Merging of Epidemic SIR Model and Semi Markov for Correlated Node Behavior in MANETs

A.,H AZNI, RABIAH, AHMAD, ZUL AZRI MOHAMAD NOH

Center for Advanced Computing Technology
Faculty of Information Technology and Communication
University Technical Malaysia Melaka, Melaka, MALAYSIA

Abstract— Correlated node behavior poses a great challenge for normal functioning of mobile ad hoc network. The impact could be devastating if the spreading of correlated node behavior will result in network failure. We model correlated node behavior by merging the principle of epidemic model and semi Markov process. Under merging condition, node behavior transition and epidemic model is converge to capture correlated node behavior. The focus of this work is to predict correlated node behavior spreads to entire network. Through modeling and analysis, the results show general applicability in understanding the spreading rate of correlated node behavior.

Keywords— correlated node behavior, epidemic model, semi Markov Process

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 affects the connectivity and availability of the network [1–3]. Furthermore, misbehave node also affect route discovery by giving fake route information, packets forwarding, and network control message [4–6] which temper network survivability.

In real network scenarios, node behavior shows temporal dependent sequence of event known as correlated behavior resulted from neighboring node activities during routing process. Node may trigger correlated event if the behavior has the capability to influence others such that when a node failed, neighboring node may need to load more traffic originally forwarded by those failed node, and 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 of this correlated event could range from insignificant topological survivability to devastating network shutdown.

In order to deal better with network survivability and provide some guidance for building survivable network in MANETs, there is an urgent need to study the correlated node behavior and identify which factors will influence the spreading behavior. Node correlated behavior can be modeled as spread of epidemic through ad hoc network. However, traditional epidemic models cannot be applied to ad hoc environment because they only consider the static network topology, but the dynamic effects of node behavior such as mobility are not modeled. Thus, correlated node behavior is also modeled based on viewing dynamic behavior of node using Semi Markov process to define node stochastic behavior. The new metrics to measure connectivity dependents behavior known as correlated degree is introduced in the model. Correlated degree can be an indicator on how well the network is connected to the network under correlated behavior situation. 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 II describes related works and Section III explain the behavior of correlated node in MANETs. In Section IV, the paper proposed correlated node behavior model and the model simulation and validation is discussed by experimenting two scenarios of correlated events in section V. Section VI will conclude the paper.

2. Related Works

There are several papers discussing correlated node effects in various contexts. In [7] 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 [8]; where correlated failures are modeled based on datasets using conditional probabilities and the beta-binomial model. A tunable failure correlation model is reported in [9] that allows different correlation levels in failures based on the traces. In [10], 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 [11] and [12] that is capable of incorporating the possible dependencies among successive software runs. None of the works above discuss the propagation of the correlated behavior such as node failures and their effects on survivability. In this work, we take epidemic model as a basis of node propagation to show node's correlated behavior. The works [13] 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 behavior and their effects on network connectivity, however, they do not provide a systematic stochastic approach to model correlated node behavior to evaluate spreading rate of correlated behavior.

3. Correlated Node Behavior

In order to model the correlated behavior of mobile node, the characteristic of node behavior is describe first and epidemic spreading on mobile node is derived. Then parameters which influence the spread speed of the epidemics are studied.

3.1. Node Behavior

To understand how nodes are correlated in ad hoc network, the characteristic of dynamic node behavior and its state transition is discussed in which it will be used to quantify correlated event in epidemic theory. Unlike node behavior describes in similar work on mobile epidemic, node behavior describe in this paper focus on its activity in routing process such as packet forwarding, energy consumption and transmission radio. Based on its routing activity, node behavior is characterized as cooperative, selfish, malicious and fail node. Table 1 shows node behavior and its characteristic.

TABLE I: NODE BEHAVIORS AND ITS 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.

Node dynamically and arbitrarily changes its behavior. For example cooperative node (*c*) is exposed to change its state behavior to either selfish, malicious or fail state. This may happened due to energy exhaustion, misconfiguration, being compromised, power depletion or out of transmission (Sundararajan, Shanmugam, 2010). However, it is also possible to convert node operating at selfish state to be cooperative again by means of proper configurations. On the other hand, once node is at malicious (*m*) state, it only can become a failed node (*f*), and 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. Fig. 1 specified node behavior state transition diagram.

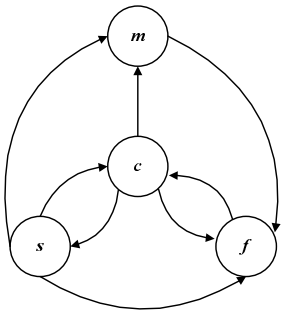

Fig. 1: Node Behavior Transition

3.2. Correlated Even

When correlated event is attempted in ad hoc network, the epidemics may spread through the following ways:

- Endogenous – The event caused by the node itself with some probability at every time step. This is also the initial start of correlated event when node changes from cooperative behavior to either selfish, malicious or fail node due to factors described above.

- Exogenous – The event is graph-based transition affected only by the neighbors of the infected nodes. For example, node may trigger correlated event if the behavior has the capability to influence others such that when a node failed, neighboring node may need to load more traffic originally forwarded by those failed node, and might become failed faster due to excessive energy consumption.

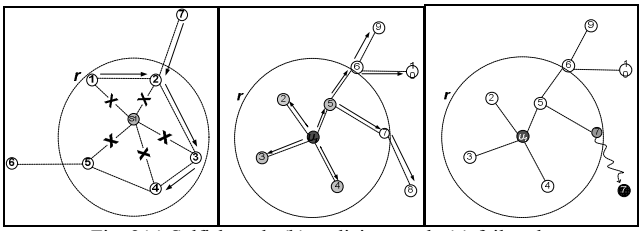

Fig. 2(a) Selfish node (b) malicious node (c) fail node

Fig. 4.2(a) (b) (c) illustrated how initial node could start the correlated event in ad hoc network. The correlated events influences by many factors. It is mostly determined by the current status of neighboring nodes. The most influential factors of node status are packet ratio, energy resources, and mobility. Example of energy factor is when node operating at selfish state, its residual energy drops below threshold level.

Then, it will drop all the forwarding packets and disconnected or become failed node. This behavior resulted from its own self activity (endogenous), thus it has a capability to create correlated event by infecting neighboring nodes (exogenous). Fig. 2(a) illustrates an example of correlated event 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 [17]. 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 may fail faster. If node *2* failed, all nodes in the transmission range unable to establish any communications with other nodes at a distance of more than one-hope away.

An example of malicious node is an increase of packets ratio (DoS attack) as illustrated in Fig. 2(b). In this example, the initial attack occurs at node u_1. 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 Fig. 4.2(b), resulted from packet injection from node u_1 , then 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. 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.

The loss packets resulted in fail node [18]. It can be due to battery depletion or mobility factors. Both factors give the same effect to topology changes. In most cases, selfish and malicious node dies out and removes from the network. The failed node has the same effect as selfish node as illustrated in Fig. 2(c).

4. The Model

In this section, a comprehensive model of correlated node behavior in MANETs is described which consider the influence of various factors mentioned in Section III. For convenience, the basic model of node behavior using Semi-Markov process to characterize node behavior transitions is described first. The model is important to describe the endogenous factors that initiated the correlated event. Next, using SIR (susceptible-infective-removed) epidemic model, the correlated event is derived to show correlated behavior of node in MANETs.

4.1. Stochastic Property of Endegenous Node Behavior

Based on node behavior describe above, Semi-Markov process is used to model stochastic node behavior transitions and analyzed the stochastic properties of correlated node behavior in epidemic theory. State space is defined as $\Omega = \{c(cooperative), s(selfish), m(malicious), f(Failed)\}$ and model node behavior transition by a stochastic process $\{Z(t)\}$ associated with space Ω. The semi-Markov process denoted by:

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

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 [19]. Thus, By Collolary 9-11 (pp 325) in [5] it is known 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:

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

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

$$\mathbb{P} = \begin{pmatrix} 0 & A & C & D \\ B & 0 & C & D \\ 0 & 0 & 0 & D \\ B & 0 & 0 & 0 \end{pmatrix} \tag{3}$$

where $P_{ii} = 0$ means that it is not possible to make transition between the two states based on the rules specify in Section III. 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 the time spend from state i to j is determined 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:

$$\mathbb{F} = \begin{pmatrix} 0 & F_A(t) & F_C(t) & F_D(t) \\ F_B(t) & 0 & F_C(t) & F_D(t) \\ 0 & 0 & 0 & F_D(t) \\ F_B(t) & 0 & 0 & 0 \end{pmatrix} \tag{4}$$

The state transition diagram of semi Markov node behavior model is shown in **Error! Reference source not found.**3.

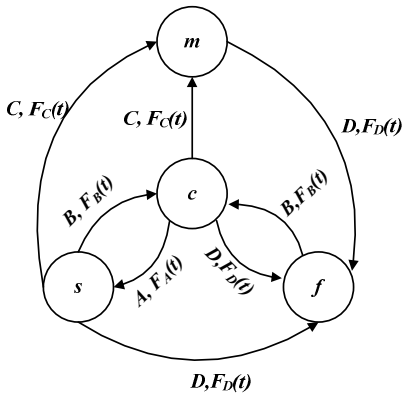

Fig. 3 Semi-Markov Processes for Node Behavior

Error! Reference source not found. 3 explain that at each discrete time step, node *u* changes its state based on the following probability:

A=probability of dropping → transition from state *c* to *s*
B=probability of forwarding → transition from *s* to *c* and *f* to *c*
C= probability of injecting → transition from *c* to *m*
D= probability of loss → transition from *c* to *f*, *m* to *f* and *s* to *f*

The steady-state transition probability distribution $\tilde{\pi}$ can then be derived by solving the following set of equations:

$$\tilde{\pi} = \tilde{\pi} P, \sum_{i \in \Omega}^{N} \pi_i = 1, \qquad \pi \geq 0,$$

$$E[T_i] = \sum_{j \in \Omega} P_{ij} E[T_{ij}]. \tag{5}$$

Given the fraction of time $\widetilde{\pi}$ that the node stays in each state and the sojourn times $E[T_i]$ for each state, it is easy to calculate P_i, the status of the node staying in transmission radius ***r*** *as*:

$$P_i \triangleq \lim_{t \to \infty} P_{ij}(t) \frac{\pi_i E[T_i]}{\sum_j^N \pi_j E[T_j]} \tag{6}$$

4.2. SIR-Epidemic Model

In this section, SIR is used to model correlated event of node behavior in MANETs. Correlated event can me mathematically describe as a time-dependent point process of $X_n(t)$, where $X_n(t)$ follow consecutive action at t_i and t_{i+1}. The concept of disease infection in epidemic theory using susceptible-infection-removed (SIR) is used to identify correlated node behavior in MANETs. Consider population of nodes *N* in MANETs will be in either one of three correlated events: susceptible (*S*), infection (*I*) or removed (*R*). In this context "removed" means fail node and no longer active in the network. It is also assumed that, once nodes enter removed events, it will not consider being in the network again.

Traditional SIR model, such as Kermack-McKendrick model [20], does not consider the uniqueness of dynamic behavior in mobile nodes. Thus, SIR model is modified to fit the characteristic of node behavior in MANETs such as energy consumption and node mobility. These characteristics have caused the main implication to node behavior transition and triggered correlated event. Thus, SIR rate is uses to denote susceptible rate δ_{uv}^{c} , infection rate β_{uv}^{s} and β_{uv}^{m}, if correlated event are resulted from selfish and malicious node respectively. On the other hand, λ_{uv}^{s} and λ_{uv}^{m} are used to denote remove event either fail due to selfish behavior or malicious node. The Events in SIR follow the current state of node behavior which is determined by equation (6). Then, SIR rate is derived within adjacent nodes in ad hoc network. Two nodes have a link if they are within transmission range ***r***. 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 v, i.e., $N_u = \{u | (u, v) \in E\}$. Consider undirected and weighted networks, in which case the adjacency matrix is symmetric with elements $a_{uv} = \omega(e)$ where weight function $\omega(e)$ represent SIR rate of adjacent node *u*. SIR rate are derived as:

$$\begin{aligned} \beta_{u,v} &= \pi_{i=s,m}^{u} \pi_{j \in \Omega}^{v} \\ \lambda_{u,v} &= \pi_{i=f}^{u} \pi_{j \in \Omega}^{v} \\ \delta_{u,v} &= \pi_{i=c}^{u} \pi_{j \in \Omega}^{v} \end{aligned} \tag{7}$$

Adjacent matrix of node *u* can be subsequently computed by constructing correlated transmission matrix (CTM) using equation (3-4). In order to formulating correlated transmission matrix, let *u* and *v* are two nodes connected in a network. The corresponding CTM for node *u* and node *v* are given below:

$$\begin{aligned} \mathbb{F}_u &= \begin{pmatrix} 0 & F_A(t) & F_C(t) & F_D(t) \\ F_B(t) & 0 & F_C(t) & F_D(t) \\ 0 & 0 & 0 & F_D(t) \\ F_B(t) & 0 & 0 & 0 \end{pmatrix} \\ \mathbb{F}_v &= \begin{pmatrix} 0 & F_A(t) & F_C(t) & F_D(t) \\ F_B(t) & 0 & F_C(t) & F_D(t) \\ 0 & 0 & 0 & F_D(t) \\ F_B(t) & 0 & 0 & 0 \end{pmatrix} \end{aligned} \tag{8}$$

Then, let $\{\delta_{uv}^{c}, \beta_{uv}^{s}, \beta_{uv}^{m}, \lambda_{uv}^{s}, \lambda_{uv}^{m}\}$ be a weighted function indicates the SIR rate of node behaviors. Denote π_i the probability of being in steady state. If the state space is finite, then the equation in (5) can be solve to obtain π_i. The status of a node at current *t* time is given by equation (6). Let $v = \{1, 2, ...n\}$, CTM is s constructed as:

$$CTM = \begin{bmatrix} F_{i1} & 0 & \dots & 0 \\ 0 & F_{i2} & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & F_{in} \end{bmatrix} \text{ and} \tag{9}$$

Parameter	Setting
Simulation area	1000 *m* x 1000 *m*
Transmission range	200 meter
Mobility model	Random Way Point
Movement features	Avg. speed 2 *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 minutes

$$a_{uv} = \begin{bmatrix} 0 & \omega_{12} & \dots & \omega_{1n} \\ \omega_{21} & 0 & \dots & \omega_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ \omega_{n1} & \omega_{n2} & \dots & 0 \end{bmatrix}$$

Then correlated degree of adjacent node *u* within transmission radius ***r*** is obtained:

$$\psi = \sum_{v=n} a_{uv}(t) \tag{10}$$

Let $S_k(t), I_{sk}(t), I_{mk}(t)$ and $R_k(t)$ 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 constant N, such that $S(t) + I_s(t) + I_m(t) + R(t) = N$ for all t. The infective nodes contact with d node degree and weight function $\omega(e) > 0$. Then, the basic differential equations that describe the rate of change of SIR rates are given by

$$\frac{dS(t)}{dt} = -\sum_{i=s,m} \beta_{uv} P_i(d)$$

$$\frac{dI_s(t)}{dt} = \left(\sum_{i=s} \beta_{uv} P_i(d)\right) - \sum_{i=c} \delta_{uv} P_i(d)$$

$$\frac{dI_m(t)}{dt} = \left(\sum_{i=m} \beta_{uv} P_i + \sum_{i=c} \gamma_{uv} P_i(d) - \sum_{i=c} \delta_{uv} P_i(d)\right. \tag{11}$$

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

Equation (11) is specially derived to take into account the change of rate of correlated node rather than individual node as in previous SIR model. Thus, correlated event can predict the spreading behavior of correlated node in MANETs.

5. Perfomance Evaluation

5.1. Simulation Setup

To evaluate the correctness of correlated node behavior model, an exhaustive simulations in the simulation tool ns2 (v2.35) and series of numerical experiments in MATLAB (7.10a) were conducted. In simulation, all network parameters are set to the default value given in TABLE2 below.

TABLE II. THE NETWORK SIMULATION SET UP

Considering MANETs environment 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 **r**. IEEE 802.11 is used for medium access control and AODV is used as the routing protocol. The time step used is 300 minutes to simulate the scenario. In simulations, nodes change their behaviors according to the energy resources available for their own use and forwarding packet ratio. 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, neighborhood statistics of each node per 10 seconds were collected, including the number of neighbors and behavior of each neighbor. 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, the number of susceptible infected and remove node from the network can be obtained.

5.2. Correlated Node Behavior Analysis

Correlated event is determined by the current status of node. At time *t* node status P_i is determine using equation (6). To calculate $P_i(i \in \Omega)$, TPM from semi Markov node behavior model is obtained using data collected from simulations.

$$\mathbb{P} = \begin{pmatrix} 0 & 0.525 & 0.071 & 0.404 \\ 0.756 & 0 & 0.022 & 0.022 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{pmatrix}$$

The steady state is

$$\tilde{\pi} = < 0.4524, 0.2375, 0.0373, 0.2728 > .$$

Then, $E[T_{ij}]$ can be calculated using equation (5). Since P_{ij} are known already, $E[T_i]$ are calculated as:

$$E[T_C] = 142.2, E[T_S] = 45.9, E[T_M] = 51.7, E[T_F] = 60.$$

Last, the value of P_i is obtained using equation (6),

$$P_C = 0.6877, P_S = 0.1167, P_M = 0.0207, P_F = 0.1750.$$

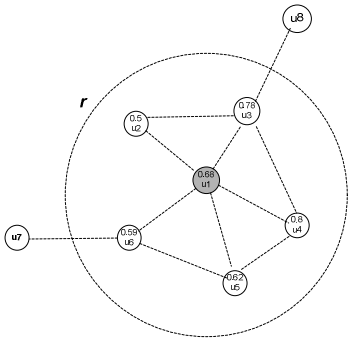

Fig..4: Susceptible Event

From P_i, it is shown that the node status is highly in cooperative state with probability of 68%. For each adjacent node *u*, the status is obtained the same method to get P_i. Let use Fig. 4 as an example of node topology in transmission radius *r*. At time *t=(0)*, all nodes are in cooperative state. Using SIR mapping in equation (9), CTM and a_{uv} is obtained for all adjacent nodes *u*. Adjacent node *u* is in cooperative state, then using equation (10), correlated degree is $\psi_{u_1,v} = 2.27$.

$$CTM_{uv} = \begin{bmatrix} 0.68 & 0 & 0 & 0 & 0 & 0 & \\ 0 & 0.5 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0.78 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0.8 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0.62 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0.59 & 0 \end{bmatrix} \text{ and}$$

$$a_{uv} = \begin{bmatrix} 0 & 0.38 & 0.53 & 0.54 & 0.42 & 0.4 \\ 0.38 & 0 & 0.39 & 0 & 0 & 0 \\ 0.53 & 0.39 & 0 & 0.62 & 0 & 0 \\ 0.54 & 0 & 0.62 & 0 & 0.5 & 0 \\ 0.42 & 0 & 0 & 0.5 & 0 & 0.37 \\ 0.4 & 0 & 0 & 0 & 0.37 & 0 \end{bmatrix}$$

According to connectivity theory in ad hoc network [21] high connectivity means low isolation and high accessibility, whereas low connectivity resulted in high isolation and low accessibility. Thus, this shows that the nodes u_1 is connected with high rate of cooperative node in transmission ***r***. Following theory of connectivity in transportation system [22], the value reflected that node u_1 is a central of routing activity. This is also true as node u_1 connected to all nodes in transmission ***r***. Another observation is that, node u_2 and u_6 shows the weakest link in the network with $\delta_{uv} = 0.77$. This is because, the chances of node changes it state to selfish or failed state is higher compared to other adjacent nodes.

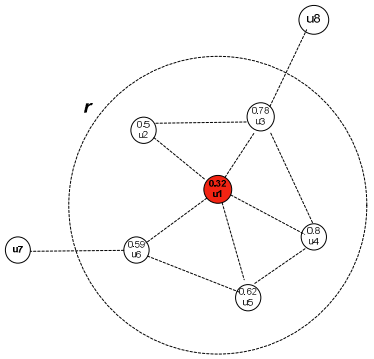

Fig. 5: Infection (Selfish) event

To see the effect of selfish node, at time *t=(0),* node u_1 as in Fig. 5 is set as selfish node and the simulation were run again to get the value of P_i. The same process were derived to obtain CTM and a_{uv} as in susceptible event. The correlated degree due to selfish node is $\psi_{u_1,v} = 1.06$. Then, the change of rate from susceptible event to infection (selfish) event is ≈ 0.5. The effect is quite noticeable as node u_1 is a central of routing activity and all the packets connecting to u_1 have to reroute to adjacent node. It can also be seen that, node u_2 and u_6 might get affected first from selfish behavior as P_i is low. It is worth to point out that, after node u_1 become selfish, node u_3 is a critical node as the node becomes the central activity of node in transmission *r* and also act as a gateway to next cluster. The selfish infection cause by node u_1 decrease its correlated degree by ≈ 0.4. In the next experiment using the same topology graph, malicious node is set at node u_1. From CTM and a_{uv}, correlated degree due to malicious node is $\psi_{u_1,v} = 0.97$ and change of rate from susceptible to infection (malicious) is ≈ 0.6. Compare to selfish node, malicious node experiencing fast infection time once it gets infected.

Fig. 6 and Fig. 7 depicted the trend that the number of nodes in different events changes with time. From the figures., the result shows that the number of infectious nodes rapidly increases at initial spreading then quickly decrease as the node fail or removed. However, number of susceptible nodes keeps decreasing since the node did not consider being in cooperative again after being removed. Notice that, malicious node stay longer in the network compared to selfish node and it keep launching an attack until it dies out. It can be concluded that correlated malicious node impact network connectivity severely.

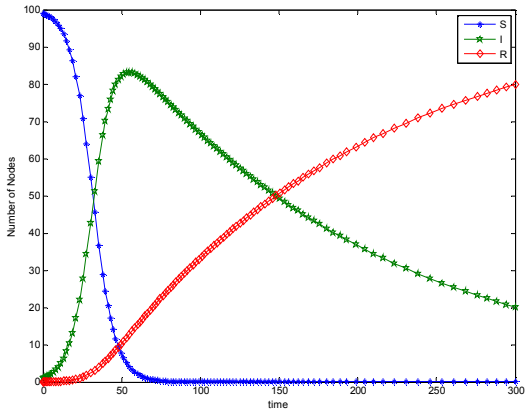

Fig. 6 Selfish Event with $\beta_s = 0.5$,$\gamma_s = 0.2$ and $k = 5$

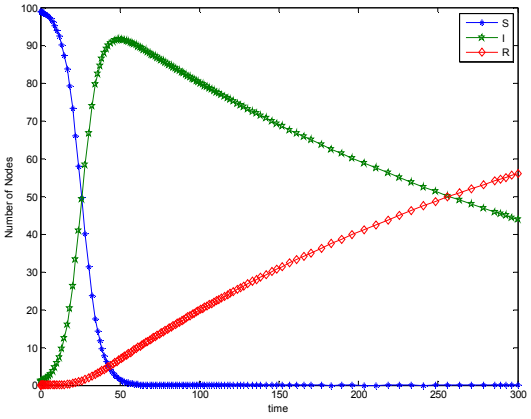

Fig. 7 Malicious Event $\beta_m = 0.6, \gamma_m = 0.1$ and $k = 5$

5.3. Network Parameters Analysis

The simulation were conducted three times by *d=2, d=3* and *d=5*, respectively. The simulation result are shown in Fig. 8 for selfish node and Fig. 9 for malicous node. Both scenario shows the same pattern that the bigger the value of *d*, the earlier the beginning time of the fast spread of correlated node behavior is. Additionally, the bigger *d* is, the bigger the maximal number of infected nodes is.

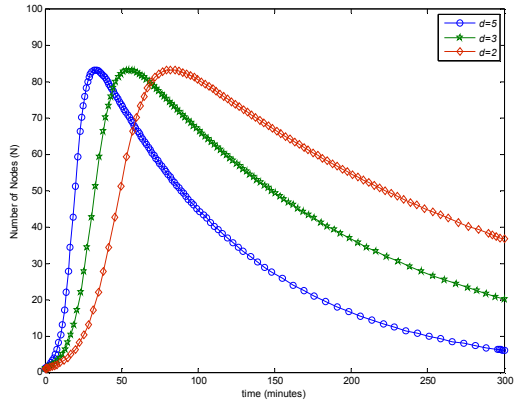

Fig. 8 Selfish node $\beta_s = 0.5$,$\gamma_s = 0.2$ vs. *d*

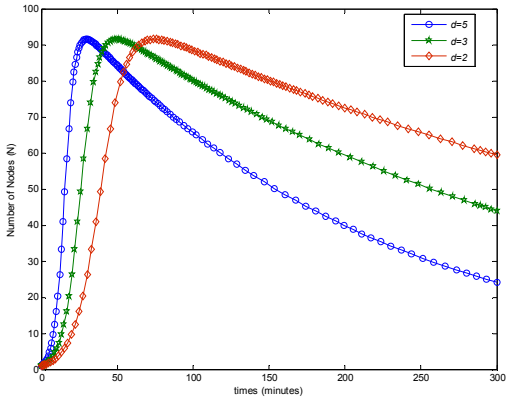

Fig. 9: Malicious Node $\beta_m = 0.6, \gamma_m = 0.1$ vs. *d*

b) Mobility

To evaluate the impact of node mobility on correlated degree, the simulation conducted using two different speeds: 20 m/s and 2 m/s with random-waypoint mobility model. Simulation result for both infection events (selfish and malicious) are shown in Fig. 10. The mobility of nodes does affect correlated degree considerably as it directly increase the energy consumption as well as dropping ratio which affect the value of P_i. The higher the mobility is, the lower the value of correlated degree in which increase infection rate. Comparing the result with selfish and malicious node, infection rate for selfish has increase to from 0.5 with 2m/s to 0.7 with 20m/s. To explain this scenario, the fact that the faster a node moves, the sooner it will travels across boundary which results in node failure and decrease node time spent in the network. As for malicious node, increase in speed gives a chance to malicious node to infect neighboring nodes faster.

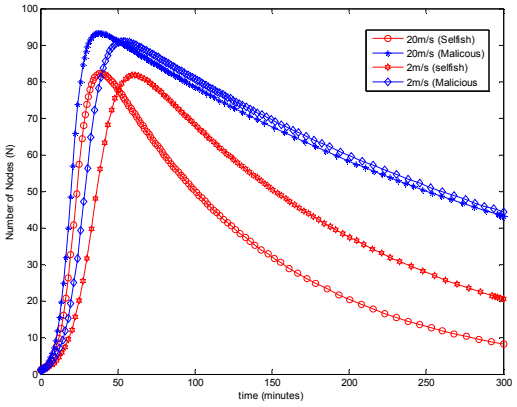

Fig. 10 Selfish and malicious node vs. mobility

c) Initial Energy

Nodes in MANETs rely on limited power resources to perform routing activity. To see the effect of initial energy, the second experiment with new initial power has been conducted with an increase from 100 Ws s to 200 W s. In Fig. 11, there is a slight increase of cooperative node in the network. This is

consistent with the intuition in [5] that a higher energy will increase node lifetime. Increase energy has lead to node acting cooperatively for longer period.

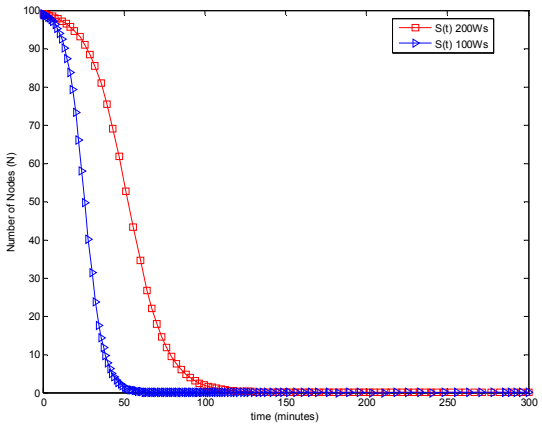

Fig. 11 The effect energy towards Susceptible Event

However, the increase of energy actually prolonged the lifetime of malicious node and slightly reduces the correlated degree because of an increase in infection rate. This can be seen in Fig. 12, node with higher energy will remain in malicious state and continue spreading correlated event. This is dangerous situation as the node may impact network survivability severely.

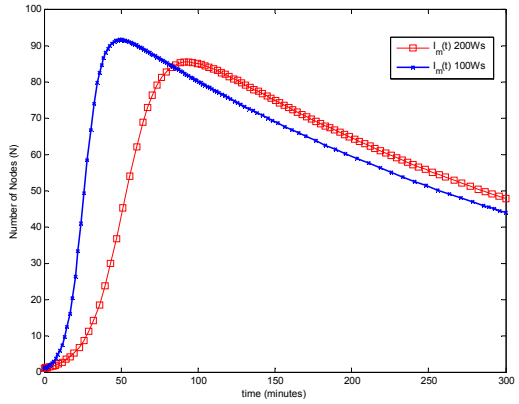

Fig. 12 The effect of energy to Infective Event (Malicious Node)

5.4. Model Validation

An extensive simulation of epidemic spread to validate the correlated node behavior model and check with analytic results have been performed. Data from simulation is compared with Weibull distribution for analytical data. Weibull distribution is widely use in reliability engineering to model lifetime distribution. $F_A(t)$ is considered as selfish cumulative distribution function (cdf) and $F_C(t)$ is malicious distribution function (cdf). The Weibull function used in this paper is known as the two-parameter Weibull distribution, define as

$$W(\alpha, \beta) = 1 - exp(-(t/\beta)^{\alpha}) \quad (12)$$

where α and β are usually called the slope (or shape) parameter and scale parameter, respectively. From simulation result, average transition from cooperative to selfish and from cooperative to malicious are $\approx 45s$ and $\approx 51s$, respectively. If let $\alpha_A = 0.5$ and $\alpha_c = 0.6$, then $\beta_A \approx 9$ and $\beta_C \approx 19$. From Fig. 13 and 14 clearly shows that Weibull function in equation (12) match with simulation results. The $S(t)$ plots show clearly how likely a node is surviving after a certain time. Further, the distribution can also be used to estimate the number of cooperative nodes. For example in Fig. 14, the probability that a node still in cooperative state within 50 minutes is 0.1, which also implies that 90% of nodes will become selfish within 50 minutes if they are compromised. On the other hand, at about 50 minutes, 100% of nodes become malicious node and the entire network is compromised. From the analysis, the spreading of correlated node behavior in malicious state is faster once more nodes are in infected state. Therefore, these accumulated malicious attacks may impact network connectivity severely and isolate more and more nodes. In the case of selfish node, the spreading time is less than malicious node; however, selfish node is capable to create severe network portioning due to node failure from energy depletion.

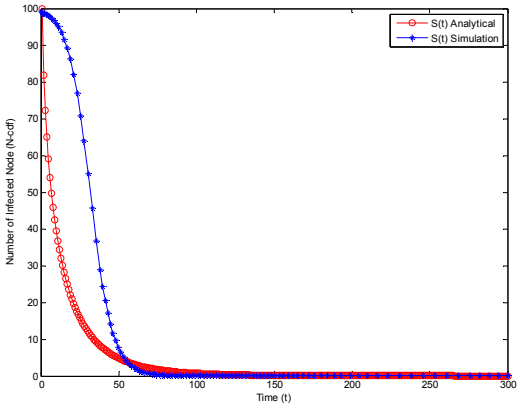

Fig. 13: Probability of nodes become selfish nodes

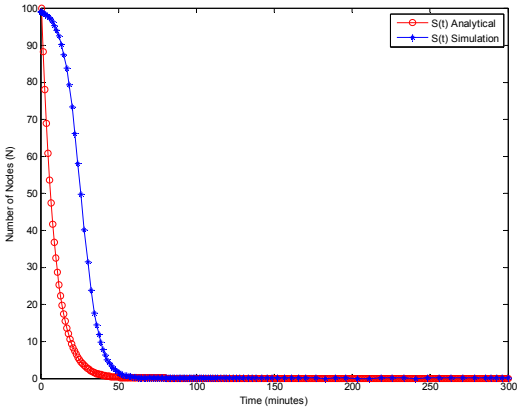

Fig. 14: Probability of nodes become malicious nodes

6. Conclusion

In this paper, stochastic correlated node behavior model is studied which enable the efficient simulation of realistic scenarios of correlated node behavior for dynamic network topology in ad hoc networks. Then correlated degree is developed based on disease spreading in SIR model 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. Numerical analysis results are provided to demonstrate the validity of the model. As future work, more other factors will be considered to measure the impact of the correlated behavior in these networks, such as security limitation.

Acknowledgment

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.

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," in *Proceedings of the 12th IEEE Mediterranean Electrotechnical Conference (IEEE Cat. No.04CH37521)*, 2004, pp. 579–582.

[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, D. Hutchison, E. K. Cetinkaya, A. Jabbar, J. P. Rohrer, M. Schöller, and P. Smith, "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] M. Rahnamay-Naeini, M. Hayat, and J. Pezoa, "Modeling Stochastic Correlated Failures and their Effects on Reliability of Distributed Computing Systems," in *Proceedings of The International Conference on Computer Communications and Networks iEEEE (ICCCN)*, 2011, pp. 1–6.

[8] M. Bakkaloglu, "On correlated failures in survivable storage systems," 2002.

[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] T. Thanakornworakij, R. Nassar, C. B. Leangsuksun, and M. Paun, "The Effect of Correlated Failure on the Reliability of HPC Systems," *2011 IEEE Ninth International Symposium on Parallel and Distributed Processing with Applications Workshops*, pp. 284–288, May 2011.

[11] N. Ning and B. Yang, "Software Reliability Models Based on Markov Renewal Process," *Journal of Science And Technology*, pp. 1–9, 2007.

[12] Y. Dai and M. Xie, "Modeling and analysis of correlated software failures of multiple types," *IEEE Transactions on Reliability*, vol. 54, no. 1, pp. 100–106, 2005.

[13] 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.

[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] 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.

[16] 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.

[17] Z. Kong and E. M. Yeh, "Percolation processes and wireless network resilience," in *Information Theory and Applications Workshop, 2008*, 2008, pp. 461–470.

[18] T. H. Kim, D. Tipper, and P. Krishnamurthy, "Connectivity and critical point behavior in mobile ad hoc and sensor networks," in *IEEE Symposium on Computers and Communications, 2009. ISCC 2009.*, 2009, pp. 153–158.

[19] 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.

[20] F. Brauer, "Models for the spread of universally fatal diseases," *Journal of Mathematical Biology*, vol. 28, no. 4, Jun. 1990.

[21] Alenazi, M. J. F, Rohrer, J. P, Sterbenz, and J. P. G, "Topology Connectivity Analysis of Internet Infrastructure Using Graph Spectra," in *IEEE/IFIP Fourth International Workshop on Reliable Networks Design and Modeling (RNDM'12)*, 2012, pp. 752–758.

[22] J.-P. Rodrigue, C. Comtois, and B. Slack, *The Geography of Transport Systems (Google eBook)*. Routledge, 2009, p. 352.