Analyzing Resilience to Node Misbehaviors in Wireless Multi-hop Networks

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

***Abstract*— The network resilience has been studied as a fault tolerance measure in wired networks for decades; however, little effort has been made to analyze the resilience of wireless multi-hop networks, especially in the presence of misbehaving nodes. In this work, we study such a problem: whether there exists an overlay achieving "strong" resilience when misbehaving nodes are present in the underlying wireless multi-hop network. To address this problem, We first introduce two new metrics, k-*connected survivability* and *resilience capacity*. The former metric is used to measure the network connectivity probabilistically; while the latter one is used to evaluate the ability of accommodating misbehaving nodes deterministically. We then derive an approximate representation of the k-connected survivability, and provide the close-form representations of resilience capacity for $k = 1$ and $k = 2$ and a heuristic algorithm to calculate it when $k \geq 3$. Finally, based on our analytical results, we prove that an overlay can achieve the derived resilience by satisfying three conditions: (i) containing *all* and *only* cooperative nodes of the original network, (ii) keeping the minimum cooperative degree at least k, (iii) having $\Theta(\log_2 N)$ neighbors of each node in average.**

I. Introduction

The term "resilience" has been used for decades in wired networks to evaluate the fault tolerance and recoverability of a network. Due to some inherent features, such as error-prone wireless channels and dynamic topology, wireless multi-hop networks are more vulnerable to potential node and link failures, compared with wired networks. Thus, the resilience to failures has become an important issue recently in the design of wireless multi-hop networks. In addition to failures caused by node mobility, it has been noticed that node misbehaviors can cause failures as well. For example, nodes may behave selfishly to refuse the packet forwarding for other nodes, or behave maliciously by launching Denial of Service (DoS) attacks. These misbehaviors can undermine the performance and even the connectivity of networks, and have prompted new open and challenging problems to the resilient wireless network design.

A few efforts have been done to analyze the impact of misbehaving nodes. For example, the average throughput was degraded by $16\% - 32\%$ if $10\% - 40\%$ of the nodes misbehave in [1]. It was shown that *Jellyfish* and *Blackhole* attacks have a network partitioning effect [2], and may isolate their neighbors [3]. Also, a number of studies were conducted to enhance the resilience to node misbehaviors. For example, *Ariadne* [4] uses symmetric cryptographic primitives to prevent attacks from tampering routing control messages. *CONFIDANT* [5] uses a reputation system to to detect misbehaving nodes and stimulate cooperation. Nevertheless, little effort has yet been made to analyze the resilience to node misbehaviors for wireless multi-hop networks, and provide quantitative evaluations to the impact of node misbehaviors. In addition, due to lack of the concrete metrics, none of the current works had resilience defined in the presence of node misbehaviors, which makes it infeasible to evaluate and compare the effectiveness of resilience designs.

The limitations above motivate us to provide concrete definitions and theoretic analysis to the resilience of wireless multi-hop networks in the presence of misbehaving nodes, and draw new insights into the design of future resilience-enhancing mechanisms. In particular, we are interested in the question: given a wireless multi-hop network in the presence of misbehaving nodes, whether we can find an *overlay* over it such that the overlay achieves "strong" resilience against misbehaving nodes, called *perfect resilient overlay (PRO)*. By the term *overlay* we refer to a network which is built on top of another network by containing only partial nodes in the original network. The significance of the PRO is in that it provides a resilient platform for network services such as routing and forwarding, and it may simplify the design of other resilient-enhancing solutions once such a resilient platform is generated.

To address this problem, we must first investigate a fundamental question, *what is the resilience of wireless multi-hop networks in the presence of misbehaving nodes?* We use two metrics, k-*connected survivability* and *resilient capacity*, to analyze the resilience of wireless multi-hop networks. The former metric measures the connectivity of a network in the presence of misbehaving nodes; while the latter metric presents the ability of a connected network to accommodate misbehaving nodes. Our resilience metrics distinguish themselves from all previous definitions, reviewed in Section II, by taking the impact of node misbehaviors into account. We then derive an approximate representation of the k-connected survivability, and provide the close-form representations of resilience capacity for $k = 1$ and $k = 2$ and a heuristic algorithm to calculate it when $k \geq 3$. Based on the theoretical analysis on the two resilience metrics, we are able to find the *essential* properties that an overlay should possess to be resilient to node misbehaviors. Finally, we prove that if an overlay contains *all* and *only* cooperative nodes of the original network, and have the minimum cooperative degree of k and the average degree of $\Theta(\log_2 N)$, then the overlay is a PRO, which achieves the maximum resilient capacity and

highest k-connected survivability.

The remainder of this paper is organized as follows. In Section II, we present an overview of previous resilience definitions and analysis. In Section III, we define two resilience metrics and formulate the problem. In Section IV, we analyze the network resilience in terms of the two resilience metrics. In Section V, we provide the essential properties of perfect resilient overlays, followed by conclusions in Section VI.

II. Related Works

To the best of our knowledge, the measure *network resilience* was first introduced by Colbourn [6], which was defined as the expected number of node pairs which can communicate. In [6], network resilience was solved by the summation of *two-terminal* reliabilities of all unordered node pairs. Another resilience definition was presented by Najjar and Gaudiot in [7], [8] which measures the maximum number of node failures that can be sustained while the network remains connected with a given probability. Our newly defined metric, resilience capacity, is partially based on the definition above; however, resilience capacity measures the relative capacity of a network to accommodate misbehaving nodes, defined in Section III-B later. In [9], [10], resilience is mainly referred as the ability of ATM and MPLS networks to recover failed paths in a timely manner. Similarly, Ganesan et al. defined *resilience to isolated failure* in [11] as the probability of at least one alternate path being available within a certain time interval given at least one node failures on the primary path. The resilience to DoS attacks was studied analytically by Aad et al in [2], in which two DoS attacks, *Jellyfish* and *Blackhole*, were introduced and their impacts on multiple performance factors, such as system fairness, throughput, and hop count, were revealed by both analysis and simulation. It was shown that DoS attacks have a network partitioning effect and cause damage to network connectivity; however, no metric was defined to measure the resilience to DoS quantitatively.

As a summary, we can see that all definitions of resilience in previous works only take node failures into consideration. Due to lack of the concrete resilience modeling, the theoretic research on the resilience of wireless multi-hop networks in the presence of node misbehaviors are also limited. We will patch this gap by introducing two new resilience metrics in the next section.

III. Resilience Definition

In this section, we define the resilience to node misbehaviors in wireless multi-hop networks and formulate the problem studied in this work. We begin with the description of the system model.

A. System Model and Assumptions

In this paper, we assume that all nodes are distributed on a two-dimensional plane, independently and uniformly. The transmission radius r of all nodes is same. When the distance of two nodes u and v, denoted by $d(u, v)$, is smaller than r, the two nodes are connected by a link. The topology of wireless multi-hop networks can be defined by a *Geometric Random Graph (GRG)* [12] model, which is defined as:

Definition 1: A GRG $G(N, r)$ is a graph in which N nodes are independently and uniformly distributed in a metric space, and a link exists between two nodes u and v if and only if $d(u, v) \leq r$.

This system model will be used in Section IV to derive our resilience metrics.

Since both selfish and malicious nodes can cause multiple failures, we refer them together as *misbehaving nodes*, denoted by $\mathcal{N}_M$. On the contrary, *cooperative nodes*, denoted by $\mathcal{N}_C$, comply with the standards in the route discovery and packet forwarding. In this paper, we consider a network comprising these two types of nodes only, so a node is either misbehaving or cooperative. Consequently, we use $\mathcal{M}(\mathcal{N})$ to denote a network $\mathcal{M}$ with the node set $\mathcal{N}$, for $\mathcal{N} \triangleq \mathcal{N}_C \cup \mathcal{N}_M$.

B. Resilience Metric Definition

In the design of resilient networks, a fundamental question is what is the resilience of networks? Though it has been well-defined and used for wired networks, as described in Section II, there is no concrete and quantitative definition of resilience for wireless multi-hop networks in the presence of misbehaving nodes. In order to understand statistical and limit of network resilience, and more importantly, to design overlay topology that is resilient to failures, we define two new metrics, *k-connected survivability* and *resilience capacity*, in this paper.

Considering that keeping the underlying network connected is a prerequisite for any networking operation, the first metric is used to evaluate the k-connectivity of wireless multi-hop networks, which is defined as:

Definition 2: A graph G is *connected* if any two distinct vertices are joined by a path, and is *disconnected* otherwise. Generally, if the removal of any $k-1$ vertices does not disconnect G, G is said to be *k-connected*. The maximal value of k for which G is k-connected is the *connectivity* of G, denoted by $\kappa(G)$ [13].

Based on *Definition 2*, for any connectivity requirement k, we define the k-connected survivability as:

Definition 3: The k-connected survivability of $\mathcal{M}$, denoted by $\Psi(k, \mathcal{M})$, is the probability that the connectivity of $\mathcal{M}$ is k conditional on the system size N, i.e.,

$$\Psi(k, \mathcal{M}) = Pr(\kappa(\mathcal{M}) = k \mid |\mathcal{N}| = N), \tag{1}$$

where $\kappa(\mathcal{M})$ is the connectivity of $\mathcal{M}$ and $|\mathcal{N}|$ is the cardinality of set $\mathcal{N}$.

For a better understanding of the resilience against misbehaving nodes, we also propose the second metric, *resilience capacity*, to evaluate the ability of accommodating additional misbehaving nodes in the following scenario. For a wireless multi-hop network $\mathcal{M}$, we assume the number of *existing* misbehaving nodes known and denote it by N_M^0. Given a connectivity requirement k and a survivability preference ψ_0 ($0 < \psi_0 \leq 1$), if $\Psi(k, \mathcal{M}) \leq \psi_0$, the resilience capacity of $\mathcal{M}$ is defined to be zero, which means no more misbehaving nodes can be accommodated by $\mathcal{M}$. If $\Psi(k, \mathcal{M}) > \psi_0$, we need to find out the maximum number of misbehaving nodes, denoted by N_M^*, that $\mathcal{M}$ can sustain and keep its survivability greater than ψ_0. Then we define the resilience capacity as:

Definition 4: The *resilience capacity* of $\mathcal{M}$, denoted by $\Lambda(\psi_0, \mathcal{M})$, is the ratio between the extra number of misbehaving nodes that can be sustained in $\mathcal{M}$ and the system size N, i.e.,

$$\Lambda(\psi_0, \mathcal{M}) = \begin{cases} 0, & \text{if } N_M^* \leq N_M^0 \\ \frac{N_M^* - N_M^0}{N}, & \text{if } N_M^* > N_M^0 \end{cases} \quad (2)$$

where N_M^* is subject to a given survivability preference ψ_0.

Note that in (2), when $N_M^* > N_M^0$, $N_M^* - N_M^0$ is divided by the system size N, which makes this metric applicable to compare the resilience between networks of different system sizes. With the two metrics defined, we can evaluate and analyze the resilience against misbehaving nodes in a quantitative manner.

C. Problem Formulation

Here we formulate the *Existence of Perfect Resilient Overlay (E-PRO)* problem, described in Section I, as follows.

Definition 5: **E-PRO Problem**: Let $\mathcal{M}_s$ denote any overlay of a wireless multi-hop network $\mathcal{M}$, given a connectivity requirement k and a survivability preference ψ_0 ($\psi_0 \to 1$), if an overlay $\mathcal{M}^-$ satisfies the following requirements:

$$\Psi(k, \mathcal{M}^-) \geq \psi_0 \text{ and } \mathcal{M}^- = \underset{\mathcal{M}_s \subseteq \mathcal{M}}{\operatorname{argmax}} \Lambda(\psi_0, \mathcal{M}_s),$$

then $\mathcal{M}^-$ is called a *perfect resilient overlay (PRO)* of $\mathcal{M}$. Now, given any $\mathcal{M}$, how to determine whether a PRO exists?

To tackle the E-PRO problem, we analyze the network resilience in terms of k-connected survivability and resilience capacity in Section IV, then find the essential attributes of a PRO in Section V.

IV. Resilience Analysis

In this section, we analyze the resilience by k-connected survivability and resilience capacity.

A. Preliminary Background

Let $\kappa(G)$ and $\delta(G)$ denote the connectivity and minimum degree of a graph G, respectively, then $\kappa(G) \leq \delta(G)$ holds generally, which implies that $Pr(\kappa(G) = k) \leq Pr(\delta(G) = k)$ for any $k \in \mathbb{N}^+$. Nevertheless, in the random graph theory, it was proved in [14] (*Theorem 6, pp. 154*) that

$$Pr(\kappa(G) = \delta(G)) \to 1. \quad (3)$$

The moral of this result is that a random graph G becomes k-connected at the instant when it achieves a minimum degree of k with a high probability. However, (3) holds for *non-geometric* random graphs, in which links may exist between any pair of nodes regardless of node distances, so this results cannot be directly applied to wireless multi-hop networks.

Fortunately, a few recent literatures shown that the similar result also holds for geometric random graphs (GRGs). According to *Definition 1*, given $r > 0$, a random set $\mathcal{X}_N$ consisting of finite N independent points in a metric space forms a GRG if there exists an edge connecting each pair of points separated by a distance of at most r. It was provide in [15] (*Theorem 1.1*) that, if let $\varrho(\mathcal{X}_N, \kappa \geq k)$ and $\varrho(\mathcal{X}_N, \delta \geq k)$ be the minimum r at which $G(N, r)$ is k-connected and has minimum degree k, respectively, then the following result holds for an arbitrary constant k ($1 \leq k < N$),

$$\lim_{N \to \infty} Pr(\varrho(\mathcal{X}_N, \kappa \geq k) = \varrho(\mathcal{X}_N, \delta \geq k)) = 1. \quad (4)$$

In words, (4) implies that, with high probability, the network becomes k-connected when the minimum node degree in the communication graph becomes k [12] (p.p. 64).

In [16], (4) was further extended to a similar format as (3). We recite this result as

Lemma 1: *Theorem 3 [16]*: For a GRG $G(N, r)$ it holds

$$Pr(\kappa(G) = k) \approx Pr(\delta(G) \geq k) \quad (5)$$

for $N \gg 1$ and $Pr(\delta(G) \geq k)$ almost one.

Lemma 1 has been verified by extensive simulations in [16], [17], and [18]. By (5), the problem of k-connectivity can be simplified by evaluating the minimum degree, which is very useful for us to analyze k-connected survivability.

B. k-connected Survivability

For a real wireless multi-hop network, due to the existence of misbehaving nodes, a node can be isolated from the rest of the network by adjacent misbehaving nodes [3]. In other words, whether a node can be connected to a network depends on whether the node has cooperative adjacent nodes. Let $D_c(u)$ be the number of cooperative adjacent nodes of a node u, called the *cooperative degree* of u, then $D_c(u)$ is i.i.d due to our network model. We define $\theta(\mathcal{M})$ as the *minimum cooperative degree* of a network $\mathcal{M}$, i.e., $\theta(\mathcal{M}) \triangleq \min\{D_c(u),\ \forall u \in \mathcal{M}\}$. Then we have

Theorem 1: Given a wireless multi-hop network $\mathcal{M}$ with the node set $\mathcal{N}$, if $|\mathcal{N}| \gg 1$ and $Pr(\theta(\mathcal{M}) \geq k) \to 1$, then

$$Pr(\kappa(\mathcal{M}) = k \mid |\mathcal{N}| = N) \approx Pr(\theta(\mathcal{M}) \geq k) \mid |\mathcal{N}| = N). \quad (6)$$

The proof of *Theorem 1* can be derived from *Lemma 1*. This result provides us an approach to approximate close-form representation of the survivability, which is shown right next.

Corollary 1: Given a network $\mathcal{M}$ with N nodes ($N \gg 1$) and a connectivity requirement k, let P_M denote the probability of a node being misbehaving, and μ denote the average number of nodes within one node's transmission range, then the k-connected survivability of $\mathcal{M}$ is approximated by

$$\Psi(k, \mathcal{M}) \approx \left(1 - \frac{\Gamma(k, \mu(1 - P_M))}{\Gamma(k)}\right)^N, \quad (7)$$

where $\Gamma(h)$ and $\Gamma(h, x)$ are complete and incomplete Gamma functions, respectively.

Proof: By omitting the notation u, we have

$$Pr(\theta(\mathcal{M}) \geq k) \mid |\mathcal{N}| = N) = (1 - Pr(D_c < k))^N, \quad (8)$$

To obtain $\Psi(k, \mathcal{M})$, $Pr(D_c < k)$ needs to be determined. We derive $Pr(D_c < k)$ by calculating the probability $Pr(D_c = k | D = d)$ and $Pr(D = d)$ first, where D is the node degree, then applying the total probability law to get $Pr(D_c = k)$.

We first derive $Pr(D_c = k | D = d)$. Since a node is either misbehaving or cooperative and P_M is the probability

of a node being misbehaving, the probability of a node being cooperative is $1 - P_M$. By a binomial distribution,

$$Pr(D_c = k|D = d) = \binom{d}{k} \cdot (1 - P_M)^k \cdot P_M^{d-k} \quad (9)$$

Second, we investigate the probability of node degree, i.e., $Pr(D = d)$. Based on our network model in *Definition 1*, all nodes are independently and uniformly distributed over a finite area at random, so node distribution can modeled by a *Poisson point process* [18]. In this process, the Poisson parameter μ actually presents the average number of nodes within the area covered by one node's transmission range. Then $Pr(D = d)$ is given by

$$Pr(D = d) = \frac{\mu^d}{d!} e^{-\mu}, \quad (10)$$

Next, by using the total probability law with (9) and (10), $Pr(D_c = k)$ is

$$Pr(D_c = k) = \sum_{d=k}^{N-1} \binom{d}{k} (1 - P_M)^k \cdot P_M^{d-k} \frac{\mu^d}{d!} e^{-\mu}. \quad (11)$$

Note that in (11), d is bounded within $[k, N-1]$. Since N is sufficiently large ($N \gg 1$), (11) can be rewritten by,

$$Pr(D_c = k) \approx \sum_{d=k}^{\infty} \binom{d}{k} (1 - P_M)^k \cdot P_M^{d-k} \frac{\mu^d}{d!} e^{-\mu}. \quad (12)$$

Then, by using (12), $Pr(D_c < k)$ can be approximated by

$$\begin{aligned} Pr(D_c < k) &\approx \sum_{m=0}^{k-1} \sum_{d=k}^{\infty} \binom{d}{m} (1 - P_M)^m \cdot P_M^{d-m} \frac{\mu^d}{d!} e^{-\mu} \\ &\approx \frac{\Gamma(k, \mu(1 - P_M))}{\Gamma(k)}. \end{aligned} \quad (13)$$

Finally, by substituting (13) into (1), (6), and (8), the k-connected survivability can be given by (7). ■

Until now, we have obtained an approximate representation of k-connected survivability, which is shown to be a function of k, μ, N, and P_M. An observation from this result is that for fixed k, μ and N, a network can have the maximum survivability only if $P_M = 0$. This metric sheds a better insight on the resilience evaluation and can be used for designing resilient, robust networks against failures.

C. Resilience Capacity to Misbehaving Nodes

In this section, we continue to analyze the resilience capacity, $\Lambda(\psi_0, \mathcal{M})$. Recall that $\Lambda(\psi_0, \mathcal{M})$ is defined as $(N_M^* - N_M^0)/N$ when $N_M^* > N_M^0$, in which N_M^* is the maximal number of misbehaving nodes with respect to a survivability preference. To analyze $\Lambda(\psi_0, \mathcal{M})$, we need to obtain N_M^*, which is derived by the following steps.

First, for a network with the node set $\mathcal{N}$, if the behavior of each node is i.i.d., we can prove that

$$\lim_{N \to \infty} \frac{N_M}{N} = P_M, \quad (14)$$

where $N_M = |\mathcal{N}_M|$ and $N = |\mathcal{N}|$. (14) implies that the limiting probability of any node being misbehaving can be calculated by the ratio between the number of misbehaving nodes and that of all nodes. By using (14), given ψ_0, we can use the following equation to derive N_M^*,

$$\psi_0 = \left(1 - \frac{\Gamma(k, \mu(1 - \frac{N_M^*}{N}))}{\Gamma(k)}\right)^N. \quad (15)$$

We next solve (15) in three cases with regard to $k = 1$, $k = 2$, and $k \geq 3$ as follows.

Case 1: $k = 1$. When $k = 1$, (15) is simplified as

$$1 - \exp(-\mu(1 - \frac{N_M^*}{N})) = \psi_0^{\frac{1}{N}}. \quad (16)$$

By calculations, we have

$$\mu(1 - \frac{N_M^*}{N}) = -\ln(1 - \psi_0^{\frac{1}{N}}). \quad (17)$$

Since $(1 - \frac{N_M^*}{N}) \leq 1$, $\mu > -\ln(1 - \psi_0^{\frac{1}{N}})$ should hold in (17). From (17), N_M^* is given by:

$$N_M^* = \lfloor N(1 + \frac{1}{\mu} \ln(1 - \psi_0^{\frac{1}{N}})) \rfloor. \quad (18)$$

Case 2: $k = 2$. When $k = 2$, (15) is

$$1 - (1 + \mu(1 - \frac{N_M^*}{N})) \cdot e^{-(1+\mu(1-\frac{N_M^*}{N}))} = \psi_0^{\frac{1}{N}}. \quad (19)$$

It is non-trivial to solve N_M^* from the equality above, so we refer to *Lambert $\mathcal{W}$ function* [19], which is defined to be the function satisfying

$$\mathcal{W}(z) e^{\mathcal{W}(z)} = z. \quad (20)$$

If z is real, then for $-1/e \leq z < 0$ there are two possible real values of $\mathcal{W}(z)$. The branch satisfying $-1 \leq \mathcal{W}(z)$ is denoted by $\mathcal{W}_0(z)$ or just $\mathcal{W}(z)$, while the branch satisfying $\mathcal{W}(z) \leq -1$ is denoted by $\mathcal{W}_{-1}(z)$. To use the $\mathcal{W}$ function defined above, we rewrite (19) as

$$-(1 + \mu(1 - \frac{N_M^*}{N})) \cdot e^{-(1+\mu(1-\frac{N_M^*}{N}))} = (\psi_0^{\frac{1}{N}} - 1) e^{-1}. \quad (21)$$

In (21), $\mathcal{W}(z) = -(1 + \mu(1 - \frac{N_M^*}{N}))$ and $z = (\psi_0^{\frac{1}{N}} - 1)e^{-1}$. Since $\mathcal{W}(z) < -1$, we can use $\mathcal{W}_{-1}(z)$ to solve N_M^* from (21) as:

$$\mu(1 - \frac{N_M^*}{N}) = -\big(\mathcal{W}_{-1}(e^{-1}(\psi_0^{\frac{1}{N}} - 1)) + 1\big). \quad (22)$$

Similarly, $\mu > -\big(\mathcal{W}_{-1}(e^{-1}(\psi_0^{\frac{1}{N}} - 1)) + 1\big)$ should hold in (22). From (22), N_M^* is given by:

$$N_M^* = \lfloor N\Big(1 + \frac{1}{\mu}\big(\mathcal{W}_{-1}(e^{-1}(\psi_0^{\frac{1}{N}} - 1)) + 1\big)\Big) \rfloor. \quad (23)$$

Case 3: $k \geq 3$. When $k \geq 3$, let $z = 1 - \psi_0^{\frac{1}{N}}$ and $x = \mu(1 - \frac{N_M^*}{N})$, then (15) is:

$$e^{-x}(1 + x + \frac{x^2}{2} + \cdots + \frac{x^{k-1}}{(k-1)!}) = z. \quad (24)$$

(24) is a *transcendental equation*. In general, there are no systematic methods of solving transcendental equations, so we use a heuristic algorithm to find the approximate value of N_M^*, which is described as follows.

Given a network $\mathcal{M}$ with N_M^0 misbehaving nodes and ψ_0, we initiate a variable N_M as N_M^0 and calculate $\Psi(k, \mathcal{M})$. If the result is greater than ψ_0, we increase the value of N_M, calculate $\Psi(k, \mathcal{M})$, and compare the result with ψ_0 again. Until the calculated result is less than ψ_0, then we obtain N_M^* as the current value of N_M. **Algorithm 1** summarizes the heuristic calculation procedure.

Algorithm 1 Calculate N_M^* for $k \geq 3$

Input: N, N_M^0, μ, k, ψ_0

$\Psi := 1,\ N_M := N_M^0$
while ($N_M < N$ AND $\Psi > \psi_0$) **do**
  $\Psi := (1 - \frac{\Gamma(k, \mu(1-\frac{N_M}{N}))}{\Gamma(k)})^N$
  $N_M := N_M + 1$
end while
return $N_M^* := N_M$

Finally, we can use the results obtained from (18), (23), and **Algorithm 1** to calculate the resilient capacity, by using the following algorithm. From **Algorithm 2**, we know that

Algorithm 2 Calculate $\Lambda(\psi_0, \mathcal{M})$

Input: N, N_M^0, μ, k, ψ_0

$\Psi := (1 - \frac{\Gamma(k, \mu(1-\frac{N_M^0}{N}))}{\Gamma(k)})^N$
if ($\Psi \leq \psi_0$) **then**
  return $\Lambda := 0$
else
  if ($k == 1$) **then**
    calculate N_M^* by (18)
  else if ($k == 2$) **then**
    calculate N_M^* by (23)
  else if ($k \geq 3$) **then**
    calculate N_M^* by Algorithm 1
  end if
  return $\Lambda := \frac{1}{N}(N_M^* - N_M^0)$
end if

decreasing N_M^0 can increase $\Lambda(\psi_0, \mathcal{M})$ effectively.

In the next section, we find the properties of a perfect resilient overlay by using the resilience metrics, thereby solving the E-PRO problem.

V. Perfect Resilient Overlay Analysis

In this section, we solve the E-PRO problem formulated in Section III-C, that is, for a given wireless multi-hop networks with misbehaving nodes, how to determine whether a PRO exists? We find the essential properties of a PRO first, then discuss how to check the existence of a PRO.

A. Perfect Resilient Overlay Properties

Based on the analysis on the two resilience metrics, we have the following conclusion.

Theorem 2: Given a wireless multi-hop network $\mathcal{M}$, if an overlay $\mathcal{M}^-$ has the following two properties:

1) $\mathcal{M}^-$ comprises *all* and *only* cooperative nodes of $\mathcal{M}$,
2) $\theta(\mathcal{M}^-) \geq k$, and the average node degree of $\mathcal{M}^-$ is $\Theta(\log_2 N)$ asymptotically,

then $\mathcal{M}^-$ is a perfect resilient overlay of $\mathcal{M}$.

The proof of *Theorem 2* is based on the following lemmas.

Lemma 2: Let N_M be a variable for the number of misbehaving nodes, if $N_M = 0$, $\Psi(k, \mathcal{M})$ is maximum as

$$\Psi_{max} = (1 - \frac{\Gamma(k, \mu)}{\Gamma(k)})^N, \text{ and}$$
$$\Psi_{max} \approx 1 - N\frac{\Gamma(k, \mu)}{\Gamma(k)}, \text{ if } \frac{\Gamma(k, \mu)}{\Gamma(k)} \to 0, \quad (25)$$

where μ and N are defined as previously.

Proof: By (7), $\Lambda(k, \mathcal{M})$ increases as P_M decreases for fixed k, μ, and N. Since $P_M \propto N_M$, the statement holds. ■

Lemma 3: If an overlay $\mathcal{M}^-$ contains *all* and *only* $\mathcal{M}$'s cooperative nodes, then $\Lambda(\psi_0, \mathcal{M}^-)$ is maximized among all overlays on $\mathcal{M}$.

To validate this lemma, we conduct a numeric simulation on three networks with 1000 nodes and different numbers of initial misbehaving nodes N_M^0. For each network, a series of overlays are constructed by removing misbehaving nodes first, then cooperative nodes afterwards. For each overlay, its resilient capacity is calculated by using *Algorithm 1*. The results of this simulation are shown in Fig.1. From this

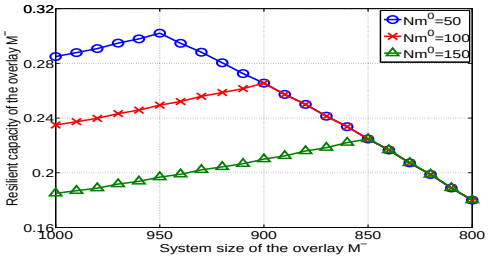

Fig. 1. Illustration of the maximized resilience capacity.

figure, we can see that for each network, the overlay with all its cooperative nodes and no misbehaving nodes has the maximal resilience capacity. Take the curve for the network with $N_M^0 = 100$ as an example, the resilient capacity of overlays reaches the maximum value 0.27 when all 100 misbehaving nodes are removed.

Lemma 4: If a wireless multihop network $\mathcal{M}$ is k-connected, i.e., $\kappa(\mathcal{M}) = k$, then the minimum cooperative degree of $\mathcal{M}$ is at least k, i.e., $\theta(\mathcal{M}) \geq k$.

Proof: The statement follows from *Theorem 1*. ■

Lemma 5: For a wireless multi-hop network $\mathcal{M}$ to be asymptotically connected ($\Psi(1, \mathcal{M}) \geq 0.95$), the average node degree, denoted by $\overline{\Delta}$, should be $\Theta(\log_2 N)$, where N is the system size of $\mathcal{M}$.

To validate this lemma, we recall the following constraint used in the derivation of resilience capacity (Section IV-C). When $k = 1$, the average number of nodes in one transmission range, μ, should satisfy $\mu > -\ln(1 - \psi_0^{\frac{1}{N}})$, which indicates that for a network to be connected with a probability ψ_0, the average node degree should be greater than $-\ln(1 - \psi_0^{\frac{1}{N}}) - 1$. To illustrate how the result above is bounded by $\Theta(\log_2 N)$ as the system size N increasing, we depict the numeric values of $-\ln(1 - \psi_0^{\frac{1}{N}}) - 1$ and $\log_2 N$, respectively, against N in Fig. 2. In the figure, we show

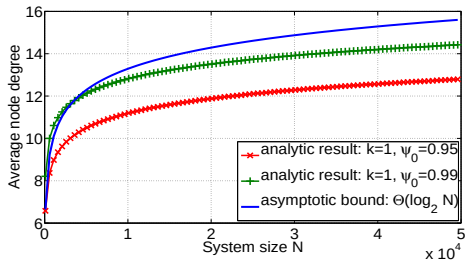

Fig. 2. Average node degree bound for a connected network.

that as N increases, the curve of $\overline{\Delta}$ can be bounded by $\log_2 N$ even for $\psi_0 = 0.99$. Nevertheless, when $\psi_0 \to 1$, the analytical value of $\overline{\Delta}$ will be eventually greater than $\log_2 N$ but still bounded by $c \log_2 N$, where c is a finite constant and $c > 1$. The result of *Lemma 5* is in accordance with the main conclusion shown in [20], where a tight bound of average node degree, $5.1774 \log N$, was provided for any connected networks.

Based on the lemmas above, we can prove *Theorem 2*. *Proof:* By *Lemma 2* and *3*, if $\mathcal{M}^-$ satisfies the first property, then $\mathcal{M}^-$ achieves the maximized resilience. By *Lemma 4* and *5*, if $\mathcal{M}^-$ satisfies the second property, then $(\mathcal{M}^-)$ is k-connected with high probability. Thus $\mathcal{M}^-$ is a perfect resilient overlay. ■

Theorem 2 provides the essential properties of a PRO, which offers us a simple method to verify the existence of a PRO, addressed right next.

B. E-PRO Problem Solution

Based on *Theorem 2*, we are ready to solve the E-PRO problem by a simple, but carefully designed, algorithm, which is described as follows. For a given wireless multi-hop network $\mathcal{M}$ in the presence of misbehaving nodes, here we assume that there exists a mechanism that can detect and remove misbehaving nodes. After all misbehaving nodes are removed from $\mathcal{M}$, an overlay $\mathcal{M}^-$ is obtained which contains all cooperative nodes. Then we calculate the minimum (cooperative) degree $\theta(\mathcal{M}^-)$ and average degree $\overline{\Delta}(\mathcal{M}^-)$ of $\mathcal{M}^-$. If $\theta(\mathcal{M}^-) \geq k$ and $\overline{\Delta}(\mathcal{M}^-) \geq \log_2 N$, then there exists a PRO, i.e., $\mathcal{M}^-$, in network $\mathcal{M}$; otherwise the PRO does not exist. We summarize this procedure in *Algorithm 3*.

Algorithm 3 Check the existence of PRO

Input: $\mathcal{M}(\mathcal{N}_M)$ with N nodes, k

initialize $\mathcal{M}^- := \emptyset$
for all $u \in \mathcal{M}$ **do**
  if $u \in \mathcal{N}_M$, remove u from $\mathcal{M}$
end for
obtain overlay $\mathcal{M}^- := \mathcal{M}$
calculate $\theta(\mathcal{M}^-) := \min\{D_c(v),\ \forall v \in \mathcal{M}^-\}$
calculate $\overline{\Delta}(\mathcal{M}^-) := \frac{1}{|\mathcal{M}^-|} \sum_{v \in \mathcal{M}^-} D_c(v)$
if ($\theta(\mathcal{M}^-) \geq k$ AND $\overline{\Delta}(\mathcal{M}^-) \geq \log_2 N$) **then**
  $\mathcal{M}^-$ is a PRO of $\mathcal{M}$
else
  NO PRO exists in $\mathcal{M}$
end if

VI. Conclusions

In this paper, We defined and analyzed the resilience against misbehaving nodes for wireless multi-hop networks by two metrics: k-connected survivability and resilience capacity. Based on our theoretical analysis, we concluded the essential properties that an overlay should have such that the overlay can achieve maximized survivability and resilience capacity. Our theoretical analysis will shed new insights into the design of resilient wireless multi-hop networks. New topology control paradigms can be developed to form co-operative platforms based on the concept of perfect resilient overlays, and evaluated by our resilience metrics, which will be our future research directions.

References

[1] Sergio Marti, T. J. Giuli, Kevin Lai, and Mary Baker. Mitigating Routing Misbehavior in Mobile Ad hoc Networks. In *Proc. of ACM MobiCom '00*, pages 255–265, 2000.

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

[3] Fei Xing and Wenye Wang. Modeling and Analysis of Connectivity in Mobile Ad Hoc Networks with Misbehaving Nodes. In *Proc. of IEEE ICC '06*, pages 1879 – 1884, 2006.

[4] YihChun Hu, Adrian Perrig, and David B. Johnson. Ariadne: A Secure OnDemand Routing Protocol for Ad Hoc Networks. In *Proc. of ACM MobiCom '02*, Atlanta, USA, Sept. 2002.

[5] HSonja Buchegger and JeanYves Le Boudec. Performance Analysis of the CONFIDANT Protocol (Cooperation Of Nodes: Fairness In Dynamic Adhoc NeTworks). In *Proc. of ACM MobiHoc '02*, volume 1, pages 226 – 236, June 2002.

[6] Charles Colbourn. Network Resilience. *SIAM Journal of Algebra and Discrete Math*, 8:404–409, 1987.

[7] Walid Najjar and Jean-Luc Gaudiot. Network Resilience: A Measure of Network Fault Tolerance. *IEEE Transactions on Computers*, 39(2):174–181, February 1990.

[8] Walid Najjar and Pradip K. Srimani. Network Resilience of Star Graphs: A Comparative Analysis. In *CSC '91: Proc. of the 19th annual conference on Computer Science*, pages 349–357. ACM Press, 1991.

[9] Paul Veitch and Dave Johnson. ATM Network Resilience. *Network, IEEE*, 11(5):26 – 33, Sep-Oct 1997.

[10] Jong T. Park. Resilience in GMPLS Path Management: Model and Mechanism. *IEEE Communication Magazine*, 42(7):128–135, Jul. 2004.

[11] Deepak Ganesan, Ramesh Govindan, Scott Shenker, and Deborah Estrin. Highly-Resilient, Energy-Efficient Multipath Routing in Wireless Sensor Networks. *Mobile Computing and Communications Review (MC2R)*, 5(4):1–13, 2001.

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

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

[14] B. Bollobas. *Random Graphs*. Academic Press, 1985.

[15] Mathew D. Penrose. On k-connectivity for a Geometric Random Graph. *Random Struct. Algorithms*, 15(2):145–164, 1999.

[16] Christian Bettstetter. On the Minimum Node Degree and Connectivity of a Wireless Multihop Network. In *Proc. of ACM MobiHoc '02*, pages 80–91. ACM Press, June 2002.

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

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

[19] R. M. Corless, G. H. Gonnet, D. E. G. Hare, D. J. Jeffrey, and D. E. Knuth. On the Lambert W Function. *Advances in Computational Mathematics*, 5(1):329–359, 1996.

[20] Feng Xue and P.R. Kumar. The Number of Neighbors Needed for Connectivity of Wireless Networks. *Kluwer Wireless Networks*, 10(2):169–181, Mar. 2004.