Survivability Analysis for a Wireless Ad Hoc Network Based on Semi-Markov Model

Zhipeng Yi†, Nonmember and Tadashi Dohi†a), Member

SUMMARY Network survivability is defined as the ability of a network keeping connected under failures and/or attacks. In this paper, we propose two stochastic models: binomial model and negative binomial model, to quantify the network survivability and compare them with the existing Poisson model. We give mathematical formulae of approximate network survivability for respective models and use them to carry out the sensitivity analysis on model parameters. Throughout numerical examples it is shown that the network survivability can change drastically when the number of network nodes is relatively small under a severe attack mode which is called the Black hole attack.

key words: network survivability, wireless ad hoc network, DoS attack, semi-Markov process, transient analysis

1. Introduction

Network survivability reflects the ability of a network to continue functioning for and/or after failures. It is a fundamental issue to design and evaluate the performance of wireless ad hoc networks. In the literature [3]–[5], some authors gave different definitions of network survivability. Xing and Wang [7] perceived the survivability of a wireless ad hoc network as the probabilistic k-connectivity, and provided a quantitative analysis on the impacts of both node misbehavior and failure on network survivability. This work was extended latter in [8] by conducting a comprehensive simulation experiment. On the probabilistic k-connectivity, significant research works were done in [1], [2] to build the node degree distribution model. However, it is worth mentioning that very little research efforts were made to analyze network survivability models quantitatively for ad hoc networks.

In this paper we develop a unified modeling approach based on a semi-Markov process and propose different stochastic models from the existing Poisson model in [8], which focuses on the microscopic behavior of the ad hoc network. More specifically, within the semi-Markov modeling framework, we apply the other probability models; binomial model and negative binomial model, and derive approximately the network survivability, from the macroscopic viewpoint of modeling [9]. It should be noted that the Poisson model in [8] is based on the physical network structure, but our models are regarded as macroscopic models in terms of statistical modeling. The basic idea on the binomial model comes from [2], though it did not consider the survivability evaluation. We refer to the asymptotic relationship among these three stochastic models, and show that our models asymptotically approach to the Poisson model as the number of active nodes increases [9], i.e., the Poisson model is a complementary approach of our macroscopic models. We further perform not only the steady-state analysis [7]–[9] but also the transient analysis of the network survivability.

The remaining part of this paper is organized as follows. In Sect.2, we define the state of each node in the stochastic model to describe a wireless ad hoc network, and refer to an isolation problem under the Black hole attack which is equivalent to the well-known DoS attack. Based on the familiar semi-Markov analysis, the transition behavior of the network node is analyzed in Sect.3. Section 4 is devoted to the network survivability analysis, where the node isolation, network connectivity and network survivability are defined. Here, we formulate a problem on network connectivity in the presence of misbehaving nodes and present two new node distribution models [9], in addition to the existing Poisson model [8]. Section 5 concerns numerical examples, where we take place the sensitivity analysis of model parameters on the network survivability and carry out the transient analysis of the network survivability by means of the Laplace inversion numerical technique. Finally, the paper is concluded with some remarks in Sect.6.

2. Model Description

2.1 Node Classification

In a wireless ad hoc network, node cooperation in the routing process is an essential requirement to maintain protocol operations and network connectivity [5]. Since every node is autonomous, it needs to decide how to act in the network by itself. Considering the potential impacts of various misbehaviors, we extend the geometric random graph model aforementioned by introducing an additional assumption that all nodes operate independently in the following five states [7], [8]:

- Cooperative state (C): a node complies with all routing and forwarding rules.
- Selfish state (S): a node may not forward control or data packets for others for the sake of power saving.
- Jellyfish state ($J$): a node being cooperative in the routing stage but reluctant in forwarding data packets.
- Black hole state ($B$): a node disrupting legitimate path selections by broadcasting fakes route replies.
- Failed state ($F$): a node is unable to initiate or response route discoveries.

For common DoS attacks, the node in Jellyfish attack receives route requests and route replies. The main mechanism of Jellyfish state is to delay packets without any reason. It is possible to convert a selfish node to be cooperative again if it is reconfigured, and so on. It is also prone to be configured on various reasons, such as energy exhaustion, misconfiguration, or to be compromised as a malicious node.

2.2 Probabilistic Node Model

In this wireless ad hoc networks, we assume that a node may change its behavior as follows.

- A cooperative node is exposed to become failed due to various reasons, such as energy exhaustion, misconfiguration, and so on. It is also prone to be configured on purpose as a selfish one for the sake of power saving, or to be compromised as a malicious node.
- It is possible to convert a selfish node to be cooperative again by means of proper configurations. A selfish node can become malicious due to being compromised or failed due to power depletion.
- A malicious node can become a failed node, but it will not be considered to be cooperative or selfish any more even if its disruptive behaviors are intermittent only.
- A failed node can become cooperative again if it is recovered and responds to routing operations.

Under the above assumptions, we consider a dynamic model to describe the probabilistic node behavior.

3. Analysis

Define a state space, $S = \{C, S, J, B, F\}$ and describe the node behavior transitions by a stochastic process, $\{Z(t), t \geq 0\}$ associated with space $S$. Let $X_n$ denote the state at transition time $t_n$. Then we have

$$
\Pr(X_{n+1} = x_{n+1}|X_0 = x_0, \ldots, X_n = x_n) = \Pr(X_{n+1} = x_{n+1}|X_n = x_n),
$$

where $x_i \in S$ for $i = 0, 1, 2, \ldots$. From Eq. (1), the stochastic process $\{X_n, n = 0, 1, 2, \ldots\}$ constitutes a Markov chain with state space $S$. However, the transition time from one state to another state is subject to random behaviors of a node and it is very difficult to characterize transition times by only exponential distributions. For instance, a node is more inclined to fail due to energy consumption as time passes, and the less residual energy left, the more likely a node changes its behavior to selfish. This implies that the future action of a node may depend on how long it has been in the current state and transition intervals may have arbitrary distributions.

From the above observation it is common to assume a semi-Markov process (SMP) for $\{Z(t), t \geq 0\}$ to model the node behavior transitions [3], which is defined by

$$
Z(t) = X_n, \forall t_n \leq t \leq t_{n+1}.
$$

Letting $T_n = t_{n+1} - t_n$ be the sojourn time between the $n$-th and $(n + 1)$-st transitions, we can define the associated semi-Markov kernel $Q = (Q_{ik}(t))$ by

$$
Q_{ik}(t) = \Pr(X_{n+1} = k, T_n \leq t|X_n = i) = p_{ik}F_{ik}(t),
$$

where $p_{ik} = \lim_{t \to \infty} Q_{ik}(t) = \Pr(X_{n+1} = k|X_n = i)$ is the transition probability between states $i, k = c, s, j, b, f$ corresponding to $S = \{C, S, J, B, F\}$, and $F_{ik}(t) = \Pr(T_n < t|X_{n+1} = k, X_n = i)$ is the transition time distribution from state $i$ to $k$.

Figure 1 illustrates the transition diagram of the homogeneous SMP $\{Z(t), t \geq 0\}$ under consideration, which is somewhat different from the model in [8], because it is much more simplified by eliminating redundant states in [8]. Based on the transition diagram, the transition probability matrix of $\{X_n\}$ is given by

$$
\begin{pmatrix}
C & S & J & B & F \\
C & 0 & p_{cs} & p_{cj} & p_{cb} & p_{cf} \\
S & p_{sc} & 0 & p_{sj} & p_{sb} & p_{sf} \\
J & 0 & 0 & 0 & 0 & 1 \\
B & 0 & 0 & 0 & 0 & 1 \\
F & 1 & 0 & 0 & 0 & 0
\end{pmatrix}
$$

Let $\mu_{ik}$ be the mean transition time from state $i$ to $k$, and define the Laplace-Stieltjes transform (LST) by $q_{ik}(s) = \int_0^\infty \exp(-st)\bar{Q}_{ik}(t)\,dt$ for $i, k = c, s, j, b, f$. From Fig. 1 it is immediate to see that

$$
q_{cs}(s) = \int_0^\infty \exp(-st)\bar{F}_{ct}(t)\bar{F}_{ct}(t)\bar{F}_{ct}(t)\,dt
$$

$$
q_{cj}(s) = \int_0^\infty \exp(-st)\bar{F}_{ct}(t)\bar{F}_{ct}(t)\bar{F}_{ct}(t)\,dt
$$

$$
q_{cb}(s) = \int_0^\infty \exp(-st)\bar{F}_{ct}(t)\bar{F}_{ct}(t)\bar{F}_{ct}(t)\,dt
$$

$$
q_{cf}(s) = \int_0^\infty \exp(-st)\bar{F}_{ct}(t)\bar{F}_{ct}(t)\bar{F}_{ct}(t)\,dt
$$
\[
q_{sc}(s) = \int_{0}^{\infty} \exp(-st)F_{sf}(t)F_{sb}(t)F_{st}(t)dF_{sc}(t) \\
q_{sf}(s) = \int_{0}^{\infty} \exp(-st)F_{sc}(t)F_{sf}(t)F_{sb}(t)dF_{sf}(t) \\
q_{sb}(s) = \int_{0}^{\infty} \exp(-st)F_{sc}(t)F_{sf}(t)F_{sb}(t)dF_{sb}(t) \\
q_{sf}(s) = \int_{0}^{\infty} \exp(-st)F_{sc}(t)F_{sf}(t)F_{sb}(t)dF_{sf}(t) \\
q_{sj}(s) = \int_{0}^{\infty} \exp(-st)dF_{sj}(t) \\
q_{bf}(s) = \int_{0}^{\infty} \exp(-st)dF_{bf}(t) \\
q_{fc}(s) = \int_{0}^{\infty} \exp(-st)dF_{fc}(t),
\]

where in general \( \bar{\psi}(-) = 1 - \psi(-) \). Define the recurrent time distribution from state \( G \) to state \( G \) and its LST by \( h_{cc}(t) \) and \( h_{cc}(s) \), respectively. Then, from the one-step transition probabilities from Eqs. (5)–(15), we have

\[
h_{cc}(s) = \int_{0}^{\infty} \exp(-st)dP_{cc}(t) \\
= q_{cc}(s)q_{cc}(s) + q_{cs}(s)q_{cs}(s)q_{sf}(s) + q_{cs}(s)q_{sb}(s)q_{sf}(s) + q_{cs}(s)q_{sf}(s)q_{fc}(s) + q_{c}(s)q_{bf}(s)q_{sf}(s) + q_{sb}(s)q_{bf}(s)q_{fc}(s) + q_{sf}(s)q_{fc}(s). \tag{16}
\]

Let \( P_{ck}(t) \) denote the transition probabilities from the initial state \( C \) to respective state \( k (= c, s, j, b, f) \). Then, the LSTs of the transition probabilities, \( p_{ck} = \int_{0}^{\infty} \exp(-st)dP_{ck}(t) \), are given by

\[
p_{cc}(s) = \{q_{cc}(s) - q_{cs}(s) - q_{cb}(s) - q_{cf}(s)\} \bar{h}_{cc}(s) \tag{17}
\]

\[
p_{cs}(s) = q_{cs}(s)\{q_{cs}(s) - q_{cf}(s) - q_{sb}(s) - q_{sf}(s)\}\bar{h}_{cc}(s) \tag{18}
\]

\[
p_{cf}(s) = \{q_{cm}(s) + q_{cs}(s)q_{sf}(s)\} \bar{q}_{mf}(s)/\bar{h}_{cc}(s) \tag{19}
\]

\[
p_{cb}(s) = \{q_{cm}(s) + q_{cs}(s)q_{sf}(s)\} \bar{q}_{mf}(s)/\bar{h}_{cc}(s) \tag{20}
\]

\[
p_{jc}(s) = \{q_{cm}(s) + q_{cs}(s)q_{sf}(s) + q_{cs}(s)q_{sb}(s) + q_{cs}(s)q_{cf}(s) + q_{cs}(s)q_{sf}(s)q_{bf}(s) + q_{cs}(s)q_{sb}(s)q_{bf}(s) + q_{cs}(s)q_{cf}(s)q_{bf}(s)\}\bar{q}_{mf}(s)/\bar{h}_{cc}(s). \tag{21}
\]

From Eqs. (17)–(21), the transient solutions, \( P_{ck}(t) \), \( k = c, s, j, b, f \), can be derived numerically by means of the Laplace inversion technique (e.g., see [6]).

Of our next concern is the derivation of the steady-state probabilities \( P_{k} = \lim_{t \to \infty} P_{ck}(t) \), \( k = c, s, j, b, f \) corresponding to \( S \). Based on the above LSTs, \( P_{ck}(s) \), we calculate \( P_{k} = \lim_{s \to \infty} P_{ck}(s) = \lim_{s \to 0} P_{ck}(s) \) and, from some algebraic manipulations, obtain

\[
P_{c} = \int_{0}^{\infty} \frac{F_{cs}(t)F_{cf}(t)F_{cb}(t)F_{cf}(t)dt}{\bar{h}_{cc}(s)} \tag{22}
\]

\[
P_{s} = \frac{1}{\bar{h}_{cc}(0)} \left\{ \int_{0}^{\infty} F_{cs}(t)F_{cf}(t)F_{cb}(t)F_{cf}(t)dt \right\} \tag{23}
\]

\[
P_{j} = \mu_{jf} \cdot \left\{ \int_{0}^{\infty} F_{cs}(t)F_{cf}(t)F_{cb}(t)F_{cf}(t)dt \right\} \tag{24}
\]

\[
P_{b} = \mu_{bf} \cdot \left\{ \int_{0}^{\infty} F_{cs}(t)F_{cf}(t)F_{cb}(t)F_{cf}(t)dt \right\} \tag{25}
\]

\[
\bar{h}_{cc}(0) = \lim_{s \to 0} \frac{d\bar{h}_{cc}(s)}{ds} = \int_{0}^{\infty} \frac{F_{cs}(t)F_{cf}(t)F_{cb}(t)F_{cf}(t)dt}{\bar{h}_{cc}(s)} + \int_{0}^{\infty} \frac{F_{cs}(t)F_{cf}(t)F_{cb}(t)F_{cf}(t)dt}{\bar{h}_{cc}(s)} + \mu_{jf} \int_{0}^{\infty} \frac{F_{cs}(t)F_{cf}(t)F_{cb}(t)F_{cf}(t)dt}{\bar{h}_{cc}(s)} + \mu_{bf} \int_{0}^{\infty} \frac{F_{cs}(t)F_{cf}(t)F_{cb}(t)F_{cf}(t)dt}{\bar{h}_{cc}(s)}.
\]
4. Analysis of Network Survivability

4.1 Node Isolation

One immediate effect of node misbehaviors and failures in wireless ad hoc networks is the node isolation problem. It is a direct cause for network partitioning, which further affects network survivability. The node isolation problem is caused by four types of neighbors: Failed, Selfish, Jellyfish and Black hole nodes. In Fig. 2, we suppose that the node $u$ has 6 neighbors when it initiates a route discovery to another node $v$. Then it must go through by its neighbors $X_i$ $(i = 1, 2, 3, 4, 5, 6)$. If all neighbors of $u$ are failed in Selfish and Jellyfish states, then $u$ can no longer communicate with other nodes. In this case, we find that $u$ is isolated by the Failed and Selfish neighbors. On the other hand, if one of neighbors is Black hole ($i.e.$ $X_2$ in Fig. 3), it gives $u$ a faked one-hop path and makes $u$ always choose it. In this case, we find that $u$ is isolated by the Black hole neighbor.

4.2 Connectivity

We define the node degree $D(u)$ for node $u$ by the maximum number of neighbors $[1]$, and let $D_i(u)$ be the number of node $u$’s neighbors at state $k = c, s, j, b, f$. The isolation problem in Sect. 2 can be formulated as follows: Given node $u$ with degree $d$, $i.e.$, $D_i(u) = d$, if $D_k(u) > D_i(u) = d$ or $D_i(B,u) \geq 1$, then the cooperative degree is zero, $i.e.$, $D_i(c,u) = 0$, and $u$ is isolated from the network, so we have

$$Pr(D_i(c,u) = 0 | D_i(u) = d) = 1 - (1 - P_c)^d + (1 - P_c - P_b)^d,$$

(28)

where $P_c$ is the steady-state probability of a node in cooperative state and $P_b$ is the steady-state probability of a node launching Black hole attack.

In this paper, a node is said to be $k$-connected to a network if its associated cooperative degree is given by $k$. Given node $u$ with degree $d$, $i.e.$, $D_i(u) = d$, $u$ is said to be $k$-connected to the network if the cooperative degree is $k$, $i.e.$ $D_i(c,u) = k$, which holds only if $u$ has no Black hole neighbor and has exactly $k$ cooperative neighbors, $i.e.$, $D_i(B,u) = 0$ and $D_i(c,u) = k$. Then it is straightforward to see that

$$Pr(D_i(c,u) = k | D_i(u) = d) = \left(\frac{d}{k}\right)(P_c)^k(1 - P_c - P_b)^{d-k}.$$

(29)

4.3 Network Survivability

Suppose that there are $N$ mobile nodes in the area $A$ which is divided into $M_a$ sub-networks. A necessary condition for a network to be $k$-connected is that every node has at least $k$ cooperative degrees. Let $\theta(M)$ denote the minimum of the cooperative degrees of all nodes in a network $M$, $i.e.$ $\theta(M) = \min(D_i(c,u), \forall u \in M)$. Then the steady-state network survivability is approximately given by

$$SVB \approx Pr(\theta(M) \geq k) = [1 - Pr(D_i(c,u) < k)]^M_a.$$

(30)

By the total probability law, we have

$$Pr(D_i(c,u) < k) = \sum_{d=k}^{\infty} Pr(D_i(c,u) < k | D_i(u) = d) Pr(D_i(u) = d),$$

(31)
so that we need to find the explicit forms of \( \Pr(D_{(a)} < k | D_{(a)} = d) \) and \( \Pr(D_{(a)} = d) \). From Eqs. (28) and (29), it is immediate to obtain

\[
\Pr(D_{(a)} < k | D_{(a)} = d) = 1 - (1 - P_b)^d + \sum_{m=0}^{k-1} \binom{d}{m} P_c^m (1 - P_c - P_b)^{d-m}
\]

\[
eq 1 - (1 - P_b)^d + \sum_{m=0}^{k-1} B_m(d, P_c, 1 - P_c - P_b).
\]  

(32)

By replacing \( P_b \) and \( P_c \) by \( P_{cb}(t) \) and \( P_{cc}(t) \) in Eqs. (28), (29) and (32), respectively, we obtain the transient network survivability at time \( t \). Since the node distribution \( \Pr(D_{(a)} = d) \) strongly depends on the model property, we introduce three specific stochastic models in the following.

(i) Poisson Model

Suppose that \( N \) mobile nodes in a wireless ad hoc network are uniformly distributed over a two-dimensional square with area \( A \). The node transmission radius, denoted by \( r \), is assumed to be identical for all nodes. To derive the degree distribution \( \Pr(D_{(a)} = d) \), we divide the area into \( N \) small grids virtually, so that the grid size has the same order as the physical size of a node. Consider the case where the network area is much larger than the physical node size. Then, the probability that a node occupies a specific grid, denoted by \( p \), is very small. With large \( N \) and small \( p \), the node distribution can be modeled by the Poisson distribution [7], [8]:

\[
\Pr(D_{(a)} = d) = \frac{\mu_0^d}{d!} e^{-\mu_0},
\]  

(33)

where \( \mu_0 = \rho r^2 \), and \( \rho = N(1 - P_f)/A \) is the node density depending on the underlying model. Finally, substituting Eqs. (31)–(33) into Eq. (29), we obtain

\[
SVB \approx \left\{ \sum_{k=0}^{n} B_d(n, p, 1 - p) \left[ (1 - P_b)^d - \sum_{m=0}^{k-1} B_m(d, P_c, 1 - P_c - P_b) \right] \right\}^{M_a}.
\]  

(36)

If each node is assigned into a sub-network with the probability \( p = \pi r^2 / A \), then the corresponding binomial model results in a different survivability measure from Eq. (34).

(ii) Binomial Model

It is evident that the Poisson model just focuses on an ideal situation of mobile nodes. As pointed out in [9], it is not always easy to measure the physical parameters such as \( r \) and \( A \). Let \( p \) denote the probability that each node is assigned into a sub-network. For the number of activate nodes \( n = N(1 - P_f) \), we describe the node distribution by the binomial distribution:

\[
\Pr(D_{(a)} = d) = \binom{n}{d} p^d (1 - p)^{n-d} = B_d(n, p, 1 - p).
\]  

(35)

Substituting Eq. (35) into Eq. (29) yields an alternative formula of the network survivability:

\[
SVB \approx \left\{ \sum_{k=0}^{n} B_d(n, p, 1 - p) \left[ (1 - P_b)^d - \sum_{m=0}^{k-1} B_m(d, P_c, 1 - P_c - P_b) \right] \right\}^{M_a}.
\]  

(36)

(iii) Negative Binomial Model

The negative binomial model [9] is an extension of the binomial model with an infinite number of populations. The probability of a node assigned into sub-networks, \( p \), is given in the same way as the binomial model. If a node enters the sub-network, we consider it as a success, otherwise as a failure. Let \( l = \lfloor aN \rfloor \) be the number of failures before the \( d \)-th success, where \( a \in (0, 1) \) is an arbitrary design parameter, and \( \lfloor \cdot \rfloor \) is the maximum integer less than \( aN \). Focusing on how network survivability changes when the number of failures increases, the node distribution is given by

\[
\Pr(D_{(a)} = d) = \binom{l + d - 1}{d - 1} p^d (1 - p)^l = L_d(l, p).
\]  

(37)

From Eq. (29), we get

\[
SVB \approx \left\{ \sum_{k=0}^{n} L_d(l, p) \left[ (1 - P_b)^d - \sum_{m=0}^{k-1} B_m(d, P_c, 1 - P_c - P_b) \right] \right\}^{M_a}.
\]  

(38)

By setting \( N \) nodes in the area \( A \), and dividing \( A \) into \( M_a \) sub-networks, the node assigned probability is given by \( p = \pi r^2 / A \), so that we can obtain alternative representation of the network survivability with an additional model parameter \( l \).

5. Numerical Illustrations

5.1 Comparison of Network Survivability

In the numerical experiment, we set model parameters in the following: \( A = 1,000,000 \) (m²), \( N = 1,000 \), \( r = 100 \) (m), \( P_c = 0.6877 \), \( P_f = 0.1750 \) and \( P_b = 0.0007 \). This situation implies that 1,000 ad hoc sensor networks with each node transmission radius \( r = 100 \) (m) are uniformly distributed in an 1 (km²) square area, where the steady-state probabilities in cooperative state, failure state and Black hole state, for each sensor network, are given by 68.77%, 17.50% and 0.07%, respectively. Table 1 presents the dependence of connectivity \( k \) and number of nodes \( N \) on the steady-state network survivability among three stochastic models: Poisson model (P), binomial model (B) and negative binomial model (NB). From these results it is shown that the steady-state network survivability is reduced as \( k \) increases with \( N = 1,000 \), but does not change with \( k \) when \( N \) is greater
than 5,000. In Fig. 4, we show the dependence of $k$ on the survivability, when $N$ is given by 1,000. In this case, the expected value of node which can enter into a sub-network is calculated as 26. From the Fig. 3, it is seen that the steady-state network survivability reduces when $k$ is larger than almost 27% of the expected value of node (i.e., $k = 7$).

On the other hand, when $k$ is almost equal to 58% of the expected value of node (i.e., $k = 15$), the survivability approaches to 0. For $N = 5,000$, the expected value is 130, which means that if $k$ is not larger than 35, the steady-state network survivability does not change. This observation enables us to understand that the network survivability in the steady state can be reduced if $N$ increases. Then our binomial model can get almost similar result to the Poisson model. In fact if $n$ is sufficiently large and $p$ is sufficiently small under $\mu_0 = np$, from the well-known small number’s law, the binomial distribution can be well approximated by the Poisson distribution, and our result can be expected asymptotically.

For the negative binomial model, on the other hand, we need an additional design model parameter $a = 0.6, 0.7, 0.8$ and 1.0. Except in the case of $N = 1,000$, the steady-state network survivability is reduced when the number of failures increases as shown in Table 1. In this table, $a = a^*$ denotes a value satisfying the equation $\mu_0 = ap/(1 - p)$. In this case, three stochastic models provide almost similar values on the steady-state network survivability. This is because the resulting negative binomial model with $a^*$ can be approximated well by both the binomial and Poisson models.

To explain the effect of node cooperativeness on network survivability in the steady state, we set $P_s = 0.007$, $k = 5$ and $N = 1,000$. In Fig. 5, as $P_c$ increases from 0.1 to 0.8, it is seen that the network survivability goes to a saturation level 0.5569. If we set both $P_s$ and $P_j$ as zero, the network survivability can go to 1 when $P_c$ is greater than 0.8. Finally, we consider an impact of Black hole attack node, and set $P_c = 0.6877$, $k = 5$ and $N = 1,000$. The result is depicted in Fig. 6. When more Black hole attack nodes exist, the network survivability in the steady state keeps lower level. If $P_h$ is greater than 0.007 with an arbitrary $P_c$, the steady-state network survivability becomes 0.

### Table 1  Steady-state network survivability based on three stochastic models.

| $N$  | $k$ | $SVB - P$ | $SVB - B$ | $SVB - NB$ |
|------|-----|-----------|-----------|-----------|
| 1000 | 1   | $0.5586$  | $0.5597$  | $0.6468$  |
|      | 5   | $0.5569$  | $0.5582$  | $0.5862$  |
|      | 10  | $0.3290$  | $0.3326$  | $0.0043$  |
|      | 15  | $0.0002$  | $0.0000$  | $0.0000$  |
|      | 20  | $0.0000$  | $0.0000$  | $0.0000$  |

**Fig. 4** The effect of $k$ on steady-state network survivability.

**Fig. 5** The effect of node cooperativeness on steady-state network survivability.
The effect of black hole nodes on network survivability.

Table 2  Transition rates in the transient analysis.

| Parameter | $\lambda_{cs}$ | $\lambda_{cj}$ | $\lambda_{cb}$ | $\lambda_{cf}$ | $\lambda_{sc}$ | $\lambda_{sj}$ |
|-----------|----------------|----------------|----------------|----------------|----------------|----------------|
| Value     | 200            | 30             | 2              | 300            | 200            | 30             |
| Parameter | $\lambda_{sb}$ | $\lambda_{sf}$ | $\lambda_{jf}$ | $\lambda_{bf}$ | $\lambda_{fc}$ |
| Value     | 2              | 200            | 400            | 400            | 400            |

Fig. 7  Limiting probabilities.

the limiting probabilities $P_{cj}$ ($j \in S = \{c, s, j, b, f\}$), by taking the Laplace inversion of Eqs. (5)–(11). We apply the well-known Abate’s algorithm [6] for the numerical inversion of Laplace transforms. To simplify the analysis, we suppose a continuous-time Markov chain instead of the semi-Markov process. Let $\lambda_{ij}$ be the transition rates from state $i$ to state $j$ in the exponential distributions. The model parameters used for the transient analysis are given in Table 2. We plot the transient behavior of the limiting probabilities at arbitrary time $t$ in Fig. 7. From these figures, it can be seen clearly that the probability $P_{cc}(t)$ decreases first and approaches to the steady-state solution. The other probabilities $P_{cs}(t)$, $P_{cj}(t)$, $P_{cb}(t)$ and $P_{cf}(t)$ increase in the first phase but converge to their associated saturation levels. In Fig. 8, we plot the transient network survivability with different value of $k$, and investigate an impact of $k$-connectivity on network survivability, where we set $k = 1, 5, 10, 15$ in the binomial model. From Fig. 8, it is seen that the binomial model has a relatively higher survivability when $k$ takes lower values, and that when the connectivity becomes larger, the network survivability tends to go to 0 as the operation time $t$ goes on.

Finally we compare three stochastic models in terms of the transient network survivability. Figure 9 illustrates the transient network survivability with three stochastic models, where two cases on connectivity; $k = 10, 15$, are considered. It can be seen that all models show the very similar behavior with the same $k$, and that even the value of $k$ tends to be irrelevant as the operation time elapses.

6. Conclusion

In this paper, we have proposed two stochastic models; binomial model and negative binomial model and carried out the transient network survivability analysis. Based on the definition of network survivability, we have quantified the survivability and shown throughout numerical examples that the network survivability could change drastically when the number of nodes $N$ was small but could not for large $N$ even if $k$ was small. For the model approximation, three models can get nearly same values under the same conditions. We have also studied the limiting probability at time $t$ and investigated the effect of time change on transient network survivability.

References

[1] C. Bettstetter, “On the minimum node degree and connectivity of a wireless multihop network,” Proc. ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc-2002), pp.80–91, ACM, 2002.
[2] C. Bettstetter, J. Klinglmayr, and S. Lettner, “On the degree distribution of $k$-connected random networks,” Proc. IEEE Conference on Communications (ICC-2010), pp.1–6, IEEE CPS, 2010.
[3] D. Chen, S. Garg, and K.S. Trivedi, “Network survivability performance evaluation: A quantitative approach with applications in
wireless ad-hoc networks,” Proc. ACM International Conference on Modeling, Analysis and Simulation of Wireless and Mobile Systems (MSWiM-2002), pp.61–68, ACM, 2002.

[4] R. Ellison, D. Fisher, R. Linger, H. Lipson, T. Longstaff, and N. Mead, “Survival network systems: an emerging discipline,” Technical Report of SEI/CMU, CMU/SEI-97-TR-013, 1997.

[5] J.C. Knight and K.J. Sullivan, “On the definition of survivability,” Technical Report of Dept. of Computer Science/University of Virginia, CS-TR-33-00, 2000.

[6] P. Valko and J. Abate, “Numerical inversion of Laplace transform with multiple precision using the complex domain,” http://library.wolfram.com/infocenter/MathSource/5026/

[7] F. Xing and W. Wang, “Modeling and analysis of connectivity in mobile ad hoc networks with misbehaving nodes,” Proc. IEEE Conference on Communications (ICC-2006), pp.1879–1884, IEEE CPS, 2006.

[8] F. Xing and W. Wang, “On the survivability of wireless ad hoc networks with node misbehaviors and failures,” IEEE Trans. Dependable and Secure Computing, vol.7, no.3, pp.284–299, 2010.

[9] Z. Yi and T. Dohi, “Quantitative comparison of survivability models for wireless ad hoc networks,” Proc. 2nd International Conference on Networking and Computing (ICNC-2011), pp.284–287, IEEE CPS, 2011.

Zhipeng Yi received the B.S.E. and M.S. degrees from University of Electronic Science and Technology of China (UESTC) and Hiroshima University in 2007 and 2012, respectively. His research area when he was a student of Hiroshima University is Network Survivability Analysis.

Tadashi Dohi received the B.S.E., M.S. and Dr. of Engineering degrees from Hiroshima University, Japan, in 1989, 1991 and 1995, respectively. Since 2002, he has been working as a Full Professor in the Department of Information Engineering, Graduate School of Engineering, Hiroshima University. In 1992 and 2000, he was a Visiting Researcher in the Faculty of Commerce and Business Administration, University of British Columbia, Canada, and Hudson School of Engineering, Duke University, USA, respectively, on the leave absent from Hiroshima University. His research areas include Reliability Engineering, Software Reliability and Security, Dependable Computing, and Performance Evaluation. He is a regular member of ORSJ, JSIAM, REAJ and IEEE.