Modeling and Analysis of Connectivity in Mobile Ad Hoc Networks with Misbehaving Nodes

Fei Xing Wenye Wang
Department of Electrical and Computer Engineering
North Carolina State University, Raleigh, NC 27695, USA
fxing@ncsu.edu, wwang@ncsu.edu

Abstract— **Mobile ad hoc networks are vulnerable to malicious attacks and failures due to their unique features, such as node mobility and dynamic network topology. The design and evaluation of routing protocols and topology control require sound analysis on network connectivity and node behaviors. However, little work has been done on how node misbehaviors affect network connectivity. Modeling and analysis of node misbehavior involves many challenges such as multiple failures caused by selfishness, mobility, and potential Denial of Service attacks. Thus, we propose a novel model to characterize node misbehaviors based on a semi-Markov process. In particular, we analyze the impact of node misbehavior on network connectivity in a mobile ad hoc network stochastically. Numerical results based on analysis and simulations are provided to demonstrate the effectiveness of our approach and results.**

I. Introduction

Compared with wired networks, mobile ad hoc networks are more vulnerable to malicious attacks as well as failures due to their unique features, such as stringent power constraints, error-prone communication media and highly dynamic network topology, which have posed a number of nontrivial challenges to the applications of mobile ad hoc networks. Significant research works have been done to investigate mobile node misbehaviors [1], [8], [12] and ad hoc network connectivity [10], [3], [6]. However, little research efforts were made to analyze to what extent these node misbehaviors can impact the connectivity of mobile ad hoc network quantitatively, which is the problem that we will address in this paper. The answer to the problem will considerably help us to understand various research problems, such as the design of fault-tolerant routing protocols and analysis of ad hoc network performance, thoroughly. Nevertheless, since mobile ad hoc networks are complex and dynamic systems, and the effects resulting from misbehaving nodes cannot be ignored, an in-depth study on the impact of node misbehaviors is quite challenging due to the multiple failures caused by node mobility, energy depletion and Denial of Service (DoS) attacks.

In this paper, we first provide a formal classification of node behaviors, then use a semi-Markov process to characterize the behaviors of mobile nodes. In our node behavior model, a mobile node may change its behaviors among four states, i.e., *cooperative, selfish, malicious* and *failed* according to an embedded Markov chain, while the transition time between two states is not necessarily exponentially distributed. Furthermore, based on the stochastic properties of the model, we analyze the problem of node isolation due to misbehaving node neighbors and obtain the probability that an ad hoc network keeps connected in the presence of misbehaving nodes finally.

The remainder of this paper is organized as follows. In Section II, we present related works on node misbehaviors and network connectivity analysis. In Section III, we define *network connectivity* and formulate the problem of network connectivity in the presence of misbehaving nodes. In Section IV, we model node behaviors by a semi-Markov process and analyze the stochastic properties of the model. In Section V, we derive the probability of the network connectivity by considering node isolation issue. In Section VI, we validate our analytical results by simulations, followed by conclusions in Section VII.

II. Related Work

Yang et al in [13] presented a good overview of potential attacks which may impact network performance and proposed a concept called *resiliency-oriented* security design. Among all security threats, we are most interested in DoS attacks, since they may have devastating influence on the network survivability. Aad and Hubaux in [1] studied a novel DoS attack perpetrated by relay nodes called *JellyFish* and a well-known attack called *Black Hole*. Hollick and Schmitt in [8] also showed that malicious attacks, especially *Black Hole*, can harm ad hoc networks more than node failures.

Besides the analytical studies on DoS attacks analysis, significant research efforts were made to analyze the connectivity of ad hoc networks as well. Li and Wan in [10] presented a localized method to control network topology such that the resulting topology is tolerant to failures with fewer communication links maintained. Bettstetter in [3] thoroughly investigated the connectivity of wireless multihop networks and analyzed the maximum number of failed nodes that a multihop wireless network can sustain so that the network still keeps connected.

Meanwhile, some schemes were proposed to make ad hoc network resilient to node failures or DoS attacks, such as the on-demand routing protocol proposed in [2], which provides resilience to byzantine failures, and the study of SCTP in mobile ad hoc networks with particular emphasis on the DoS resistance [9]. However, none of these works endeavored to reveal the quantitative impact of node misbehaviors and failures on the connectivity of a mobile ad hoc network.

1-4244-0355-3/06/$20.00 (c) 2006 IEEE

III. Network Model and Problem Formulation

A mobile node can become a failed node for many reasons, such as moving out of the transmission ranges of its neighbors, exhausting battery power, malfunctioning in software or hardware, or even leaving the network. Besides these potential failed nodes, each ad hoc network is composed of some cooperative nodes and misbehaving nodes, which are *active* in terms of their participation in the route discovering operation. In this paper, we categorize mobile nodes into two disjoint sets, *failed nodes* and *active nodes*, and represent a mobile ad hoc network with only active nodes by $\mathcal{M}_A$. Next we define the network connectivity formally.

Definition 1: (*Network Connectivity*) A mobile ad hoc network $\mathcal{M}_A$ is k-connected $(k \geq 2)$ if for each node pair there exist at least k mutually independent paths (or k node-disjoint paths) connecting them. For a k-connected network $\mathcal{M}_A$, the maximum value of k is defined as the *connectivity* of $\mathcal{M}_A$, denoted by $\kappa(\mathcal{M}_A)$ [4].

Then we formulate the problem of *network connectivity to misbehaving nodes (NCMN) problem* as: *Given a mobile ad hoc network $\mathcal{M}_A$ with a number of active nodes N_a, what is the probability that $\mathcal{M}_A$ can keep k-connected*, i.e., $Pr(\kappa(\mathcal{M}_A) = k \mid N_a)$? We identify the following steps to solve the NCMN problem:

1) The evolution of a node's behavior should be described properly such that the stochastic properties of the node behavior can be found.
2) The node isolation resulting from misbehaving nodes should be analyzed thoroughly such that the condition for node's being connected can be drawn.

The NCMN problem describes the possibility that an ad hoc network can survive in a hostile environment with failures and security attacks, so its solution will have a profound contribution to a variety of research topics, such as fault-tolerant routing design, resilient-oriented secure application, multihop wireless network performance evaluation, and mobility and topology management.

IV. Node Behavior Modeling

In this section, we use a semi-Markov process to model the evolution of node's behavior, then analyze the stochastic properties of node behaviors.

A. Semi-Markov Node Behavior Model

Since malicious and selfish nodes may not forward packets properly, they are not considered as cooperative in this paper, then the behaviors of mobile nodes are classified as follows:

- *Cooperative Nodes* are active in route discovery and packet forwarding, but not in DoS attack launching.
- *Failed Nodes* are not active in route discovery.
- *Selfish Nodes* are active in route discovery, but not in packet forwarding and DoS attack launching.
- *Malicious Nodes* are active in route discovery and DoS attack launching.

Notice the fact that a mobile node is more inclined to be failed due to energy consumption over time, we find that the probability that a node changes its behavior is dependent on time. Therefore, the revolution of node behaviors cannot be simply described by a *Markov chain* because of its time-dependent property. We propose a node behavior model in this paper by a *semi-Markov process*, denoted by $Z(t), t \geq 0$, with a state space $\mathcal{S} = \{C\ (cooperative),\ S\ (selfish), M\ (malicious),\ F\ (failed)\}$. $Z(t)$ is determined by two matrices, $\mathbb{P} = (p_{ij})$ and $\mathbb{F}(t) = (F_{ij}(t))$, where p_{ij} is the transition probability of a node's behavior becoming state j from i, while $F_{ij}(t)$ is the distribution function of the time spent from state i to j. Fig. 1 depicts the node behavior model defined above.

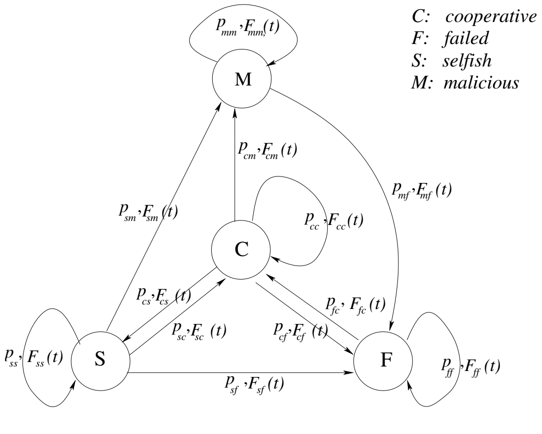


Fig. 1. Semi-Markov Process for Node Behavior.

B. Stochastic Properties of Node Behavior Model

In particular, we are interested in the probability that $Z(t)$ is in a certain state i, i.e., $P_i \triangleq \lim_{t\to\infty} P(Z(t) = i|Z(0) = j)$. Nevertheless, the existence of the limiting distribution needs to be verified.

From Fig. 1, we can see that the *embedded* Markov chain of $Z(t)$, denoted by X_n, has a finite state space $\mathcal{S}$, and in X_n each state can reach other states within finite steps and itself within one step. Thus, X_n is *irreducible* and *ergodic*. By *Corollary 9-1 (pp. 325)* in [7], we know that $Z(t)$ is *irreducible*. Next, let μ_{ij} denote the expected transition time from state i to j, since node behaviors change within finite time, then $\mu_{ij} < \infty$ holds $\forall i, j \in \mathcal{S}$. If let μ_i denote the expected holding time in state i, we have $\mu_i = \sum_{j\in\mathcal{S}} p_{ij}\mu_{ij}$. Thus, $\sum_{i\in\mathcal{S}} \mu_i < \infty$ holds, which implies that $Z(t)$ is also *positive recurrent* by *Theorem 9-2 (pp. 325)* in [7]. Therefore, by *Theorem 9-3 (pp. 327)* in [7], the limiting distribution can be obtained by:

$$P_i \triangleq \lim_{t\to\infty, \forall j\in\mathcal{S}} P(Z(t) = i|Z(0) = j) = \frac{\pi_i \mu_i}{\sum_{j\in\mathcal{S}} \pi_j \mu_j}, \quad (1)$$

where π_i is the stationary probability of state i of X_n.

In order to calculate π_i and μ_i in (1), we must obtain transition probabilities p_{ij} and transition time distributions $F_{ij}(t)$, which are described as follows.

1) Transition Probabilities: To determine p_{xf} $(x \in \{C, S, M\})$, we consider both energy consumption and node mobility behavior, which are characterized by an average node lifetime, $\overline{T}_{life}$, and average node residence time, $\overline{T}_{in}$, respectively. To determine p_{xm} ($x \in \{C, S, F\}$), we assume an attack model in which an attacker chooses k_a out of total N nodes as victims with probability q_a and needs an average time of $\overline{T}_{attk}$ to compromise these victim nodes. Notice that a failed node is not affected by attacks, we apply the attack model to cooperative and selfish nodes only. To determine p_{xs} ($x \in \{C, M, F\}$), we assume that malicious and failed nodes will not become selfish. As for cooperative nodes, they are assumed to turn off the packet forwarding function if their residual energies drop below $1/\eta$ of their initial energies, so that they become selfish at time $T_{TS} = \frac{\eta-1}{\eta} \cdot \overline{T}_{life}$. To determine p_{xc} ($x \in \{S, M, F\}$), we assume that a cooperation stimulating mechanism such as *nuglet counter* [5] is used, where each selfish node possesses a certain number of tokens TC_{max} initially and spends tokens when it sends or receives packets for its own benefit. So selfish nodes must become cooperative if the number of remaining tokens drops below a threshold TC_{thr}. For simplicity, we consider that malicious nodes cannot become cooperative, while it is possible for a failed node to be repaired or recharged with an average recovery time $\overline{T}_{recr}$. Consider that $\mathbb{P}$ is a stochastic matrix, we can determine p_{xx} ($x \in \mathcal{S}$) correspondingly. The complete definitions of p_{ij} are given by (2) as follows:

$$
\begin{aligned}
& p_{cf} = p_{mf} = p_{sf} = \max(\frac{1}{\overline{T}_{life}}, \frac{1}{\overline{T}_{in}}), \\
& p_{cm} = p_{sm} = q_a \cdot \frac{k_a}{N} \cdot \frac{1}{\overline{T}_{attk}}, \ p_{fm} = 0, \\
& p_{cs} = \frac{1}{T_{TS}} = \frac{\eta}{\eta - 1} \cdot \frac{1}{\overline{T}_{life}}, \ p_{ms} = p_{fs} = 0, \\
& p_{sc} = \frac{TC_{thr}}{TC_{max}}, \ p_{mc} = 0, \ p_{fc} = \frac{1}{\overline{T}_{recr}}, \\
& \sum_{i \in \mathcal{S}} p_{ij} = 1, \ \forall j \in \mathcal{S}.
\end{aligned} \tag{2}
$$

2) Transition Time Distributions: We use two-parameter *Weibull* distribution from reliability engineering to define $F_{xf}(t)$ as: $F_{xf}(t) = 1 - \exp(-(t/\hat{\beta})^{\hat{\alpha}})$ ($x \in \{C, S, M\}$), where $\hat{\alpha}$ is the *slope* parameter, $\hat{\beta} = \overline{T}_{life}/\Gamma(1 + 1/\hat{\alpha})$ is the *scale* parameter, and $\Gamma(\cdot)$ is the gamma function. $F_{cm}(t)$, $F_{sm}(t)$ and $F_{cs}(t)$ are defined by Weibull distribution similarly. In this paper, we assume that $F_{sc}(t)$ is a uniform distribution with the range of $[a, b]$. We further define $F_{fc}(t)$ and $F_{xx}(t)$ ($x \in \mathcal{S}$) by exponential distributions.

$$
\mathbb{F}(t) = \begin{pmatrix}
\mathcal{E}(\lambda) & \mathcal{W}(\hat{\alpha}, \frac{T_{TS}}{\gamma}) & \mathcal{W}(\hat{\alpha}, \frac{\overline{T}_{attk}}{\gamma}) & \mathcal{W}(\hat{\alpha}, \frac{\overline{T}_{life}}{\gamma}) \\
\mathcal{U}(a, b) & \mathcal{E}(\lambda) & \mathcal{W}(\hat{\alpha}, \frac{\overline{T}_{attk}}{\gamma}) & \mathcal{W}(\hat{\alpha}, \frac{\overline{T}_{life}}{\gamma}) \\
1 & 1 & \mathcal{E}(\lambda) & \mathcal{W}(\hat{\alpha}, \frac{\overline{T}_{life}}{\gamma}) \\
\mathcal{E}(\frac{1}{\overline{T}_{recr}}) & 1 & 1 & \mathcal{E}(\lambda)
\end{pmatrix}, \tag{3}
$$

Then the complete definitions of $F_{ij}(t)$ are given by (3), where $\mathcal{W}(\hat{\alpha}, \hat{\beta})$ denotes Weibull distribution with parameter $\hat{\alpha}$ and $\hat{\beta}$, $\mathcal{E}(\lambda)$ denotes exponential distribution with parameter λ, $\mathcal{U}(a, b)$ denotes uniform distribution with range $[a, b]$ and $\gamma = \Gamma(1 + 1/\hat{\alpha})$.

After determing p_{ij} and $F_{ij}(t)$, we obtain π_i by:

$$
\vec{\pi} = \vec{\pi}\mathbb{P}, \ \sum_{i \in \mathcal{S}} \pi_i = 1, \ \pi_i \geq 0, \tag{4}
$$

where $\vec{\pi} \triangleq (\pi_i)$ for $i \in \mathcal{S}$. We further obtain μ_i by:

$$
\mu_{ij} = \int_0^\infty t dF_{ij}(t), \ \mu_i = \sum_{j \in \mathcal{S}} p_{ij} \mu_{ij}, \ \forall i \in \mathcal{S}. \tag{5}
$$

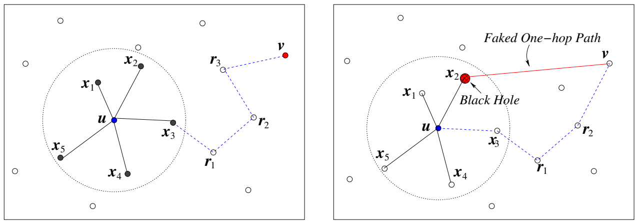
By substituting the results from (4) and (5) into (1), the limiting probability, P_i, can be obtained.

V. Analysis of Network Connectivity

Recall that our objective is to find out the probability of an ad hoc network keeping k-connectivity in the presence of misbehaving nodes and node failures. Based on the proposed node behavior model in Section IV, we are ready to analyze the connectivity of ad hoc networks stochastically in this section.

A. Node Isolation due to Misbehavior

We begin our analysis by examing the effects of node misbehaviors, which is so called *node isolation* problem. Fig. 2(a) shows the scenario where all the neighbors of node u are selfish nodes. In this case, the number of node-disjoint *outgoing paths* of u is zero, where the term outgoing path refers the path through which a node can communicate the nodes of at least two-hop away. In the scenario shown in Fig. 2(b), one of the neighbors of node u is *Black Hole*. In fact, only one *Black Hole* neighbor x_2 is sufficient to trap all traffic initiated from node u if the destination is beyond the neighborhood of node u. In this case, the number of node-disjoint outgoing paths for node u is also zero. If node u is surrounded by one or more *JellyFish* node(s), then the throughput of the data stream via the *JellyFish* node will become zero after a short time period, which is especially harmful for long communication sessions.



(a) (b)

Fig. 2. Node Isolated by Misbehaving Neighborhood.

Let $N_{op}(u)$ denote the number of node-disjoint outgoing paths of node u, then node u is isolated from the network if $N_{op}(u) = 0$. Considering that there exist only two types of malicious nodes in this context, *Black Hole* and *JellyFish* nodes, we have the following observation:

Lemma 1: A node u is isolated if it has at least one *Black Hole* neighbor or the total number of selfish, *JellyFish*, and failed neighbors is d, given it has d neighbors.

By *Lemma* 1, let D denote the number of neighbors of a node, then we obtain the probability of a node being isolated, given that the node has d neighbors, as

$$Pr(N_{op}=0|D=d) = 1-(1-P_{BH})^{d}+(1-P_c-P_{BH})^{d}, \quad (6)$$

where P_c and P_{BH} are the probabilities that a node is cooperative and a *Black Hole*, respectively. Consequently, a node must have at least one cooperative and no *Black Hole* neighbor to keep it connected to the network.

B. Condition of Keeping A Node k-Connected

Let $\hat{n}_c(u)$, $\hat{n}_{BH}(u)$ and $\hat{n}_g(u)$ denote the number of cooperative, *Black Hole* and all other neighbors of node u, respectively, then based on the analysis to node isolation problem, we have

Theorem 1: A node u has k node-disjoint outgoing paths if and only if u has k cooperative neighbors and no *Black Hole* neighbor, i.e., $\{N_{op}(u)=k\} \Leftrightarrow \{\hat{n}_c(u)=k, \hat{n}_{BH}(u)=0\}$ for $k \geq 1$.

Notice that the events of any node being in a certain behavior state are mutually independent, then by *multinomial probability law*, we know that the joint distribution of $\hat{n}_c, \hat{n}_{BH}, \hat{n}_g$ is a multinomial distribution. By *Theorem* 1, the probability of a node being k-connected to network, given that the node has d neighbors, is defined as

$$\begin{aligned} Pr(N_{op}=k|D=d) &= Pr(\hat{n}_c=k, \hat{n}_{BH}=0, \hat{n}_g=d-k) \\ &= \frac{d!}{k!(d-k)!}(P_c)^k \cdot \bar{P}^{d-k}, \ k \geq 1, \quad (7) \end{aligned}$$

where $\bar{P} = 1-P_c-P_{BH}$ denotes the probability of a node being neither cooperative nor *Black Hole*.

C. Probability of k-Connectivity

Let $\theta(\mathcal{M}_A) = \min\{N_{op}(u)|N_{op}(u) \in \mathbb{N}, u \in \mathcal{M}_A\}$, we have the condition to keep a network k-connected as follows:

Theorem 2: An ad hoc network $\mathcal{M}_A$ with N_a nodes is k-connected if and only if any active node u of $\mathcal{M}_A$ has at least k node-disjoint outgoing paths, when N_a is sufficiently large.

Therefore, by *Theorem* 2, the probability of a network being k-connected can be represented by:

$$Pr(\kappa(\mathcal{M}_A)=k) = Pr(\theta(\mathcal{M}_A) \geq k). \quad (8)$$

We assume that the number of outgoing paths for each node u, $N_{op}(u)$, is independent, then from (8), we have:

$$Pr(\kappa(\mathcal{M}_A)=k|N_a) = (1-Pr(N_{op}<k))^{N_a}, \quad (9)$$

where N_a is the number of active nodes. By the total probability law, we have

$$Pr(N_{op}<k) = \sum_{d=k}^{\infty} Pr(N_{op}<k|D=d)Pr(D=d). \quad (10)$$

To solve this problem, we need to find $Pr(N_{op}<k|D=d)$ and $Pr(D=d)$. By (7), $Pr(N_{op}<k|D=d)$ is given immediately by:

$$\begin{aligned} &Pr(N_{op}<k|D=d) \\ &= 1-(1-P_{BH})^d + \sum_{m=0}^{k-1} \frac{d!}{m!(d-m)!}(P_c)^m \cdot \bar{P}^{d-m} \quad (11) \end{aligned}$$

To derive $Pr(D=d)$, we assume that all nodes move randomly over a finite area with size A. We divide the area into N' small grids virtually so that the grid size is in the same order of the physical size of a node. Consider that the network area is normally much larger than the node physical size, the probability that a node occupies a specific grid, denoted by p', is very small. With large N' and small p', node distribution can be modeled by a *Poisson point process*. Then we have

$$Pr(D=d) \approx \frac{\mu_0^d}{d!}e^{-\mu_0}, \quad (12)$$

where $\mu_0 = \rho\pi r_0^2$. ρ is the node density depending on the underlying mobility model, and r_0 is the transmission range of nodes.

Finally, by (9), (10), (11) and (12), we obtain:

$$\begin{aligned} &Pr(\kappa(\mathcal{M}_A)=k|N_a) \\ &= \left[\frac{\Gamma(k,\mu_0)}{\Gamma(k)} + e^{-\mu_0 P_{BH}}\left(1-\frac{\Gamma(k,\mu_0(1-P_{BH}))}{\Gamma(k)}\right)\right. \\ &\left. -e^{-\mu_0 P_{BH}} \cdot \frac{\Gamma(k,\mu_0 P_c)}{\Gamma(k)}\right]^{N_a}. \quad (13) \end{aligned}$$

where $\Gamma(\cdot)$ and $\Gamma(h,x) = (h-1)!e^{-x}\sum_{l=0}^{h-1} x^l/l!$ are complete and incomplete Gamma function, respectively.

VI. Simulation Results

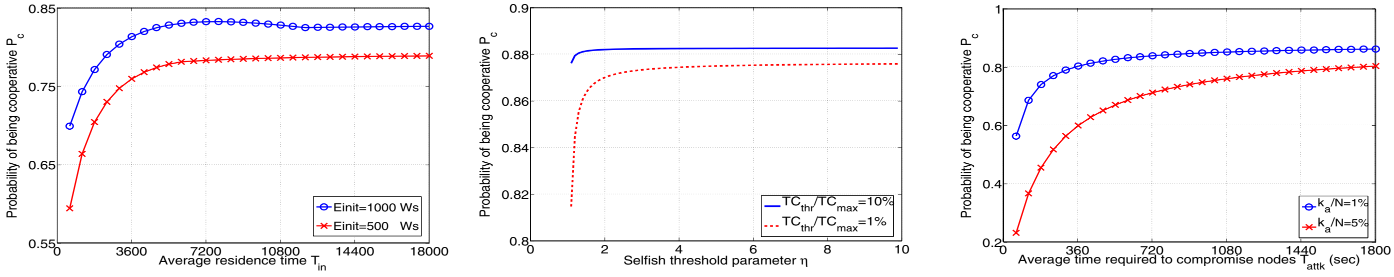
Up to now, we have obtained the stochastic properties of the impact of node behaviors on network connectivity. In this section, we evaluate our node behavior model and network connectivity of ad hoc networks by simulations.

A. Simulation Environment

In this work, we use NS2-v2.27 and MATLAB-v6.5 to perform the simulations. Unless specified otherwise, all simulations are performed in a 1000×1000 m^2 square area, over which 200 mobile nodes with transmission range 150 m are distributed uniformly. IEEE 802.11 is used for medium access control and AODV is used as the routing protocol. *BonnMotion* [11] is used to generate *Gauss-Markov* modeled movement scenarios. In order to calculate the probability of connectivity, we collected the neighborhood statistics of each node per 10 seconds, including the number of neighbors and the behavior of each neighbor. With these information, the number of outgoing paths of each node can be obtained, then the probability of k-connectivity can be calculated.

B. Probability of A Node Being Cooperative

As explained in Section IV-B, node mobility is represented by the average residence time $\overline{T}_{in}$. The smaller $\overline{T}_{in}$ is, the faster a node will leave a network, which implies that the node is less cooperative to its neighbors. As shown in Fig. 3(a), the cooperative probability P_c is proportional to $\overline{T}_{in}$ when $\overline{T}_{in} \leq \overline{T}_{life}$ and remains a constant of $1/\overline{T}_{life}$ afterward. From Fig. 3(a), P_c is affected by the initial energy E_{init} as well, i.e., a node with a higher E_{init} is more likely to be cooperative. By (2), as η increases, p_{cs} keeps deceasing until $1/\overline{T}_{life}$, which



(a) Effect of Node Mobility

(b) Effect of Selfishness

(c) Effect of DoS Attacks

Fig. 3. Probability of A Node Being Cooperative P_c.

reflects the fact that a node is more likely to be cooperative if it takes longer time to become selfish. Therefore, in Fig. 3(b), P_c increases quickly at the beginning, then almost remains constant afterwards. Meanwhile, we can see that a higher token threshold TC_{thr} can increase P_c effectively, which shows that it is necessary to use a cooperation stimulating mechanism to mitigate selfish behavior. Moreover, by (2), the shorter $\overline{T}_{attk}$ is, the more likely a node is compromised to become malicious, which leads P_c in proportion to $\overline{T}_{attk}$, as shown in Fig. 3(c). If the fraction of vulnerable nodes within total nodes, k_a/N, is increased from 0.01 to 0.05, then cooperative probability P_c drops dramatically for the same $\overline{T}_{attk}$. Thus, we conclude that external attacks can impact P_c substantially.

C. Probability of k-connectivity

In this section, we study how network connectivity is impacted by misbehaving nodes and node failures. Fig. 4(a) shows the simulation results of the probabilities of k-connectivity against P_c for $k = 1, 2, 3, 4$, respectively. In this experiment, P_f and P_{BH} are set to 0 such that we can observe the effect of P_c clearly. From Fig. 4(a), the probability of k-connectivity is inversely proportional to k given constant P_c, and proportional to P_c given constant k. To obtain a higher k-connectivity, it is necessary to have a higher P_c.

In order to see the effect of probability of node failure P_f, we set both P_s and P_m as zero to eliminate the impact of misbehaving nodes in our simulations. From Fig. 4(b), the probability of k-connectivity decreases very fast as P_f increases. As we expected, for a highly connected network, the impact of P_f is more significant, e.g., the probability of $k = 3$-connectivity drops to 0.4 even as $P_f = 0.2$.

In the same way, we obtain the results from node selfishness as shown in Fig. 4(c). Similar to that in Fig. 4(b), the plot in this figure indicates that the probability of k-connectivity decreases as selfish probability P_s increases. Nevertheless, differing from the results in Fig. 4(b), the probability of k-connectivity does not change significantly when P_s is increased at the beginning, especially for lower k. Notice that the number of active nodes N_a decreases as P_f increases, which makes the network sparser in terms of the decreased node density (e.g., $\rho = N_a/A$ if the node distribution is uniform). Therefore, node failures have severer partitioning effects than selfish nodes.

Compared to the analytical results, the simulation results are lower than analytical ones, which can be explained by the border effect, i.e., the nodes at the vicinity of the simulation boundary have less neighbors and thus become isolate easily. Therefore, the analytical result provides a upper bound for the probability of k-connectivity.

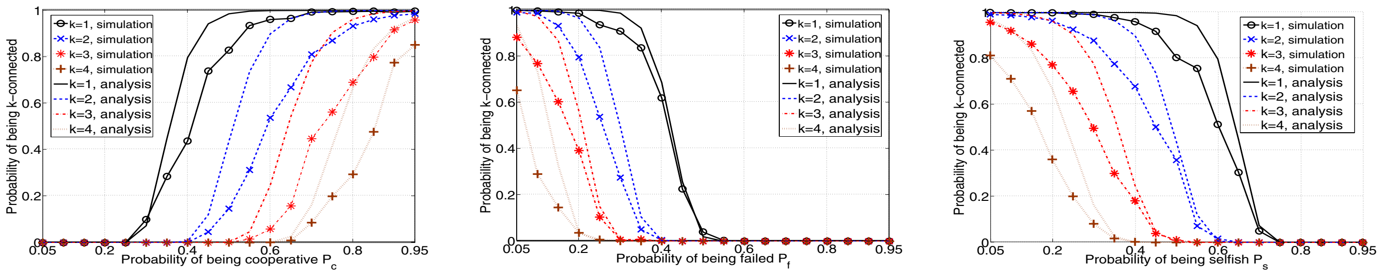
D. k-connectivity Impacted by Other Parameters

In addition to node behaviors, we continue to evaluate the impact of other system parameters on network connectivity. Here we look at the effect of *Black Hole* with the probability of P_{BH}. By (13), P_{BH} has tremendous influence on the probability of k-connectivity. Analytical results are illustrated in Fig. 5(a) from which we can see that $Black\ Hole$ is the most harmful behavior since it destroys network connectivity much severer than node failures do. Recall the node isolation issue discussed in Section V-A, we find that a *Black Hole* actually can isolate all its neighbors, and its influential scope will be extended when it roams in the network.

Next, we discuss the effect of system size N on the network connectivity. In this simulation, the transmission range r_0 is set as $100m$ to enlarge system size N. Fig. 5(b) shows that the required network size N should be enlarged to guarantee the same k-connectivity when malicious or failed nodes are in present. To discuss the effect of the node's transmission range r_0 on the network connectivity, we change the system size N to 150 from 200 to enlarge the change of r_0. Fig. 5(c) shows that the higher k-connectivity is required, the larger r_0 is needed. Similar to the analysis to Fig. 5(b), we conclude that the required r_0 has to be increased to guarantee the same k-connectivity if malicious or failed nodes exist in a mobile ad hoc network.

VII. Conclusion

In this paper, we focused on the modeling and analysis of the impact of node misbehaviors to network connectivity of mobile ad hoc networks, which has been rarely studied before. We first classified node behaviors into four types:

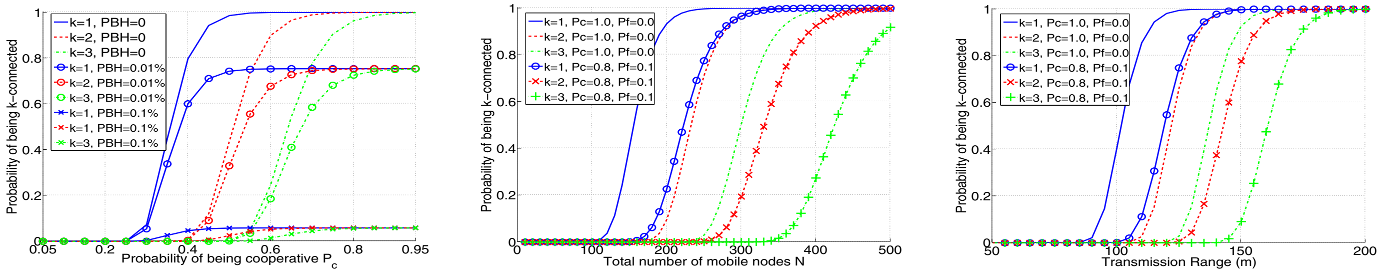


(a) Effect of Cooperative Probability P_c

(b) Effect of Failed Probability P_f

(c) Effect of Selfish Probability P_s

Fig. 4. Probability of k-connectivity: Effects of Node Behaviors.



(a) k-Connectivity Impacted by P_{BH}

(b) k-Connectivity Impacted by N

(c) k-Connectivity Impacted by r_0

Fig. 5. Probability of k-Connectivity: Effects of System Parameters.

cooperative, selfish, malicious and *failed*, then proposed a node behavior model by employing a semi-Markov process. In our model, mobile nodes change their behaviors according to the well-defined transition probability matrix and transition time distribution matrix. After obtaining the limiting probability of a node being in each behavior state. we analyzed the node isolation problem resulting from misbehaving neighbor nodes and provided the condition under which mobile nodes can be connected with a mobile ad hoc network. In consequence, we obtained the probability of a network being k-connected. Finally, our analytical results were explained by simulation experiments. As a conclusion, besides mobility-induced failures, node misbehaviors can cause node isolation problem as well, which impacts the network connectivity significantly. Our work also provides a deeper understanding to network performance evaluation and multiple failure detection in the presence of node misbehaviors.

REFERENCES

[1] Imad Aad, Jean-Pierre Hubaux, and Edward W Knightly. Denial of Service Resilience in Ad Hoc Networks. In *Proc. of ACM MobiCom '04*, pages 202–215, 2004.

[2] Baruch Awerbuch, David Holmer, Cristina Nita-Rotaru, and Herbert Rubens. An On-demand Secure Routing Protocol Resilient to Byzantine Failures. In *Proc. of the ACM workshop on Wireless security, WiSE '02*, pages 21–30. ACM Press, 2002.

[3] Christian Bettstetter. On the Connectivity of Ad Hoc Networks. *The Computer Journal, Special Issue on Mobile and Pervasive Computing*, 47(4):432–447, July 2004.

[4] B. Bollobas. *Modern Graph Theory*. Springer, 1998.

[5] Levente Butty and Jean-Pierre Hubaux. Stimulating Cooperation in Self-Organizing Mobile Ad Hoc Networks. *Mobile Networks and Applications*, 8(5):579–592, 2003.

[6] Trajanov Dimitar, Filiposka Sonja, Makraduli Jani, and Grnarov Aksenti. Connection Resilience to Nodes Failures in Ad Hoc Networks. In *Proc. of IEEE MELECON '04*, Dubrovnik, Croatia, May 2004.

[7] Daniel Heyman and Mattlew Sobel. *Stochastic Models in Operations Research*. McGraw-Hill, 1982.

[8] Matthias Hollick, Jens Schmitt, Christian Seipl, and Ralf Steinmetz. On the Effect of Node Misbehavior in Ad Hoc Networks. In *Proc. of IEEE ICC'04*, volume 6, pages 3759–3763, Jun. 2004.

[9] Inwhee Joe. SCTP with An Improved Cookie Mechanism for Mobile Ad-Hoc Networks. In *Proc. of IEEE GLOBECOM '03*, volume 7, pages 3678–3682, Dec. 2003.

[10] Xiang-Yang Li, Peng-Jun Wan, Yu Wang, and Chih-Wei Yi. Fault Tolerant Deployment and Topology Control in Wireless Networks. In *Proc. of ACM MobiHoc '03*, pages 117–128, Jan. 2003.

[11] University of Bonn. BonnMotion: A Mobility Scenario Generation and Analysis Tool, available at *http://web.informatik.uni-bonn.de/IV/Mitarbeiter/dewaal/BonnMotion/*, 2005.

[12] Vikram Srinivasan, Pavan Nuggehalli, Carla F. Chiasserini, and Ramesh R Rao. Cooperation in Wireless Ad Hoc Networks. In *Proc. of IEEE INFOCOM '03.*, pages 808 –817, Mar. 30 - Apr. 3 2003.

[13] Hao Yang, Haiyun Luo, Fan Ye, Songwu Lu, and Lixia Zhang. Security in Mobile Ad Hoc Networks: Challenges and Solutions. *IEEE Wireless Communications*, pages 38 – 47, Feb 2004.