

# On Pairwise Connectivity of Wireless Multihop Networks

Fangting Sun and Mark Shayman

Department of Electrical and Computer Engineering

University of Maryland, College Park, MD 20742

{ftsun, shayman}@eng.umd.edu

## Abstract

This paper experimentally investigates the service availability of wireless multihop networks based on the following two metrics: *average pairwise connectivity* and *pairwise connected ratio*, where the former denotes the average number of node-disjoint paths per node pair in a network and the latter is the fraction of node pairs that are pairwise connected. Further, a theoretical upper-bound has been derived for the average pairwise connectivity, which can approximate the exact value very well. Since in wireless multihop networks nodes may fail either naturally or maliciously, the fault tolerance and attack resilience are important issues. In this paper we have also studied the fault tolerance and attack resilience of wireless multihop networks, and proposed a new resilience metric,  $\alpha$ - $p$ -resilience, where a network is  $\alpha$ - $p$ -resilient if at least  $\alpha$  portion of nodes pairs remain connected as long as no more than  $p$  fraction of nodes are removed from the network. Three different node removal patterns have been studied: random removal, selective removal according to node degree, and partition, and the experimental studies show that wireless multihop networks are more sensitive to partition attacks than random removal and selective removal attacks, and selective removal attacks are a little bit more severe than random removal attacks.

## I. INTRODUCTION

Wireless multihop networks are formed by a group of nodes connected by wireless links where nodes can communicate with other nodes beyond their direct transmission range by cooperatively forwarding packets for each other [1]. Some typical examples of such networks include wireless ad hoc and sensor networks. Since such networks can be easily and inexpensively set up as needed in a decentralized manner, they have a wide range of applications, such as military exercises, disaster rescue, mine site operations, environment monitoring, and so on.

In this paper we investigate the network service availability of wireless multihop networks by focusing on the average case. To measure the network service availability, the following two metrics are proposed: *average pairwise connectivity* (APC) and *pairwise connected ratio* (PCR), where the former denotes the average number of node-disjoint paths per node pair and the latter indicates the fraction of node pairs that are connected, or in other words, the proportion of nodes to which each node can communicate (directly or indirectly) in average. Extensive experiments have been conducted to study the APC and PCR of wireless multihop networks under different scenarios and configurations. In these experiments, the following types of random graphs have been used to model wireless multihop networks: Poisson random graphs and geometric random graphs. Beside studying the relationship between node density and pairwise connectivity, we have derived an analytical upper-bound for APC and demonstrated that the APC can be approximated by its upper-bound very well, especially in Poisson random graphs. Meanwhile, we have also investigated the effects of (physical) boundary in wireless multihop networks, which can introduce discrepancy between the APC and its upper-bound.

In wireless multihop networks, due to the fragile wireless connections and possible mobility, link breakages may happen very frequently. Meanwhile, some nodes may be removed from the network due to the exhaustion of battery power. Therefore, the study of fault tolerance should be an indispensable component, where the network fault tolerance denotes the ability of a network to continue operating even though some of its components have malfunctioned or failed<sup>1</sup>. Furthermore, such networks may also be deployed in adversarial environments, and some parts of the network may become unusable due to the attacks from malicious parties.

<sup>1</sup>In this paper “fault” refers to those link or node removals caused unintentionally, that is, no malicious parties are involved. Those link or node removals involving malicious parties will be referred to as “attack”.

For example, in wireless sensor networks, due to lacking enough physical protection, nodes can be easily captured, compromised, or hijacked. Since nodes in such networks usually share the common communication channels, malicious parties can also launch jamming attacks to disrupt the normal communications, which can consequently result in some nodes or links becoming disconnected from the network. In such circumstances, the ability of a network to continue operating even under attacks becomes critical, which is referred to as *attack resilience*.

To measure the network fault tolerance and attack resilience, one widely used metric is network connectivity. For example, network fault tolerance has been defined as the maximum number of elements that can fail without inducing a possible disconnection in the network [2], [3], that is, the network connectivity [4]. However, the use of network connectivity to measure network fault tolerance only focuses on the worst case. First, a network not being  $k$ -connected only implies that there exists some choice of  $k - 1$  nodes whose removal would disconnect the network, but does not mean that if  $k - 1$  nodes are removed, it is likely that the network will be disconnected. Second, even if the removal of a group of nodes disconnects the network, it is still possible that only one or a small number of nodes become isolated from the rest, and may not have a significant impact on the usefulness of the network, and the network may have high average pairwise connectivity and pairwise connected ratio. Recently, the attack resilience issues have also drawn extensive attention. In [5], Albert et. al. first studied the attack resilience issues in scale-free networks. Following this, the attack resilience of some other networks have been studied, such as Internet [6]–[8], food web [9], [10], protein network [11], email network [12], complex network [13], and so on. To measure the attack resilience, one candidate is the average vertex-to-vertex distance as a function of the number of vertices removed [5], or equivalently, the average inverse geodesic length [13], where both measure the average distance between node pairs in a network. However, such a metric may not be appropriate to measure the attack resilience of wireless multihop networks for the reason that in such networks the average vertex-to-vertex distance will increase with the increase of network size for a fixed node density, while it is not necessarily accompanied by a decrease in the network attack resilience.

To overcome the limitation of the existing metrics to measure the fault tolerance and attack resilience of wireless multihop networks, we propose a new metric:  $\alpha$ - $p$ -resilience. Specifically, a network being  $\alpha$ - $p$ -resilient means that its expected PCR is no less than  $\alpha$  as long as no more than  $p$  fraction of nodes are removed. It is worth pointing out that the  $\alpha$ - $p$ -resilience of a network

may not be the same under different node removal patterns. For example, a network is usually more  $\alpha$ - $p$ -resilient to random fault than to attack. A similar metric can be used to measure the decrease of APC under fault or attack.

In this paper, the following three node removal patterns are investigated: random node removal, selective node removal according to node degree, and partition. Random node removal means that nodes are removed randomly. Selective node removal means that nodes are removed in decreasing order of degree with ties being broken randomly as in [5], where the degrees will be recalculated following the removal of each node. Partition means that removing nodes in such a way that the remaining network will be partitioned into disconnected components, where the specification of the nodes to be removed will be given later. In this paper extensive experiments have been conducted to study the fault tolerance and attack resilience of wireless multihop networks under the above three node removal patterns. The results show that when the APC is high, the networks are very sensitive to partition attacks, but are robust to random removal and selective removal, and selective node removal can cause a little bit more damage than random node removal when a large portion of nodes are removed. When the APC is low, the three attacks have similar effects with selective node removal and partition attacks being a little bit more damaging than random node removal.

The rest of this paper is organized as follows. Section II introduces the network model and the metrics. Section III investigates the properties of the pairwise connectivity for Poisson and geometric random graphs. The network fault tolerance is studied in Section IV, and the attack resilience is studied in Section V. Finally, Section VI concludes this paper.

## II. NETWORK MODELS AND METRIC DEFINITIONS

In this section, we first introduce the random graph models used to model the wireless multihop networks, then describe the different connectivity definitions as well as  $\alpha$ - $p$ -resilience, and finally compare pairwise connectivity with network connectivity.

### A. Network Modeling

In the literature, random graphs have been widely used to model various networks [4], [14]–[16]. In order to model wireless multihop networks, such as ad hoc networks, Poisson random graphs have been suggested by Chlamtac and Faragó [17]. However, since Poisson random

graphs have not considered correlations between different links, in many situations it may not be the best model. To fix this problem, a modified version of Poisson random graphs, geometric random graphs, have been widely used recently [15]. In this paper, both models will be studied, though the geometric random graph model will be the focus.

1) *Poisson Random Graphs*: After being independently proposed by Solomonoff and Rapoport [18], and Erdos and Renyi [19], [20], Poisson random graphs have been widely applied to model various networks [4], and have been well studied by mathematicians, and many results, both approximate and exact, have been proved [21], [22]. In general, a *Poisson random graph*  $G(N, p)$  is a graph with  $N$  nodes in which for each pair of nodes, with probability  $p$  there is an edge between them. By holding the average node degree  $\lambda = p(N - 1)$  constant, the probability of a node having degree  $k$  can be calculated as

$$p_k = \binom{N-1}{k} p^k (1-p)^{N-1-k} \simeq \frac{e^{-\lambda} \lambda^k}{k!}, \quad (1)$$

with the last approximate equality becomes exact in the limit of large  $N$  and fixed  $k$ , from which the name ‘‘Poisson random graph’’ comes.

2) *Geometric random graph*: In the literature, geometric random graphs have also been widely used to model various multihop wireless networks [14]–[16]. Since the construction of geometric random graphs has incorporated the spatial correlations between nodes and edges, it can better model the topologies of wireless multihop networks. In this paper we will mainly focus on the two-dimensional case, where now a *geometric random graph*  $G(N, r)$  is a graph in which  $N$  nodes are independently deployed inside a large area of size  $A$  according to the 2D uniform distribution<sup>2</sup>, and for any pair of nodes there exists an edge between these two nodes if and only if the distance between them is no more than  $r$  (e.g., in wireless multihop networks,  $r$  is nodes’ maximum transmission range). Let  $\gamma = \frac{N\pi r^2}{A}$  denote the *normalized average node density* of such a random graph, which denotes the average number of nodes inside a circle with radius being  $r$ . In this paper, we simply refer to normalized average node density as average node density. For any node not lying in the boundary area<sup>3</sup> of the network deployment, the

<sup>2</sup>A node  $v$  is deployed inside an area  $A$  according to the 2D uniform distribution if for any subarea  $A_1 \subset A$ ,  $P(v \in A_1 | v \in A, A_1 \subset A) = A_1/A$ .

<sup>3</sup>In this paper, we say a node  $v$  lies in the boundary area of a network deployment if and only if there exists at least one location which does not lie in the deployment area and whose distance to node  $v$  is less than  $r$

probability of a node having degree  $k$  can be calculated as

$$p_k = \binom{N-1}{k} \left( \frac{\pi r^2}{A} \right)^k \left( 1 - \frac{\pi r^2}{A} \right)^{N-1-k} \simeq \frac{e^{-\gamma} \gamma^k}{k!}, \quad (2)$$

with the last approximate equality becomes exact in the limit of large  $A$  and  $N$  and fixed  $k$ . That is, the distribution of degree also follows Poisson distribution with the average degree being  $\gamma$ . It is worth mentioning that due to the boundary effects (e.g., the average degree of nodes inside the boundary area is less than the average degree of nodes not inside the boundary area), the average node degree of a geometric random graph is less than its average node density.

### B. Pairwise Connectivity and $\alpha$ - $p$ -resilience

Based on the above network models, a wireless multihop network can be represented as an undirected graph  $G = G(V, E)$  at each time instant, which comprises  $|V|$  nodes and  $|E|$  edges, and for any  $u, v \in V$ , if  $(u, v) \in E$ , then  $(v, u) \in E$ . Two nodes  $u$  and  $v$  are said to be connected if there exists at least one path between  $u$  and  $v$ ; otherwise these two nodes are said to be disconnected. Given any pair of nodes  $u, v \in V$ , let  $C(u, v)$  denote the maximum number of node-disjoint paths<sup>4</sup> from node  $u$  to node  $v$ , which we refer to as the *pairwise connectivity* of node pair  $(u, v)$ . Equivalently,  $C(u, v) = k$  means that there exist no such set of  $k - 1$  nodes whose removal would make  $u$  and  $v$  disconnected, and there exists at least one set of  $k$  nodes whose removal would make  $u$  and  $v$  disconnected. A node pair  $(u, v)$  is said to be  $k$ -pairwise-connected if  $C(u, v) \geq k$ . Since  $G$  is undirected, we always have  $C(u, v) = C(v, u)$ .

According to [4], a graph  $G = G(V, E)$  is said to be connected if any pair of nodes in  $G$  is connected, and  $G$  is said to be  $k$ -connected if for any pair of nodes  $u, v \in V$ ,  $C(u, v) \geq k$ . It is easy to see that this measure focuses on the worst case scenario. However, in many situations, even if the network becomes disconnected, i.e., some nodes become isolated, the remaining nodes in the network can still communicate with each other with very high probability. For example, in a self-organized wireless multihop network [23], individual nodes are only interested in whether their own communication request can be satisfied, and in general a single node isolated from the network will not significantly affect the other nodes, although the network is disconnected.

<sup>4</sup>A set of paths from  $u$  to  $v$  are said to be node-disjoint if these paths do not share any common nodes except  $u$  and  $v$ .

In order to measure the average case network service availability, we introduce the following metrics: *average pairwise connectivity* and *pairwise connected ratio*. For any graph  $G$ , the average pairwise connectivity (APC) of  $G$ , denoted by  $C(G)$ , is defined as follows:

$$C(G) = \frac{1}{N(N-1)} \sum_{u \in V} \sum_{v \neq u \in V} C(u, v), \quad (3)$$

which is the average number of node-disjoint paths between any pair of nodes in the network. Similarly, pairwise connected ratio (PCR) is defined as follows:

$$PCR(G) = \frac{1}{N(N-1)} \sum_{u \in V} \sum_{v \neq u \in V} \mathbf{1}[C(u, v) \geq 1], \quad (4)$$

which is the indicator version of APC. It is the proportion of node pairs that are pairwise connected, i.e., can communicate with each other. In other words, from an individual node's point of view, this is the proportion of nodes in average that it can reach in the network. Meanwhile, a network with PCR being  $\alpha$  indicates that there exists at least one connected component which comprises at least  $\alpha$  portion of the total nodes.

In general, fault tolerance or attack resilience can be measured as the decrease of network performance due to node or edge removal. In this paper we propose  $\alpha$ - $p$ -resilience to measure the decrease of network service availability under node removal. Specifically, given a network  $G$ , if it is  $\alpha$ - $p$ -resilient in PCR, then even after removing  $p$  portion of nodes, the PCR is still no less than  $\alpha$ , that is, for any remaining node in the network, it can still expect to connect to  $\alpha$  portion of the remaining nodes. Similarly, given a network  $G$ , if it is  $\alpha$ - $p$ -resilient in APC, then even after removing  $p$  portion of nodes, the APC is still no less than  $\alpha$ , that is, the average number of node-disjoint paths between any pair of remaining nodes is at least  $\alpha$ .

### C. Pairwise Connectivity vs. Network Connectivity

In this subsection we study the difference between pairwise connectivity and network connectivity through experiments. In the experiments, a set of geometric random graphs are generated with the deployment areas varying from  $10r \times 10r$  to  $50r \times 50r$ , where  $r$  is node's transmission range. The PCR and network connected ratio (NCR) for different network size and node density are illustrated in Fig. 1, where NCR denotes the percentage of connected networks among all the generated networks. In Fig. 1 each data point is the average result over 1000 independently generated random graphs.

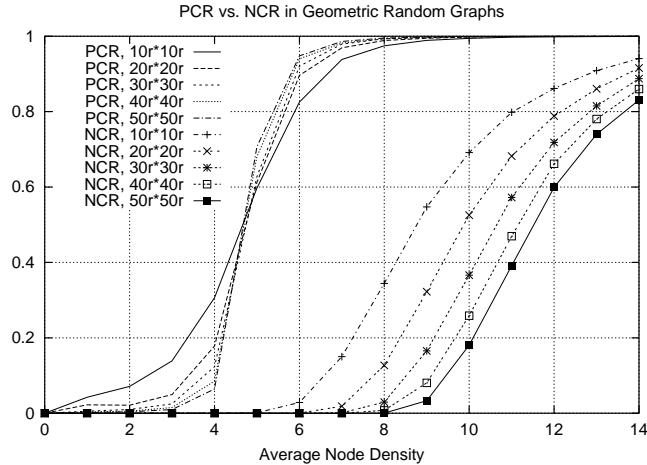


Fig. 1. Comparison between pairwise connected ratio and network connected ratio

First, from these results we can see that although in many situations the network connected ratio is low, that is, a large portion of the generated networks are not connected, almost all pairs of nodes in the network can communicate with each other. For example, for the network size being  $20r \times 20r$  and node density being 10, which can be a very reasonable configuration for a wireless multihop network, only about 14% of the generated networks are connected, while more than 99.9% of node pairs in the generated networks can communicate with each other through one or more routes. This suggests that in many situations network connectivity may not be an appropriate metric to measure the average case network service availability.

Second, by comparing the NCR values illustrated in Fig. 1 under different network configuration, we can see that with the increase of network size, the network connected ratio will decrease, which is easy to understand: the more the number of nodes in the network, the higher the probability that some nodes will become isolated. However, from Fig. 1 it is surprising to see that whenever the node density is no less than 5, by fixing the node density, the larger the network size, the higher the PCR, although more nodes will become isolated. That indicates that the more the number of nodes in the network, usually the better the service availability that the network may provide, since each node may have more resources to use and more options to take. This also suggests that network connectivity may not be appropriate when used to measure the network service availability.

Third, from these results we can see that the PCR curves exhibit sharp threshold behaviors,

where the PCR increases dramatically when the node density increases from 4 to 6. With node density 4 the PCR is less than 20% for most cases, while with node density 6 the PCR becomes more than 90% in most cases. Furthermore, all these PCR curves intersect with each other at around density 5. When the node density is less than 5, the larger the network, the lower the PCR; while when the node density is greater than 5, the larger the network, the higher the PCR. This is the combined effect of path length and available resources: the longer the path length, the lower the probability that a pair of nodes can connect; while the more the resources, the higher the probability that a pair of nodes can connect. When node density is very low, the effect of path length will dominate the effect of available resources (the average path length in the networks with size  $10r \times 10r$  is only about half of that in the networks with size  $20r \times 20r$ ). When the node density becomes high, the effect of available resources will play a dominant role.

Finally, from these results we can see that to maintain high pairwise connectivity, the node density should be no less than 7. From the results in this figure we can see that when the density is less than 7, in all five cases the PCR is less than 95%. The network size may affect this threshold, but not significantly. Meanwhile, we can see that when the node density is larger than a certain value (e.g., 10), the PCR will closely approach 1. In other words, as long as the node density is higher than some threshold, a certain level of service availability can be guaranteed.

### III. THE PAIRWISE CONNECTIVITY OF WIRELESS MULTIHOP NETWORKS

In this section we focus on studying the service availability of wireless multihop networks based on the following two metrics: APC and PCR. When studying the APC, we have derived an analytical upper-bound for APC, and demonstrated that the APC can be approximated by its upper-bound very well for Poisson random graphs and for the inner part of geometric random graphs.

Given any graph  $G(V, E)$  and any node  $u \in V$ , let  $d(u)$  denote the degree of node  $u$ , that is, the number of neighbors of node  $u$ . Then for any pair of nodes  $u, v \in V$ , let

$$C_{upper}(u, v) = \min\{d(u), d(v)\}. \quad (5)$$

Since it is obvious that the number of node-disjoint paths between  $u$  and  $v$  cannot exceed the degrees of  $u$  and  $v$ ,  $C_{upper}(u, v)$  is always an upper bound of  $C(u, v)$ . Accordingly, we can

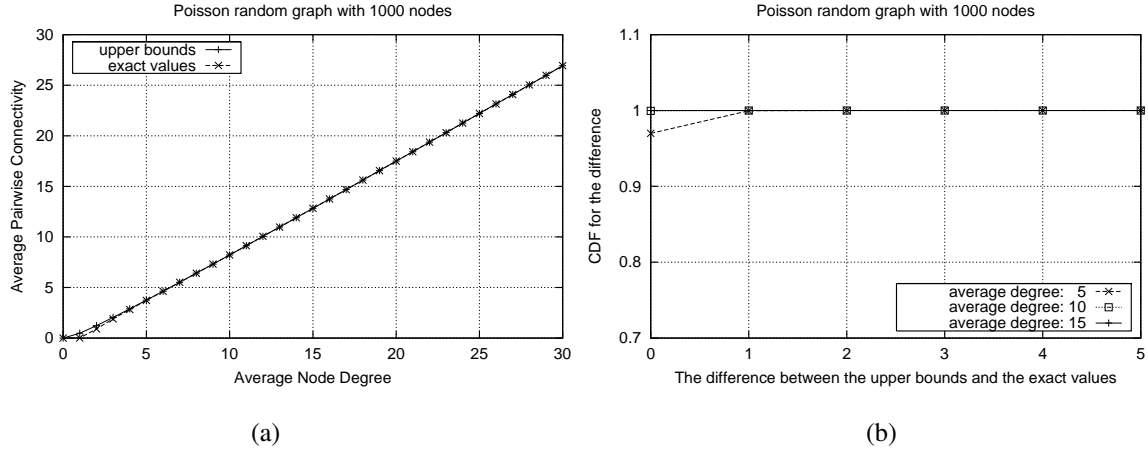


Fig. 2. Upper bounds and exact values of APC for Poisson random graphs

define the upper bound of  $C(G)$  as follows:

$$C_{upper}(G) = \frac{1}{N(N-1)} \sum_{u \in V} \sum_{v \neq u \in V} C_{upper}(u, v). \quad (6)$$

For any graph  $G(V, E)$  and any pair of nodes  $u, v \in V$ , let  $d_{diff}(u, v)$  denote the difference between  $C_{upper}(u, v)$  and  $C(u, v)$ , that is,

$$d_{diff}(u, v) = C_{upper}(u, v) - C(u, v). \quad (7)$$

Let  $d_{diff}$  denote the random variable representing the difference between the upper bound and exact value of any pair of nodes in the network. In other words, given a graph,  $d_{diff}$  corresponds to picking a pair of nodes  $(u, v)$  at random and taking  $d_{diff}(u, v)$ . Then for any pair of nodes, the probability that the difference between their upper bound of pairwise connectivity and the exact pairwise connectivity is equal to  $k$  can be calculated as follows:

$$P(d_{diff} = k) = \sum_{u \in V} \sum_{v \neq u \in V} \frac{\mathbf{1}[d_{diff}(u, v) = k]}{N(N-1)}, \quad (8)$$

where  $\mathbf{1}[condition]$  is an indicator function defined as follows:

$$\mathbf{1}[condition] = \begin{cases} 1 & \text{condition is true} \\ 0 & \text{condition is false} \end{cases} \quad (9)$$

### A. Poisson Random Graphs

We first study the APC in Poisson random graphs through experiments, which are set up as follows: the total number of nodes, denoted by  $N$ , is fixed to be 1000, and for any pair of nodes, with probability  $p$  there is an edge to directly connect them. Different values of  $p$  are tested, and the average node degree can be calculated as  $(N - 1)p$ . The experimental results with different average node degrees are shown in Fig. 2, where Fig. 2(a) illustrates the relationship between the average node degree and the APC (both  $C_{upper}(G)$  and  $C(G)$  are shown), and Fig. 2(b) demonstrates the distribution of  $D_{diff}$ , the difference between the upper bound and exact value of the APC, under three different average node degrees: 5, 10, and 15. For each average node degree, the results are averaged over 1000 independently generated Poisson random graphs.

First, from these results we can see that the APC increases monotonically with the increase of average node degree, which is easy to understand. Second, it is surprising to see that the upper bounds and exact values of the APC are almost equal in all configurations, except when the average node degree is extremely low (e.g., average node degree is less than 5), which indicates that the APC of Poisson random graphs can be almost completely characterized by the corresponding upper bounds. These results also indicate that in Poisson random graphs, when the average node degree is large, the bottleneck to find multiple node-disjoint paths between a pair of nodes lies in the degrees of the two nodes themselves.

Now we show how to directly calculate the upper bound of APC for Poisson random graphs. Here we make the simplifying assumption that the degree distributions for different nodes are independent in Poisson random graphs, though it may not be strictly true. When  $N$  is large and  $(N - 1)p = \lambda$ , given any pair of nodes  $u$  and  $v$ , it is easy to show that the probability of  $C_{upper}(u, v)$  equal to  $k$  can be calculated as follows:

$$\begin{aligned}
 & P(C_{upper}(u, v) = k) \\
 &= P(d(u) = k)P(d(v) > k) + P(d(u) \geq k)P(d(v) = k) \\
 &= \frac{e^{-\lambda}\lambda^k}{k!} \left( \sum_{i=k+1}^{\infty} \frac{e^{-\lambda}\lambda^i}{i!} + \sum_{i=k}^{\infty} \frac{e^{-\lambda}\lambda^i}{i!} \right) \tag{10}
 \end{aligned}$$

Under the simplifying assumption of independence, according to the Strong Law of Large Numbers [24], for large  $N$ ,  $C_{upper}(G)$  is approximately equal to  $E[C_{upper}(u, v)]$ , where  $E[C_{upper}(u, v)]$

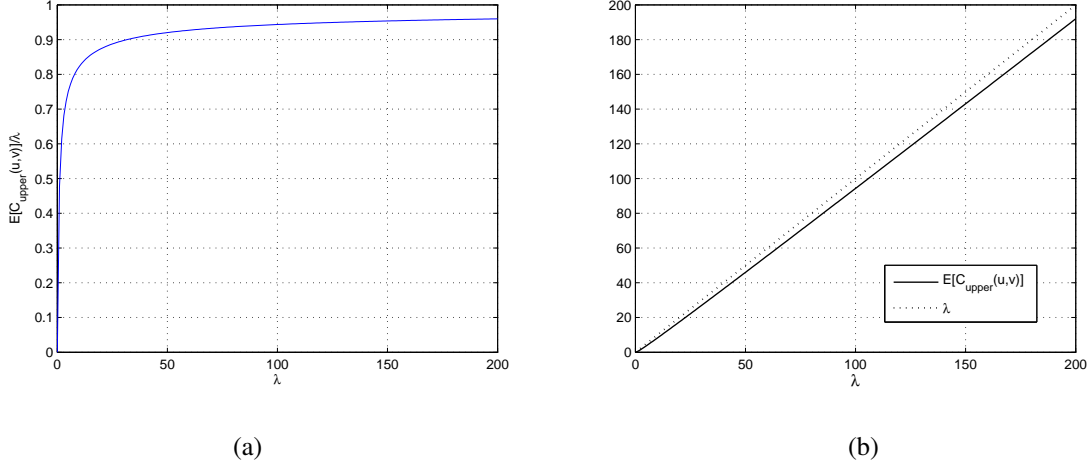


Fig. 3. Relationship between  $E[C_{upper}(u, v)]$  and  $\lambda$

can be calculated as follows:

$$\begin{aligned}
 & E[C_{upper}(u, v)] \\
 &= \sum_{k=0}^{\infty} k \frac{e^{-\lambda} \lambda^k}{k!} \left( 1 - \sum_{i=0}^k \frac{e^{-\lambda} \lambda^i}{i!} + \sum_{i=k}^{\infty} \frac{e^{-\lambda} \lambda^i}{i!} \right) \\
 &= \lambda - \lambda \left( \sum_{k=0}^{\infty} \frac{e^{-\lambda} \lambda^k}{k!} \sum_{i=0}^{k+1} \frac{e^{-\lambda} \lambda^i}{i!} - \sum_{k=0}^{\infty} \frac{e^{-\lambda} \lambda^k}{k!} \sum_{i=k+1}^{\infty} \frac{e^{-\lambda} \lambda^i}{i!} \right) \\
 &= \lambda - \lambda \sum_{k=0}^{\infty} \frac{e^{-\lambda} \lambda^k}{k!} \left( \frac{e^{-\lambda} \lambda^k}{k!} + \frac{e^{-\lambda} \lambda^{k+1}}{(k+1)!} \right) \tag{11}
 \end{aligned}$$

Since there is no closed form for (11), next we study the relationship between  $E[C_{upper}(u, v)]$  and the average node density  $\lambda$  by truncating the equation at  $k = 2000$ . Fig. 3 illustrates the computed results based on Eqn. (11). Fig. 3(a) illustrates the ratio between  $E[C_{upper}(u, v)]$  and  $\lambda$ , which demonstrates that the ratio increases fast when  $\lambda$  is small, then increases slowly. Fig. 3(b) illustrates the values of  $E[C_{upper}(u, v)]$  for different average node degrees, which indicates that although the ratio is not constant,  $E[C_{upper}(u, v)]$  is approximately a linear function of the average node degree. This is also consistent with the experimental findings illustrated in Fig. 2(a). From Fig. 3(b) we can also see that the absolute difference between  $E[C_{upper}(u, v)]$  and  $\lambda$  will increase with the increase of  $\lambda$ , which indicates that the ratio can never be equal to 1.

It is easy to check that  $E[C_{upper}(u, v)]$  is an unbiased estimator for  $C_{upper}(G)$ . Now we study

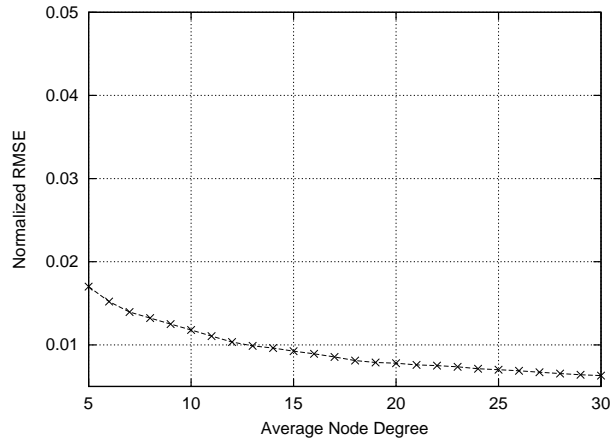


Fig. 4. Relationship between normalized RMSE and average node degree

the normalized root mean square error (NRMSE) associated with the estimator  $E[C_{upper}(u, v)]$ , which is defined as

$$NRMSE = \frac{\sqrt{E[(E[C_{upper}(u, v)] - C_{upper}(G))^2]}}{E[C_{upper}(u, v)]}.$$

The experimental results are illustrated in Fig. 4, which are based on 1000 independently generated Poisson random graphs. From these results we can see that the normalized RMSE is very small and decreases with the increase of average node degree, so  $C_{upper}(u, v)$  is well-approximated by its mean value  $E[C_{upper}(u, v)]$ .

### B. Geometric Random Graphs

Now we study the pairwise connectivity in geometric random graphs. In this set of experiments, the geometric random graphs are generated as follows: nodes are independently deployed inside a rectangular area of  $10r \times 10r$  according to the 2D uniform distribution, and the total number of nodes in the network changes with the change of average node density. The experimental results with different average node densities are illustrated in Fig. 5, where Fig. 5(a) shows the relationship between the average node density and the sample mean of APC (both  $C_{upper}(G)$  and  $C(G)$  are shown), Fig. 5(b) demonstrates the distribution of  $d_{diff}$ , that is, the difference between the upper bound and exact value of the APC, under three different average node densities: 10, 20, and 30, and Fig. 5(c) exhibits the standard deviation of APC. Similar to the case of Poisson

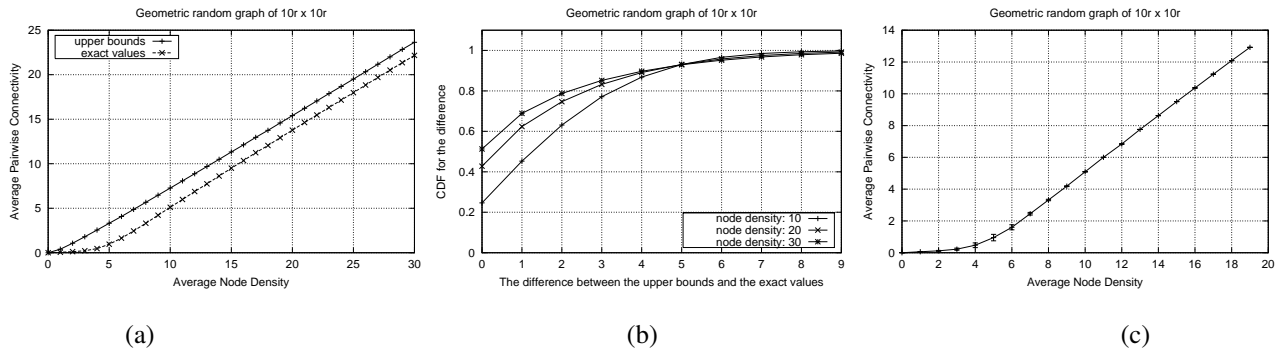


Fig. 5. Upper bounds and exact values of APC in geometric random graphs

random graphs, for each average node degree, the results are averaged over 1000 independently generated geometric random graphs.

First, from Fig. 5(a) we can see that the APC increases with the increase of node density, which is easy to understand. Second, unlike in Fig. 2(a) (Poisson random graphs), the upper bounds and exact values of the APC are not approximately equal in the Fig. 5(a) (geometric random graphs). The distributions of  $d_{diff}$  are illustrated in Fig. 5(b), which shows that the difference between the upper bounds and exact values can become large in certain situations. For example, for average node density 10, with probability only 20% the upper bounds are equal to the exact values. Further, for all the three node densities shown in Fig. 5(b), with about probability of 15% the difference is larger than 3. The standard deviations exhibited in Fig. 5(c) show that when the average node density is larger than 7, the standard deviation becomes negligible. In other words, for any arbitrary geometric random graph generated according to the above procedure, its actual APC can be approximated by the sample mean (illustrated in Fig. 5(a)) very well.

One possible reason for the existence of a gap between the upper bounds and the exact values is the existence of boundary effects and the non-homogeneity of geometric random graphs. Unlike Poisson random graphs, in which all nodes are homogeneous and there is no such concept of boundary, in geometric random graphs, some nodes may lie in the boundary areas and may have less resources when trying to discover routes to the other nodes, which can greatly reduce the pairwise connectivity.

To investigate the boundary effects in geometric random graphs, we have conducted another set of experiments, where only nodes inside the inner area of geometric random graphs are con-

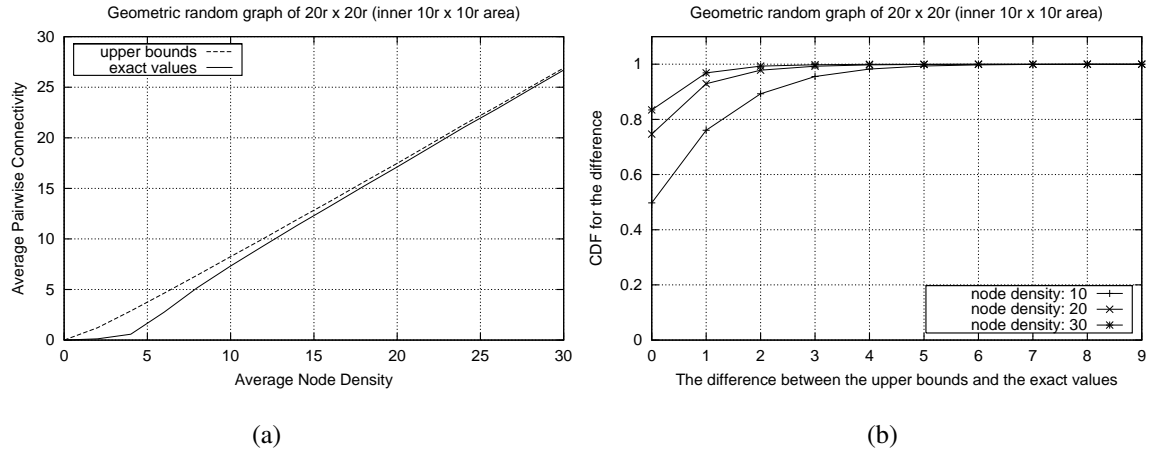


Fig. 6. Upper bounds and exact values of APC in the inner part of geometric random graphs

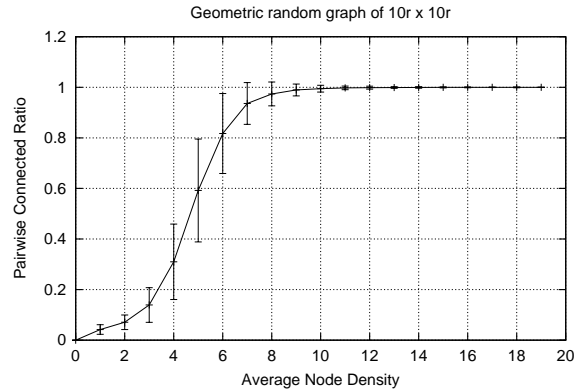


Fig. 7. Sample mean and standard deviation for PCR in geometric random graph

sidered when calculating the APC. Specifically, given a geometric random graph in a rectangular area of  $20r \times 20r$ , only node pairs with both inside the inner area of  $10r \times 10r$  are considered. The new experimental results are illustrated in Fig. 6. From these results we can see that with the increase of node density, the exact values of the APC are almost equal to the upper bounds. Meanwhile, the distribution of the difference between the upper bound and exact value also demonstrates that the differences become much smaller than the results shown in Fig. 5(b), and with only very small probability the gap is larger than 3. In other words, when the boundary effects are removed and the node density is not too low, the pairwise connectivity of each node pair can be completely characterized by their own node degrees.

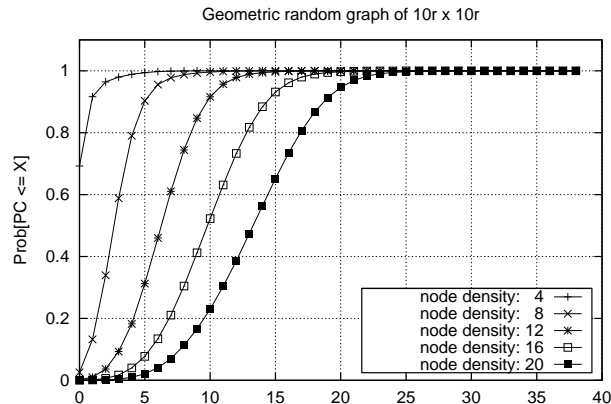


Fig. 8. Distribution of Pairwise Connectivity

The PCR in geometric random graphs has also been studied with the same configuration, where the results are illustrated in Fig. 5. The sample mean and standard deviation of PCR are illustrated in Fig. 7. Except for the sharp threshold behavior, which has been illustrated in Section II(C), from these results we can also see that the standard deviation becomes very small when the average node density becomes large (i.e., PCR approaches to 1). This indicates that for an arbitrary geometric random graph with large average node density (e.g., larger than 10), with very high probability nearly every pair of nodes can communicate, though the network may be disconnected.

### C. Distribution of Pairwise Connectivity

We have also conducted a set of experiments to further study the distribution of pairwise connectivity in geometric random graphs, and the results are illustrated in Fig. 8. In this set of experiments, the network deployment area is fixed to be  $10r \times 10r$ , and for each node density, the results are averaged over 1000 independently generated random graphs. For each curve in Fig. 8, each data point denotes the total fraction of node pairs whose pairwise connectivity is no more than certain value (i.e., x-axis value). Based on these results, we can not only calculate the APC, but also find the distribution of node pairs with different pairwise connectivity.

First, comparing the results in Fig. 8 and Fig. 5 we can see that the average values match the median values very well. For example, as illustrated in Fig. 5, the APC for node density 20 is about 13, while as shown in Fig. 8, the median point corresponding to node density 20 is also

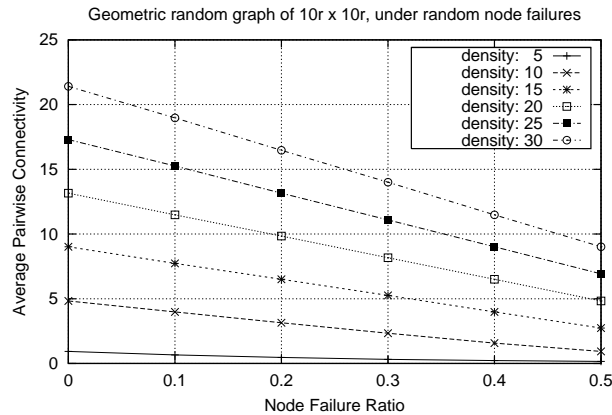


Fig. 9. The  $\alpha$ - $p$ -resilience in APC for geometric random graphs under random node failures

around 13. This is also true for other node densities. This is because the pairwise connectivity for different nodes pairs is distributed almost uniformly in a small region and centered at their median point. Second, from the results illustrated in Fig. 8 we can see that these curves exhibit some threshold behaviors where the curves change sharply from 0 to 1 for most node densities. That is, with very high probability most node pairs' pairwise connectivity is around the APC, which also shows that APC can be a very good metric from each individual node's point of view.

#### IV. EXPERIMENTAL EVALUATION OF FAULT TOLERANCE

In wireless multihop networks, some nodes may be removed from the network due to exhaustion of battery power and some nodes may be disconnected from the network due to unintentional configuration errors. Meanwhile, due to the fragile wireless connections and possible mobility, link breakage may happen very frequently. The measure of fault tolerance is thus critical in wireless multihop networks. In this section, we study the fault tolerance of such networks under random node failures based on the proposed  $\alpha$ - $p$ -resilience measure, where both APC and PCR have been studied.

We first conduct a set of experiments to study the decrease of APC in geometric random graphs under random node failures. In this set of experiments, the initial network is deployed in a rectangular area of  $10r \times 10r$ , and the average node density ranges from 5 to 30. The experimental results are illustrated in Fig. 9, where each data point represents the APC after a portion of nodes

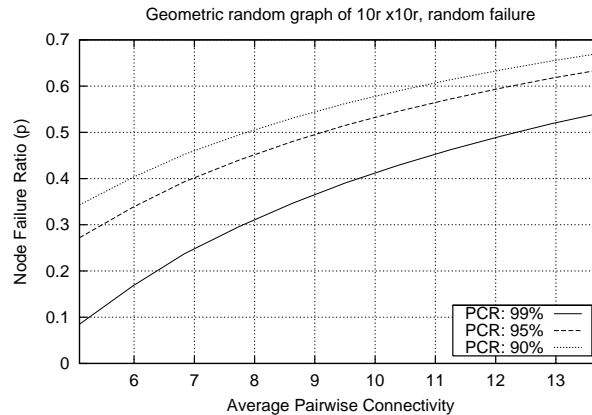


Fig. 10. The  $\alpha$ - $p$ -resilience in PCR for geometric random graphs under random node failures

are randomly removed from the network, which corresponds to random node failure with certain failure ratio, and are obtained through averaging over 1000 independently generated geometric random graphs. In other words, for any point  $(x, y)$  in the curve corresponding to the original average node density  $\gamma$ , this indicates that the above geometric random network with average node density  $\gamma$  is  $y$ - $x$ -resilient in APC. From these results we can see that the APC decreases linearly with the increase of node failure ratio. The results also confirm that the random failure of nodes with failure ratio  $p$  has exactly the same effect as reducing the node density to  $1 - p$  of the original density, which is trivial to understand.

The experimental studies of  $\alpha$ - $p$ -resilience in PCR for geometric random graphs are illustrated in Fig. 10, where the same experiment configurations are used as in Fig. 9. In this figure, each curve corresponds to a specific PCR (that is,  $\alpha$ ) under certain portion of random node removal. For example, for the point  $(8, 0.3)$  in the curve corresponding to PCR = 99%, this indicates that a network with APC being 8 is 99%-30%-resilient under random node failure, i.e., up to 30% of the nodes can be randomly failed while maintaining a PCR of at least 99%. From these results we can see that the network resilience increases with the increase of APC, which is trivial to understand. These results also demonstrate that the extra portion nodes that can be removed when decreasing the PCR from 99% to 95% is much larger than that when decreasing the PCR from 95% to 90%. This can be explained by the sharp threshold behavior: according to the results illustrated in Fig. 7, with the decrease of average node density, the decrease of PCR from

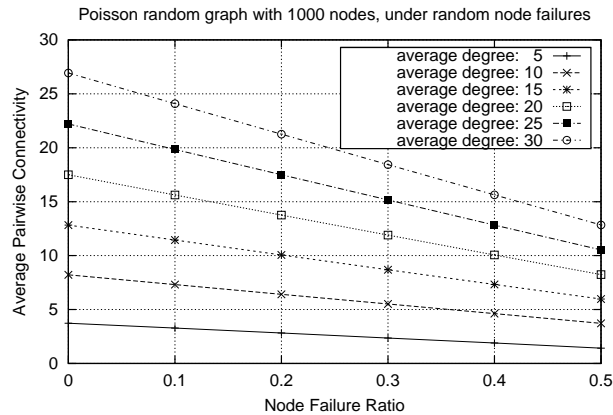


Fig. 11. The  $\alpha$ - $p$ -resilience in APC for Poisson random graphs under random node failures

95% to 90% is much quicker than the decrease of PCR from 99% to 95%.

Random failure experiments have also been conducted on Poisson random graphs, and the results are illustrated in Fig. 11. In this set of experiments, there are 1000 nodes in the initial deployment of each network, and the average node degree ranges from 5 to 30. The results confirm that the random failure of nodes with failure ratio  $p$  has exactly the same effect as reducing the average node degree to  $1 - p$  of the original average node degree.

## V. EXPERIMENTAL EVALUATION OF ATTACK RESILIENCE

This section evaluates the attack resilience of wireless multihop networks based on the metric of  $\alpha$ - $p$ -resilience. In many situations the networks are deployed in adversarial environments, and some nodes may become dysfunctional under attacks. Thus the study of attack resilience is also critical. In this section, the following two attack models are considered: selective node removal attacks according to node degree and partition attacks.

When selective node removal attacks are applied, nodes in the network are removed one by one, and at each step the node with the highest degree is removed. This type of attack can degrade the network performance drastically in scale-free networks, such as the Internet [5]. However, since randomly deployed wireless multihop networks are not scale-free, selective node removal attacks may not be the best attack model from the attackers' point of view. In this section, we also consider another type of attack whose goal is to partition the network into many disconnected components through removal of nodes in certain areas. We refer to this type

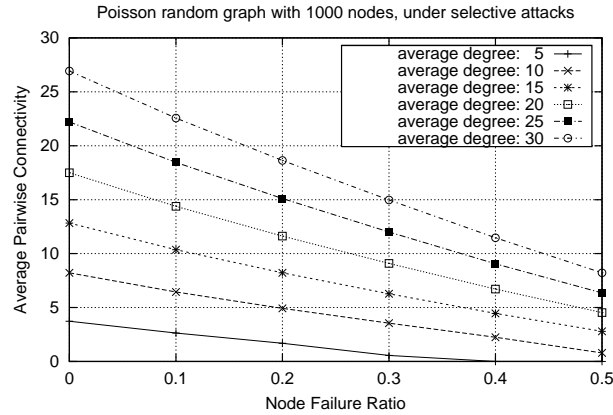


Fig. 12. The  $\alpha$ - $p$ -resilience in APC for Poisson random graphs under selective node removal attacks

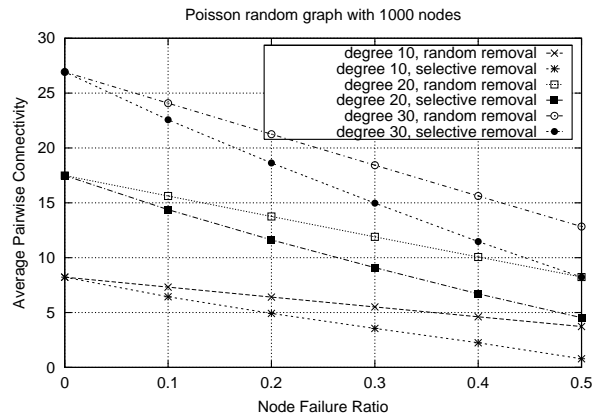


Fig. 13. Comparison of APC for Poisson random graphs under different attacks

of node removal attacks as partition attacks.

Fig. 12 shows the experimental results of  $\alpha$ - $p$ -resilience for Poisson random graphs under selective node removal attacks, or more specifically, the decrease of APC with the increase of node removal fraction for a given network configuration. In this set of experiments, the original number of nodes in the network is set to be 1000, the average node degree varies from 5 to 30. Each data point in this figure corresponds to the APC under the selective removal of a certain fraction of nodes, The result is obtained through 1000 independently generated Poisson random graphs. From these results we can see that the APC decreases approximately linearly with the increase of node removal percentage, similar to the case of random node failure shown in Fig. 11.

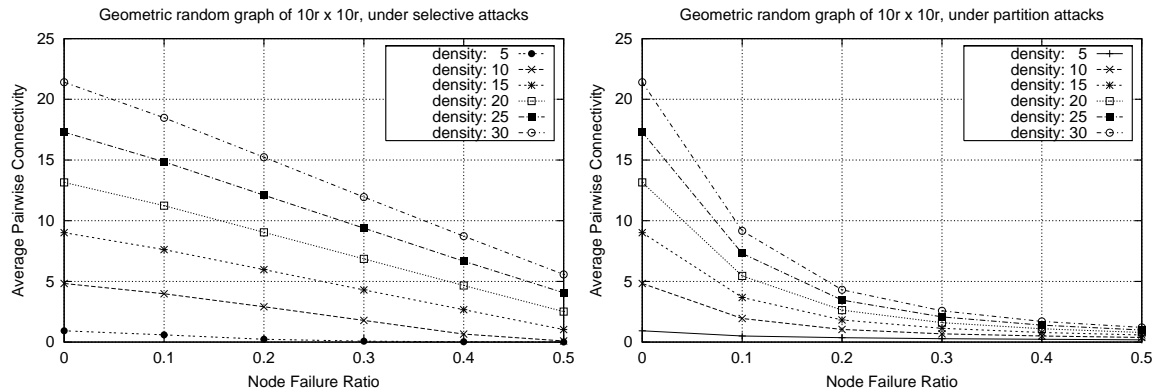


Fig. 14. The  $\alpha$ - $\beta$ -resilience in APC for geometric random graphs under selective node removal and partition attacks

The comparisons between random node removal and selective node removal have also been performed, as illustrated in Fig. 13. From these comparisons we can see that although in both cases the APC will approximately decrease linearly with the increase of node removal fraction, selective node removal can cause more degradation than random node removal. Meanwhile, even under selective node removal attacks, the APC in Poisson random graphs still decreases very gracefully, which indicates that Poisson random graphs are robust to selective node removal attacks.

Since geometric random graphs can better capture the spatial correlation among nodes in wireless multihop networks, in the remainder of this section we will focus on geometric random graphs. Further, besides selective node removal attacks, the effect of partition attacks will be studied. Fig. 14 illustrates the experimental results for geometric random graphs. In this set of experiments, the network deployment area is fixed to be  $10r \times 10r$ , the original node density ranges from 5 to 30, and the fraction of nodes removed varies from 10% to 50%.

From the results illustrated in Fig. 14(a), which correspond to the case of selective node removal attacks, we can see that the APC decreases linearly and gracefully with the increase of node removal percentage, similar to the case of Poisson random graphs shown in Fig. 12. This also indicates that geometric random graphs are robust to selective node removal attacks unless the node density is too low, although the selective node removal attacks may cause more damage than the random node failures.

Now we study the effects of partition attacks, where the partition strategies are illustrated in

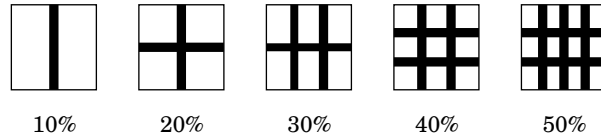


Fig. 15. Partition methods for different node removal ratios. In these figures, the dark areas denote those areas from which all nodes have been removed, and the width of each dark area is at least  $r$ .

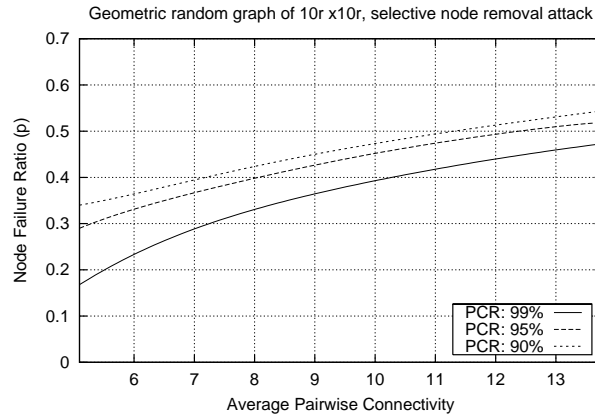


Fig. 16. The  $\alpha$ - $p$ -resilience in PCR for geometric random graphs under selective node removal attacks

Fig. 15. From the experimental results presented in Fig. 14(b) we can see that partition attacks can cause severe performance degradation in geometric random graphs. For example, when only 10% of nodes are removed, the APC will decrease to about 40% of the original value. This makes sense since according to the partition strategy shown in Fig. 15, after 10% of nodes are removed, the network will be partitioned into two disconnected parts. In other words, for any node in the network, it will lose connection to about half of the nodes in the network. Further, due to the reduction of available resources and network size, the number of node-disjoint paths between pairs of nodes that remain connected also decreases, which explains why the obtained APC is only about 40% of the original value.

Fig. 16 demonstrates the  $\alpha$ - $p$ -resilience in PCR for geometric random graphs under selective node removal attacks, that is, the fraction of nodes that can be selectively removed without letting the PCR below a certain threshold (i.e.,  $\alpha$ ). The results are similar to those illustrated in Fig. 10 and they are compared in Fig. 17. First, when the original APC is large, the network is more robust to random node removal attacks than to selective node removal attacks. For example,

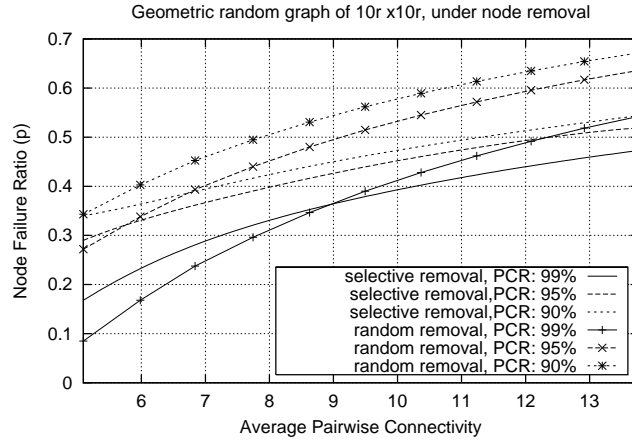


Fig. 17. Comparison of  $\alpha$ - $p$ -resilience in PCR for geometric random graphs between random failure and selective attack

for  $\alpha$  being 95% and the original APC being 12, when nodes are removed randomly,  $p$  can be 0.6, while under selective node removal attacks,  $p$  is 0.5. This indicates that selective node removal can cause more damage than random node removal when the original network density is high. Second, it is surprising to see that when the original APC is relatively small and the PCR requirement is high, random node removal can cause even more damage than selective node removal attacks. For example, for  $\alpha$  being 99% and the original APC being 5,  $p$  is 18% under selective node removal, while  $p$  is 9% under random node removal. This can be explained as follows: when nodes are removed in decreasing order of degrees, those nodes being first removed are usually in areas with higher node density, and removal of such nodes may cause less effect on node isolation or network disconnection comparing to removal of nodes from low density area. This is why there is less effect on PCR.

Fig. 18 demonstrates the comparisons under different node removal patterns in geometric random graphs. In these comparisons, three node densities are studied: 5, 10, 15. Fig. 18(a) shows the comparison results with the original node density being 5. From this set of comparisons we can see that when the node removal ratio is larger than 10%, selective node removal attacks may cause more damage than partition attacks. This makes sense, since under low node density and with a considerable amount of selective node removal, the network will be partitioned into many small disconnected pieces, while partition attacks give rise to larger connected subsets. Further, from this set of comparisons we can also see that when the node removal percentage

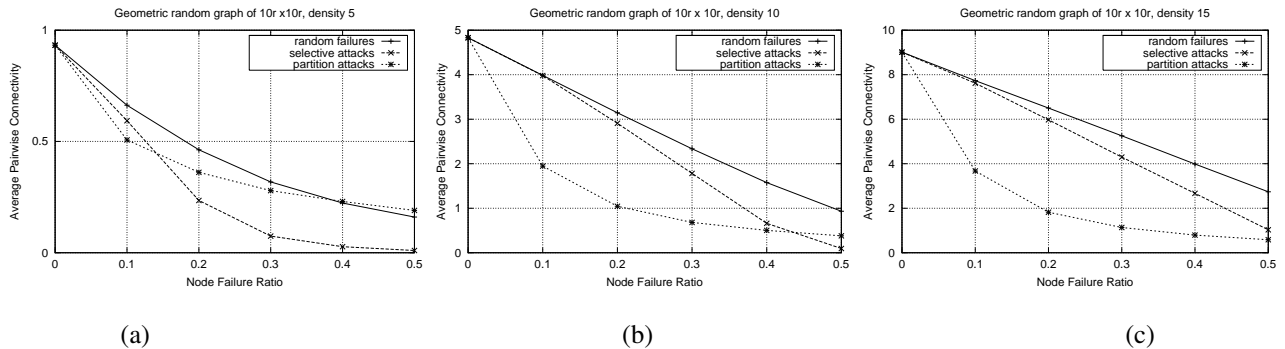


Fig. 18. Comparison of APC under different attacks in geometric random graphs

is more than 40%, the APC corresponding to partition attacks is actually higher than the APC corresponding to random node failure.

Fig. 18(b) and Fig. 18(c) show the comparison results for node densities 10 and 15. From these comparisons we can see that with the increase of node density, the effects of partition attacks become more and more severe. For example, when the original node density is 10, in only one situation (i.e., node failure ratio 50%) partition attack can cause more damage than selective attack, while when node density is 15, in no situations does selective attack perform better than partition attack from the attackers' point of view. Thus, partition attacks can cause more damage than selective node removal attacks when the network node density is high.

We have also compared the evolution of pairwise connectivity ratio (PCR) under different node removal patterns, with the results being illustrated in Fig. 19. First we examine the comparison under node density 5. Similar to the case of Fig. 18(a), selective attacks can cause more damage than partition attacks when the node failure ratio is larger than 20%, which has been explained before. One very interesting observation from Fig. 19(a) is that PCR under selective attacks is even a little bit higher than PCR under random node removal when the node failure ratio is 10%. This can be explained as follows. For geometric random graphs, selective node removal according to degree distribution tends to remove nodes in denser regions. Since the regions are denser it is less likely that this will cause a neighbor to become isolated. Another interesting observation is that although the APC under selective attack is lower than the APC under partition attack when the node failure ratio is 20% (shown in Fig. 18(a)), the PCR is still a little bit higher (shown in Fig. 19(a)). This observation implies that under some attacks a higher APC may not

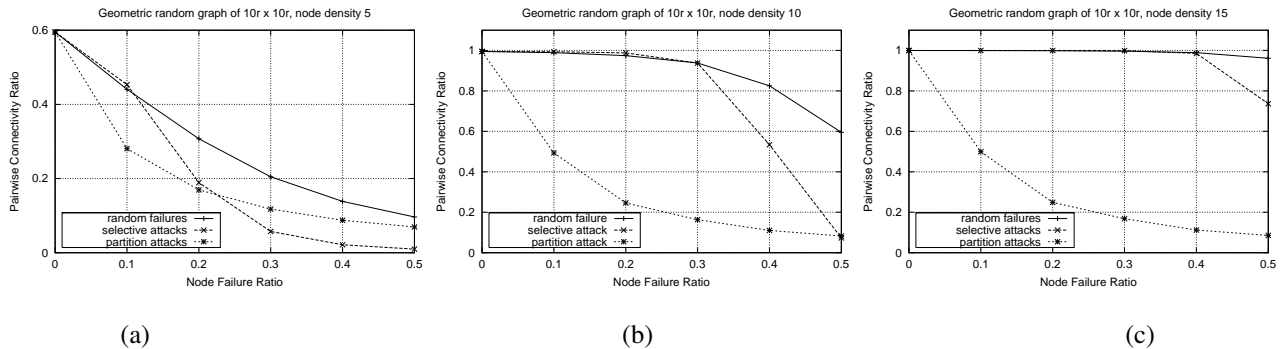


Fig. 19. Comparison of PCR under different attacks in geometric random graphs

indicate a higher PCR.

The comparison of PCR under various attacks for node densities 10 and 15 have also been illustrated in Fig. 19. From the comparisons presented in Fig. 19(b) and Fig. 19(c) we can see that when the node density is high, partition attacks become very severe in degrading the pairwise connectivity ratio, which is also consistent with the results presented in Fig. 18(b) and Fig. 18(c). Further, when the node density is very high (e.g., 15), even selective attacks can cause almost no degradation to the pairwise connectivity ratio. In other words, selective attack is not an effective attacking strategy when the node density is high.

## VI. CONCLUSION

In this paper, we have studied the service availability of wireless multihop networks based on average pairwise connectivity and pairwise connected ratio, and derived theoretical upper-bound for the average pairwise connectivity which can approximate the exact value very well. Based on the proposed metric,  $\alpha$ - $p$ -resilience, we have also studied the fault tolerance and attack resilience of wireless multihop networks under different node failure patterns: random node removal, selective node removal, and partition attack. Experimental studies have demonstrated that when the node density is relatively high, wireless multihop networks are more sensitive to partition attacks than selective node removal attacks and random node failures, and selective node removal attacks are a little bit more damaging than random node removal; when the node density is extremely low, all the three node removal methods have similar effects, with partition attacks and selective node removal attacks being a little bit more damaging than random node

removal.

## REFERENCES

- [1] C. Perkins, Ed., *Ad Hoc Networking*. Addison-Wesley, 2001.
- [2] D. Pradhan, "Dynamically restructurable fault-tolerant processor network architectures," *IEEE Transactions on Computers*, vol. C-34, pp. 434–447, May 1985.
- [3] W. Najjar and J.-L. Gaudiot, "Network resilience: A measure of network fault tolerance," *IEEE Transactions on Computers*, vol. 39, no. 2, pp. 174–181, February 1990.
- [4] B. Bollóbas, *Modern Graph Theory*. Springer, 1998.
- [5] R. Albert, H. Jeong, and A.-L. Barabási, "Error and attack tolerance of complex networks," *Nature*, vol. 406, pp. 378–382, 2000.
- [6] A. Broder, R. Kumar, F. Maghoul, P. Raghavan, S. Rajagopalan, R. Stata, A. Tomkins, and J. Wiener, "Graph structure in the web," *Computer Networks*, vol. 33, pp. 309–320, 2000.
- [7] R. Cohen, K. Erez, D. ben Avraham, and S. Havlin, "Resilience of the internet to random breakdowns," *Phys. Rev. Lett.*, vol. 85, pp. 4626–4628, 2000.
- [8] —, "Breakdown of the internet under intentional attack," *Phys. Rev. Lett.*, vol. 86, pp. 3682–3685, 2001.
- [9] J. A. Dunne, R. J. Williams, and N. D. Martinez, "Network structure and biodiversity loss in food webs: Robustness increases with connectance," *Ecology Lett.*, vol. 5, pp. 558–567, 2002.
- [10] —, "Food-webstructure and network theory: The role of connectance and size," in *Proc. Natl. Acad. Sci. USA*, vol. 99, 2002, pp. 12 917–12 922.
- [11] H. Jeong, S. Mason, A.-L. Barabási, and Z. N. Oltvai, "Lethality and centrality in protein networks," *Nature*, vol. 411, pp. 41–42, 2001.
- [12] M. E. J. Newman, S. Forrest, and J. Balthrop, "Email networks and the spread of computer viruses," *Phys. Rev. E*, vol. 66, no. 035101, 2002.
- [13] P. Holme, B. J. Kim, C. N. Yoon, and S. K. Han, "Attack vulnerability of complex networks," *Phys. Rev. E*, vol. 65, no. 056109, 2002.
- [14] M. D. Penrose, "On  $k$ -connectivity for a geometric random graph," *Wiley Random Structures and Algorithms*, vol. 15, no. 2, pp. 145–164, 1999.
- [15] C. Bettstetter, "On the minimum node degree and connectivity of a wireless multihop network," in *MOBIHOC*, 2002.
- [16] X. Li, P. Wan, Y. Wang, and C. Yi, "Fault tolerant deployment and topology control in wireless networks," in *MobiHoc03*, Annapolis, MD, June 2003.
- [17] I. Chlamtac and A. Faragó, "A new approach to the design and analysis of peer-to-peer mobile networks," *ACM/Baltzer Wireless Networks*, vol. 5, Aug 1999.
- [18] R. Solomonoff and A. Rapoport, "Connectivity of random nets," *Bull. Math. Biophys.*, vol. 13, pp. 107–117, 1951.
- [19] P. Erdős and A. Rényi, "On random graphs," *Publ. Math. Debrecen*, vol. 6, pp. 290–297, 1959.
- [20] —, "On the evolution of random graphs," *Publ. Math. Inst. Hungar. Acad. Sci.*, vol. 5, pp. 17–61, 1960.
- [21] B. Bollóbas, *Random Graphs*, 2nd ed. Academic Press, 2001.
- [22] M. E. J. Newman, "The structure and function of complex networks," *SIAM Review*, vol. 45, no. 2, pp. 167–256, 2003.
- [23] W. Yu and K. J. R. Liu, "Attack-Resistant Cooperation Stimulation in Autonomous Ad Hoc Networks," *To appear in IEEE Journal on Selected Areas in Communications: Autonomic Communication Systems*, 2005.
- [24] O. Kallenberg, *Foundations of Modern Probability*. New York: Springer-Verlag, 1977.