1) with the *ARR* ${\mu_1}'$. Then, the attack arrives at the second MoSN, the state will transfer from (1′1) to (1′0) with the *AAR* ${\lambda_2}'$. It is the same to the other case. When the first attack arrives at the second MoSN, and the state of the subnets goes into (10), the state of the subnets will soon transit into (1′0). No matter which kinds of states the system stays at, it will jump into the absorbing state finally.

Similar to the DRS model, the probability of mobile subnet attack or repair should be considered. As a result, the new damage rate and repair rate are as follows:

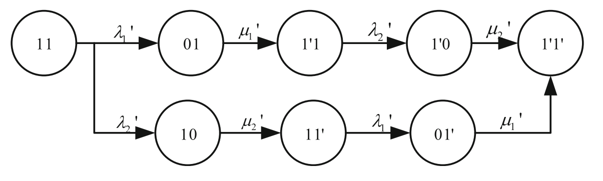

Fig. 7 State-transition rate diagram of IRS

$$\begin{aligned}
\lambda_1{}' &= \lambda_1 p_{10} = \lambda_1 e^{-\alpha t_{\lambda_1}}\\
\lambda_2{}' &= \lambda_2 p_{10} = \lambda_2 e^{-\alpha t_{\lambda_2}}\\
\mu_1{}' &= \mu_1 p_{01'} = \mu_1 e^{-\alpha t_{\lambda 1+\mu 1}}\\
\mu_2{}' &= \mu_2 p_{01'} = \mu_2 e^{-\alpha t_{\lambda 2+\mu 2}}.
\end{aligned} \tag{24}$$

Thus, it takes the form of the transition matrix as follows:

$$P = \begin{pmatrix}
-\lambda_1{}'-\lambda_2{}' & \lambda_1{}' & \lambda_2{}' & 0 & 0 & 0 & 0 & 0 & 0\\
0 & -\mu_1{}' & 0 & \mu_1{}' & 0 & 0 & 0 & 0 & 0\\
0 & 0 & -\mu_2{}' & 0 & 0 & \mu_2{}' & 0 & 0 & 0\\
0 & 0 & 0 & -\lambda_2{}' & 0 & 0 & \lambda_2{}' & 0 & 0\\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\
0 & 0 & 0 & 0 & 0 & -\lambda_1{}' & 0 & \lambda_1{}' & 0\\
0 & 0 & 0 & 0 & 0 & 0 & -\mu_2{}' & 0 & \mu_2{}'\\
0 & 0 & 0 & 0 & 0 & 0 & 0 & -\mu_1{}' & \mu_1{}'\\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0
\end{pmatrix}$$

Similarly, based on the convolution integration approach, we can obtain the transient probability in a closed-form as follows:

$$\frac{df_1(t)}{dt} = -(\lambda_1{}' + \lambda_2{}')f_1(t) \tag{25}$$

$$\frac{df_2(t)}{dt} = \lambda_1{}'f_1(t) - \mu_1{}'f_2(t) \tag{26}$$

$$\frac{df_3(t)}{dt} = \lambda_2{}'f_1(t) - \mu_2{}'f_3(t) \tag{27}$$

$$\frac{df_4(t)}{dt} = \mu_1{}'f_2(t) - \lambda_2{}'f_4(t) \tag{28}$$

$$\frac{df_6(t)}{dt} = \mu_2{}'f_3(t) - \lambda_1{}'f_6(t) \tag{29}$$

$$\frac{df_7(t)}{dt} = \lambda_2{}'f_4(t) - \mu_2{}'f_7(t) \tag{30}$$

$$\frac{df_8(t)}{dt} = \lambda_1{}'f_6(t) - \mu_1{}'f_8(t) \tag{31}$$

$$\frac{df_0(t)}{dt} = \mu_2{}'f_7(t) + \mu_1{}'f_8(t) \tag{32}$$

4 Performance analysis

In this section, we analyze the numerical results of two strategies. For the sake of illustrating the applicability of the above method, the worm propagation is adopted to evaluate the network system survivability performance.

First, we apply and compare DRS and IRS for the four different values of attack propagation rates schemes in each strategy. The first is called the fast propagation fast repair scheme (FF for short), which means its *AAR* is high and its *ARR* is low. Similarly, the other three are fast propagation slow repair scheme called FS, slow propagation fast repair scheme called SF, and slow propagation slow repair scheme called SS. Then, we compare different strategies of one scheme and discuss the proper survivable strategy for malicious attack propagation in NEMO scenario.

We use reward rate $E[H(t)]$ in Eq. 11 to measure the system survivability performance, which is described by the impact of active users at time *t*. In the system, we define the normal value as all the MoSNs in the system have been repaired, and the fraction of active of users is 1. Two subnets are considered in the analysis. They consist of 150 hosts and 200 hosts, respectively, since the maximum host supported by a subnet is usually 255.

For parameter setting of the *AAR* and *ARR*, we refer to the data from [13]. It is believable that the value of *AAR* is more than 2 orders of magnitude than the value of *ARR*, and the unit of repair time is in hours. Based on the different rates of attack propagation and repair, we study four different propagation schemes to study the impact on survivability performance. For simplicity, the high rates of *AAR or ARR* are three times of low rates. In doing so, our model parameters can represent the behavior of typical real network system.

As displayed in Table 2, we define four different schemes based on setting different propagation rates and repair rates.

One result is summarized in Fig. 8, where the chosen repair strategy is DRS. From Fig. 8a, b, we can easily get that if the repair speed is the same, it will have the same fraction of active users (FAU) in the final. Different malicious attack propagation rates will have the same impact on the active users in the beginning. Comparing Fig. 8a with Fig. 8d, it is easily known when MoSNs have the same attack propagation rates, the performance of the system survivability is better if it has the higher repair speed. Different repair speed will have the impact on the time of system back to the normal value. Comparing Fig. 8b with Fig. 8c when repair speed is higher, it could have the higher FAU at the same time.

As shown in Fig. 8, when malicious propagation rate is faster, it will have the lower FAU at start. When the moving speed of MoSN is getting higher, FAU decreases. The reason is that mobility increases the difficulty of repairing MoSN. Even worse, in Fig. 8c, d, when the moving speed increases to the certain value, FAU will

Table 2 Parameters setting

Parameter	λ_1 (h^{-1})	λ_2 (h^{-1})	μ_1 (h^{-1})	μ_2 (h^{-1})
Scenario				
FF	10	20	0.12	0.24
FS	10	20	0.04	0.08
SF	1	2	0.12	0.24
SS	1	2	0.04	0.08

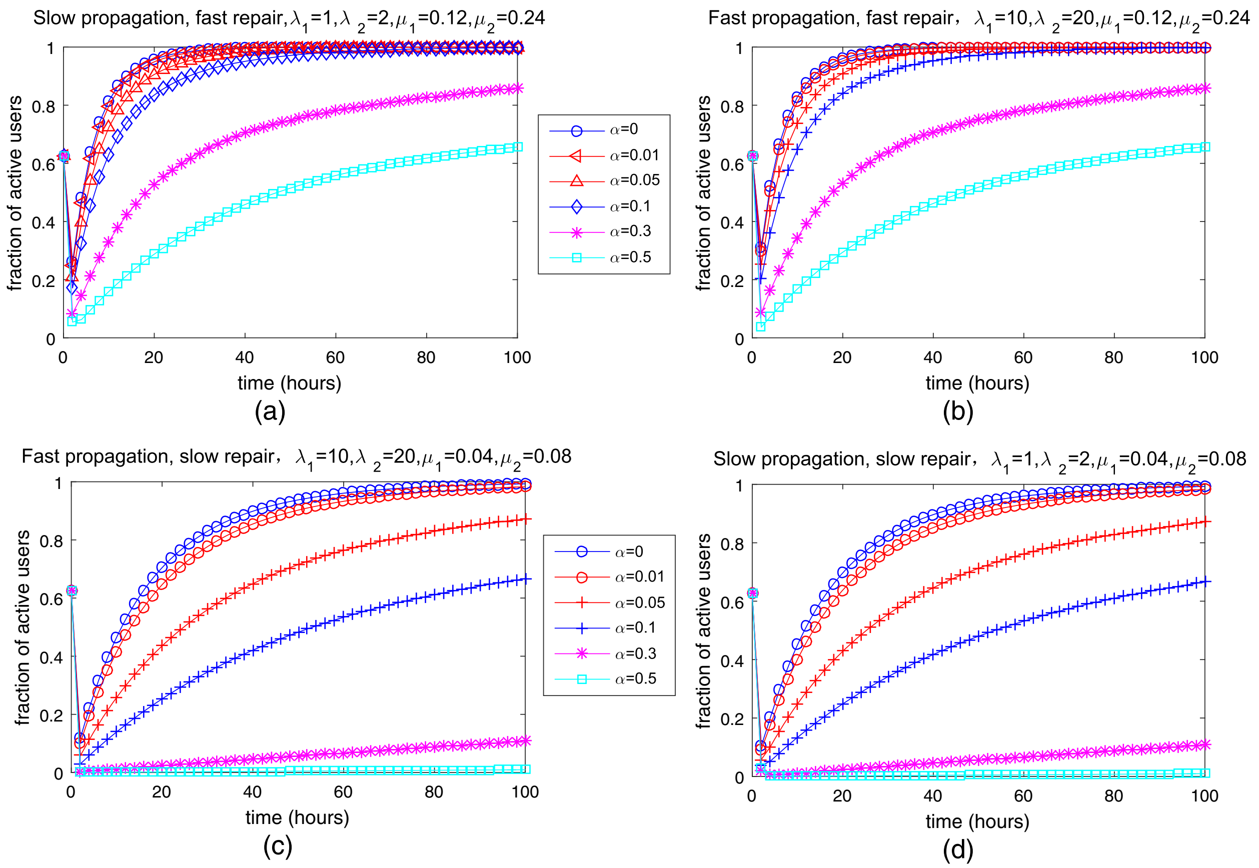

Fig. 8 Survivability impact of different schemes (**a**–**d**) in DRS

stay at very low value. It is possible, if the moving speed is extremely high, the MoSN in the system could not be repaired to the IM state. The reason is that the time of repairing to the IM state is beyond the limit of MoSN dwell time.

Figure 9 shows the result of IRS. In the DRS strategy, FAU keeps the certain value in the beginning. It is not affected by the increasing of the attack propagation rates. As time passed by, all the MoSNs will be repaired to the *IM* state and the system will be back to the normal value. Similar to the DRS strategy, the system could not be recovered to the normal value. Different from DRS strategy, FAU increases in the beginning but soon afterwards has the trend of declining. It means that the mobility of MoSN is helpful to improve the performance of the system survivability at the initial stage. The reason goes to that damage time of MoSN exceeds the range of MoSN dwell time. Therefore, the attack to MoSN has not become effective in the beginning. However, as time goes on, the mobility has prolonged the time of the system back to the normal value.

To better understand of the difference between DRS and IRS, we choose the same scheme of two strategies. As depicted in Fig. 10, the system survivability of different moving speeds in the SF scheme is given. It is easy to get that as the moving speed increase, it has the same effect on the fraction of users in the two strategies. As the moving speed is getting bigger, MoSN is getting more difficult to transfer to the IM state. As a result, the system has less active users at the same time. There is another important thing can be drawn from Fig. 9. Compared to DRS, IRS has better survivability performance in the beginning, but it has to spend much more time repairing to the normal value. The reason for this is that MoSN starts to repair as soon as it has been attacked in IRS. However, according to the model stated before, the time of MoSN being repaired to IM state in IRS is more than that in DRS. As a result, it is more difficult for the system in IRS to repair to the normal value.

Finally, we can summarize two useful results from the above. In IRS, the system spends much more time repairing to the normal state but has the higher FAU at the beginning stage. Therefore, IRS is applicable for the system to keep the fine survivability performance in a certain time. Another conclusion is that the system under the DRS spends less time repairing to the normal

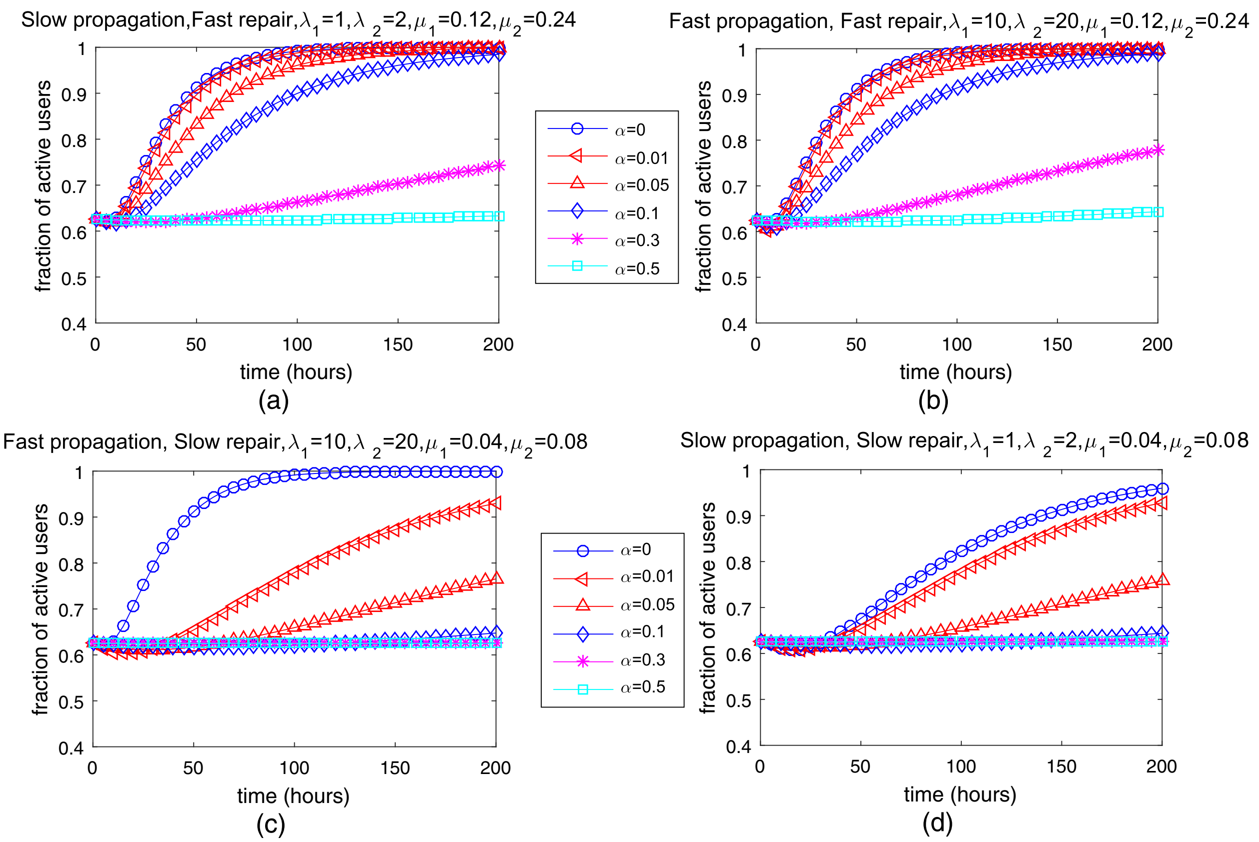

Fig. 9 Survivability impact of different schemes (**a**–**d**) in IRS

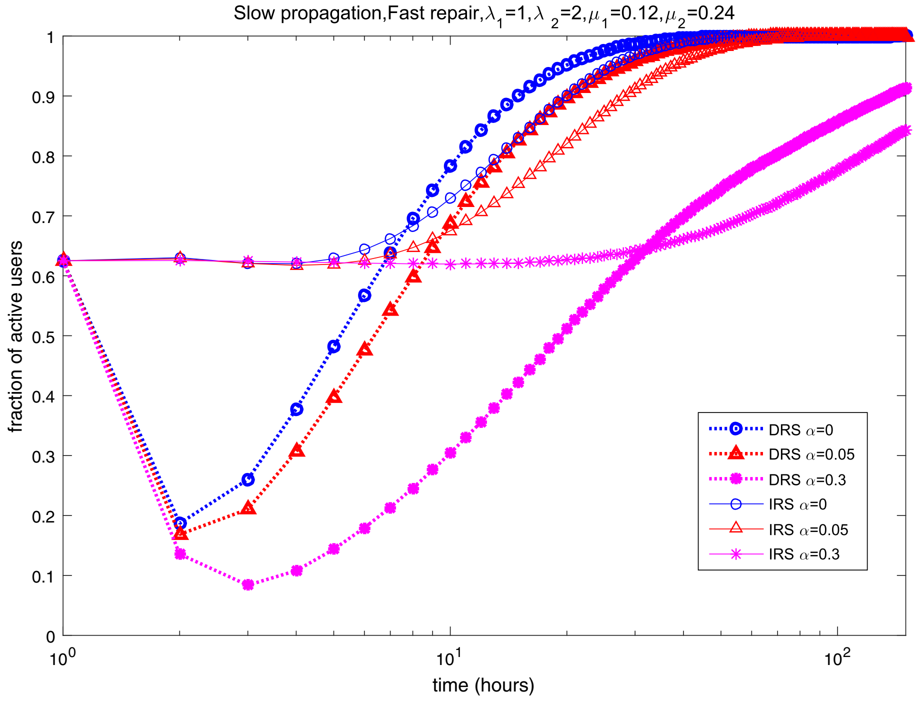

Fig. 10 Survivability impact of two strategies

value. Therefore, DRS could be applied to the system which should achieve better survivability performance after some time.

5 Conclusions

In this paper, we have presented two new survivable strategies when facing malicious attack propagation in NEMO scenario. In our approach, we use CTMC analytical model to compare two strategies by analyzing their dynamic behaviors. Simulation results have demonstrated that DSR provides less repair time for IM state in the NEMO scenario. Moreover, our results suggested how to set the proper survival strategy for system with higher FAU. For the future work, it would be helpful to add optimization considerations [14, 15] into current survivability research and extend our analysis to more general mobile network scenarios.

Acknowledgements

The authors thank the reviewers for their detailed and constructive comments, which helped us to greatly improve the quality of the paper.

Funding

This work was supported by the National Science and Technology Major Projects of the Ministry of Science and Technology of China under Grant No. 2013ZX03006002, the Beijing Natural Science Foundation under Grant No. 4132053, and the Natural Science Foundation of China under Grant Nos. 61301081 and 61003283.

Competing interests

The authors declare that they have no competing interests.

Author details

[1]School of Electronics and Information Engineering, Beijing Jiaotong University, Beijing 100044, China. [2]China Aero-Polytechnology Establishment, Beijing 100028, China. [3]Beijing University of Posts and Telecommunications, Beijing 100876, China.

Received: 25 December 2015 Accepted: 6 September 2016
Published online: 29 September 2016

References

1. A Kitana, I Traore, I Woungang, Impact study of a mobile botnet over LTE networks. J. Internet Serv. Inf. Secur. **6**(2), 1–22 (2016)
2. F Song, R Li, H Zhou, Feasibility and issues for establishing network-based carpooling scheme. Pervasive Mob. Comput. **24**, 4–15 (2015)
3. NSFOCUS DDoS Threat Report 2015. http://www.nsfocus.com.cn/upload/contents/2016/04/20160406113345_86183.pdf. Accessed 20 Aug 2016.
4. A Zolfaghari, F Kaudel, Framework for network survivability performance. IEEE J. Select. Areas Commun. **12**(1), 46–51 (1994)
5. S Dharmaraja, V Jindal, U Varshney, Reliability and survivability analysis for UMTS networks: an analytical approach. IEEE Trans. Netw. Serv. Manag. **5**(3), 132–142 (2008)
6. V Jindal, S Dharmaraja, S Kishor, *Analytical survivability model for fault tolerant cellular networks supporting multiple services*. IEEE international symposium on performance evaluation of computer and telecommunication systems, 2006, pp. 505–512
7. PE Heegaard, KS Trivedi, Network survivability modeling. Comput. Netw. **53**, 1215–1234 (2009)
8. Y Liu, V Mendiratta, KS Trivedi, *Survivability analysis of telephone access network, 15th international symposium on software reliability engineering, 367–377*, 2004
9. L Xie, PE Heegaard, Network survivability under disaster propagation: modeling and analysis. IEEE Wireless Communications and Networking Conference (2013)
10. F Song, Y Zhang, Z An, H Zhou, I You, The correlation study for parameters in four tuples. Int. J. Ad Hoc Ubiquitous Comput. **19**(1/2), 38–49 (2015)
11. V. Devarapalli, R. Wakikawa, A. Petrescu, et al., Network mobility (NEMO) basic support protocol. IETF RFC 3963, (2005)
12. ANSI T1A1.2 Working Group on network survivability performance, technical report on enhanced network survivability performance. 2001. p. 68
13. S Wen, W Zhou, J Zhang et al., Modeling propagation dynamics of social network worms. IEEE Trans. Parallel Distrib. Syst. **24**, 1633–1643 (2013)
14. F Song, D Huang, H Zhou, H Zhang, I You, An optimization-based scheme for efficient virtual machine placement. Int. J. Parallel Prog. **42**(5), 853–872 (2014)
15. M Johnston, H-W Lee, E Modiano, A robust optimization approach to backup network design with random failures. IEEE/ACM Trans. Netw. **23**(4), 1216–1228 (2015)