On the Survivability of Wireless Ad Hoc Networks with Node Misbehaviors and Failures

Fei Xing *Student Member, IEEE,* and Wenye Wang *Member, IEEE,*

***Abstract*— Network survivability is the ability of a network keeping connected under failures and attacks, which is a fundamental issue to the design and performance evaluation of wireless ad hoc networks. In this paper, we focus on the analysis of network survivability in the presence of node misbehaviors and failures. First, we propose a novel semi-Markov process model to characterize the evolution of node behaviors. As an immediate application of the proposed model, we investigate the problem of node isolation where the effects of Denial-of-Service (DoS) attacks are considered. Then we present the derivation of network survivability and obtain the lower and upper bounds on the topological survivability for k-connected networks. We find that the network survivability degrades very quickly with the increasing likelihood of node misbehaviors, depending on the requirements of disjoint outgoing paths or network connectivity. Moreover, DoS attacks have a significant impact on the network survivability, especially in dense networks. Finally, we validate the proposed model and analytical result by simulations and numerical analysis, showing the effects of node misbehaviors on both topological survivability and network performance.**

***Index Terms*— network survivability, node misbehaviors, semi-Markov process, node behavior modeling, node isolation problem, k-connectivity, wireless ad hoc networks**

I. Introduction

Network survivability is an essential aspect of reliable communication services. In literature, the network survivability has been defined from different perspectives [2]–[10]. These network survivability definitions provide a general intuitive notion of the concept of survivability and are applicable for traditional telecommunication networks, where traffic capacity and service restorability are of main concerns. However, they do not have the mathematical precision to lead to a quantitative characterization and do not grasp the fundamental aspect of the survivability of wireless ad hoc networks. Compared with traditional networks, wireless ad hoc networks are more vulnerable to malicious attacks as well as random failures due to their unique features, such as constrained node energy, error-prone communication media, and dynamic network topology. Thus, as pointed out in [11], it is the first major goal for a survivable wireless ad hoc network to establish and maintain a connected topology, whenever it is practical. Based on this observation, as a fundamental topology property and prerequisite for all networking operations, topology connectivity is a critical index for the survivability of wireless ad hoc networks, especially in the presence of malicious attacks and random failures.

We notice that network connectivity has been used as a metric in evaluating the survivability of ad hoc networks by a number of works [8]–[10]. In addition, extensive research efforts have been made to understand fundamental properties for asymptotic connectivity of wireless multi-hop networks [12]–[16]. In these studies, a common premise is that as long as a node has active neighbors, the node is connected to the network "physically" via wireless links. Nevertheless, the premise can hardly hold in real networks by considering potential node misbehaviors and random failures. For example, selfish nodes may not forward control and/or data packets for other nodes for the sake of saving their own energy and malicious nodes may launch Denial of Service (DoS) attacks, such as *Jellyfish* and *Blackhole*, to interrupt normal routing and forwarding procedures. We notice that substantial works have been done to characterize various node misbehaviors and evaluate their effects on network performance [17]–[19]. However, little research efforts were made to analyze to what extent these node misbehaviors can impact the topological survivability of wireless ad hoc networks quantitatively.

Therefore, the presence of node misbehaviors and multiple failures yields new challenges to the survivability of wireless ad hoc networks and motivates us to reveal their fundamental impacts on network survivability. More precisely, in this paper we perceive the survivability of a wireless ad hoc network as the probabilistic k-connectivity and provide a quantitative analysis on the impacts of both node misbehavior and failure on network survivability. We summarize the contributions of this work as follows.

- A generic model based upon semi-Markov process is proposed to characterize the evolution of node behaviors and the stochastic property of the model is analyzed to disclose the effects of node behaviors.
- The node isolation problem is revisited by examining the *cooperative degree* and the probabilistic k-connectivity of individual nodes is obtained by using the stochastic property of node behaviors.
- The survivability of wireless ad hoc networks is analyzed probabilistically and its theoretical bounds are derived in closed forms, which enables us to quantify the impacts of different behaviors.

The remainder of this paper is organized as follows. In Section II, we classify node behaviors and define the problem of *network survivability*. In Section III, we propose a semi-Markov process model to characterize node behavior transitions. In Section IV, we discuss node isolation problem as a case study and derive the probability of node isolation. In Section V, we find the closed-form approximation of network survivability by deriving its theoretical bounds for k-connected networks. In Section VI, we validate our findings by simulations and provide

This work is supported in part by National Science Foundation (NSF) under award CAREER CNS-0546289 and Defense Threat Reduction Agency (DTRA) under award HDTRA-1-08-1-0024.

F. Xing is with the Department of Electrical and Computer Engineering, North Carolina State University. Email: fxing@ncsu.edu.

W. Wang is with the Department of Electrical and Computer Engineering, North Carolina State University. Email: wwang@ncsu.edu.

Parts of this paper appeared in the Proceedings of the IEEE International Conference on Communications 2006 [1].

performance evaluations. In Section VII, we compare our work with related works, followed by conclusions in Section VIII.

II. Problem Formulation

A. Preliminaries

1) Network Model: In this paper, N mobile nodes in a wireless ad hoc network are randomly and uniformly distributed over a 2-D square with area A. The node transmission radius, denoted by r, is assumed to be identical for all nodes. Thus, the underlying communication graph of a wireless ad hoc network is modeled by a geometric random graph $\mathcal{G}(\mathcal{N}, r)$ [20] where $\mathcal{N}$ denotes the vertex set with $|\mathcal{N}| = N$ and an edge exists between two vertices only if their distance is no greater than r. Analogous to $\mathcal{G}(\mathcal{N}, r)$, a wireless ad hoc network is denoted by $\mathcal{M}(\mathcal{N}, r)$ (or $\mathcal{M}$ for clarity). These denotations will be used in the succeeding definitions and analysis.

2) Node Classification: In a wireless ad hoc network, node cooperation in routing process is an essential requirement to maintain protocol operations and network connectivity [21]. However, since every node is an autonomous system, it may decide how to act in the network by itself. Considering the potential impacts of various misbehaviors, we extend the geometric random graph model aforementioned by introducing an additional assumption that all nodes operate independently in the following $four$ states:

- *Cooperative state (C)*: if a node complies with all routing and forwarding rules, i.e., being able to initiate and response route discoveries correctly and forward control and data packets for others at the best effort;
- *Selfish state (S)*: if a node can initiate and response route discoveries for its own purpose but may not forward control or data packets for others for the sake of power saving;
- *Malicious state (M)*: if a node launches DoS attacks on the network layer, e.g., being cooperative in the routing stage but reluctant in forwarding data packets, or disrupting legitimate path selections by broadcasting fake route replies;
- *Failed state (F)*: if a node is unable to initiate or response route discoveries.

Particularly, we focus on two types of malicious behaviors in this paper: *Jellyfish* and *Blackhole* attacks [19]. Slightly different from the descriptions in literature, in this paper the *Jellyfish* attack is referred as to any malicious behavior that complies with all routing rules but reorders, delays, or drops data packets; while the *Blackhole* attack is referred as to a brutal behavior that always claims the shortest path to the destination so that path selections and all data traffics can be trapped later on. In the succeeding context, we refer nodes launching these two attacks as *Jellyfish* and *Blackhole* nodes, respectively.

B. Network Survivability Definitions

Various survivability definitions have been proposed in different disciplines. For example, Ellison et al. defined the $survivability$ as the capability of a system to fulfill its mission, in a timely manner, in the presence of attacks, failures, or accidents [2]. In the updated Federal Standard 1037C [3], $survivability$ is defined as the property of a system, subsystem, equipment, process, or procedure that provides a defined degree of assurance that the named entity will continue to function during and after a natural or man-made disturbance. While these definitions provide a good description of the concept of survivability, they do not have mathematical precision to lead to any quantitative interpretation of survivability. It is difficult to determine whether a given system is survivable, and it is difficult to compare the survivability of two systems [6].

A more general survivability definition was introduced by Knight and Sullivan [4] for critical information systems as follows. A survivability specification is a four-tuple, $\{\mathscr{E}, \mathscr{R}, \mathscr{P}, \mathscr{M}\}$ where $\mathscr{E}$ is the assumed operating environment for the system, $\mathscr{R}$ is a set of specifications of tolerable services to be provided by the system, $\mathscr{P}$ is a probability distribution across $\mathscr{R}$, and $\mathscr{M}$ is a finite-state machine (FSM) defining tolerable service transitions. Although this definition provides a comprehensive framework in defining the survivability of critical infrastructure applications, such as banking systems, it still lacks mathematical precision and leaves a number of open questions. For example, it did not take into account the impact of any failures. In addition, this definition can hardly be applied for wireless ad hoc networks since these networks are normally highly dynamic systems without predefined specifications of tolerable services $\mathscr{R}$.

Other than above qualitative definitions, we notice that a variety of metrics have been used to define survivability in wireless networks. For example, the survivability of wireless mobile networks was defined in [5] as a networks ability to perform its designated set of functions given network infrastructure component failures resulting in a service outage, and measured by traditional registration blocking probability and call blocking probability. Obviously, this definition applies for cellular networks but not for ad hoc networks since blocking probabilities are not of major concern in ad hoc networks. In another recent work, the excess packet loss due to failures (ELF) was taken as the survivability performance measure [6], which is essentially a traditional network performance metric for data networks and not necessarily specific for wireless ad hoc networks.

Therefore, network survivability must be defined concretely with mathematical precision for wireless ad hoc networks. In general, the topology of a wireless ad hoc network keeps changing dynamically due to various reasons, such as node mobility and channel randomness (i.e., multipath fading, path loss, shadowing, etc.), even when node failures or security attacks are not present. For wireless ad hoc networks, maintaining a connected topology is an important design issue; otherwise, no network operations (such as routing and forwarding) can be guaranteed, not even to say quality of service. As a result, whether a network is survivable largely depends on whether outgoing paths are available for every node so that they can be used for communications. Thus, we consider the survivability of a wireless ad hoc network to be a basic network capability to maintain a connected topology in the presence of malicious adversaries and random failures and use *connectivity* as the metric to define it as follows,

Definition 1: Given a wireless ad hoc network $\mathcal{M}$, let $\kappa(\mathcal{M})$ denote the (vertex)-connectivity of $\mathcal{M}$. The *network survivability* of $\mathcal{M}$, denoted by $NS_k(\mathcal{M})$, is defined as the probability that all *active (un-failed)* nodes are k-connected, i.e.,

$$NS_k(\mathcal{M}) = Pr(\kappa(\mathcal{M}_a) = k), \tag{1}$$

where $\mathcal{M}_a$ is the network induced by all active nodes of $\mathcal{M}$.

Note that in the definition above, we are particularly interested in the connectedness of active nodes including cooperative, selfish, and malicious nodes. This is because of the fact that failed nodes, being unable to participate in routing operations, do not

contribute to the topological connectedness.

C. Problem Formulation

With the definition of network survivability, the problem studied in this work can be formulated as the *Survivability to Node Misbehaviors (SNM)*:

SNM-Problem: *Given a wireless ad hoc network $\mathcal{M}$ with four node behavior states described in Section II-A, find out the quantitative relationship between four behaviors and the network survivability, i.e., $NS_k(\mathcal{M})$, in closed forms.*

Intuitively, the solution to the SNM-Problem should depend on basic network properties, such as the number of nodes (N) and transmission radius r, and stochastic (statistic) properties of node behaviors, such as the probability of a node being in a certain state. Nevertheless, to the best of our knowledge, little work has been done in modeling node misbehaviors, which makes it difficult to estimate node behavior properties. In addition, although a few of works have studied the connectivity of ad hoc networks by analyzing the node isolation probability where a node is isolated because of no neighbors [15], [22], the impact of node misbehaviors was never taken into account. Thus, it is quite challenging to solve the SNM-Problem and provide a closed-form approximation for survivability.

In this work, we use a two-step approach to tackle the SNM-Problem. First, we use a semi-Markov process to characterize the evolution of node behaviors, so that the stochastic property of node behaviors can be estimated from both complete and incomplete data in Section III. Second, we reevaluate the problem of node isolation by considering the scenario with node misbehaviors in Section IV-A, where the node isolation probability is proved to be a function of the stochastic property of node behaviors. Based on our study of node isolation, we are able to reveal the impact of node behaviors on network survivability.

III. Node Behavior Modeling

In this section, we use a semi-Markov process to model the evolution of node behaviors, and analyze the stochastic property of the node behavior model.

A. Node Behavior Transitions

Wireless ad hoc networks are complex and dynamic systems due to unexpected random node behaviors. In real networks, the behavior of a node may change at any time due to various of reasons. For example, a node can be failed due to energy depletion or even a turn-off of transceivers triggered by end-users, or a node's security can be compromised by other attackers so that the node is utilized to launch new attacks. In this work, we assume that a node may change its behavior as follows.

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

The above assumptions do not specify any particular reason for a behavior transition, so they can provide a general exposure to the most common behavior transitions and are applicable to a wide range of network scenarios. Further, these assumptions are simple enough for us to model both node misbehaviors and failures in one mathematical framework, which is presented next.

B. Semi-Markov Node Model

Based on the node classification described in Section II-A, we define a state space, $\mathcal{S} \triangleq \{C(cooperative),\ S(selfish),\ M(malicious),\ F(failed)\}$ and model node behavior transitions by a stochastic process, $\{Z(t)\}$ associated with space $\mathcal{S}$. Because the future behavior depends on the current behavior but not previous behaviors, if let X_n denote the state at transition time t_n, we have,

$$\begin{aligned} &Pr(X_{n+1} = x_{n+1} \mid X_0 = x_0., \cdots, X_n = x_n) \\ &= Pr(X_{n+1} = x_{n+1} \mid X_n = x_n), \end{aligned} \tag{2}$$

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

Therefore, we use a *semi-Markov process (SMP)* $\{Z(t)\}$ to model node behavior transitions [23], which is defined by

$$Z(t) = X_n,\ \forall t_n \le t < t_{n+1}. \tag{3}$$

In (3), $Z(t)$ refers to the state of the process during the period from the most recent transition, and $\{X_n\}$ is called the *embedded Markov chain (EMC)* of the process $\{Z(t)\}$.

The SMP model defined above enables us to consider the evolution process of node behaviors without the assumption of memoryless property; additionally, this model can be used to describe a wide variety of random threats caused by node misbehaviors, depending on how to diffuse data into it. Specifically, let $T_n = t_{n+1} - t_n$ be the *sojourn* time between the n-th and $(n+1)$-th transition, we can define the associated (*time-homogeneous*) *semi-Markov kernel* $\mathbb{Q} = (Q_{ij}(t))$ by

$$Q_{ij}(t) = Pr(X_{n+1} = j, T_n \le t | X_n = i) = p_{ij} F_{ij}(t), \tag{4}$$

where $p_{ij} = \lim_{t\to\infty} Q_{ij}(t) = Pr(X_{n+1} = j | X_n = i)$ is the transition probability between states i and j, and $F_{ij}(t) = Pr(T_n \le t | X_{n+1} = j, X_n = i)$ is the transition time distribution from states i to j.

Based on assumptions in Section III-A, the transition probability matrix (TPM) of $\{X_n\}$ is given by

$$\mathbb{P} = \begin{pmatrix} 0 & p_{cs} & p_{cm} & p_{cf} \\ p_{sc} & 0 & p_{sm} & p_{sf} \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{pmatrix}, \tag{5}$$

where $p_{ii} = 0$ is in that $\{X_n\}$ only has transitions from a state to another different state. In (5), a transition probability of 0 like $p_{mc} = 0$ or $p_{ms} = 0$ means a malicious node will not become cooperative or selfish, according to our assumptions in Section III-A. Since the summation of transition probabilities to a state must be equal to 1 in a stochastic matrix, we know that $p_{mf} = 1$ and $p_{fc} = 1$ hold in (5) for this unity requirement. Recall that $\{Z(t)\}$ is also associated with a number of transition time distributions $F_{ij}(t)$, which are cumulative distribution functions of transition times from states i to j. Based on the TPM defined in (5), we have $F_{ii}(t) = 1$ and $F_{mc}(t) = F_{ms}(t) = F_{fs}(t) = F_{fm}(t) = 1$ since corresponding transition probabilities are 0 [23]. Nevertheless, determining other transition time distributions is not trivial since they are dependent on further assumptions, real applications, and transition time measurements.

Finally, the state transition diagram of the homogeneous SMP $\{Z(t)\}$ can be shown in Fig. 1. In the figure, state transitions between states i and j for $i, j \in \mathcal{S}$ are represented by edges associated with p_{ij} and $F_{ij}(t)$.

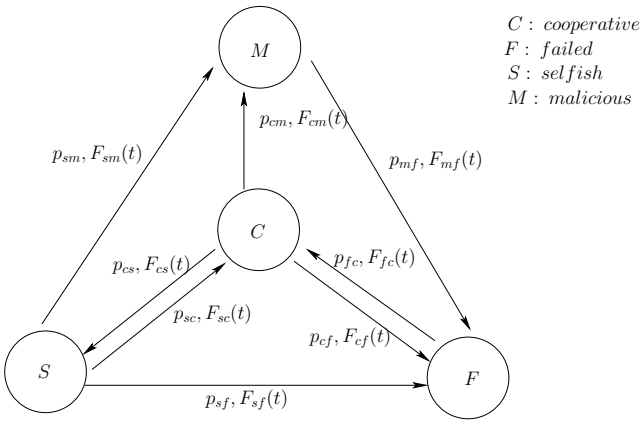


Fig. 1. The semi-Markov process for node behavior evolution.

One of the concerns for an analytic model is whether it can be used to estimate or predict future behaviors. More important, the model itself must be sufficiently generic for data diffusion, given complete or incomplete data. With the consideration of node misbehaviors, we intuitively perceive that the connectivity of a network will be affected by how likely a node behaves cooperatively as time goes. Hence, we will show how to use our model to find state probabilities (especially the probability of a node in cooperative status) at any time $t > 0$ for complete and incomplete data traces next.

C. State Distributions with Complete and Incomplete Data

The transient distributions of the SMP $\{Z(t)\}$, with state space $\mathcal{S}$ and semi-Markov kernel $\mathbb{Q}$ in (4), satisfy

$$\begin{aligned} P_{ij}(t) &\triangleq Pr(Z(t) = j | Z(0) = i) \\ &= (1 - H_i(t))\delta_{ij} + \sum_{l \in \mathcal{S}} \int_0^t \dot{Q}_{il}(\tau) P_{lj}(t - \tau) d\tau, \quad (6) \end{aligned}$$

where $H_i(t) \triangleq Pr(T_n < t | X_n = i) = \sum_{j \in \mathcal{S}} Q_{ij}(t)$ is the sojourn time distribution in state i, and δ_{ij} is the Kronecker δ function and defined by 1 for $i = j$ and 0 otherwise.

Without losing generality, we can assume that all nodes in the network are cooperative at the initial time, i.e., $Pr(Z(0) = c) = 1$. Then the transient distribution $P_{cc}(t)$ is of particular interest, since it indicates the cooperativeness of any node at time $t > 0$. To calculate $P_{cc}(t)$ by using (6), the function $Q_{ij}(t)$ should be given in a closed form, which is, however, normally difficult to provide in continuous time domain [24]. Nevertheless, a numerical solution can be used to solve (6) by rewriting the transient distributions in discrete-time domain as follows [24],

$$P_{ij}(mh) = (1 - H_i(mh))\delta_{ij} + \sum_{l \in \mathcal{S}} \sum_{x=1}^{m} h \dot{Q}_{il}(xh) P_{lj}(mh - xh), \quad (7)$$

where h is the discretization step. In addition, $\dot{Q}_{il}(xh)$ can be further approximated by the difference quotient as,

$$\dot{Q}_{il}(xh) = \frac{1}{h} \left(\hat{Q}_{il}(xh) - \hat{Q}_{il}((x-1)h) \right) \text{ for } x > 1, \quad (8)$$

where $\hat{Q}_{il}(xh)$ is the empirical distribution of $Q_{il}(\tau)$.

By using this method, when all state transitions and time instants of transitions are available, the difference quotient $\dot{Q}_{il}(xh)$ can be computed by (8), then $P_{ij}(mh)$ can be computed by (7). Indeed, this method has already been used in [25] to model behaviors of user mobility based on a tremendous trace database.

Unfortunately, to the best of our knowledge, there are no complete trace data recording user behaviors in wireless ad hoc networks. Thus, we strive to grasp the stochastic properties of node behaviors by utilizing any statistics available and reasonable estimations to derive the limiting state distributions.

Let T_i be the sojourn time in state i, T_{ij} be the transition time from states i to j, $E[\cdot]$ be the conventional notation for expectation, then we have $E[T_i] = \int_0^\infty (1 - H_i(t)) dt$ and $E[T_{ij}] = \int_0^\infty (1 - F_{ij}(t)) dt$. We have the result as follows

Theorem 1: Given the SMP $\{Z(t)\}$ associated with state space $\mathcal{S}$ and TPM $\mathbb{P}$ defined by (5), the transient distribution $P_{ij}(t)$ converges to a limiting probability P_j as $t \to \infty$; further, P_j can be calculated by

$$P_j \triangleq \lim_{t \to \infty} P_{ij}(t) = \frac{\pi_j E[T_j]}{\sum_{l \in \mathcal{S}} \pi_l E[T_l]}, \quad (9)$$

where $\vec{\pi} = < \pi_i >$ is the stationary distribution of $\{X_n\}$.

Proof: First, for the given EMC $\{X_n\}$ associated with the state space $\mathcal{S}$ and t.p.m. $\mathbb{P}$ defined by (5), it is trivial to prove that $\{X_n\}$ is irreducible and positive recurrent. Thus, the SMP $\{Z(t)\}$ is irreducible. Second, based on our assumptions in Section III.A, a node works in any behavior state for a finite time, which implies $E[T_i] < \infty$ and $\sum_{i \in \mathcal{S}} E[T_i] < \infty$. Thus, the SMP $\{Z(t)\}$ is positive recurrent as well. Finally, by *Theorem 9-3* [26], the limiting probability exists and can be given by (9). ■

Theorem 1 provides us a method to estimate the probability of a node in cooperative status when we do not have a complete set of trace data. To calculate P_j, we only need to estimate p_{ij} and $E[T_{ij}]$, which are normally easier to obtain from the statistics, then we can use the following equations to calculate π_i and $E[T_i]$.

$$\vec{\pi} = \vec{\pi}\mathbb{P}, \ \sum_{i \in \mathcal{S}} \pi_i = 1, \text{ and } E[T_i] = \sum_{j \in \mathcal{S}} p_{ij} E[T_{ij}]. \quad (10)$$

After π_i and $E[T_i]$ are obtained, we can use (9) to derive P_j, especially, the cooperative probability P_c.

In Section VI.A, we will provide a specific case study to show how to estimate $E[T_{ij}]$ and p_{ij} by using the statistics from measurements, and by using the assumptions on the network itself. In addition, in Section VI.C, we will demonstrate how

transient distributions can converge to limiting probabilities by using collected data from simulation experiments.

In summary, due to node misbehaviors, the likelihood of any node working cooperatively varies from time to time, depending on many factors such as resource level, movement, and attack. By using a general semi-Markov process to model the evolution of node behaviors, we are able to estimate either transient or limiting probability of a node in cooperative status, which will be shown to be a key factor impacting the connectivity of a network. Since limiting probabilities (P_j) stand for *long-term* average distributions of node behaviors and they are normally more accessible, in the succeeding analysis, we use P_j (e.g., P_c) directly. Nevertheless, when transient distributions $P_{ij}(t)$ can be computed based on sufficient trace data, all succeeding derivations still hold by substituting P_j with $P_j(t)$ with the assumption on the same initial state.

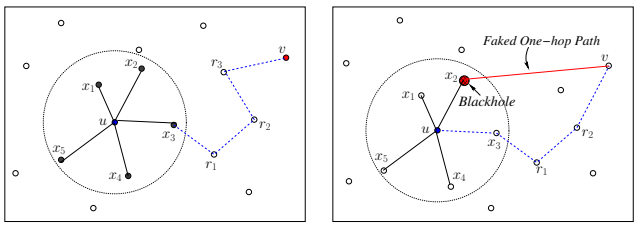
IV. Node Isolation: A Case Study

One immediate effect of node misbehaviors and failures in wireless ad hoc networks is the *node isolation problem* due to the fact that communications between nodes are completely dependent on routing and forwarding packets. In turn, the problem of node isolation is a direct cause for network partitioning, which further affects network survivability. Traditionally, node isolation refers to the phenomenon in which nodes have no (active) neighbors; however, we will show that due to the presence of node misbehaviors and failures a node can be isolated even if active neighbors are available. In this section, we present several typical cases for this sophistic problem first, then derive the probabilistic connectivity of individual nodes.

A. Node Isolation Problem

A trivial case of node isolation occurs when a node becomes failed. In this case, the failed node can be detected by routing protocols, normally, and is said to be disconnected or isolated from the network. We study more general cases of node isolation by considering the following three scenarios: *(i)* the effect of failed neighbors with no routing ability, *(ii)* the effect of selfish neighbors with reluctance in forwarding (control) packets, and *(iii)* the effect of malicious neighbors with intent of disrupting routing operations.

1) Effect of Failed Neighbor(s): In Fig. 2(a), suppose node x_3 is a failed node. When node u initiates a route discovery to another node v, the failed neighbor x_3 is unable to forward the route discovery. When all neighbors of u are failed, then u can no longer communicate with other nodes. In this case, we say that u is *isolated* by its failed neighbors.



(a) Failed or Selfish neighbors (b) Malicious neighbors

Fig. 2. Node isolation problem.

2) Effect of Selfish Neighbor(s): In Fig. 2(a), suppose node x_3 is a selfish node. When node u initiates a route discovery to another node v, the selfish neighbor x_3 may be reluctant to broadcast the route request from u. In this case, x_3 behaves like a failed node. It is also possible for x_3 to forward control packets; however, the situation could be worse since u may select x_3 as the next hop and send data to it. Consequently, x_3 may discard all data to be forwarded via it, then communications between u and v cannot proceed. When all neighbors of u are selfish, u is unable to establish any communications with other nodes at a distance of more than one-hop away. In this case, we say that a node is *isolated* by its selfish neighbors. Note that selfish nodes can still communicate with other nodes (via their cooperative neighbors), which is different from failed nodes.

3) Effect of Malicious Neighbor(s): Now we consider the scenario that one or more malicious nodes in the neighborhood of node u. Suppose that in Fig. 2(b) node x_2 is a *Jellyfish* node. Different from selfish nodes, *Jellyfish* nodes are always active in forwarding control packets; however, if *Jellyfish* nodes are en-route, they will selectively or randomly drop data packets, reorder packets, or increase jitters, which is especially harmful to TCP traffics. Thus, if u has x_2 as the next hop, then u will eventually lose communications with the nodes at least two-hop away. In the case that all neighbors are *Jellyfish* nodes, node u is said to be *isolated* by malicious neighbors, which is similar to the case of having selfish neighbors.

As mentioned in Section II-A, we further consider *Blackhole* attacks in this paper due to their severe impact on network survivability. For example, as illustrated in Fig. 2(b), suppose AODV is used as the routing protocol, when node u discovers the route to node v by broadcasting $RREQ$ messages, a *Blackhole* neighbor, say node x_2, can response u with a fake $RREP$ message immediately claiming that it is in the optimal path or only one-hop away to node v. Consequently, u selects x_2 as the next hop and sends data to it, but x_2 will just dump all packets. Without proper countermeasures, just a single *Blackhole* node may trap all traffic initiated from u whenever the destination is beyond its one-hop neighborhood. Moreover, the *Blackhole* node may be able to trap all traffics of its neighbors, which implies multiple node isolations in the worst case.

Based on above analysis, we know that node misbehaviors and DoS attacks make node isolation a more complicated problem and may affect the connectedness of every node. Next, we utilize the analysis above and the state distributions derived in Section III to derive the probabilistic connectivity of individual nodes.

B. Probability of Node Isolation

Based on the investigation of node isolation problem, we have an immediate observation that if a node does not have cooperative neighbors or have at least one *Blackhole* neighbor then the node is isolated from the network beyond its neighborhood. To present this observation in a formal way and facilitate the derivation on the node isolation probability, we first define the *outgoing path* for a node.

Definition 2: For a pair of nodes (u, v), if the length of the shortest path between them is no less than two, i.e., u and v are at least two hops away, then all paths connecting u and v are called as the *outgoing (u, v)-paths* for u or v.

Fig. 3 illustrates this definition, where Fig. 3(a) shows three outgoing (u, v)-paths. The reason for having outgoing path lengths

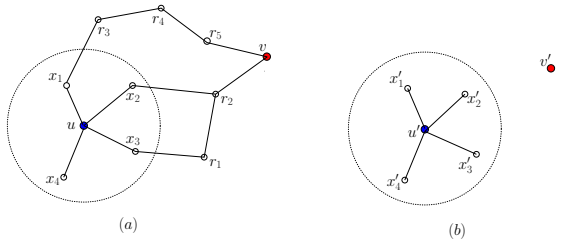


Fig. 3. Samples of outgoing paths of node u.

larger than one hop is that the path with only one hop may not make a node able to communicate with other nodes beyond its neighborhood. For example, when a node u has selfish neighbors only, it is actually isolated by its selfish neighbors and thus having no outgoing (u', v') paths, as shown in Fig. 3(b).

With the definition of outgoing path, we further define the the *cooperative degree*, denoted by $D_c(u)$, of node u as the maximum number of outgoing paths of u. Note that the cooperative degree does not necessarily equal to the number of cooperative neighbors, due to the effect of *Blackhole* attacks; while, when *Blackhole* nodes are not present, the maximum number of outgoing paths for a node is equivalent to the number of cooperative neighbors, so is the cooperative degree.

Next, let $n_i(u)$ be the number of node u's neighbors at state i ($i \in \mathcal{S}$), and let $n_J(u)$ and $n_B(u)$ be numbers of u's *Jellyfish* and *Blackhole* neighbors, respectively, then we can formulate the observation on node isolation problem as follows,

Proposition 1: Given node u with degree d, i.e., $D(u) = d$, if $n_s(u) + n_f(u) + n_J(u) = d$ or $n_B(u) \geq 1$, then the cooperative degree is zero, i.e., $D_c(u) = 0$, and u is isolated from the network.

Now, *Proposition 1* provides us a direct method to find the probability of node isolation in a network with misbehaving nodes, which is calculated as follows.

$$\begin{aligned} & Pr(D_c = 0|D = d) \\ = \; & Pr(n_B \geq 1|D = d) + Pr(n_s + n_f + n_J = d|D = d) \\ = \; & 1 - (1 - P_B)^d + (1 - P_c - P_B)^d, \end{aligned} \tag{11}$$

where P_c is the probability of a node in cooperative state defined in Section III and P_B is the probability of a node launching *Blackhole* attack. Note that we omit the notation u since the derivation applies to any generic node u.

From (11), we see the direct impact of node misbehaviors on the node isolation probability: the severer node misbehaviors present in a network, the less likely a node's neighbors are cooperative, thus the more likely the node is isolated from the network. For a given P_B, the cooperative probability P_c plays an important role in determining the connectivity of individual nodes. For example, when $P_c = 0$, $Pr(D_c = 0|D = d) = 1$, which means a node isolation because of no cooperative neighbors, and when $P_c = 1$, $Pr(D_c = 0|D = d) = 0$, which means node isolation is not caused by any node misbehaviors and failures.

In fact, besides representing the node isolation probability, the cooperative degree can be used to define the connectivity of individual nodes. Since a network is composed of individual nodes and its survivability is largely dependent on the connectedness between nodes, evaluating the probabilistic connectivity of a generic node will be one more step towards the analysis of network survivability, described right next.

C. Probabilistic k-connectivity of Individual Node

In this paper, a node is said to be k-connected to a network if its cooperative degree is k. The physical meaning of this definition is that if a node's cooperative degree is k then it may communicate with the nodes other than its neighborhood via k disjoint outgoing paths. Thus, we have the following conclusion for the k-connectivity of individual nodes.

Proposition 2: Given node u with degree d, i.e., $D(u) = d$, u is said to be k-connected to the network if its cooperative degree is k, i.e., $D_c(u) = k$, which is satisfied only if u has no *Blackhole* neighbor and has exact k cooperative neighbors, i.e., $n_B(u) = 0$ and $n_c(u) = k$.

Proposition 2 enables us to derive the probability of a node u being k-connected conditional on $D(u) = d$.

$$\begin{aligned} & Pr(D_c = k|D = d) \triangleq Pr(n_c = k, n_B = 0|D = d) \\ = \; & Pr(n_c = k, n_B = 0, n_s + n_f + n_J = d - k). \end{aligned} \tag{12}$$

Since the events of any node being in a certain behavior state are mutually independent, by the *multinomial probability law*, then (12) can be rewritten as:

$$Pr(D_c = k|D = d) = \binom{d}{k} (P_c)^k (1 - P_c - P_B)^{d-k}, \; k \geq 1. \tag{13}$$

Note that (13) holds for $d \geq k \geq 1$ only. When $d < k$, $Pr(D_c = k|D = d)$ obviously is 0 since the cooperative degree cannot be more than the degree.

Until now, we have analyzed the node isolation problem and revealed the direct impact of node misbehaviors on the connectivity of individual nodes. Since node isolation is a direct cause for network partitioning, we can use the results in (11) and (13) as cornerstones to derive the network survivability.

V. Network Survivability Analysis

After modeling the evolution of node behaviors by a semi-Markov process and analyzing the impact of node misbehaviors on the connectivity of individual nodes, we are ready to solve the SNM-Problem defined in Section II-C. In this section, we present how to approximate the topological survivability of a wireless ad hoc network in a closed form by using theoretical upper and lower bounds when node misbehaviors and failures are present in the network. Before we present our main result, we introduce the methodology of our solution first.

A. Methodology of Derivation

Let $\delta(\mathcal{G})$ denote the minimum vertex degree of a graph $\mathcal{G}$, then it is well known that $\kappa(\mathcal{G}) \leq \delta(\mathcal{G})$ [27], which implies that the connectivity of a network is no greater than the minimum number of neighbors of any node. Nevertheless, in the random graph theory, it was proved in [28] that

$$Pr(\kappa(\mathcal{G}) = \delta(\mathcal{G})) \to 1. \tag{14}$$

The moral of this result is that a random graph $\mathcal{G}$ becomes k-connected at the instant when it achieves a minimum degree of k with high probability (w.h.p.) [29]. However, (14) holds for *non-geometric* random graphs, in which links may exist between any pair of nodes regardless of node distances. This results cannot be directly applied to wireless ad hoc networks.

Fortunately, a few recent literatures shown that the similar result also holds for geometric random graphs [12], [14], [15], [20],

[29]–[31]. Let $\varrho(\mathcal{N}, \kappa \geq k)$ and $\varrho(\mathcal{N}, \delta \geq k)$ be the minimum (transmission radius) r at which $\mathcal{G}(\mathcal{N}, r)$ is at least k-connected and has minimum degree at least k, respectively. Then it is proved in [30] that for an arbitrary constant k $(1 \leq k < N)$ we have

$$\lim_{N\to\infty} Pr(\varrho(\mathcal{N}, \kappa \geq k) = \varrho(\mathcal{N}, \delta \geq k)) = 1. \tag{15}$$

The above result implies that w.h.p. a network becomes k-connected when the minimum node degree in the communication graph becomes k [29] and N goes to infinity. Based on this seminal result, it was shown that

Lemma 1: ([14, Theorem 3]) For a geometric random graph $\mathcal{G}$ with N vertices, the probability that $\mathcal{G}$ is k-connected approximately equals to the probability that every vertex has at least k neighbors, i.e.,

$$Pr(\kappa(\mathcal{G}) = k) \approx Pr(\delta(\mathcal{G}) \geq k), \tag{16}$$

when N is sufficiently large and $Pr(\delta(\mathcal{G}) \geq k)$ is almost one.

This result has been verified by extensive simulations in [12], [14], [15], [31]. Especially, it was shown in [12] that $Pr(\delta(\mathcal{G}) \geq k)$ is a good estimation for $Pr(\kappa(\mathcal{G}) = k)$ even if N is in the order of 50. Further, even when $Pr(\delta(\mathcal{G}) \geq k)$ is not close to one, it still provides a close approximation for $Pr(\kappa(\mathcal{G}) = k)$.

The seminal results aforementioned offer us a methodology in finding the topological survivability of wireless ad hoc networks. However, due to the presence of node misbehaviors, not every neighbor provides *effective* outgoing paths, as discussed in Section IV-B. Hence, a necessary condition for a network to be k-connected is that every node has at least k cooperative degree (or disjoint outgoing paths). Let $\theta(\mathcal{M})$ denote the minimum of the cooperative degrees of all nodes in a network $\mathcal{M}$, i.e., $\theta(\mathcal{M}) \triangleq \min\{D_c(u),\ \forall u \in \mathcal{M}\}$, we have

Lemma 2: For a wireless ad hoc network $\mathcal{M}$ of N nodes in the presence of node misbehaviors, if $\mathcal{M}$ achieves the minimum cooperative degree at least k and N is sufficiently large, then $\mathcal{M}$ is k-connected asymptotically, i.e.,

$$Pr(\kappa(\mathcal{M}) = k) \approx Pr(\theta(\mathcal{M}) \geq k). \tag{17}$$

Proof: Since $D_c(u) \leq D(u)\ \forall u \in \mathcal{M}$, then $\theta(\mathcal{M}) \leq \delta(\mathcal{M})$, which indicates $Pr(\theta(\mathcal{M}) \geq k) \leq Pr(\delta(\mathcal{M}) \geq k)$. Further, the connectivity cannot be greater than the minimum cooperative degree, i.e., $\kappa(\mathcal{M}) \leq \theta(\mathcal{M})$, thus, $\kappa(\mathcal{M}) \leq \theta(\mathcal{M}) \leq \delta(\mathcal{M})$. Thus, $Pr(\kappa(\mathcal{M}) = k) \leq Pr(\kappa(\mathcal{M}) \geq k) \leq Pr(\theta(\mathcal{M}) \geq k)$ holds in general. Based on (1) given in *Lemma 1*, the lemma follows. ■

Recall that the network survivability has been defined in (1) as the probability that all active nodes are k-connected to a network. By *Lemma 2*, the survivability of a network $\mathcal{M}$ can be given by the probability that all active nodes have at least k cooperative degree, i.e.,

$$NS_k(\mathcal{M}) \approx Pr(\theta(\mathcal{M}_a) \geq k), \tag{18}$$

where $\mathcal{M}_a$ is the sub-network of $\mathcal{M}$ induced by all active nodes. Based on above equation, we are ready to derive the bounds for network survivability next.

B. Bounds of Network Survivability

Although (18) offers a guideline on deriving $NS_k(\mathcal{M})$, it is quite challenging to find the distribution of $\theta(\mathcal{M}_a)$. Indeed, $Pr(\theta(\mathcal{M}_a) \geq k)$ is equivalent to the joint probability of every active node being at least k-connected to the network, i.e.,

$$NS_k(\mathcal{M}) \approx Pr\Big(\bigcap_{u\in\mathcal{M}_a} D_c(u) \geq k\Big). \tag{19}$$

We notice that it has been shown that some random graph models do not generate the correlation of the degrees in a pair of adjacent nodes [32]; however, this non-correlation does not imply the independence of node degrees and even cooperative degrees. Considering that deriving the joint probability is actually intractable, we approximate the survivability by finding its asymptotic upper and lower bounds.

To provide an upper bound, recall that out network model described in Section II-A is a geometric random graph $\mathcal{G}(\mathcal{N}, r)$, in which N vertices are uniformly and randomly distributed on a 2-D square with area A. The vertex set can actually be represented by a (homogeneous) Poisson point process $\mathcal{H}_\lambda$ with density $\lambda = N/A$. Based on the definition of (homogeneous) Poisson point process, the numbers of points within disjoint subareas are mutually independent random variables (with identical distribution). Thus, we can find $N/(\lambda\pi r^2)$ (active) points, denoted by $\mathcal{N}_D$, so that their transmission ranges (πr^2) are disjoint (non-overlapped) subareas (disks). As a result, the degrees of two nodes u and v are mutually independent as $u, v \in \mathcal{N}_D$. Similarly, $D_c(u)$ and $D_c(v)$ are mutually independent as well. Based on the explanation above, we have an upper bound for $NS_k(\mathcal{M})$ given by

$$\begin{aligned} NS_k(\mathcal{M}) &\leq Pr\Big(\bigcap_{u\in\mathcal{N}_D} D_c(u) \geq k\Big) \\ &= \Big(1 - Pr(D_c(u) < k)\Big)^{\frac{N}{\lambda\pi r^2}}. \end{aligned} \tag{20}$$

Thus, once we obtain the distribution function of cooperative degree, we can calculate the upper bound of survivability.

Next, we explain how to obtain a lower bound for survivability. We first rewrite (19) as

$$NS_k(\mathcal{M}) \approx 1 - Pr\Big(\bigcup_{u\in\mathcal{M}_a} D_c(u) < k\Big). \tag{21}$$

Let N_a denote the number of active nodes in the network, $\mathbf{1}_{\{\mathcal{E}\}}$ denote the indicator function, then we can bound $Pr(\cup_{u\in\mathcal{M}_a} D_c(u) < k)$ from above by using ***Boole's inequality***,

$$\begin{aligned} Pr\Big(\bigcup_{u\in\mathcal{M}_a} D_c(u) < k\Big) &= E\left[E\left[\mathbf{1}_{\{\bigcup_{u=1}^{N_a} D_c(u)<k\}} | N_a\right]\right] \\ &\leq E\left[\sum_{u=1}^{N_a} E\left[\mathbf{1}_{\{D_c(u)<k\}}\right]\right] \\ &= E[N_a] \cdot Pr(D_c(u) < k). \end{aligned} \tag{22}$$

Notice that the expected value of N_a is actually equal to $N(1 - P_f)$, i.e., $E[N_a] = N(1 - P_f)$, where P_f is the (limiting) probability of a node in the failed state, defined in (9). We obtain a lower bound for $NS_k(\mathcal{M})$ as

$$NS_k(\mathcal{M}) \geq 1 - N(1 - P_f) \cdot Pr(D_c(u) < k). \tag{23}$$

Again, to solve (23), we need to determine $Pr(D_c < k)$.

By the total probability law, $Pr(D_c < k)$ is given by,

$$Pr(D_c < k) = \sum_{d=0}^{\infty} Pr(D = d) Pr(D_c < k | D = d). \tag{24}$$

Now, we need to find $Pr(D = d)$ and $Pr(D_c < k | D = d)$.

First, to derive $Pr(D = d)$, we use the (de)Poissonization technique presented in [20], [30]. As we mentioned previously, the communication graph of a network $\mathcal{M}$ is associated with a homogeneous Poisson process $\mathcal{H}_\lambda$ with density $\lambda = N/A$. Since we are particularly interested in the topological survivability of

active nodes, let $A_0 = \pi r^2$ denote the area covered by a node's transmission range, it is known that the number of active nodes within A_0 is a Poisson random variable with density $A_0 \cdot (N_a/A)$. Thus, $Pr(D = d)$ can be approximated by

$$Pr(D = d) = \frac{\mu_a^d}{d!} e^{-\mu_a}, \tag{25}$$

where $\mu = \pi r^2 N(1 - P_f)/A$ is the Poisson density. A similar result was also presented in [15], in which more general results were presented for non-uniform node distributions.

Second, we derive $Pr(D_c < k|D = d)$. Since the cooperative degree cannot be greater than the degree for any node, $Pr(D_c < k|D = d)$ is always equal to 1 when $d < k$. When $d \geq k$, $Pr(D_c < k|D = d)$ ($k \geq 1$) can be calculated by

$$\begin{aligned} Pr(D_c < k|D = d) &= \sum_{m=1}^{k-1} Pr(D_c = m|D = d) \\ &+ Pr(D_c = 0|D = d), \end{aligned} \tag{26}$$

in which $Pr(D_c = 0|D = d)$ is the node isolation probability given by (11), and $Pr(D_c = m|D = d)$ is the probability of a node being k-connected given by (13). By substituting (11) and (13) into (26), we can re-write (26) as

$$\begin{aligned} &Pr(D_c < k|D = d) = 1 - (1 - P_B)^d \\ &+ \sum_{m=0}^{k-1} \binom{d}{m} P_c^m \cdot (1 - P_c - P_B)^{d-m}. \end{aligned} \tag{27}$$

Thus, by utilizing (25) and (27), $Pr(D_c < k)$ can be obtained from (24), and the upper and lower bounds of the network survivability can be further obtained from (20) and (23). We present our main result next.

C. Main Result and Implications

Theorem 2: For a wireless ad hoc network $\mathcal{M}$ in the presence of node misbehaviors and failures, when the number of nodes N is sufficiently large, the network survivability defined in (1) is upper bounded asymptotically by

$$NS_k(\mathcal{M}) \leq \left(e^{-\mu_a P_B} \left(1 - \frac{\Gamma(k, \mu_a P_c)}{\Gamma(k)} \right) \right)^{\frac{N}{\lambda \pi r^2}}, \tag{28}$$

and lower bounded asymptotically by

$$NS_k(\mathcal{M}) \geq 1 - N(1 - P_f) \left(1 - e^{-\mu_a P_B} \left(1 - \frac{\Gamma(k, \mu_a P_c)}{\Gamma(k)} \right) \right), \tag{29}$$

where $\mu_a = N(1 - P_f)/(\lambda \pi r^2)$ and λ is the node density, and $\Gamma(h) = (h-1)!$ and $\Gamma(h, x) = (h-1)! e^{-x} \sum_{l=0}^{h-1} x^l / l!$ are the complete and incomplete Gamma functions, respectively.

Proof: By considering $Pr(D_c < k|D = d) = 1$ for $k > d$ and substituting (25) and (27) into (24), $Pr(D_c < k)$ is given by

$$\begin{aligned} &Pr(D_c < k) \\ = &\sum_{d=0}^{k-1} Pr(D = d) + \sum_{d=k}^{\infty} Pr(D_c < k|D = d) Pr(D = d) \\ = &\sum_{d=0}^{\infty} \frac{\mu_a^d}{d!} e^{-\mu_a} - \sum_{d=k}^{\infty} \frac{(\mu_a(1 - P_B))^d}{d!} e^{-\mu_a} \\ &+ \sum_{d=k}^{\infty} \sum_{m=0}^{k-1} \binom{d}{m} P_c^m (1 - P_c - P_B)^{d-m} \frac{\mu_a^d}{d!} e^{-\mu_a}. \end{aligned} \tag{30}$$

The first item on the right hand side (RHS) of (30) equals to one. By using the complete Gamma function $\Gamma(h)$ and incomplete Gamma function $\Gamma(h, x)$, the second item on the RHS of (30) can be simplified as:

$$\sum_{d=k}^{\infty} \frac{(\mu_a(1 - P_B))^d}{d!} e^{-\mu_a} = e^{-\mu_a P_B} \left(1 - \frac{\Gamma(k, \mu_a(1 - P_B))}{\Gamma(k)} \right). \tag{31}$$

The third item on the RHS of (30) is given by

$$\begin{aligned} &\sum_{d=k}^{\infty} \sum_{m=0}^{k-1} \binom{d}{m} P_c^m (1 - P_c - P_B)^{d-m} \frac{\mu_a^d}{d!} e^{-\mu_a} \\ = \; &e^{-\mu_a P_B} \frac{\Gamma(k, \mu_a P_c)}{\Gamma(k)} - e^{-\mu_a P_B} \frac{\Gamma(k, \mu_a(1 - P_B))}{\Gamma(k)}. \end{aligned} \tag{32}$$

By combining (31) and (32), we have (30) simplified as

$$Pr(D_c < k) = 1 - e^{-\mu_a P_B} \left(1 - \frac{\Gamma(k, \mu_a P_c)}{\Gamma(k)} \right) \tag{33}$$

Finally, by substituting (33) into (20) and (23), we obtain the asymptotic upper and lower bounds of network survivability given by (28) and (29), respectively. ■

The above theorem answers the SNM-Problem defined in Section II-C and quantifies the impact of different node behaviors on survivability directly. From the upper and lower bounds given in (28) and (28), respectively, we have the following observations by numeric analysis.

1) In general, the survivability is increasing in the cooperative probability P_c, which is accordant with our intuition. When the network area A is fixed, the higher the number of nodes N is, the higher the survivability is, due to the increased density. While if the density is fixed, increasing N will reduce the survivability. This implies that it will become more difficult to achieve the same survivability level as a network scale gets larger without increasing node density accordingly.
2) Given two networks $\mathcal{M}_1$ and $\mathcal{M}_2$ with the same N, λ, and P_c, besides cooperative nodes, suppose that $\mathcal{M}_1$ has failed nodes only and $\mathcal{M}_2$ has misbehaving (selfish and *Jellyfish*) nodes only, then $NS_k(\mathcal{M}_1) < NS_k(\mathcal{M}_2)$ always holds. The severer impact of node failures is due to the fact that node failures are also isolated from the network, which reduces the density of active nodes (e.g., μ_a).
3) For given N, P_f, and P_c, both upper and lower bounds of the survivability decreases almost exponentially in $\mu_a P_B$. An interesting observation is that when P_B is not zero, a network with higher density can have a lower survivability. Recall that in Section IV-A we have mentioned that a *Blackhole* node may mislead path selections of its neighborhood and trap surrounding traffics, thus the negative impact of *Blackhole* nodes will be exaggerated if they are located in the area with high density.

Note that in real networks the nodes at the vicinity of the network (simulation) boundary have less (active) neighbors and thus become isolated easily, which is known as the *border effect*. As pointed out in [31], the border effect is negligible in analysis if the network area is much larger than the transmission coverage area of a single node and the node density is not high. Since the survivability bounds given in (28) and (29) are all asymptotic for sufficiently large N and we are particularly interested in large-scale extended networks (with fixed density) [31], the border

effect is not considered in our derivation. For further discussions on the border effect, readers are suggested to refer to [15], [31] and the references therein.

Remark 1: It is a premise that $Pr(D_c < k) < 1/N(1-P_f)$ should hold to guarantee a positive lower bound given in (29); otherwise, the lower bound is zero. When $Pr(D_c < k) = o(1/N)$, we have the following approximation

$$1 - N(1-P_f)\left(1 - e^{-\mu_a P_B}\left(1 - \frac{\Gamma(k, \mu_a P_c)}{\Gamma(k)}\right)\right) \approx \left(e^{-\mu_a P_B}\left(1 - \frac{\Gamma(k, \mu_a P_c)}{\Gamma(k)}\right)\right)^{N(1-P_f)}, \quad (34)$$

and the left hand side (LHS) is always less than the RHS in the above equation as $N \cdot Pr(D_c < k) \ll 1$. Since the upper bound given in (28) is quite loose, we conjecture that the RHS of (34) is a tight upper bound for network survivability. Indeed, if cooperative degrees, $D_c(u)$, are assumed to be independent (as independent degrees assumed in [14]), the RHS of (34) becomes the closed-form approximation for network survivability.

Remark 2: A special case of our result in *Theorem 2* is that all nodes are cooperative and node isolations are due to the lack of neighbors only. In this case, the survivability of a network can be simplified to $(1 - \Gamma(k, \lambda\pi r^2)/(k-1)!)^N$ by considering (29) and (34), which is the exact probabilistic k-connectivity approximation given in [14]. This indicates that our result provides a more generalized quantitative evaluation on the topological survivability. Moreover, our result, especially the lower bound, is of interest not only for theoretical analysis but also for practical design of survivable wireless ad hoc networks. For example, if the statistics of user behaviors are available, we can use the methods proposed in Section III to estimate state probabilities. Then given a desired survivability preference (e.g., > 0.9), the minimum cooperative degree or the number of nodes can be calculated as theoretical guidances to determine a proper network deployment so that the survivability preference can be achieved with high probability.

Up to now, we have solved the SNM-Problem by providing the loose upper and tight lower bounds to approximate the network survivability in closed forms, in which the impacts of node misbehaviors and failures can be evaluated directly. Next, we conduct exhaustive simulations to confirm our analytical result.

VI. Scenario Study and Simulation Results

In this part, we provide simulation results of limiting probability estimation, bounds of network survivability, and impact of misbehaviors on network performance.

A. Scenario Study

Recall that we have proposed a semi-Markov node behavior model and provided (9) as the solution for the limiting state probability (P_j for $j \in \mathcal{S} = \{C, S, M, F\}$) in Section III. Even with this formula, calculating P_j is a non-trivial task due to the difficulty in determining the transition probabilities (p_{ij}) and expected sojourn times ($E[T_i]$). Since these parameters are dependent on specific application scenarios, we first establish an example network scenario and incorporate the following policies in our case study and succeeding simulations.

- Every node has the same initial energy E_{init}; and may turn off packet forwarding functionality once its residual energy (normalized by E_{init}) belows a threshold ξ.
- A simplified version of *nuglet counter* [21] scheme is implemented to stimulating selfish nodes to be cooperative again. In this scheme, each node possesses a positive number of tokens I_{init} initially, earns tokens when it forwards packets for other nodes, and spends tokens when it sends or receives its own packets. We assume every selfish node spends $\Delta\bar{I}$ tokens in average per unit time (e.g., 1 s).
- Each cooperative or selfish node has an equal probability to be compromised by an exterior attacker, which can start to compromise a node at any (random) time. The time to compromise a node is assumed to be $\bar{T}_a$ in average. Once a node is compromised, it becomes malicious.
- The time that any node resides in the network (called residence time) is random, depending on the movement pattern of individual nodes, but with a finite expected value $\bar{T}_{in}$. A node is claimed to be failed once it leaves the network.
- At last, we assume an average recovery time $\bar{T}_R$ so that failed nodes can become operative again (e.g., by recharging the battery or rejoining the network).

Remark 3: The above network scenario is simple enough for us to validate our analytical models; while it is general enough to represent a wide range of network scenarios by tuning parameters properly and can be extended to more complicated scenarios by adding more factors.

Given the above scenario, two methods are used in this paper to estimate p_{ij} and $E(T_i)$ (or $E[T_{ij}]$).

1) Empirical Estimation: The empirical estimation largely depends on the statistics of the data collected from real measurements or simulation experiments. First, we use the method proposed in [24] to determine p_{ij} as follows: given the time period $[0, t]$, record the total number of transitions from state i to all other states k and denote it by n_{ik} ($i, k \in \mathcal{S}, k \neq i$), then p_{ij} is approximated by $n_{ij}/\sum_{k\in\mathcal{S}} n_{ik}$. Next, we estimate the expected transition time $E[T_{ij}]$ by using the average value of all observed transition time (from states i to j) of all nodes. Note $E[T_i]$ is derivable from p_{ij} and $E[T_{ij}]$ by using (10), i.e., $E[T_i] = \sum_{j\in\mathcal{S}} p_{ij} E[T_{ij}]$. Obviously, the accuracy of this empirical method depends on the size of data set; in other words, the more nodes and the longer time we can observe, the closer the obtained average values can approach to their expectations.

2) Heuristic Estimation: In this method, we determine p_{ij} by using the same way described in the empirical estimation since no heuristic is known so far to provide an analytical solution of transition probabilities. Nevertheless, given the above network scenario, we can estimate expected transition times by using following heuristics. First, we estimate $E[T_{cf}]$ by considering two factors: energy consumption and node mobility. Let T_{cL} and T_{in} be the lifetime and residence times of a cooperative node, respectively, then the actual time that a cooperative node participating in network activities is the minimum of its lifetime and residence time, i.e., $T_{cf} = \min(T_{cL}, T_{in})$. Thus $E[T_{cf}]$ can be upper bounded by

$$E[T_{cf}] = E[\min(T_{cL}, T_{in})] \leq \min(\bar{T}_{cL}, \bar{T}_{in}), \quad (35)$$

where $\bar{T}_{cL}$ is the mean of node lifetime and $\bar{T}_{in}$ is the average residence time aforementioned. We can further quantify $\bar{T}_{cL}$ by

$$\bar{T}_{cL} \approx \frac{E_{init}}{\alpha P_{Tx} + (1-\alpha) P_{Rx}}, \quad (36)$$

where P_T and P_R denote the average transmitting and receiving power, respectively. And α denotes the ratio between the number

of transmitted packets and that of processed packets. To estimate $E[T_{sf}]$, it is noticed that a cooperative node becomes selfish if its residual energy is below $\xi \cdot E_{init}$ according to our scenario settings aforementioned. Further, considering that a selfish node does not forward packets, if let β denote the ratio between the number of forwarded packets and that of processed packets, we can have the average lifetime of a selfish node approximated by

$$\frac{\xi E_{init}}{(1-\beta)(\alpha P_{Tx} + (1-\alpha)P_{Rx})} = \frac{\xi}{1-\beta}\bar{T}_{cL}.$$

With a similar reasoning, we have $E[T_{sf}]$ upper bounded by

$$E[T_{sf}] \leq \min(\frac{\xi}{1-\beta}\bar{T}_{cL}, \bar{T}_{in}). \quad (37)$$

To estimate $E[T_{mf}]$, recall that a node can be compromised at any time and become malicious after an average (attack) period $\bar{T}_a$, thus we can bound $E[T_{mf}]$ from above as

$$E[T_{mf}] \leq \min(\frac{\bar{T}_{cL}}{2} - \bar{T}_a, \bar{T}_{in}). \quad (38)$$

Other expected transition times are approximated by:

$$\begin{aligned} E[T_{cm}] = E[T_{sm}] &\approx \frac{\bar{T}_{cL}}{2} + \bar{T}_a, \\ E[T_{cs}] &\approx (1-\xi)\bar{T}_{cL}, \\ E[T_{sc}] &\approx \frac{I_{init}}{\Delta I},\ E[T_{fc}] \approx \bar{T}_R. \end{aligned} \quad (39)$$

At last, $E[T_i]$ can be calculated by using (10), similarly.

Now we give an example to show how to calculate P_j by using the heuristic estimation. First, all parameters aforementioned are assigned with the following values, shown in Table I, in order for us to conduct simulation experiments (shown in Section VI-C) and estimate $E[T_i]$ heuristically.

TABLE I
DEFAULT VALUES OF PARAMETERS.

Parameter	E_{init}	α	β	P_{Tx}	P_{Rx}	ξ
Value	$100\ Ws$	0.5	0.5	$0.705\ W$	$0.385\ W$	0.25
Parameter	$\bar{T}_a$	I_{init}	ΔI	$\bar{T}_{in}$	$\bar{T}_R$	
Value	$40\ s$	1500	50	$150\ s$	$60\ s$	

In reality, typical batteries of current laptops can have much higher energy than E_{init} (e.g., the battery for IBM X41 provides 4.4 Ampere Hour with 14.4 Volts output, which supports the energy consumption of all parts including CPU and display). In our work, E_{init} is referred to as the energy consumed by wireless transceivers only. Consequently, $\bar{T}_{in}$ and $\bar{T}_R$ are set to small values in accordance with the short "lifetime". The value for $\bar{T}_a$ is borrowed from the statistics of worm infections (e.g., the *Slammer worm* can infect about 75000 hosts within 30 minutes [33]). The values for P_{Tx} and P_{Rx} are actually derived from the the per-packet energy consumption model proposed in [34].

Next, we obtain the TPM of our semi-Markov model as follows by using the data collected from our simulations:

$$\mathbb{P} \approx \begin{pmatrix} 0 & 0.525 & 0.071 & 0.404 \\ 0.756 & 0 & 0.022 & 0.222 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{pmatrix},$$

then the stationary distribution of the EMC is

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

Then, $E[T_{ij}]$ can be calculated by using (35)-(39). Since p_{ij} are known already, $E[T_i]$ are calculable:

$$E[T_c] = 142.2,\ E[T_s] = 45.9,\ E[T_m] = 51.7,\ E[T_f] = 60.$$

Last, we obtain the limiting probabilities P_i by using (9),

$$P_c = 0.6877,\ P_s = 0.1167,\ P_m = 0.0207,\ P_f = 0.1750.$$

Remark 4: Although the accuracy of using the heuristic method depends on the soundness of the heuristics established (in (35)-(39), for example), the heuristic method provides us an approach to analyze the effect of a specific dynamic factor, such as node mobility, on the stochastic property of node behaviors. Since we have proved that the network survivability also depends on the behavior state distributions, the limiting probability plays an important role in bridging the gap between the network survivability and any specific dynamic that directly affects the limiting probability. Therefore, the semi-Markov node behavior model proposed in this paper does not only provides us a general mathematical framework in describing node behaviors, but also applies to evaluate the impact of a wide variety of random dynamics on the network survivability, via its state distributions.

B. Simulation Setup

To evaluate the correctness of our theoretical analysis, we conducted exhaustive simulations in the simulation tool $ns2$ (v2.28) and a series of numerical experiments in $MATLAB$ (v7). In simulations, the network area approximately represents the center of a town. The number of nodes (network size N) is ranging from 100 to 900 to represent small and large networks. The mobility model chosen is the *Semi-Markov Smooth (SMS) model* [35], which provides the uniform node distribution and more realistic movement patterns. Unless otherwise indicated, the speed is uniformly distributed between 0 and 10 m/s to represent the movements of pedestrians and cars. Constant Bit Rate (CBR) is chosen for traffic and 100 sessions are constantly maintained, in each traffic pattern, 100 sessions are constantly maintained to keep every node involved in networking.

Moreover, in simulations nodes change their behaviors according to the policies described in Section VI-A. For cooperative nodes, AODV is used as the routing protocol; while for misbehaving 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. Specifically, selfish nodes do not forward $RREQ$ and $RREP$ messages for others; malicious nodes forward $RREQ$ and $RREP$ messages but drop data packets to be forwarded. The results are averaged over multiple simulation rounds conducted with various random seeds. The simulation time is set to $2000s$ so that the system can reach steady states. The default network parameters are listed in Table II.

C. Limiting Probability Evaluation

To demonstrate the existence of limiting probabilities, all parameters are set as the values in Table I. We calculated P_j ($j \in \mathcal{S}$) every 10 s based on the cumulated statistics, by using the empirical method introduced in Section VI-A, and illustrated the results with respect to the simulation time in Fig. 4. From the figure, we can see clearly that as more and more statistics are used, the vibration of P_j keeps attenuating and P_j finally reaches to the limiting value after about 1000 s. We also annotated

TABLE II
THE NETWORK SETUP IN SIMULATIONS.

Parameter	Setting
Simulation area	1000 $m \times 1000$ m
System size	500 (100, 900)
Transmission range	100 m
Mobility model	SMS model (uniform placement)
Movement features	avg. speed 5 m/s / pause time 1 s
Link capacity	11 $Mbps$ (1 $Mbps$ for broadcast)
Application	CBR (64 bytes)
Traffic load	100 connections, 8 packet per sec
Simulation time	2000 s

heuristic values of P_j (calculated in Section VI-A already) in the figure (shown as solid and dash lines), from which we can see a good match between the limiting probabilities and heuristic values. This observation confirms the existence of the limiting probabilities and the soundness of our heuristics.

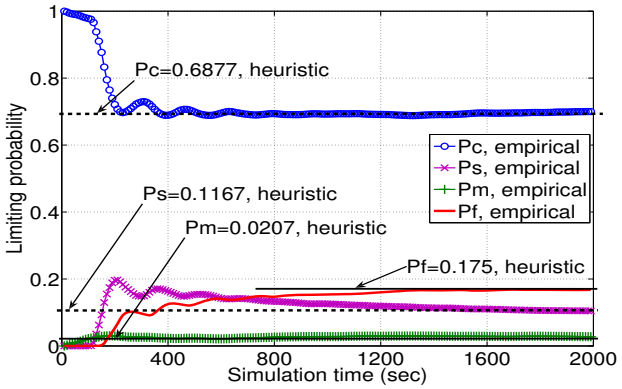


Fig. 4. Limiting probabilities.

Next, we demonstrate how to use our model to investigate the impact of different parameters, including the initial energy E_{init} and node mobility (in terms of $\bar{T}_{in}$), on the limiting probability. In particular, the cooperative probability P_c is of our concern due to its importance in network survivability.

1) Effect of Initial Energy: In Fig. 5, the heuristic value of P_c is increased from 0.69 to 0.74 when the initial energy E_{init} is increased from 100 Ws to 200 Ws, which is consistent with the intuition that a higher initial energy will increase the node lifetime. Nevertheless, the increase is not significant, which is partially due to the fact that the time spent in the selfish state may also be increased given the selfish threshold ξ fixed. Moreover, it is worthy of mentioning that P_m is almost doubled after the increase of E_{init} since the lifetime of a malicious node is actually prolonged. Thus, the impacts of energy are two folds, that is, increasing energy can make end-users behave cooperatively for a longer time but may also exaggerate the impact of malicious nodes on network survivability.

2) Effect of Node Mobility: To evaluate the impact of node mobility on P_c, we conducted simulations using two different average speeds: 20 m/s and 2 m/s, with 10 movement patterns corresponding to each of them. The SMS mobility model used in our paper provides the uniform node distribution, which eliminates the side effect of some artifacts, such as inhomogeneous node density induced by the Random-waypoint model [36] such that the effect of speed can be evaluated accurately. When

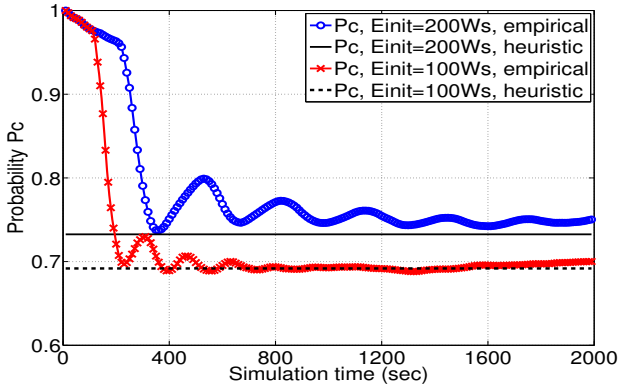


Fig. 5. The effect of E_{init} on P_c.

the simulation area is bounded, we did not observe substantial difference in P_c for both average speed settings. The reason is quite simple: since all nodes are constrained within the boundary, different speeds have no effect to the node residential time, which in turn do not affect P_i. However, in real networks, the boundary does often not exist and nodes can hardly be confined in a given area. To demonstrate the impact of node mobility in real environment, we enlarged the simulation area but still assigned a 1000 $m \times 1000$ m square as the predefined network, such that the churn due to movements can be detected. The simulation results are shown in Fig. 6, in which we can see that the average speed affects P_c considerably, i.e., the higher the mobility is, the lower P_c is. To explain this phenomenon, notice the fact that the faster a node moves, the sooner the node traverses the boundary, yielding a smaller average residence time $\bar{T}_{in}$. Consequently, P_c is decreased due to the decreased time spent in the network. The heuristic values of P_c, annotated in the figure, are calculated by varying $\bar{T}_{in}$, which is simply estimated by dividing the diagonal of the network by the average speed.

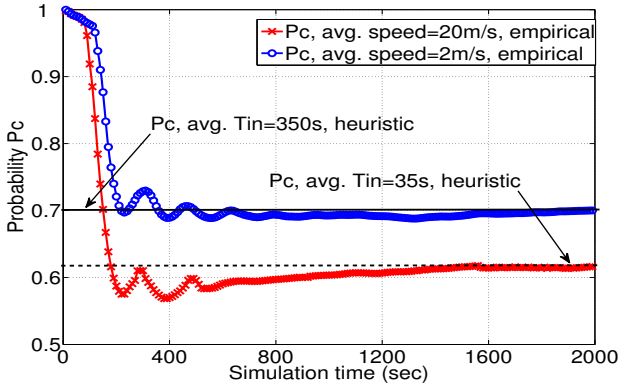


Fig. 6. The effect of nodal mobility on P_c.

D. Network Survivability Evaluation

In this section, we verify the correctness of our theoretical bounds on the network survivability. In simulations, the k-connected survivability is calculated by the ratio between the number of k-connected topologies and that of all topologies studied (around 1000). Since detecting the connectivity of a

network requires extensive computing time, we only consider k up to 3. In order to eliminate the border effect described in Section V-C, we used a wrap-around distance (i.e., toroidal distance [15]) so that nodes at the border are considered as being close to nodes at the opposite border and they are allowed to have links. Further, only the lower bound given in (29) will be depicted as the analytical approximation to the network survivability because the upper bound ((28)) is quite loose compared to the simulation results. In simulation, all network parameters are set to the default values given in Table II. Next, we explain our simulation results.

1) The Effect of Node Cooperativeness: To observe the effect of node cooperativeness clearly, we set the recovery time as 0 so that the effect of node failures is eliminated. We also set $P_B = 0$ so that P_c varies only due to the node selfishness and *Jellyfish* attack. By adjusting the selfish threshold ξ and attack time T_a, a series of P_c values ranging from 0.05 to 0.95 (roughly) were obtained by using the heuristic estimation. The analytical survivability (lower bound) was then calculated for $k = 1, 2, 3$ by using (29) with these P_c values. The simulation and analytic results are shown in Fig. 7, where the curves with markers represent the network survivability measured from simulation data and the ones without markers are for analytical results. From this figure, it is obvious that the network survivability increases when we decreases the connectivity requirement (k), which indicates that the stronger connectivity a network has, the more survivable the network is in terms of its topology. An interesting observation is that the survivability increases very fast from 0 to 1 as P_c increases, for example, the survivability for $k = 2$ is almost 0 as $P_c \leq 0.4$; while it jumps to almost 1 as $P_c \geq 0.7$. This observation is actually in accordance with the so-called *phase transition* phenomenon in (geometric) random graphs (see [27] and [20]) and indicates there exists a critical value of P_c for network survivability. Finally, we can see that the analytical results match with the simulation results with only minor deviation, and especially, the deviation becomes almost invisible when the survivability is above 0.8. This confirms the tightness of the asymptotic lower bound derived from our theoretical analysis.

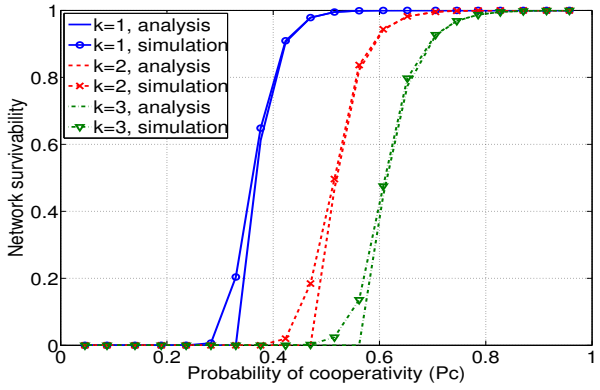


Fig. 7. The effect of node cooperativeness on network survivability.

2) The Effect of Node Failures: To explain the effect of node failures on network survivability, we set both P_s and P_m as zero, by tuning ξ and $\bar{T}_a$, to eliminate the impact of misbehaving nodes. By adjusting initial energy E_{init} and recharging time T_R, we obtain P_f in the range of 0.0376 to 0.8177. Then the network survivability for $k = 1, 2, 3$ is calculated against each of P_f ($P_c = 1 - P_f$) values. The simulation and analytical results are plotted in Fig. 8. From this figure, we observed the similar "phase transition" phenomenon, that is, the network survivability decreases very fast as P_f increasing, especially after a certain value. For example, when $P_f \geq 0.5$, the survivability for $k = 1$ is almost zero, which implies that the network is disconnected almost surely; while an almost sure survivability is achievable only if $P_f \leq 0.3$.

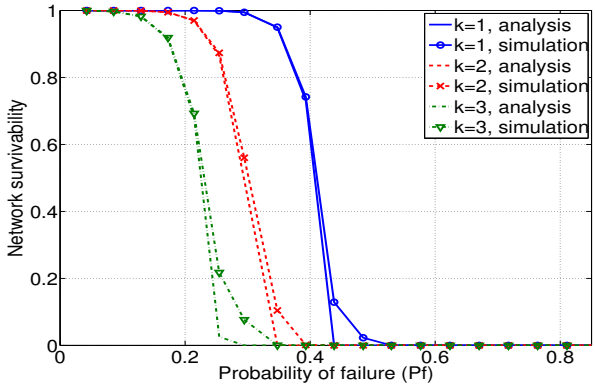


Fig. 8. The effect of node failures on network survivability.

3) The Effect of Node Misbehaviors: In the similar way, we eliminated the effect of node failures in order to study the impact of node misbehaviors only. The simulation and analytical results are depicted in Fig. 9. Similar to the plots in Fig. 8, the curves in Fig. 9 also indicate that the survivability decreases when more and more misbehaving nodes are present, which is consistent with our intuition and the fact of decreased P_c. Nevertheless, compared with the results shown in Fig. 8, we observed that the change of survivability due to node misbehaviors is less significant than that due to node failures, especially for lower connectivity requirement. For example, the survivability for $k = 1$ does not decrease considerably until $P_s + P_m \leq 0.5$ and it keeps positive till $P_s + P_m \geq 0.7$. As we have mentioned in Section V-C, this observation is accordant with the fact that misbehaving nodes are still active in the network layer so that they do not affect the density of active nodes μ_a, which is, however, an important factor for network survivability.

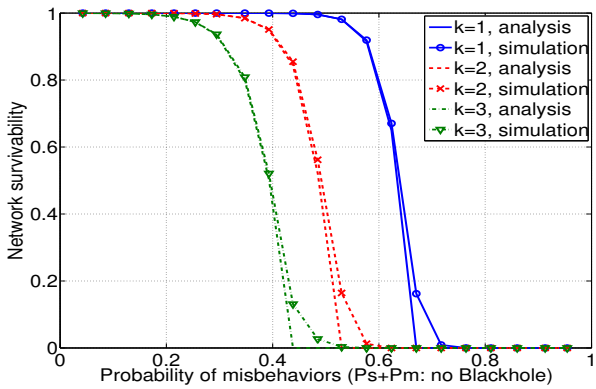


Fig. 9. The effect of selfish and malicious nodes on network survivability.

E. Impacts on Network Performance

To provide a complete picture of the negative effect of node misbehaviors, we also evaluated the network performance when misbehaving nodes are present by simulations, where misbehaving nodes simply drop all data packets to be forwarded once paths are established. This is a *special case* of the traditional *Jellyfish* attack and actually called as the "Blackhole" attack in [19] (different from the *Blackhole* concept in our work). It was pointed out that the performance impact caused by this particular misbehavior is nearly the *same* as that caused by traditional *Jellyfish* attacks that manipulate the delay, reordering, and selective dropping. Thus, we can use CBR (over UDP) to obtain a similar performance evaluation as we use TCP for traditional *Jellyfish* attacks aforementioned, as conducted in [19]. In simulations, the following metrics are considered in the evaluation: normalized goodput, average end-to-end delay, and average hop-count, with all network parameters set to the default values in Table II. The simulation results are shown in Fig. 10.

In Fig. 10(a), the normalized goodputs are shown to decrease significantly when more misbehaving nodes perform abnormal routing operations. This impact is particularly severe to the well-connected network with $N = 500$ nodes. The reason for the drastic degradation on goodput is partially due to the fact of substantial network partitioning effect caused by node misbehaviors, corresponding to the decreased survivability. In particular, the goodput for the network with $N = 100$ nodes is quite low due to the fact that the network is actually disconnected all the times. An interesting observation is that this node misbehavior can shorten end-to-end delays significantly, especially for dense networks (e.g., $N = 900$), as shown in Fig. 10(b). However, this plausible "improvement" is at the cost of suffocating the traffic on long paths, which is explained by the results in Fig. 10(c). In fact, the decrease of average hop-count is not because shorter paths can be found; instead, it captures the effect of network partitioning and survivability downgrading.

Nevertheless, although a low survivability results in a low performance, we cannot conclude a similar implication in the opposite direction. Indeed, providing a theoretical analysis on the impact of node behaviors on network performance is still an open and interesting problem, which will be our future research topic.

VII. Related Work

As aforementioned in Section II-B, although network survivability has been defined from different perspectives and analyzed extensively for wired and infrastructure wireless networks, only a few of survivability studies were made for wireless ad hoc networks. Chen et al. presented a quantitative approach to evaluate the system survivability performance in [6] and introduced the excess packet loss due to failures (ELF) as the survivability measure for wireless ad hoc networks. To obtain ELF, authors assumed Markovian property for the network and conducted an end-to-end availability analysis by solving a set of CTMC models. This work considered both node failure durations and their impacts on the network. Nevertheless, based on our analysis, the Markovian assumption may not hold in wireless ad hoc networks in general. Further, an assumption of the Markov availability model is that for any pair of nodes, other $(N - 2)$ nodes may act as routers, which is, however, not true due to the limitation of node degrees.

In another experimental study [8], Paul et al. analyzed the survivability of wireless ad hoc networks with respect to the dynamic topology changes. In this study, the network survivability was perceived by a number of metrics, such as average connectivity efficiency, average network stability, and service efficiency. Nevertheless, this work did not provide any theoretical analysis to all survivability measures aforementioned and did not take any failure model into consideration. Similarly, although network connectivity was used by a few of other survivability studies, such as [9], [10], no analysis has ever been conducted to reveal the impact of failures on the topological survivability.

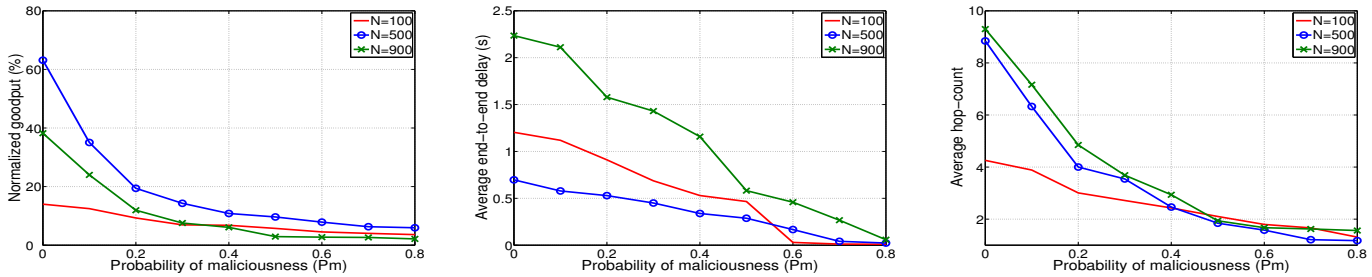
Contrary to the limited theoretical result in the current survivability analysis, there have been abundant theories available from the state-of-the-art connectivity studies. For example, in [15], the connectivity of wireless multi-hop networks was studied thoroughly and a tight bound was given to the problem of finding (r, n) pairs which achieves an almost surely connected network, where r and n denote the transmission range and number of nodes, respectively. An earlier work [14] even provided a closed-form approximation of probabilistic k-connectivity, which can be deduced from our main result (29) by assuming all nodes cooperative. Nevertheless, node degree was considered as the only criteria to decide node isolation and the scenario where nodes might be isolated by misbehaving neighbors has never been considered in previous connectivity studies.

In summary, we can see that previous works either concentrated on the impact of node misbehaviors or DoS attacks on network performance but with no consideration to topology survivability [17]–[19], or focused on the survivability of wireless networks without considering the unique feature of ad hoc networks and the potential impact of all kinds of node behaviors. We hope our paper is the first unified study to provide a theoretical approach for the survivability of wireless ad hoc networks in the presence of both node misbehaviors and random failures.

VIII. Conclusion

In this paper, we developed an analytic framework to study the impact of node misbehaviors and failures on network survivability, which is defined as the probabilistic k-connectivity of the network induced by active nodes. We first classified node behaviors and proposed a novel semi-Markov behavior model to characterize the behavior transitions. With the limiting distribution obtained from the model, we next studied node isolation problem and derived the probabilistic connectivity of individual nodes. Finally, we derived the closed-form approximation of the network survivability by using an (loose) upper bound and (tight) lower bound, which turns out to be a function of the network properties (network size N, transmission range r, and initial density λ) and node behavior distributions.

As a conclusion, the impact of node behaviors (failures) on network survivability can be evaluated quantitatively from our analytical result (*Theorem 2*), which can be further used as a guideline to design or deploy a survivable ad hoc network given a predefined survivability preference. Further, the semi-Markov node behavior model can be used as a bridge between any dynamic factors, such as node mobility or attack intensity (ratio), and network survivability, as long as the factor affects state distributions explicitly. Last but not least, it is surprising that node misbehaviors may "improve" network performance in terms of end-to-end delays in some scenarios; however, this plausible performance improvement sacrifices the survivability of wireless ad hoc networks because of increased node isolations.



(a) Normalized goodput (b) End-to-end delay (c) Average hop-count

Fig. 10. Impacts of misbehaving nodes on network performance.

REFERENCES

[1] F. Xing and W. Wang, "Modeling and Analysis of Connectivity in Mobile Ad Hoc Networks with Misbehaving Nodes," in *Proc. of IEEE Conference on Communications (ICC '06).*, Jun. 2006, pp. 1879–1884.

[2] R. Ellison, D. Fisher, R. Linger, H. Lipson, T. Longstaff, and N. Mead, "Survival Network Systems: An Emerging Discipline," SEI, CMU, Tech. Rep. CMU/SEI-97-TR-013, 1997. [Online]. Available: http://www.cert.org/research/97tr013.pdf

[3] "Telecom Glossary 2000," Institute for Telecommunication Services, NTIA, DOC, Tech. Rep. ANS T1.523-2001, Feb. 2001. [Online]. Available: http://www.atis.org/tg2k/

[4] J. C. Knight and K. J. Sullivan, "On the Definition of Survivability," Dept. of Computer Science, University of Virginia, Technical Report CS-TR-33-00, Jan. 2000.

[5] A. P. Snow, U. Varshney, and A. D. Malloy, "Reliability and Survivability of Wireless and Mobile Networks," *IEEE Computer Magazine*, vol. 33, no. 7, pp. 449–454, Jul. 2000.

[6] D. Chen, S. Garg, and K. S. Trivedi, "Network Survivability Performance Evaluation: A Quantitative Approach with Applications in Wireless Ad-hoc Networks," in *Proc. of the ACM International Workshop on Modeling, Analysis, and Simulation of Wireless and Mobile Systems (MSWiM' 02)*, Sep. 2002, pp. 61–68.

[7] E. Mannie and D. P. (Eds.), "Recovery (Protection and Restoration) Terminology for Generalized Multi-Protocol Label Switching (GMPLS)," IETF, RFC 4427, Mar. 2006. [Online]. Available: http://www.ietf.org/rfc/rfc4427.txt

[8] K. Paul, R. R. Choudhuri, and S. Bandyopadhyay, "Survivability Analysis of Ad Hoc Wireless Network Architecture," in *Mobile and Wireless Communications Networks, LNCS 1818*, C. G. O. (Ed.), Ed. Springer, 2000, pp. 31–46.

[9] D. Goyal and J. J. Caffery, "Partitioning Avoidance in Mobile Ad Hoc Networks Using Network Survivability Concepts," in *Proc. of the 7th International Symposium on Computers and Communications (ISCC'02)*, May 2002.

[10] H. Kawahigashi, Y. Terashima, N. Miyauchi, and T. Nakakawaji, "Designing Fault Tolerant Ad Hoc Networks," in *Proc. of IEEE/AFCEA Military Communications Conference (Milcom '05)*, 2005.

[11] J. P. Sterbenz, R. Krishnan, and et. al, "Survivable Mobile Wireless Networks: Issues, Challenges, and Research Directions," in *Proc. of ACM Workshop on Wireless Security (WiSe'02)*, Sept. 2002, pp. 31–40.

[12] X.-Y. Li, P.-J. Wan, Y. Wang, and C.-W. Yi, "Fault Tolerant Deployment and Topology Control in Wireless Networks," in *Proc. of ACM MobiHoc '03*, Jan. 2003, pp. 117–128.

[13] F. Xue and P. Kumar, "The Number of Neighbors Needed for Connectivity of Wireless Networks," *Kluwer Wireless Networks*, vol. 10, no. 2, pp. 169–181, Mar. 2004.

[14] C. Bettstetter, "On the Minimum Node Degree and Connectivity of a Wireless Multihop Network," in *Proc. of ACM MobiHoc '02*, Jun. 2002, pp. 80–91.

[15] ——, "On the Connectivity of Ad Hoc Networks," *The Computer Journal, Special Issue on Mobile and Pervasive Computing*, vol. 47, no. 4, pp. 432–447, 2004.

[16] P.-J. Wan and C.-W. Yi, "Asymptotic Critical Transmission Radius and Critical Neighbor Number for k-Connectivity in Wireless Ad Hoc Networks," in *Proc. of ACM MobiHoc '04*, 2004.

[17] S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating Routing Misbehavior in Mobile Ad hoc Networks," in *Proc. of ACM MobiCom '00*, 2000, pp. 255–265.

[18] V. Srinivasan, P. Nuggehalli, C. F. Chiasserini, and R. R. Rao, "Cooperation in Wireless Ad Hoc Networks," in *Proc. of IEEE Infocom '03.*, Mar. 2003, pp. 808 – 817.

[19] I. Aad, J.-P. Hubaux, and E. W. Knightly, "Denial of Service Resilience in Ad Hoc Networks," in *Proc. of ACM MobiCom '04*, 2004.

[20] M. Penrose, *Random Geometric Graphs*. Oxford University Press, 2003.

[21] L. Buttyan and J.-P. Hubaux, "Stimulating Cooperation in Self-Organizing Mobile Ad Hoc Networks," *Mobile Networks and Applications*, vol. 8, no. 5, pp. 579–592, Oct. 2003.

[22] D. Miorandi and E. AltmanA, "Coverage and Connectivity of Ad Hoc Networks in Presence of Channel Randomness," in *Proc. of IEEE Infocom '05*, Mar. 2005, pp. 491–502.

[23] J. Medhi, *Stochastic Processes*. John Wiley and Sons, 1994.

[24] G. Corradi, J. Janssen, and R. Manca, "Numerical Treatment of Homogeneous Semi-Markov Processes in Transient Case – a Straightforward Approach," *Methodology and Computing in Applied Probability*, vol. 6, pp. 233–246, 2004.

[25] J.-K. Lee and J. C. Hou, "Modeling Steady-state and Transient Behaviors of User Mobility: Formulation, Analysis, and Application," in *Proc. of ACM MobiHoc '06*, May 2006, pp. 85–96.

[26] D. Heyman and M. Sobel, *Stochastic Models in Operations research*. McGraw-Hill, 1982.

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

[28] ——, *Random Graphs*. Academic Press, 1985.

[29] P. Santi, *Topology Control in Wireless Ad Hoc and Sensor Networks*. John Wiley and Sons Inc., 2006.

[30] M. D. Penrose, "On k-connectivity for a geometric random graph," *Random Struct. Algorithms*, vol. 15, no. 2, pp. 145–164, 1999.

[31] R. Hekmat, *Ad-hoc Networks: Fundamental Properties and Network Topologies*, 1st ed. Springer Netherlands, 2006.

[32] Z. Nikoloski1, N. Deo, and L. Kucera, " Degree-correlation of a Scale-free Random Graph Process," in *Proc. of European conference on Combinatorics, Graph Theory and Applications (Eurocomb'05)*, 2005, pp. 239–244.

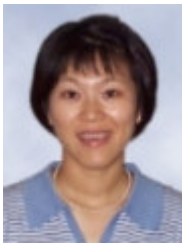
[33] D. Moore, V. Paxson, S. Savage, C. Shannon, S. Staniford, and N. Weaver, "Inside the Slammer Worm," *IEEE Security and Privacy*, vol. 1, no. 4, pp. 33–39, Jul.-Aug. 2003.

[34] L. M. Feeney and M. Nilsson, "Investigating the Energy Consumption of a Wireless Network Interface in An Ad Hoc Networking Environment," in *Proc. of IEEE Infocom '01*, vol. 3, Apr. 2001, pp. 1548–1557.

[35] M. Zhao and W. Wang, "A Unified Mobility Model for Analysis and Simulation of Mobile Wireless Networks," *ACM-Springer Wireless Networks (WINET)*, September 2007.

[36] N. Sadagopan, F. Bai, B. Krishnamachari, and A. Helmy, "PATHS: Analysis of PATH Duration Statistics and their Impact on Reactive MANET Routing Protocols," in *Proc. of ACM MobiHoc '03*, Jun. 2003.

Fei Xing (S'06) received the B.S. and M.S. degrees from Xian Jiaotong University, Xian, China, in 1999 and 2002, respectively. Since 2004, he has been working toward the Ph.D degree in computer engineering at North Carolina State University. His research interests include resilient wireless networks design, mobile ad hoc networks and wireless communication systems. Before joining the doctoral program, he has worked as an engineer for FujiXerox Japan, Huawei Technologies, and Infineon Technologies, sequentially.



Wenye Wang (M'98/ACM'99) received the B.S. and M.S. degrees from Beijing University of Posts and Telecommunications, Beijing, China, in 1986 and 1991, respectively. She also received the M.S.E.E. and Ph.D. degree from Georgia Institute of Technology, Atlanta, Georgia in 1999 and 2002, respectively. She is an Associate Professor with the Department of Electrical and Computer Engineering, North Carolina State University. Her research interests are in mobile and secure computing, network topology and architecture, fault-tolerant computing in single- and multi-hop networks. She has served on many program committees, including IEEE INFOCOM, ICC, ICCCN, and GLOBECOM since 2003. Dr. Wang is a recipient of NSF CAREER Award in 2006. She has been a member of the Association for Computing Machinery since 2002.