International Journal of Cryptology Research 4(1): 1 - 16 (2013)

Modeling Stochastic Correlated Node Behavior for Survivability in Ad Hoc Networks

[1*]A.H Azni, [2]Rabiah Ahmad and [3]Zul Azri Mohamad Noh

[1,2,3]Center for Advanced Computing Technology,
Faculty of Information Technology and Communication,
University Technical Malaysia Melaka

E-mail: [1]ahazni@gmail.com, [2]rabiah@utem.edu.my and [3]zulazri@utem.edu.my

*Corresponding author

ABSTRACT

This paper presents new model to study the survivability of ad hoc network in which node behaviors are statistically correlated. The model tries to identify explicitly the correlated node events that cause network to isolate. The model characterizing the node behavior transition based on Semi Markov process and predicts how nodes affected neighboring activity to which it is important for understanding their potential damages, and for developing countermeasures to secure and ensure survivable of mobile ad hoc network. For survivability analysis, the model introduces correlated degree ω as a new function of survivability to measure nodes connectivity. The study evaluates the impact of correlated node behavior particularly selfish, malicious and fails nodes toward network resilience and survivability. The results show that correlated node behaviors have more adverse effects on the survivability.

Keywords: Semi Markov process, survivability analysis, correlated degree, nodes connectivity.

1. INTRODUCTION

Node behavior plays an important role in performance analysis of mobile and wireless networks. In large ad hoc networks, node may change its behavior from behave to misbehave unavoidably which threaten the correct functioning of nodes. When node misbehave, it directly affects the connectivity and availability of the network (Xing and Wang (2006a)). Furthermore, misbehave node also has major effect on route discovery, packets forwarding, and network control message (Rai (2010), Xing and Wang (2006b) and Sterbenz *et al.* (2010)). In real network scenarios, misbehave nodes can be resulted from other nodes behavior as well. This scenario is called correlated behavior. For example, if a node has more and more neighbors failed, it may need to load more traffic originally forwarded by those failed neighbors, and thus might become failed faster due to excessive energy consumption. Similarly, it is also possible that the more malicious neighbors a node has, the more likely the node will be compromised by its malicious neighbors. Eventually, misbehave node leads to node failures. When failures occur, the network suffers from degraded performance because of the unavailability of the failed nodes. The subsequent impact could range from insignificant topological survivability to devastating network shutdown.

In this paper, we study correlated node behavior using epidemic-based propagation model to capture correlated behavior events. We developed a correlated node behavior model that captures the spatial dependent between nodes, thereby capturing the isolation effect of misbehave node across the network. Our approach is based on viewing dynamic topology of ad hoc network and using Semi Markov process to define stochastic node behavior. To evaluate the survivability of ad hoc networks, we extend the model presented in (Xing (2010)) to a setting where nodes are spatially correlated.

2. RELATED WORKS

There are several researches discussing on correlated node behavior in various contexts. In Neumayer *et al.* (n.d.) a framework is presented to model correlated effects caused by disasters on networks; nonetheless, the model is limited to bipartite networks and vertical regional disasters. Another work discusses availability of storage systems in the presence of independent and correlated failures (Bakkaloglu (n.d.)), where correlated failures are modeled based on datasets using conditional probabilities and the beta-binomial model. A tunable failure correlation model is reported in Nath *et al.* (2006) that allows different correlation levels in failures based on the traces. In Thanakornworakij *et al.* (2011), the reliability of a grid-computing system is evaluated considering the failure correlation of different subtasks executed by the grid; component failures are assumed independent, however. Moreover, a framework for modeling software reliability based on Markov renewal processes has been reported in Ning and Yang (2007) and Dai and Xie (2005) that is capable of incorporating the possible dependencies among successive software runs.

Albeit the works discussed in above studies on correlated behavior specifically node failure which deal with systems or network reliability and availability, nevertheless none of them is considering the unique feature of ad hoc networks and the potential impact of all kinds of node behaviors. We know that from literature (Azni *et al.* (2011)), correlated node behavior will result in unstable network which impact survivability, reliability and availability. It is also proven that the impact of correlated misbehave node is quite challenging due to multiple attacks and failures caused by node mobility, energy depletion and Denial of Services (DoS) attacks. Therefore, it is vital to model correlated node behavior to evaluate the survivability of a topological network that closely represents the actual behavior. The works (Xu and Wang (2010) and Kong and Yeh (2009)) are relevant to this work as they assess survivability of two common types of networks, random and scale-free, in the presence of independent failures. While these papers consider both independent and correlated failures and their effects on network survivability, however, they do not provide a systematic stochastic approach to model correlated node behavior.

3. STOCHASTIC CORRELATED NODE BEHAVIOR

To understand how nodes are correlated in ad hoc network, we first show the characteristic of node behavior transition which will be later used to quantify correlated node behavior model using propagation theory in epidemiology. In ad hoc networks, nodes are dynamically and arbitrarily change its behavior from cooperative to misbehave node. For example, nodes may fail due to software bugs or battery depletion, so a node may be unable to communicate with other nodes if its neighbors are all failed. Nodes may also behave selfishly by not forwarding packets for other nodes in order to save their battery energy, which will also tamper a normal communication services. Nevertheless, once a cooperative node is compromised by malicious nodes, it may launch aggressive attacks to other cooperative nodes. For example, Dos attacks with node mobility capability may be able to move around the entire network, to adjust transmission power dynamically, or even to propagate DoS attacks by compromising their cooperative neighbors (Xing and Wang (2006a)). Considering the potential impacts of various correlated node behaviors, we characterize node behavior transition according to Figure 1 below and introducing an additional assumption that all nodes operate independently in the following four states:

- ***Cooperative Nodes*** are active in route discovery and packet forwarding, but not in launching attacks.
- ***Failed Nodes*** are not active in route discovery.
- ***Malicious Nodes*** are active both in route discovery and launching attacks.

- ***Selfish Nodes*** are active in route discovery, but not in packet forwarding. They tend to drop data packets of others to save their energy so that they could transmit more of their own packets and also to reduce the latency of their packets.

Whenever node joints the network, it is assume as normal or cooperative. In epidemiology term, we define *cooperative* node as *susceptible* assuming that all nodes have the capability to change their state to misbehave (*infective*) nodes and failed (*remove*) nodes due to various reasons.

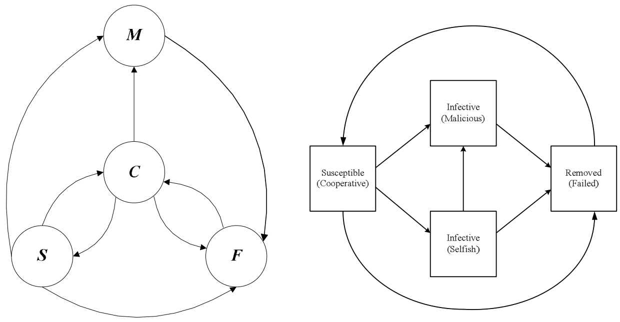

Figure 1: Node behavior transition vs. Compartmental diagram

Unlike existing epidemic models, this model captures that a node u may become infected by its own behavior such that at cooperative state (C), node is exposed to become failed node due to energy exhaustion, misconfiguration, and thus it may change its state either to selfish (S), malicious (M) or failure (F) node. On the other hand, a selfish or cooperative 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 responded to routing operations.

Based on the node classification describe above and in Azni *et al.* (2012), we use a Semi-Markov process to model node behavior transitions and analyzed the stochastic properties of correlated node behavior on epidemic theory. Due to the fact that node in MANETS is more inclined to be failed over time, we find that, the probability that node changes its behavior dependent on time. Therefore, node transition cannot simply described by Markov chain because of its time-dependent property. The semi-Markov process denoted by

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

with a state space $\Omega = \{C, S, M, F\}$. X_n denotes the *embedded* Markov chain of $Z(t)$, which has a finite state space Ω, and the *n*th state visited (Wang and Park (2010)). Thus, X_n is *irreducible* and ergodic and $Z(t)$ is the state of process at its most recent transition. The transition probability from state i to state j is defined as follows

$$\begin{aligned} P_i &= \lim_{t\to\infty} \Pr(X_{n+1} = j, t_{n+1} - t_n \leq t \mid X_n = i) \\ &= \Pr(X_{n+1} = j \mid X_n = i) \end{aligned} \tag{2}$$

Let P_{ij} and T_{ij} be the transition probability and transition time from state i to j respectively, for $i, j \in \Omega$, then the process $\{Z(t)\}$ can be described by a transition probability matrix (TPM) $\mathbb{P} = (P_{ij})$ and a transition time distribution matrix $\mathbb{F} = (F_{ij}(t))\cdot$ $\mathbb{P} = (P_{ij})$ and $\mathbb{F} = (F_{ij}(t))$ are given by

$$\begin{gathered} \mathbb{P} = \begin{pmatrix} 0 & a & c & d \\ b & 0 & c & d \\ 0 & 0 & 0 & d \\ e & 0 & 0 & 0 \end{pmatrix}, \text{ and} \\ \mathbb{F} = \begin{pmatrix} 0 & F_a(t) & F_c(t) & F_d(t) \\ F_b(t) & 0 & F_c(t) & F_d(t) \\ 0 & 0 & 0 & F_d(t) \\ F_e(t) & 0 & 0 & 0 \end{pmatrix}, \end{gathered} \tag{3}$$

where $F_x(t)$ is the cumulative distribution function (CDF) of T_{ij} for $i,\ j \in \Omega$. The state transition diagram of semi Markov node behavior model is shown in Figure 2.

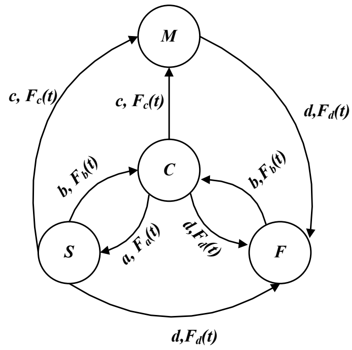

Figure 2: Semi-Markov Process for Node Behavior

For simplicity, we define state transition probability of P_{ij} as a, b, c and d. Let the probability of dropping packets due to selfishness and the probability of forwarding packets due to altruistic nature shown by the node *a* and *b* respectively and they are independent of each other. Let *c* be the probability of injecting packets due to malicious activity and *d* is the probability of loss packets due to exhausted battery power, out of transmission range or malfunction. Probability of recovery shown by *e* define the recovery of node from failure state to cooperative again after it has been recovered, recharged or repaired. We can then derive the steady-state transition probability distribution $\tilde{\pi}$ by solving the following set of equations

$$\begin{aligned} \tilde{\pi} &= \tilde{\pi} P \\ \sum_{i \in \Omega} \pi_i &= 1, \quad \pi \geq 0. \end{aligned} \tag{4}$$

Given the fraction of time $\tilde{\pi}$ that the node stays in each state and the mean residence times T_i for each state, it is easy to calculate the steady-state probability π_i of the node staying in transmission radius r

$$\pi_i = \frac{\pi_i E[T]}{\sum_j \pi_j E[T_j]} \tag{5}$$

We model correlated node behavior using epidemiology theory by Andersson (2000) and represent the network topology as undirected weighted graph. In the network, two nodes have a link if they are within the transmission range with each other and a neighborhood of node u, denoted by N_u, is a subset of such that every node in this subset has an edge from node u to node υ, i.e., $N_u = \{u | (u,\upsilon) \in E\}$. Thus, each edge $(u,\upsilon) \in E$ is associated with correlated function $\omega(e)$ which represent infection rate $\beta_{u\upsilon}^{S}$, $\beta_{u\upsilon}^{M}$ or removed rate λ_{uv}^{S} or λ_{uv}^{M}. The model also allows node to join the network after node recovery or forwarding with $\delta_{u\upsilon}$. Thus, the correlated functions of node u can be subsequently computed using equation (5) are then given by

$$\beta_{u,\upsilon} = \sum_{i=S,M} \pi_i^u \pi_i^\upsilon \tag{6}$$

$$\lambda_{uv} = \sum_{i=C,S,M} \pi_i^u \pi_i^\upsilon \tag{7}$$

$$\delta_{u,\upsilon} = \sum_{i=S,F} \pi_i^u \pi_i^\upsilon \tag{8}$$

where π_i^u is the percentage of the time spend by node u in state i. As node u can be infected only by its neighbors, $N_u(t)$ is statically dependent on $N_u(t-1)$ and the status of its neighbors. It means node u is not infected at time step t if and only if it was not infected by time step $t-1$ and no infected nodes in the transmission radius it resides connected to node u during the last time step. Since the status of a neighbor also depends on its own neighbors, conceptually, the status of all nodes is statically correlated in space and time. Therefore, the dependence of node u can be shown as

$$\begin{aligned}
&P[N_{(t-1)}^{(u)} = C | N_{(t)}^{(u)} = S] = a = \beta_{uv}^{(S)} \\
&P[N_{(t-1)}^{(u)} = C | N_{(t)}^{(u)} = M] = c = \beta_{uv}^{(M)} \\
&P[N_{(t-1)}^{(u)} = S | N_{(t)}^{(u)} = M] = c = \gamma_{uv} \\
&P[N_{(t-1)}^{(u)} = C | N_{(t)}^{(u)} = F] = d = \lambda_{uv}^{C} \\
&P[N_{(t-1)}^{(u)} = S | N_{(t)}^{(u)} = F] = d = \lambda_{uv}^{S} \\
&P[N_{(t-1)}^{(u)} = M | N_{(t)}^{(u)} = F] = d = \lambda_{uv}^{M} \\
&P[N_{(t-1)}^{(u)} = S | N_{(t)}^{(u)} = C] = b = \delta_{uv}^{S} \\
&P[N_{(t-1)}^{(u)} = F | N_{(t)}^{(u)} = C] = b = \delta_{uv}^{F}
\end{aligned} \tag{9}$$

where *a, b, c* and d is used to denote the status of node u at time t as in Figure 2. Given node u is susceptible at time t, the probability that the node u remains susceptible at the next time step can be defined as

$S_u(t) = P(N_u(t-1) = b \mid N_u(t) = b)$. From equation (10), the model implies that

$$I_{s_u}(t) = \beta_{uv}^{S} P(N_u(t) = a) \quad (10)$$

$$I_{m_u}(t) = \beta_{uv}^{M} P(N_u(t) = c) \quad (11)$$

$$R_u(t) = \lambda_{uv} P((N_u(t) = a) + (N_u(t) = b) + (N_u(t) = c)) \quad (12)$$

Therefore the definition of $I_{s_u}(t)$, $I_{m_u}(t)$ and $R_u(t)$ yield that for $R_u(t) = \forall u \in \{1,2,3,\ldots,N\}$

$$S_u(t) = \sum_{(u,v)\in E} [P(N_u(t) = b \mid N_u(t) = b)(1 - (I_{s_u} + I_{m_u} + R_u) \quad (13)$$

Combine with (10), (11) and (12), (13) provides recursive relationship between $N_u(t)$ and $N_u(t+1)$, for $u \in N_u$, and gives a formal stochastic correlated node behavior model. This model characterized the evolution of correlated node transition probabilities P_{ij}, with β_{uv}, λ_{uv}, δ_{uv} due to node infection and removal. Thus, the basic differential equations that describe the rate of change of susceptible, infective, and remove nodes are given by

$$\frac{dS(t)}{dt} = -\sum_{i=S,M} \beta_{uv} P_i \frac{\sigma \pi r^2}{N} + \sum_{i=F,S} \delta_{uv} P_i \quad (14)$$

$$\frac{dI_s(t)}{dt} = \sum_{i=S} \beta_{uv} P_i \frac{\sigma \pi r^2}{N} - \sum_{i=S} \delta_{uv} P_i \quad (15)$$

$$\frac{dI_m(t)}{dt} = \sum_{i=M} \beta_{uv} P_i + \sum_{i=C} \gamma_{uv} P_i \frac{\sigma \pi r^2}{N} \quad (16)$$

$$\frac{dR(t)}{dt} = \sum_{i=S,M} \lambda_{uv} P_i \quad (17)$$

4. K- CORRELATED SURVIVABILITY

In this section, we describe a model to evaluate the survivability of ad hoc networks in the presence of correlated behavior. *K*-correlated is a study of edge connectivity of the correlated function known as *correlated degree*. Previous study (Xing (2010)) has shown survivability on *k*-

connectivity on individual nodes, however, due to correlated nature of nodes behavior, *k*-connectivity it is not accurate to analyze the survivability on correlated node behavior. Supposed that *N* nodes in a mobile ad hoc network are randomly and uniformly distributed over a 2-D square with area *A*. The node transmission radius, denoted by *r*, is assumed to be identical for all nodes. Thus, the underlying communication graph of a mobile ad hoc network is modeled by a undirected weighted graph $G = G(V, E)$ where V denotes the vertex set with $|N| = N$ and an edge E exists between two vertices only if their distance is no greater than *r* with the correlated function $P : E(G) \to \omega,$ interpreted as the probability of the edge being connected. The weighted assign to the edge $e \in E(G)$ denoted with $\omega(e)$ also known as edge connectivity. We assume that $\omega(e) \geq 0$ for all edges *e*. Figure 3 shows the network model of an ad hoc network describes above.

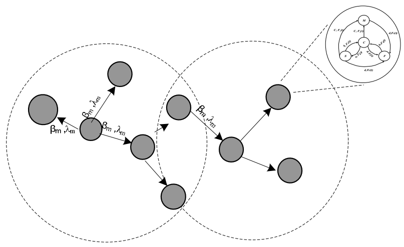

Figure 3: Network Model with correlated node behavior

In order for nodes to get connected, the edge connectivity must satisfy the following requirements

$$\omega(u,v) = \omega(d_{uv}, \leq d_{\max})$$

$$\omega(u,v) \geq \delta_{uv}, \text{ if and only if } \vartheta_u,\ \vartheta_v \text{ are adjacent in } (G,\omega). \qquad (18)$$

where d_{uv} is the Euclidean distance between u and v and δ_{uv} are the forwarding capacity of node u and v. Let ω_u denote the correlated degree of $N_u \in E(G,\omega),$ that is calculated using equation (6-8). We say that G is *k*-correlated if $\omega(u,v) \geq \delta$ hold for every pair of $u, v \in N.$ δ denotes the forwarding capacity of ω_u which indicate cooperative behavior of neighboring nodes. If $\omega(u,v) \geq \delta,$ node is dropping its packets and connection could not be establish, thus node will be isolated from the networks.

To explain node isolation problem, let N_u^i refer to the number of neighbors of node u at state $i \in \{S, M, F\}$. We refer selfish and malicious nodes together as misbehaving nodes, denoted as n_{SM} and n_F as failed nodes. A set of $N_u^i \subseteq \vartheta$ of k vertices is called *k*-isolated if it has edge connectivity $\omega(u,v) \leq \delta,$ where an outgoing edge is an edge between a vertex in N_u^i and vertex in ϑ.

Proposition 1: *Given the correlated degree of node* $\omega(u) \geq \delta$ *then node u is connected to the network, and if otherwise node u is isolated from the network. Probability of node being isolated denoted by*

$$
\begin{aligned}
P_{SM} &= \omega_{(u)} < \delta \big| \omega_{(u)} = \delta \\
&= P(n_{SM} + n_F) = \delta \big| \omega = \delta) \\
&= 1 - (1-b)^{\delta}
\end{aligned}
\tag{19}
$$

where b is the probability of node in cooperative state define in node transition above.

Proposition 2: *Given a network G with N nodes* $(N \gg 1)$ *and a connectivity requirement* w, *let* P_{SM} *denote the probability of node being misbehave and isolated, and* μ *denote the average number of nodes within one nodes transmission range, then the k-correlated survivability of* G *is approximated by*

$$
S_{uv}(w, G) \approx \left(1 - \frac{\Gamma(w, \mu(1 - P_{sm}))}{\Gamma(w)} \right)^N \tag{20}
$$

Given proposition 2, the node is said to be *k*-correlated if it is (ω, δ)-edge-connected. The physical meaning of this definition is that if a node's cooperative degree is ω then it may communicate with the nodes other than its neighborhood via ω disjoint outgoing paths. Thus, the network survivability of G, denoted by $S_{uv}(G)$, is defined as the probability that nodes in G are connected with cooperative edge δ.

5. NETWORK SURVIVABILITY EVALUATION

We verify the correctness of our correlated node behavior theory on the network survivability. In simulation, all network parameters are set to the default value given in Table 1 below. Next, we explain our simulation results.

Table 1: The Network Simulation Set Up

Parameter	Setting
Simulation area	1000 *m* x 1000 *m*
Transmission range	200 meter
Mobility model	Random Way Point
Movement features	Avg. speed 4 *m/s/* pause time 1 *s*
Initial Energy	100 Ws
Link capacity	11 Mbps
Traffic load	100 connections, 8 packet per sec
Simulation time	300*s*

The effect of Cooperativeness of Correlated Node

As explain above, correlated node degree is represented by edge connectivity δ. The higher the δ, it implies that the node is strongly connected. To observe the effect of probability of cooperation b, we set $\delta = 0.7$ for cooperative threshold. Figure 4 shows the analytic results of survivability under different nodes range 5, 15, 25, 50 nodes respectively. It is observed that survivability incline steady line with fewer nodes. This is due to the misbehavior node effect are less. Thus, the effect of node behavior is tractable with fewer nodes. Cooperative nodes are affected by correlated degree ω to obtain a higher survivability. Due to that, it is necessary to have a higher packet forwarding rate b in order for network to survive. When drop packets are higher, the nodes become less cooperative and network survivability is impossible to achieve.

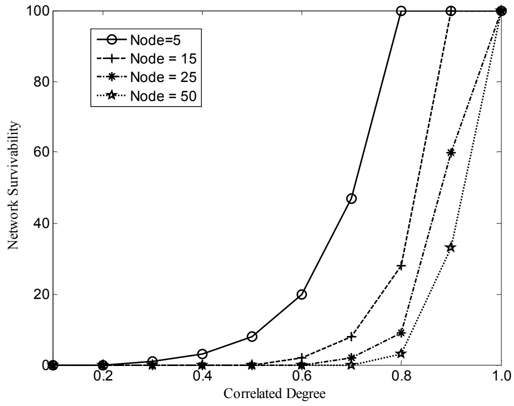

Figure4: Effect on survivability of correlated degree ω

The effect of Correlated Misbehave Node (selfish and malicious)

Similar to that in Figure 4, the plot in Figure 5 shows that the survivability decreases as b decrease. The survivability does not change significantly at the beginning especially if network scalability is less. In contrast, survivability for fewer nodes starts to decline faster compared to networks with large nodes. Network also becomes unstable when the δ less than 0.7. From Figure 5 the network survivability decreases very fast due to the packet loads increase. This is due to nodes behave maliciously and disconnected from the network. Thus the load originally routed to the node will be redistributed to neighboring nodes which cause chain reaction. This cause the node cluster will be isolated from the giant network as explain in equation (19). It also can be seen that network with more nodes could not sustain it survivability when network under attacks.

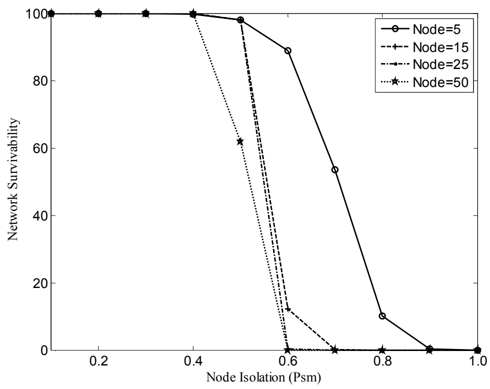

Figure 5: Effect on survivability of node isolation P_{SM}

The Effect of Correlated Node Failure

For highly survival network, the effect of node failure is more significant, e.g., the survivability drop to almost 0 when $\delta < 0.7$. Compare to malicious and selfish nodes, failed nodes shown severe effect on network survivability. The severer impact of node failures is due to the fact that node failures are also isolated from the network, which reduces the density of active nodes. Therefore, the probability of network failure cannot be ignored especially for a large scale network.

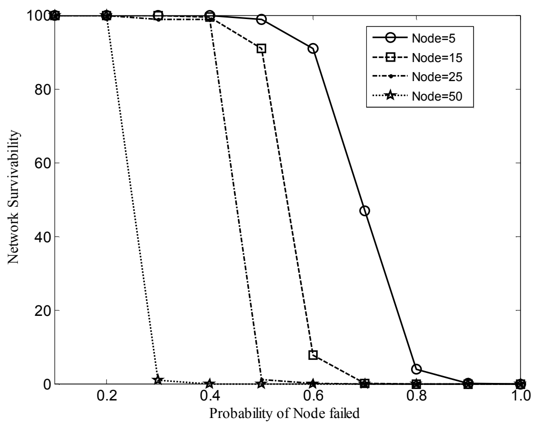

Figure 6: Effect on survivability of probability of failed node (P_{N_F})

6. CONCLUSION

In this paper, we developed an analytical model to study the impact of correlated node behavior on network survivability, which is defined as the probabilistic *k*-correlated of the network. We derived the approximation of the network survivability by using an edge connectivity function ω. As a conclusion, the impact of node behaviors on network survivability can be evaluated probabilistically from equation (20) which can be further used as a guideline to design or deploy a survivable of wireless ad hoc network given a predefined survivability preference.

REFERENCES

Azni, A. H., Ahmad, R., and Noh, Z. A. M. 2011. Resilience and Survivability in MANET: Discipline, Issues and Challenge. *Proceeding of the 3rd International Conference on Computing and Informatics, ICOCI 2011*. Bandung, Indonesia.

Andersson, H. (2000). Epidemics and Graphs. *Stochastic Epidemic Models and Their Statistical* (pp. 63-72). Springer New York. doi:10.1007/978-1-4612-1158-7_7

Azni, A., Ahmad, R., Noh, Z., & Basari, A. (2012). Correlated Node Behavior Model based on Semi Markov Process for MANETS. *Journal of Computer Science Issues*, *9*(1), 50-59. Retrieved from http://www.ijcsi.org/papers/IJCSI-9-1-1-50-59.pdf

Bakkaloglu, M. (n.d.). *On correlated failures in survivable storage systems*. *Information Systems* (pp. CMU-CS 02-129). Retrieved from http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA461303

Dai, Y., & Xie, M. (2005). Modeling and Analysis of Correlated Software Failures of Multiple Types. *IEEE Transactions on Reliability*, *54*(1), 100-106. Retrieved from http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=1402688

Kong, Z., & Yeh, E. M. (2009). Wireless Network Resilience to Degree-Dependent and Cascading Node Failures. *Modeling and Optimization in Mobile, Ad Hoc, and Wireless Networks, 2009. WiOPT 2009. 7th International Symposium on* (pp. 1–6). IEEE. Retrieved from http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=5291573

Nath, S., Yu, H., Gibbons, P. B., & Seshan, S. (2006). Subtleties in Tolerating Correlated Failures in Wide-Area Storage Systems. *Proc. of the Third USENIX Symp. on Networked Systems Design and Implementation* (pp. 225–238). Retrieved from http://www.usenix.org/events/nsdi06/tech/full_papers/nath/nath_html/

Neumayer, S., Zussman, G., & Cohen, R. (n.d.). Assessing the Impact of Geographically Correlated Network Failures. *Military*

Communications Conference, 2008. MILCOM 2008. IEEE, (pp. 1-6). doi:10.1109/MILCOM.2008.4753111

Ning, N., & Yang, B. (2007). *Software Reliability Models Based on Markov Renewal Process*. *Journal of Science And Technology* (pp. 1-9).

Rai, P. (2010). A Review of "MANET"s Security Aspects and Challenges'. *International Journal of Computer Applications IJCA*, *4*(Special Issues in MANET), 162-166. Retrieved from http://www.ijcaonline.org/archives/manets/number4/1038-89

Sterbenz, J. P. G., Hutchison, D., Cetinkaya, E. K., Jabbar, A., Rohrer, J. P., Schöller, M., & Smith, P. (2010). Resilience and Survivability in Communication Networks: Strategies, Principles, And Survey Of Disciplines. *Journal of Computer Networks*, *54*(8), 1245–1265. Elsevier. doi:10.1016/j.comnet.2010.03.005

Thanakornworakij, T., Nassar, R., Leangsuksun, C. B., & Paun, M. (2011). The Effect of Correlated Failure on the Reliability of HPC Systems. *2011 IEEE Ninth International Symposium on Parallel and Distributed Processing with Applications Workshops*, 284-288. IEEE. doi:10.1109/ISPAW.2011.55

Wang, S., & Park, J. T. (2010). Modeling and Analysis of Multi-Type Failures in Wireless Body Area Networks With Semi-Markov Model. *IEEE Communications Letters*, *14*(1), 6–8. IEEE. doi:10.1109/LCOMM.2010.01.091719

Xing, F. (2010). On The Survivability of Wireless Ad Hoc Networks with Node Misbehaviors and Failures. *Secure Computing, IEEE Transactions on*, *7*(3), 284-299. Retrieved from http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=4674373

Xing, F., & Wang, W. (2006a). Understanding Dynamic Denial of Service Attack in Mobile Ad Hoc Networks. *IEEE Military communication conference (MILCOM)* (pp. 1-7). IEEE. doi:10.1109/MILCOM.2006.302178

Xing, F., & Wang, W. (2006b). Modeling and Analysis of Connectivity in Mobile Ad Hoc Networks with Misbehaving Nodes. *IEEE International Conference on Communications, 2006* (Vol. 4, pp. 1879–1884). IEEE. doi:10.1109/ICC.2006.254994

Xu, Y., & Wang, W. (2010). Characterizing the Spread of Correlated Failures in Large Wireless Networks. *2010 Proceedings IEEE INFOCOM*, *56*(11), 1–9. IEEE. Retrieved from http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=5462009