Epidemic Modeling for Correlated Node Behavior in Ad Hoc Networks

A.H Azni, Rabiah Ahmad, and Zul Azri Mohamad Noh
Center for Advanced Computing Technology
Faculty of Information Technology and Communication
University Technical Malaysia Melaka

Abstract

In ad hoc networsk, nodes operating under dynamic topology are often correlated in their behavior. Correlated behavior may poses devastating impact towards network survivability. It can be investigated by observing node activities such as forwarding and malicious activity. To assess systematic network survivability in providing efficient communication in the events of correlated behaviors, it requires a stochastic abstraction of node behavior to capture correlated event. We proposed in this paper, a novel Semi Markov with epidemic model for modeling correlated node behavior in mobile ad hoc networks. The model consists of two stages. First stage characterizes node behavior and its transition based on Semi Markov process while at second stage correlated degree is proposed using epidemic model to generated correlated behavior event sequence. The model is able to predict correlated degree of nodes from the current status of neighboring nodes. This criteria is important in understanding the spread of node particularly for misbehave node and in developing counter measures for survival network.

1. Introduction

Node behavior plays an important role in network performance of mobile and wireless networks. In dynamic networks such as mobile ad hoc networks (MANETs), node changes its behavior from behave to misbehave unavoidably which may threaten the correct functioning of nodes. These change of behavior directly will affects the connectivity and availability of the network [1][2][3]. Furthermore, misbehave node also effect route discovery by giving fake route information, packets forwarding, and network control message [4][5][6] which temper network survivability. In real network scenarios, node behavior shows temporal dependent sequence of event known as correlated behavior resulted from node activities during routing process. Node may trigger correlated event if the behavior has the capability to infect others such that when a node failed, neighboring node may need to load more traffic originally forwarded by those failed node, 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 degradation of network performance because of the unavailability of the failed nodes. The subsequent impact of this correlated event could range from insignificant topological survivability to devastating network shutdown.

In view of the potentially devastating impact caused by correlated node behavior, we model correlated node behavior that captures the temporal dependent of node activity which cause event sequence in the network. The model is based on viewing dynamic behavior of node using Semi Markov process to define node stochastic behavior. We also introduce a new measure of temporal dependents behavior known as correlated degree. Correlated degree indicates the probability of neighboring node will get infected by misbehave activity of its neighbors. In Epidemic theory, correlated degree represent infection rate of node spreads to the network. With correlated degree the model is able to predict the evolution of correlated behavior and when the spreading becomes an outbreak. The layout of this paper is as follows. Section 2 gives a background review of previous studies. In Section 3, we describe our proposed correlated node behavior model. In Section 4, we assess and validate the model using simulation by experimenting two scenarios of correlated events. We create scenarios where selfish and malicious nodes are present and created a correlated effect to neighboring nodes. Section 5 will conclude the paper.

2. Related Works

There are several researches discussing on correlated behavior and events in various contexts such as network survivability caused by natural phenomena [7] , the availability of data storage system in the presence of independent and correlated event failures [8] and the reliability of grid computing system executing different subtasks [9]. Most of the previous works deal with specific network resilience problem in the event of correlated behavior; nevertheless none of them is considering the unique feature of ad hoc networks and the potential impact of correlated behavior. On another research, correlated behaviors and events were model through social behavior theory [10][11][12] to capture the spreading news in community, percolation theory to tackle the failure spreading problem [13][14][15] and epidemic theory in virus and malware infection [16][17][18][19].

In this work, we take epidemic model as a basis of node spreading to show node's correlated behavior. The works [15] and [14] are relevant to this work as they characterizes the spread of correlated failure due to misbehave nodes. While these papers consider both independent and correlated behaviors however, previous works do not provide a systematic stochastic approach to model correlated node behavior and to evaluate spreading rate of correlated behavior.

3. Correlated Node Behavior Model

In this section, we use a Semi-Markov process to characterize node behavior transitions, analyzed the stochastic properties of node behavior, formulating the transition matrix and model state transition for correlated node behavior.

3.1 Node Behavior

To understand how nodes are correlated in ad hoc network, we first show the characteristic of node behavior and its state transition which will be used to quantify temporal dependent of event sequence in epidemic theory to capture correlated behavior. We characterize node behavior as cooperative, selfish, malicious and fail node. Table 1 shows node behavior and it characteristic.

Behavior	Characteristic
Cooperative (C)	Active in route discovery and packet forwarding, but not in launching attacks.
Selfish (S)	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.
Malicious (M)	Active both in route discovery and launching attacks.
Fail (F)	Not active in route discovery.

Table 1. Node behavior and its characteristic

Node behavior in MANET is more formally specified by the state transition diagram in Figure 1. The node dynamically and arbitrarily changes its behavior from one state to another state dependent on state probability and time. Whenever node joints the network, it is assume as normal or cooperative. At cooperative state (C), node is exposed to be either at selfish (S), malicious (M) or fail (F) state. If node enters selfish (S) state, it may change its state to malicious (M) or fail (F) state. This is happened due to energy exhaustion, misconfiguration, being compromised or power depletion [20][21]. However, it is also possible to convert node operating at selfish state to be cooperative again by means of proper configurations. On the another hand, once node is at malicious (M) state, it only can become a failed node (F), but it will not be considered to be cooperative or selfish any more even if its disruptive behaviors are intermittent only. A failed node (F) can become cooperative again if it is recovered and responds to routing operations.

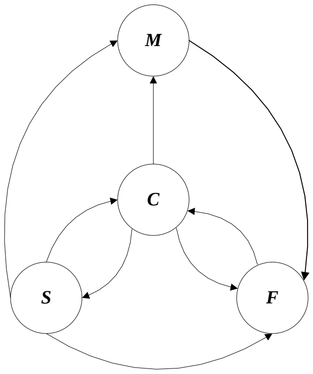

Figure 1. Node behavior transition

Based on node behavior describes above, we use a Semi-Markov process to model behavior transitions and analyzed the stochastic properties of correlated node behavior on epidemic theory. Due to the fact that probability node changes its state is temporal dependent on current state and time, node transition cannot simply described by Markov chain because of its time-dependent property. We define state space $\Omega = \{C(cooperative), S(selfish), M(malicious), F(Failed)\}$ and model node behavior transition by a stochastic process $\{Z(t)\}$ associated with space Ω. The semi-Markov process denoted by:

$$Z(t) = X_n, \forall t_n \leqslant t < \forall t_{n+1} \qquad (1)$$

In Equation (1), $\{Z(t)\}$ refers to the current state process, and $\{X_n\}$ denotes the *embedded* Markov chain of $\{Z(t)\}$ which has a finite state space Ω**,** and the *n*th state visited [22]. Thus, By Collolary 9-11 (pp 325) in [5] we know that $\{Z(t)\}$ is irreducible 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:

$$P_i = \lim_{t\to\infty} \quad Pr(X_{n+1}) = j, t_{n+1} - t_n \leqslant t | X_n = i)$$

$$= Pr(X_{n+1} = j | X_n = i) \qquad (2)$$

To obtain transition probabilities of $P_{ij}(i, j \in \{\Omega\})$, we need the appropriate input parameters from routing packets to determine node behavior state. Whenever node initiates the link, it will periodically broadcast a message to update its link information with its neighbors. The message carries routing information such as number of packets, number of bytes sent and received, and its residual energy [23]. Initially, every node has the same initial energy and in cooperative state. Cooperative state influences by packet forwarding probabilities which denoted by *b* can be derived from forwarding activity of each node as:

$$b = \frac{\text{Number of packets forwarded}}{\text{Number of packets received}} \qquad (3)$$

Any cooperative node is assumed to turn off its packet forwarding function if its residual energy drops below $1/\eta$ of its initial energy. The nodes tend to drop all the packets forwarded and become selfish at a time $T_{selfish}$ as given below:

$$T_{selfish} = (1 - 1/\eta)\bar{L} \qquad (4)$$

where η is the selfish threshold parameter and $\bar{L}$ is the average life time of a node derived from:

$$\bar{L} = \frac{\text{Remaining power}}{\text{Power consumption rate}} \qquad (5)$$

Thus, the probability of dropping denotes as *a* and node become selfish is given as:

$$a = \frac{\eta}{(\eta - 1)} * \frac{1}{\bar{L}} \qquad (6)$$

The node behavior model proposed malicious node as an attack of injecting a large amount of spurious traffic to exhaust the battery of cooperative node or crowd out the traffic. We indicate probability of injecting packet as c and can be derived from:

$$c = \frac{\text{Number of packets received by the neighbors}}{\text{Number of packets forwarded by the neighbors}} \qquad (7)$$

If it the packet received more than bandwidth allocation for wireless, the node will be congested and the energy will drain faster. The node also tend to loss it packets when the energy power is exhausted or out of transmission range. Therefore, probability of loss d is given as average node life time in equation (5) and mobility behavior.

Based on assumption discuss above, the transition probability matrix (TPM) $\mathbb{P} = (P_{ij})$ of $\{X_n\}$ is given by

$$\mathbb{P} = \begin{pmatrix} 0 & a & c & d \\ b & 0 & c & d \\ 0 & 0 & 0 & d \\ b & 0 & 0 & 0 \end{pmatrix} \qquad (8)$$

where $P_{ii} = 0$ means that it is not possible to make transition between the two states based on the rules specify in Figure 1. Since it is a stochastic matrix, the summation of transition probabilities to a state must be equal to 1. Node behavior is also time dependent, thus we determine time spend from state i to j as cumulative distribution function (CDF) of sojourn time T_{ij} for $i, j \in \Omega$. Then, transition time distribution matrix $\mathbb{F} = (F_{ij}(t))$ is given by:

$$\mathbb{F} = \begin{pmatrix} 0 & F_a(t) & F_c(t) & F_d(t) \\ F_b(t) & 0 & F_c(t) & F_d(t) \\ 0 & 0 & 0 & F_d(t) \\ F_b(t) & 0 & 0 & 0 \end{pmatrix} \qquad (9)$$

The state transition diagram of semi Markov node behavior model is shown in Figure 2.

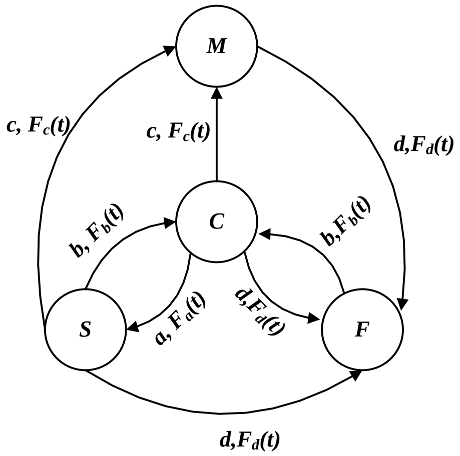

Figure 2. Semi-Markov Process for Node Behavior

After determining P_{ij} and F_{ij}, we can derive the steady-state transition probability distribution $\tilde{\pi}$ by solving the following set of equations:

$$\tilde{\pi} = \tilde{\pi} P$$

$$\sum_{i \in S}^{N} \pi_i = 1, \qquad \pi \geq 0 \tag{10}$$

Given the fraction of time $\tilde{\pi}$ that the node stays in each state and the sojourn 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*** :

$$\pi_i = \frac{\pi_i E[T_i]}{\sum_j^N \pi_j E[T_j]} \tag{11}$$

3.2 Correlated Behavior

Correlated behavior is defined as a sequence of temporal dependent events which can be interpreted as a time-dependent point process of $X_n(t)$, where $X_n(t)$ follow consecutive action at t_i and t_{i+1}. To detect correlated behavior in this event sequence we have to identify those events we consider correlated. Thus, we study the concept of event sequence in epidemic theory using susceptible-infection-removed (SIR) dynamic spreading to identify correlated node behavior. A node in SIR will be in either one of three events sequence: susceptible, infection or removed:

- *Susceptible*: the node in cooperative (C) state will be in susceptible events before it infected its neighbors or get infected by its neighbors.
- *Infection*: Once the node change its state to misbehavior (malicious and selfish state), it is infectious and has some probability of infecting its cooperative neighbors.
- *Removed*: After node is infected, this node may be in fail state and no longer active in the network. For some reason, cooperative node may also be in removed event if the connection is loss (e.g: out of transmission range)

Event sequence in SIR follows the current state of node behavior. In this paper, we interested to model correlated behavior in the presence of selfish and malicious behavior. Node operating at selfish (*infected*) state when its residual energy drops below threshold level. When node becomes selfish, it will drop all the forwarding packets then it disconnected or become failed node. This behavior resulted from its own self activity thus it has a capability to create event sequence by infecting neighboring nodes. Figure 3 illustrates an example of infection event sequence triggered by selfish node s_1. In this case, s_1 behaves like a fail node because selfish node drop all packets routing and cause the path that uses this node has to be rerouted and its load has to be redistributed to the neighboring nodes. The redistribution of the load may increase energy consumption due to packets overload.

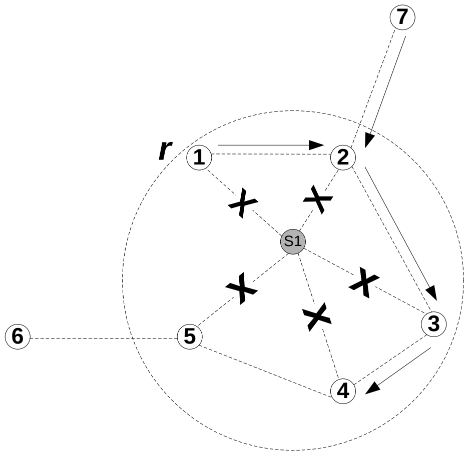

Figure 3. Infection Event triggered by selfish node

After node s_1 refuse to forward the packets, node *1* who initiates a route discovery to node *4*, has to go through via node *2* and *3* which takes longer route than before. Furthermore, node *2* also has to route the packets from node *7* which gives extra burden to node *2*. This consequence will lead to extra energy consumption and node failed faster. If node *2* failed, all nodes in the transmission *r* unable to establish any communications with other nodes at a distance of more than one-hope away.

We assign variable β^s_{uv} as infection rate for correlated selfish node behavior. Infection rate is determined by energy consumption, nodes mobility (speed) and Euclidian distance of node *u* and *v*. The calculation for node to infect its neighbors and perform correlated behavior is as follows:

1. Energy consumption denotes as:

   $$E_{con} = E_{tx} + \sum_{adjNode}(E_{rx})$$
2. Nodes mobility *m*
3. Euclidian distance $d_{u,v} = \parallel X_u - X_v \parallel$ if and only if $d_{uv} \leq r$.

Then, infection rate is computed for selfish node between nodes u and v as :

$$\beta^s_{uv} = \frac{E_{con} * m}{d_{uv}} \tag{12}$$

An example of another infection event is malicious node as illustrated in Figure 4. In this example, the initial attack occurs at node u_1. We assumed node u_1 is a malicious node in which it injects a huge number of junk packets into an ad hoc network because it has been compromised or it intentionally does it, with a goal to depleting the energy of the node that relay the packets. Once it infected, the malicious node will impersonate neighboring node by forwarding high volume of packets. In Figure 5, resulted from packet injection from node u_1 , node 2, *3*, *4* and *5* will suffer from congestion packets forwarded by node u_1. To be able for node u_1 to extend the correlated behavior to the next hop, node *5*, which reacts as an intermediate node to hop may exhaust the wireless bandwidth before overloading the node in the next hop.

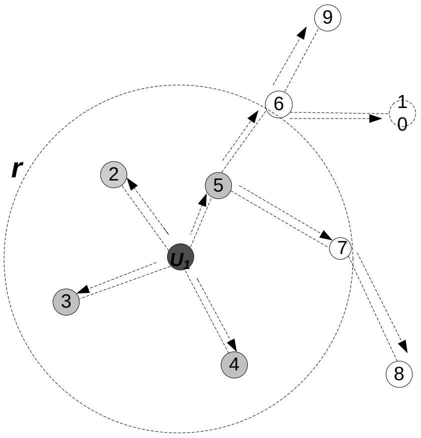

Figure 4. Infection Event triggered by malicious node

We determine infection rate of node *u* to *v* based on bandwidth usage per second and distance between them. The closer the node toward malicious node, the faster it will get infected. Thus, infection rate β_{uv}^m is calculated as:

$$\beta_{uv}^m = \frac{B}{p_{sc}} * d_{uv} \qquad (13)$$

Assume the bandwidth is *B* and the average size of a packet is P_{sc}. If β_{uv}^m exceed the maximum available bandwidth supported by wireless device, it will congested and cause transmission failure. Even though neighboring nodes will not forward junk packets injected by malicious node, they will have to spend some energy resources on verifying these packets.

In most cases, selfish and malicious node dies out and removes from the network. The failed node has the same effect as selfish node. The removed rate after nodes becomes infected is based on average node life time and average node residence time calculated as

$$\lambda_{uv} = \frac{E_R(t)}{E_{con}(t)} * \frac{E_R(t-1)}{E_{con}(t-1)} \qquad (14)$$

where E_R is residual energy of node *u* at time *t* and E_{con} is energy consumption of node *u* at time *t*. Basically it calculates how much average energy is consumed by node *u* per *t* second during the interval. This value represents how long the remaining energy can keep up the connections with these conditions.

4. Correlated Degree

Using this event sequence for behavior at each node, we model node correlated behavior for ad hoc networks as a weighted, undirected graph ***G = G (V, E)***, where V and E are set of vertices (nodes) and edges (links), respectively at a time instant t. Two nodes (*u*,*v*) have an edge if they are within the transmission range which each other and each edge has an efficiency $\omega(e)$ which refers to correlated degree captures the spreading capability of the nodes to perform correlated behavior in the network. The model describes correlated degree $\omega(e)$ of each edge as β_{uv}^s or β_{uv}^m , at which a *susceptible* (cooperative) node can become infective (*selfish or malicious*) node and infected its neighbor. In such cases, the selfish node change its state to malicious node, the infection rate is then γ_{uv}. If node is below infective threshold level, it then becomes failed node and removed from the network. The failure rate at which an infected node become failed node is associated with λ_{uv} . When a node is removed from infected neighbors, it may be recovered with a probability δ_{uv}^f. Based on the above assumption and the SIR model [24], the nodes state transition relationship and correlated degree of each event sequence in ad hoc network can be shown in Figure 5.

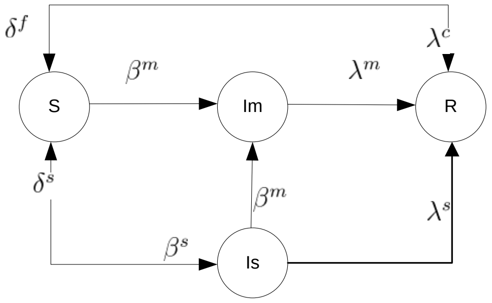

Figure 5. SIR State Diagram

However, in this paper, we only interested to capture the spreading of misbehave node which are selfish, malicious and fail node for analysis. Thus, for the next evaluation we assume node infected will node be in cooperative state again. We will discuss susceptible event of cooperative nodes in the next paper. Infection rate and remove rate can be subsequently computed using Equation (12-14). As node u may become infected by its own behavior and its neighbors, $X_n(t)$ is statically dependent on $X_n(t-1)$ 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 r connected to node u during the last time step. Since the status of a neighbor also depends on its own neighbors, therefore, the temporal dependence of node u can be shown as:

$$\begin{aligned}
&\mathrm{P}[\mathrm{N}_{(t-1)}^{(u)} = C|N_{(t)}^{(u)} = S] = a = \beta_{uv}^{(s)} \\
&P[N_{(t-1)}^{(u)} = C|N_{(t)}^{(u)} = M] = c = \beta_{uv}^{(m)} \\
&P[N_{(t-1)}^{(u)} = S|N_{(t)}^{(u)} = M] = c = \gamma_{uv} \\
&P[N_{(t-1)}^{(u)} = C|N_{(t)}^{(u)} = F] = d = \lambda_{uv}^{c} \\
&P[N_{(t-1)}^{(u)} = S|N_{(t)}^{(u)} = F] = d = \lambda_{uv}^{s} \\
&P[N_{(t-1)}^{(u)} = M|N_{(t)}^{(u)} = F] = d = \lambda_{uv}^{m} \\
&P[N_{(t-1)}^{(u)} = S|N_{(t)}^{(u)} = C] = b = \delta_{uv}^{s} \\
&P[N_{(t-1)}^{(u)} = F|N_{(t)}^{(u)} = C] = b = \delta_{uv}^{f}
\end{aligned} \tag{15}$$

Let $S(t), I_s(t), I_m(t)$ and $R(t)$ denote the number of nodes in susceptible, infection (selfish and malicious) and removed events at time t respectively. Assume that the total node population is a constant N, such that $S(t)+I_s(t)+I_m(t)+R(t)=N$ for all t. Since the nodes are uniformly distributed with density σ, nodes are connected in the order of $\sigma\pi r^2$ neighbor nodes. The basic differential equations that describe the rate of change of susceptible, infection, and removed nodes are given by

$$\frac{dS(t)}{dt} = -\sum_{i=s,m} \beta_{uv} P_i \frac{\sigma\pi r^2}{N} \tag{16}$$

$$\frac{dI_s(t)}{dt} = \left(\sum_{i=s} \beta_{uv} P_i\right) \frac{\sigma\pi r^2}{N} - \sum_{i=c} \delta_{uv} P_i \tag{17}$$

$$\frac{dI_m(t)}{dt} = \left(\sum_{i=m} \beta_{uv} P_i + \sum_{i=c} \gamma_{uv} P_i \frac{\sigma\pi r^2}{N}\right) - \sum_{i=c} \delta_{uv} P_i \tag{18}$$

$$\frac{dR(t)}{dt} = \sum_{i=s,m} \lambda_{uv} P_i \tag{19}$$

5. Simulation Evaluation

To evaluate the correctness of correlated node behavior model, we conducted exhaustive simulations in the simulation tool ns2 (v2.35) and series of numerical experiments in MATLAB (7.10a). We considered a MANET with 100 nodes randomly distributed in a 1000 m x 1000 m area. Each node is free to move following random waypoint mobility model with an average speed 4 m/s and has a 200*m* transmission range. IEEE 802.11 is used for medium access control and AODV is used as the routing protocol. We have used a time step of 300s to simulate the scenario. In simulations, nodes change their behaviors according to the energy resources available for their own use and forwarding packet ration. To simulate infection event for selfish, malicious and failed nodes, a modified version of AODV was developed so that their behaviors do not comply with the routing and forwarding rules defined in the standard. In order to calculate the correlated degree, we collected neighborhood statistics of each node per 10 seconds, including the number of neighbors and behavior of each neighbors. The model study the correlated node behavior without the effect of defends mechanism which means once infected by directly or indirectly, the node will not be repaired or removed. It remains in the infective state until it dies out. With this information, we can obtain the number of susceptible, infected and remove node from the network. In simulation, all network parameters are set to the default value given in Table 2 below.

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*

Table 2. Network Simulation Set Up

5.1 Infection Event Analysis

Initial state infected node was set as $I_s(0)=1$, $I_m(0)=0, R(0)=0$ then $S(0)=N-1$. To see the effect of correlated behavior we turn off β_{uv}^{m} malicious node infection rate and λ_{uv}^{s} remove rate. The number of node infected by this event sequence with infection rate β_{uv}^{s}= 0.1, 0.5, 0.8 are recorded. The nodes started with single node that is randomly chosen to be a selfish node. From Figure 6, we can see that as infection rate increasing, more nodes infected at less than 50 seconds. At *t* =50, the network is experiencing an outbreak from selfish correlated behavior and it started to infected the entire network within just 100 seconds. For example at β^{s}_{uv} = 0.8, within 100 seconds, almost all cooperative nodes become selfish and dropping all the packets forwarded to them. Although we turn off remove rate of selfish node, the nodes isolated themselves whenever the energy level below threshold η . In this case, as more nodes continue to behave selfishly, it will create an isolated cluster thus reduce the network density.

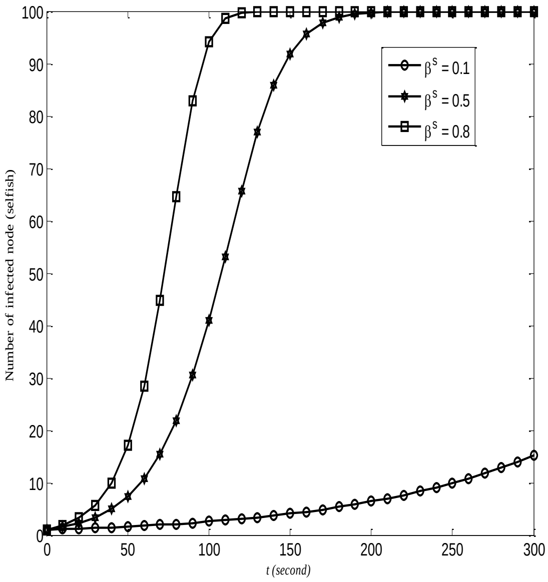

Figure 6. Infection rate for correlated selfish node

Next, we see the effect of correlated selfish node against node Euclidian distance and energy consumption. Euclidian distance used to measure node proximity in the network. From Figure 7, the result tally with the assumption describe in section 3. As node distance closer to infected node, it is likely to get infected first than the nodes in further position. Within 50 meters radius of infected node, the infection rate has a linear relationship with energy consumption of neighboring nodes. It chances to severely infect is higher with higher energy consumption. It means that the node has received high packets forwarding due to selfish behavior and thus the energy will drain faster as well.

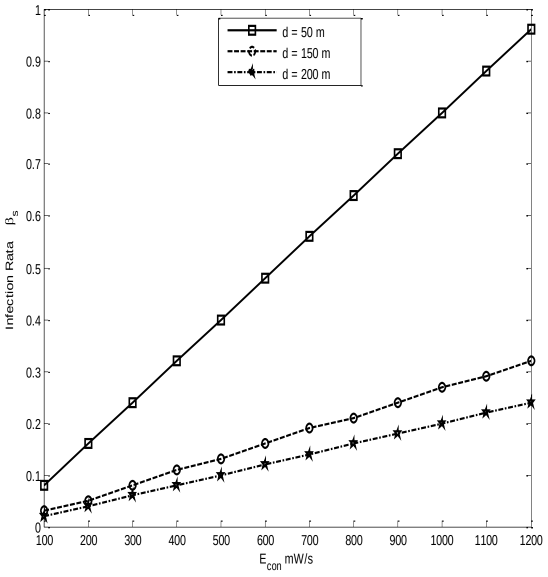

Figure 7. Infection rate β^{s}_{uv} impacted by Euclidian distance d and energy consumption

In simulating infection event for malicious node, initial state was set the same as selfish node except $I_m(0) = 1$ and $I_s(0) = 0$. We also set parameter of $\beta^{m}_{uv} = 0.1, 0.5$ and 0.8 to see the effect of correlated malicious node spreading. We turn off λ^{m}_{uv} to eliminate the effect of remove event sequence. We also assume that, malicious node will never become selfish node in this simulation. Figure 8 show that the infection rate for malicious node is constant at lower rate. It is also implies that 90% of nodes become malicious within 100 seconds if they are compromised with higher infection rate. Since we turn off failure rate, malicious nodes are still actives in the network and thus do not affect nodes density.

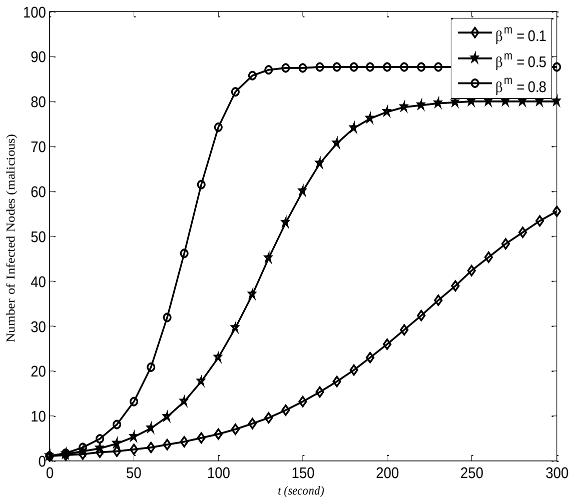

Figure 8. Malicious node against infection rate β^{m}_{uv}

5.2 Model validation

To validate the model, we used data collected from simulation and Weibull distribution for comparison. Weibull distribution is widely used in reliability engineering to model lifetime distribution [4]. Thus, Weibull distribution is used to find $f_a(t)$ and $f_c(t)$ which are time spend at infection events of selfish and malicious respectively. Thus $f_a(t)$ and $f_c(t)$ can be treated as life time distribution of nodes. Weibull function used in this work is define as

$$F(t) = 1 - e^{-(\frac{t}{\beta})^{\alpha}} \tag{20}$$

Since the average transition time from susceptible to infection (malicious) state and susceptible to infection (selfish) state are 8.91 and 7.53 respectively in Weibull distribution , we choose $\alpha = 2$ and $\beta^m = 8 \quad and \quad \beta^s = 7$ for malicious and selfish node from simulation. From Figure 9 and 10, we can see that the Weibull function in Equation (20) match very well with simulation results. The Cumulative Distribution Function (CDF) plots show clearly how likely a node is infected after a certain time. Further, the distribution can also be used to estimate the number of infected nodes. For example, in Figure 9, the probability that a node becomes malicious within 10s is almost 0.9, which also implies that 90% of nodes will become malicious within 100s if they are compromised. On the other hand, at 100s, probability of selfish node infected at about 70% of and the entire network is infected with less than 200s.

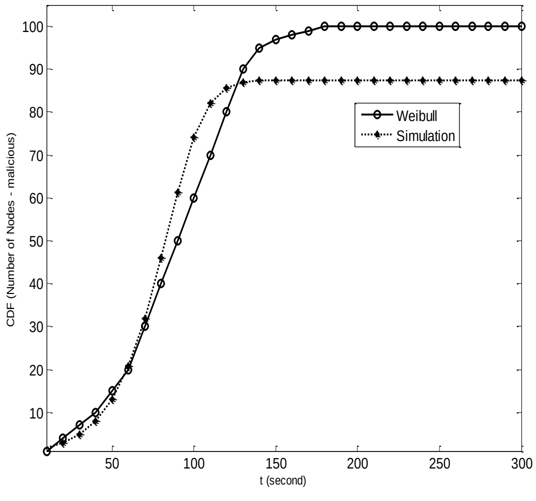

Figure 9. Probability of nodes become malicious nodes

From the analysis, we found that the spreading of malicious node is faster once more nodes are in infected state. To explain this, we consider that as long as a susceptible node is compromised, it can launch malicious attacks as described in Section III. Therefore, these accumulated malicious nodes may impact network connectivity severely and isolate more and more nodes. In the case of selfish node, we notice that, the infection time is less than malicious node, however, selfish node capable to create severe network portioning due to node failure from energy depletion.

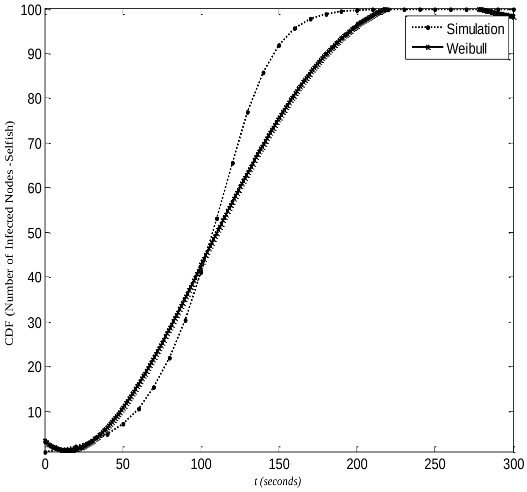

Figure 10. Probability of nodes become selfish nodes

6. Conclusion

In this work, we have studied stochastic correlated node behavior models which enable the efficient simulation of realistic scenarios of correlated node behavior for dynamic network topology in ad hoc networks. Then we developed correlated degree based on even sequence in epidemic-like models to capture the spread of correlated behavior. According to this model, a necessary condition for correlated behavior to spread in ad hoc networks is theoretically derived. Our numerical analysis results are provided to demonstrate the validity of the model. As future work, we plan to consider more other factors on the impact of the correlated behavior in these networks, such as the security limitation and transaction delay.

10. Acknowledgements

A.H.Azni would like to thank Universiti Sains Islam Malaysia (USIM) and Ministry of Higher Education (MOHE) for financial support throughout her studies in Universiti Teknikal Melaka Malaysia (UTEM), Melaka, Malaysia.

11. References

[1] F. Xing and W. Wang, “Understanding Dynamic Denial of Service Attack in Mobile Ad hoc Networks,” in *IEEE Military communication conference (MILCOM)*, 2006, pp. 1-7.

[2] T. Dimitar, F. Sonja, M. Jani, and G. Aksenti, “Connection resilience to nodes failures in ad hoc networks,” *Proceedings of the 12th IEEE Mediterranean Electrotechnical Conference (IEEE Cat. No.04CH37521)*, pp. 579-582, 2004.

[3] P. Manohar, M. Vereshchaka, and D. Manjunath, “Survivability analysis under non-uniform stochastically dependent node damages,” *2010 National Conference On Communications (NCC)*, pp. 1-5, Jan. 2010.

[4] P. Rai, “A Review of ‘MANET’s Security Aspects and Challenges’,” *International Journal of Computer Applications IJCA*, vol. 4, no. Special Issues in MANET, pp. 162-166, 2010.

[5] F. Xing and W. Wang, “Modeling and analysis of connectivity in mobile ad hoc networks with misbehaving nodes,” in *IEEE International Conference on Communications, 2006*, 2006, vol. 4, no. c, pp. 1879–1884.

[6] J. P. G. Sterbenz et al., “Resilience and survivability in communication networks: Strategies, principles, and survey of disciplines,” *Journal of Computer Networks*, vol. 54, no. 8, pp. 1245–1265, Jun. 2010.

[7] S. Neumayer, G. Zussman, and R. Cohen, “Assessing the impact of geographically correlated network failures,” in *Military Communications Conference, 2008. MILCOM 2008. IEEE,*, pp. 1-6.

[8] M. Bakkaloglu, “On correlated failures in survivable storage systems.”

[9] S. Nath, H. Yu, P. B. Gibbons, and S. Seshan, “Subtleties in tolerating correlated failures in wide-area storage systems,” in *Proc. of the Third USENIX Symp. on Networked Systems Design and Implementation*, 2006, pp. 225–238.

[10] L. Zhang and W. Zhang, “Edge Anonymity in Social Network Graphs,” *2009 International Conference on Computational Science and Engineering*, pp. 1-8, 2009.

[11] W. Gao and G. Cao, “On Exploiting Transient Social Contact Patterns for Data Forwarding in Delay-Tolerant Networks,” *IEEE Transaction on Mobile Computing*, vol. 12, no. 1, pp. 151-165, 2013.

[12] P. Dodds and J. Payne, “Analysis of a threshold model of social contagion on degree-correlated networks,” *Physical Review E*, pp. 1-9, 2009.

[13] J. P. Gleeson, “Cascades on correlated and modular random networks,” *Physical Review E*, vol. 77, no. 4, p. 046117, Apr. 2008.

[14] Z. Kong and E. M. Yeh, “Wireless network resilience to degree-dependent and cascading node failures,” in *Modeling and Optimization in Mobile, Ad Hoc, and Wireless Networks, 2009. WiOPT 2009. 7th International Symposium on*, 2009, pp. 1–6.

[15] Y. Xu and W. Wang, “Characterizing the spread of correlated failures in large wireless networks,” *2010 Proceedings IEEE INFOCOM*, vol. 56, no. 11, pp. 1–9, 2010.

[16] P. De, Y. Liu, S. K. Das, and Y. Street, “Modeling Node Compromise Spread in Wireless Sensor Networks Using Epidemic Theory,” in *Proceedings of the 2006 International Symposium on on World of Wireless, Mobile and Multimedia Networks*, 2006, pp. 237-243.

[17] S. Tang, “A Modified SI Epidemic Model for Combating Virus Spread.pdf,” *International Journal Wireless Infrastructure Networks*, no. 18, pp. 319-326, 2011.

[18] X. Li, T. P. Parker, and S. Xu, “Towards an Analytic Model of Epidemic Spreading in Heterogeneous Systems,” in *The Fourth International Conference on Heterogeneous Networking for Quality, Reliability, Security and Robustness & Workshops*, 2007.

[19] X. I. A. Wei, L. I. Zhaohui, C. Zengqiang, and Y. Zhuzhi, “Dynamic epidemic model of smart phone virus propagated through Bluetooth and MMS,” *IET Conference on Wireless, Mobile and Sensor Networks 2007 (CCWMSN07)*, vol. 2007, pp. 948-953, 2007.

[20] A. Azni, R. Ahmad, Z. Noh, and A. Basari, “Correlated Node Behavior Model based on Semi Markov Process for MANETS,” *Journal of Computer Science Issues*, vol. 9, no. 1, pp. 50-59, 2012.

[21] T. Sundararajan and A. Shanmugam, “Modeling the Behavior of Selfish Forwarding Nodes to Stimulate Cooperation in MANET,” *International Journal*, vol. 2, no. 2, pp. 147-160, Apr. 2010.

[22] S. Wang and J. T. Park, “Modeling and analysis of multi-type failures in wireless body area networks with semi-Markov model,” *IEEE Communications Letters*, vol. 14, no. 1, pp. 6–8, Jan. 2010.

[23] K. Komathy and P. Narayanasamy, “A Probabilistic Behavioral Model for Selfish Neighbors in a Wireless Ad Hoc Network,” *IJCSNS*, vol. 7, no. 7, p. 77, 2007.

[24] H. Andersson, “Epidemics and graphs,” in *Stochastic Epidemic Models and Their Statistical*, Springer New York, 2000, pp. 63-72.