Discrete Mathematics, Algorithms and Applications

ASYMPTOTIC DISTRIBUTION OF THE NUMBER OF ISOLATED NODES IN WIRELESS AD HOC NETWORKS WITH UNRELIABLE NODES AND LINKS

Chih-Wei Yi
Department of Computer Science, National Chiao Tung University
Hsinchu City 30010, Taiwan
yi@cs.nctu.edu.tw

Peng-Jun Wan
Department of Computer Science, Illinois Institute of Technology
Chicago, IL 60616, USA
wan@cs.iit.edu

Chao-Min Su and Kuo-Wei Lin
Department of Computer Science, National Chiao Tung University
Hsinchu City 30010, Taiwan
vodkasu@gmail.com, alec.cs94g@nctu.edu.tw

Scott C.-H. Huang
Department of Computer Science, City University of Hong Kong
Kowloon, Hong Kong, PRC
shuang@cityu.edu.hk

Received Day Month Year
Accepted Day Month Year

In this paper, we study the connectivity of wireless ad hoc networks that are composed of unreliable nodes and links by investigating the distribution of the number of isolated nodes. We assume that a wireless ad hoc network consists of n nodes distributed independently and uniformly in a unit-area disk or square. All nodes have the same maximum transmission radius r_n, and two nodes have a link if their distance is at most r_n. Nodes are active independently with probability $0 < p_1 \leq 1$, and links are up independently with probability $0 < p_2 \leq 1$. Nodes are said *isolated* if they do not have any links to active nodes. We show that if $r_n = \sqrt{\frac{\ln n + \xi}{\pi p_1 p_2 n}}$ for some constant ξ, then the total number of isolated nodes (or isolated active nodes, respectively) is asymptotically Poisson with mean $e^{-\xi}$ (or $p_1 e^{-\xi}$, respectively). In addition, in the secure wireless networks that adopt m-composite key predistribution schemes, a node is said *isolated* if it does not have a secure link. Let p denote the probability of the event that two neighbor nodes have a secure link. If all nodes have the same maximum transmission radius $r_n = \sqrt{\frac{\ln n + \xi}{\pi p n}}$, the total number of isolated nodes is asymptotically Poisson with mean $e^{-\xi}$.

Keywords: Asymptotic distribution; Connectivity; Isolated nodes; Random key predis-

tribution; Random geometric graphs

Mathematics Subject Classification 2000: 60D05

1. Introduction

A wireless ad hoc network is composed of a collection of wireless devices distributed over a geographic region. A communication session is established either through a single-hop radio transmission if the communication parties are close enough, or through relaying by intermediate devices otherwise. Due to the nonnecessity of a fixed infrastructure, wireless ad hoc networks can be flexibly deployed at low cost for various missions.

In many applications, wireless sensors are deployed in a large volume in the sensor field. They can be deployed by dropping from a plane or delivered in a missile. Specific applications include environmental monitoring, habitat monitoring, and intrusion detection. In environmental monitoring, temperature, heat, pressure, sound, or light can be constantly monitored, helping scientists in the task of detecting specific events. In habitat monitoring, biologists can get the observation data gathered from sensors and try avoiding disturbing the nature. The wireless sensor networks deployed over a battlefield or secured region can propagate messages to the outside in case there are intruders. In the applications above, a great quantity of sensors is usually needed. The sheer large number of devices deployed in potentially harsh environments often makes deterministic device placement impractical. Consequently, random deployment is often the only viable option.

To model a randomly deployed wireless ad hoc network, it is natural to represent the ad hoc devices by a finite random point process over the deployment region [1,2,3,4,5]. In addition, due to the short transmission range of radio links, two wireless devices can build a communication link only if they are within each other's transmission range. Assume all devices have the same transmission radius r, then the induced network topology is a r-disk graph in which two nodes are joined by an edge if and only if their distance is at most r. This is a variant of the model proposed by Gilbert [6] and referred as a *random geometric graph*.

The connectivity of a wireless ad hoc network is a fundamental requirement. The connectivity of random geometric graphs has been studied by Dette and Henze [7], Penrose [8], and others [1,9,10,5]. For a uniform n-point process over a unit-area square, Dette and Henze [7] showed that for any constant ξ, the $\left(\sqrt{\frac{\ln n+\xi}{\pi n}}\right)$-disk graph has no isolated nodes with probability $\exp\left(-e^{-\xi}\right)$ asymptotically. Later, Penrose [8] established that if a random geometric graph induced by a uniform point process or Poisson point process has no isolated nodes, then it is almost surely connected. Besides the overall connectivity, some applications concern about if there exists a giant connected component. Continuum percolation [11] is a useful theorem in analyzing threshold phenomena. Ammari and Das [12] focused on percolation in coverage and connectivity in three-dimensional space and found out whether the

network provides long-distance multihop communication.

However, in a realistic system, nodes may become inactive due to internal breakdown or being in the monitoring state, and links may be down due to harsh environment or barriers between nodes. The inactive nodes and down links cannot take part in routing/relaying and thus may affect the connectivity. Recently, Franceschetti and Meester [13] used the Chen-Stein method of Poisson approximation to find the critical time at which isolated nodes begin to appear in the system as its size tends to infinity in networks where nodes are connected randomly and can fail at random times. Wan and Yi *et al.* [10,5] showed that if every node independently breaks down with the same probability p, the network is connected with probability $\exp\left(-pe^{-\xi}\right)$ asymptotically. In this paper, based on the work in [5], we study the connectivity of a wireless network with unreliable nodes and links by investigating the number of isolated nodes. We assume nodes are active independently with the same probability p_1 and links are up independently with the same probability p_2. It is referred to as a Bernoulli model. In this model, depending on the meaning of the "inactive" nodes, we may have two types of network connectivity: (1) all active nodes form a connected network; and (2) all active nodes form a connected network and each inactive node is with up-links to active nodes. In both cases, a node is said *isolated*, if it doesn't have an up-link to an active nodes. The inexistence of isolated nodes is a prerequisite for connectivity. We shall prove that the number of isolated nodes has an asymptotic Poisson distribution.

In addition, the work described above is extended for secure wireless networks with m-composite key predistribution schemes [14,15,16]. In many applications, a wireless sensor network is composed of low cost devices. Due to the limited capacity, traditional security schemes and key management algorithms are too complicated and not feasible for such a system. The m-composite key predistribution schemes are proposed to offer security for randomly-deployed wireless sensor networks. In the previous schemes, K distinct keys are randomly chosen from the key space to form the key pool. A key ring is a k-element subset of the key pool. Before being deployed, each node randomly loads a key ring into its memory. Two nodes within each other's transmission range have a secure link if their key rings have at least m common keys. Only secure links can participate in the communication. Hence, the secure wireless network is the graph in which two nodes have an edge if their distance is at most r and have at least m common keys in their key rings. A secure wireless network is said to be connected if all nodes form a connected network by secure links. A node is said *isolated*, if it doesn't have a secure link. Similarly, we shall prove that the number of isolated nodes in the secure wireless network has an asymptotic Poisson distribution.

The model proposed in this paper is quite basic and it can still have different variants. From this fundamental model, some behaviors of the network can be known well. The insight should serve a baseline when facing those more complicated models. The explicit formulas given in this work allow scientists or engineers, based on the knowledge of the network, to control the expected number of isolated nodes by

tuning the node density or even transmission power. Thus, the desired level of connectivity can be expected.

In what follows, all integrals considered will be Lebesgue integrals. For any set S and positive integer k, the k-fold Cartesian product of S is denoted by S^k. The disk of radius r centered at x is denoted by $B(x,r)$. The special unit-area disk or square centered at the origin is denoted by Ω. The symbols o and $\sim$ always refer to the limit $n \to \infty$. To avoid trivialities, we tacitly assume n to be sufficiently large if necessary. For the simplicity of notation, the dependence of sets and random variables on n will be frequently suppressed.

The rest of this paper is organized as follows. In Section 2, the main results of this paper are given. In Section 3, we present several useful lemmas. In Section 4, we derive the distribution of the number of isolated nodes. In Section 5, under various network scenarios, simulation results are given to show the trend of convergency of our asymptotics. Section 6 is the conclusion.

2. Main Results

The approach used in this paper is based on the method developed in [5]. We assume that a wireless ad hoc network is represented by a uniform n-point process over Ω. All nodes are associated with the maximal transmission radius r_n, which is a function of n, and two nodes have a link if the distance between them is at most r_n. For the sake of simplicity, in what follows, the dependency on n will be frequently suppressed.

In the Bernoulli model, nodes are active independently with probability p_1 for $0 < p_1 \leq 1$, and links are up independently with probability p_2 for $0 < p_2 \leq 1$. Here p_1 and p_2 can be constants or functions of n. A node is said *isolated* if it does not have an up-link with an active node. We have the following theorem about the total number of isolated (active) nodes.

Theorem 2.1. *Suppose that* $\lim_{n\to\infty} p_1 p_2 \ln n = \infty$ *and nodes have the same maximum transmission radius* $r = \sqrt{\frac{\ln n + \xi}{n p_1 p_2 \pi}}$ *for some constant* ξ*. Then the total number of isolated nodes is asymptotically Poisson with mean* $e^{-\xi}$*, and the total number of isolated active nodes is also asymptotically Poisson with mean* $p_1 e^{-\xi}$*.*

This work can be extended for secure wireless networks which adopt m-composite key predistribution schemes. In the m-composite key predistribution scheme, the key pool contains K distinct keys, which are randomly chosen from the key space, and a key ring is composed of k distinct keys drawn from the key pool. Before being deployed, each node randomly loads a key ring into its memory. After being deployed, two nodes within each other's transmission range have a secure link if their key rings have at least m common keys. A node is said *isolated* if it does not have a secure link.

Let q_i denote the probability of the event that two key rings have exactly i common keys. If two key rings have exactly i common keys, the second one contains

i keys from the k keys of the first one and $k-i$ keys from the remaining $K-k$ keys not of the first one. Therefore,

$$q_i = \frac{\binom{k}{i}\binom{K-k}{k-i}}{\binom{K}{k}}.$$

Let p denote the probability of the event that two nodes (or key rings) have at least m common keys and q denote the probability of the event that two key rings have at most $m-1$ common keys. Then,

$$\begin{aligned} q &= q_0 + q_1 + \cdots + q_{m-1} \\ p &= 1 - q \end{aligned} \tag{2.1}$$

We have the following theorem about the total number of isolated nodes in the secure wireless network.

Theorem 2.2. *In m-composite key predistribution schemes, let p be given by Eq. (2.1). If $\lim_{n\to\infty} p \ln n = \infty$ and nodes have the same maximum transmission radius $r = \sqrt{\frac{\ln n+\xi}{\pi pn}}$ for some constant ξ, then the total number of isolated nodes is asymptotically Poisson with mean $e^{-\xi}$.*

3. Preliminaries

We adopt notations and terminologies used in [5]. Let r be the transmission radius of the nodes. For any finite set of nodes $\{x_1, \cdots, x_k\}$ in Ω, we use $G_r(x_1, \cdots, x_k)$ to denote the r-disk graph over $\{x_1, \cdots, x_k\}$ in which there is an edge between two nodes if and only if their distance is at most r. For any positive integers k and m with $1 \le m \le k$, let C_{km} denote the set of $(x_1, \cdots, x_k) \in \Omega^k$ satisfying that $G_{2r}(x_1, \cdots, x_k)$ has exactly m connected components. For any set $S \subseteq \Omega$ and $r > 0$, the r-neighborhood of S is the set $\bigcup_{x\in S} B(x, r) \cap \Omega$. Recall that the disk of radius r centered at x is denoted by $B(x, r)$. We use $\nu_r(S)$ to denote the area of the r-neighborhood of S, and sometimes by slightly abusing the notation, to denote the r-neighborhood of S itself.

In the rest of this section, we give the limits of several integrals. Similar lemmas can be found in [5], but here they are introduced with some extensions.

Lemma 3.1. *If $\lim_{n\to\infty} p \ln n = \infty$ and $r = \sqrt{\frac{\ln n+\xi}{\pi pn}}$ for some constant ξ, then*

$$n \int_\Omega e^{-np\nu_r(x)} dx \sim e^{-\xi},$$

$$n \int_\Omega (1 - p\nu_r(x))^{n-1} dx \sim e^{-\xi}.$$

Lemma 3.2. *If $\lim_{n\to\infty} p \ln n = \infty$ and $r = \sqrt{\frac{\ln n+\xi}{\pi pn}}$ for some constant ξ, then for*

any fixed integer $k \geq 2$,

$$n^k \int_{C_{k1}} e^{-np\nu_r(x_1,x_2,\cdots,x_k)} \prod_{i=1}^{k} dx_i = o(1),$$
$$n^k \int_{C_{k1}} (1 - p\nu_r(x_1, x_2, \cdots, x_k))^{n-k} \prod_{i=1}^{k} dx_i = o(1).$$

Lemma 3.3. *Let* $\lim_{n\to\infty} p \ln n = \infty$ *and* $r = \sqrt{\frac{\ln n+\xi}{\pi pn}}$ *for some constant* ξ. *Then for any fixed integers* $2 \leq m < k$,

$$n^k \int_{C_{km}} e^{-np\nu_r(x_1,x_2,\cdots,x_k)} \prod_{i=1}^{k} dx_i = o(1),$$
$$n^k \int_{C_{km}} (1 - p\nu_r(x_1, x_2, \cdots, x_k))^{n-k} \prod_{i=1}^{k} dx_i = o(1).$$

Lemma 3.4. *Let* $\lim_{n\to\infty} p \ln n = \infty$ *and* $r = \sqrt{\frac{\ln n+\xi}{\pi pn}}$ *for some constant* ξ. *Then for any fixed integer* $k \geq 2$,

$$n^k \int_{C_{kk}} e^{-np\nu_r(x_1,x_2,\cdots,x_k)} \prod_{i=1}^{k} dx_i \sim e^{-k\xi},$$
$$n^k \int_{C_{kk}} (1 - p\nu_r(x_1, x_2, \cdots, x_k))^{n-k} \prod_{i=1}^{k} dx_i \sim e^{-k\xi}.$$

In short, Lemma 3.1 to 3.4 are for estimating the probability of existence of isolated nodes under different kind of spacial distribution. Since the proof of Lemma 3.1, 3.2, 3.3 and 3.4 are similar to those in [5], to avoid triviality, we skip the proofs and readers can refer to [5] to develop the proofs.

4. Asymptotic Distribution of The Number of Isolated Nodes

Theorem 2.1 and 2.2 will be proved using *Brun's sieve*, which is an implication of the Bonferroni inequalities, in the form described in [17].

Theorem 4.1. *Let* $B_1, \cdots, B_n$ *be events and* Y *be the number of* B_i *that hold. Suppose that for any set* $\{i_1, \cdots, i_k\} \subseteq \{1, \cdots, n\}$,

$$\Pr(B_{i_1} \wedge \cdots \wedge B_{i_k}) = \Pr(B_1 \wedge \cdots \wedge B_k),$$

and there is a constant μ *so that for any fixed* k,

$$n^k \Pr(B_1 \wedge \cdots \wedge B_k) \sim \mu^k.$$

Then Y *is also asymptotically Poisson with mean* μ.

4.1. *Networks with Bernoulli Nodes and Links*

In the Bernoulli model, in order to apply Theorem 4.1, let B_i be the event that X_i is isolated for $1 \leq i \leq n$ and Y be the number of B_i that hold. Then Y is exactly the number of isolated nodes. Similarly, let B_i' be the event that X_i is isolated and active for $1 \leq i \leq n$ and Y' be the number of such B_i' events that hold. Then Y' is exactly the number of isolated active nodes. Obviously, for any set $\{i_1, \cdots, i_k\} \subseteq \{1, \cdots, n\}$,

$$\begin{aligned}
\Pr\left(B_{i_1} \wedge \cdots \wedge B_{i_k}\right) &= \Pr\left(B_1 \wedge \cdots \wedge B_k\right), \\
\Pr\left(B_{i_1}' \wedge \cdots \wedge B_{i_k}'\right) &= \Pr\left(B_1' \wedge \cdots \wedge B_k'\right).
\end{aligned}$$

In addition,

$$\Pr\left(B_1' \wedge \cdots \wedge B_k'\right) = \left(p_1\right)^k \Pr\left(B_1 \wedge \cdots \wedge B_k\right).$$

Thus, in order to prove Theorem 2.1, it suffices to show that if $r = \sqrt{\frac{\ln n + \xi}{\pi p_1 p_2 n}}$ for some constant ξ, then for any fixed k,

$$n^k \Pr\left(B_1 \wedge \cdots \wedge B_k\right) \sim e^{-k\xi}. \tag{4.1}$$

The proof of this asymptotic equality will use the following two lemmas. For convenience, let $q_1 = 1 - p_1$ and $q_2 = 1 - p_2$.

Lemma 4.2. *For any $x \in \Omega$,*

$$\Pr\left(B_1 \mid X_1 = x\right) = \left(1 - p_1 p_2 \nu_r\left(x\right)\right)^{n-1}.$$

Proof. For any $x \in \Omega$, let N_1 and N_2 denote the number of active nodes and the number of inactive nodes of $X_2, \cdots, X_n$ within $\nu_r\left(X_1\right)$ respectively. There are exactly N_1 links between X_1 and those N_1 active nodes. If X_1 is isolated, all of those N_1 links must be down. So

$$\begin{aligned}
&\Pr\left(B_1 \mid N_1 = i, N_2 = j\right) \\
&= \Pr\left(\begin{array}{l|l} \text{all links of } X_1 \text{ to active} & N_1 = i, \\ \text{nodes are down} & N_2 = j \end{array}\right) \\
&= \left(q_2\right)^i,
\end{aligned}$$

and

$$\begin{aligned}
&\Pr\left(N_1 = i, N_2 = j \mid X_1 = x\right) \\
&= \binom{n-1}{i, j} \left(1 - \nu_r\left(x\right)\right)^{n-1-i-j} \\
&\cdot \left(p_1 \nu_r\left(x\right)\right)^i \left(q_1 \nu_r\left(x\right)\right)^j.
\end{aligned}$$

Thus,

$$\begin{aligned}
&\Pr\left(B_1 \mid X_1 = x\right) \\
&= \sum_{i+j=0}^{n-1} \Pr\left(B_1 \mid N_1 = i, N_2 = j\right) \cdot \\
&\quad \Pr\left(N_1 = i, N_2 = j \mid X_1 = x\right) \\
&= \sum_{i+j=0}^{n-1} \frac{\left(q_2\right)^i \binom{n-1}{i,j} \left(1-\nu_r\left(x\right)\right)^{n-1-i-j} \cdot}{\left(p_1\nu_r\left(x\right)\right)^i \left(q_1\nu_r\left(x\right)\right)^j} \\
&= \left(1 - p_1p_2\nu_r\left(x\right)\right)^{n-1}.
\end{aligned}$$

Therefore, the lemma is proved. □

Lemma 4.3. *For any $k \geq 2$ and $(x_1, \cdots, x_k) \in \Omega^k$,*

$$\begin{aligned}
&\Pr\left(B_1 \wedge \cdots \wedge B_k \mid X_i = x_i, 1 \leq i \leq k\right) \\
&\leq \left(1 - p_1p_2\nu_r\left(x_1, \cdots, x_k\right)\right)^{n-k}.
\end{aligned}$$

In addition, the equality is achieved for $(x_1, \cdots, x_k) \in C_{kk}$.

Proof. For any $(x_1, \cdots, x_k) \in \Omega^k$, let N_1 and N_2 be the number of active nodes and the number of inactive nodes of $X_{k+1}, \cdots, X_n$ within $\nu_r\left(X_1, \cdots, X_k\right)$ respectively. There are at least N_1 links between $X_1, \cdots, X_k$ and those N_1 active nodes. If $X_1, \cdots, X_k$ are isolated, all of those links must be down. So

$$\begin{aligned}
&\Pr\left(B_1 \wedge \cdots \wedge B_k \,|N_1 = i, N_2 = j\,\right) \\
&= \Pr\left(\begin{array}{l|l} \text{links of } X_1, \cdots, X_k \text{ to} & N_1 = i, \\ \text{active nodes are down} & N_2 = j \end{array}\right) \\
&\leq \left(q_2\right)^i.
\end{aligned}$$

Thus,

$$\begin{aligned}
&\Pr\left(B_1 \wedge \cdots \wedge B_k \mid X_i = x_i, 1 \leq i \leq k\right) \\
&= \sum_{i+j=0}^{n-k} \Pr\left(B_1 \wedge \cdots \wedge B_k \mid N_1 = i, N_2 = j\right) \cdot \\
&\quad \Pr\left(N_1 = i, N_2 = j \mid X_i = x_i \text{ for } 1 \leq i \leq k\right) \\
&\leq \sum_{i+j=0}^{n-k} \frac{\left(q_2\right)^i \binom{n-k}{i,j} \left(1-\nu_r\left(x_1, \cdots, x_k\right)\right)^{n-k-i-j} \cdot}{\left(p_1\nu_r\left(x_1, \cdots, x_k\right)\right)^i \left(q_1\nu_r\left(x_1, \cdots, x_k\right)\right)^j} \\
&= \left(1 - p_1p_2\nu_r\left(x_1, \cdots, x_k\right)\right)^{n-k}.
\end{aligned}$$

For any $(x_1, \cdots, x_k) \in C_{kk}$,

$$\begin{aligned}
&\Pr\left(B_1 \wedge \cdots \wedge B_k \mid X_i = x_i, 1 \le i \le k\right) \\
&= \Pr\begin{pmatrix} \forall 1 \le i \le k, X_i \text{ has no up-links} \\ \text{to active nodes in } X_{k+1}, \cdots, X_n \end{pmatrix} \\
&= \sum_{m_1+\cdots+m_k=0}^{n-k} \Pr\begin{pmatrix} \forall 1 \le i \le k, \nu_r(x_i) \text{ contains} \\ m_i \text{ active nodes, } m_i' \text{ inactive} \\ \text{nodes, and links of } X_i \text{ to} \\ \text{active nodes are down} \end{pmatrix} \\
&= \sum_{\substack{m_1+\cdots+m_k+ \\ m_1'+\cdots+m_k'=0}}^{n-k} \binom{n-k}{m_1, \cdots, m_k, m_1', \cdots, m_k'} \\
&\cdot \prod_{i=1}^{k} \left(q_2 p_1 \nu_r(x_i)\right)^{m_i} \prod_{i=1}^{k} \left(q_1 \nu_r(x_i)\right)^{m_i'} \\
&\cdot \left(1 - \nu_r(x_1, \cdots, x_k)\right)^{n-k-\sum_{i=1}^{k}\left(m_i+m_i'\right)} \\
&= \left(1 - p_1 p_2 \nu_r(x_1, \cdots, x_k)\right)^{n-k}.
\end{aligned}$$

Therefore, the lemma is proved. □

Now we are ready to prove the asymptotic equality (4.1). From Lemma 4.2 and 3.1,

$$n \Pr(B_1) = n \int_\Omega \left(1 - p_1 p_2 v_r(x)\right)^{n-1} dx \sim e^{-\xi}.$$

So the asymptotic equality (4.1) is true for $k = 1$. Now we fix $k \ge 2$. From Lemma 4.3, 3.2 and 3.3,

$$\begin{aligned}
&n^k \Pr\left(B_1 \wedge \cdots \wedge B_k \text{ and } (X_1, \cdots, X_k) \in \Omega^k \setminus C_{kk}\right) \\
&\le n^k \int_{\Omega^k \setminus C_{kk}} \left(1 - p_1 p_2 \nu_r(x_1, \cdots, x_k)\right)^{n-k} \prod_{i=1}^{k} dx_i \\
&= o(1).
\end{aligned}$$

From Lemma 4.3 and 3.4,

$$\begin{aligned}
&n^k \Pr\left(B_1 \wedge \cdots \wedge B_k \text{ and } (X_1, \cdots, X_k) \in C_{kk}\right) \\
&= n^k \int_{C_{kk}} \left(1 - p_1 p_2 \nu_r(x_1, \cdots, x_k)\right)^{n-k} \prod_{i=1}^{k} dx_i \\
&\sim e^{-k\xi}.
\end{aligned}$$

Thus, the asymptotic equality (4.1) is also true for any fixed $k \ge 2$. This completes the proof of Theorem 2.1.

We have applied Theorem 4.1 (*Brun's sieve*) to show the total number of (active) isolated nodes is asymptotically Poisson in the Bernoulli model. Now we switch to the secure wireless networks.

4.2. *Secure Wireless Networks*

In secure wireless networks, in order to apply Theorem 4.1, let B_i be the event that X_i is isolated for $1 \leq i \leq n$ and Y be the number of such B_i events that hold. Then Y is exactly the number of isolated nodes. Obviously, for any set $\{i_1, \cdots, i_k\} \subseteq \{1, \cdots, n\}$,

$$\Pr\left(B_{i_1} \wedge \cdots \wedge B_{i_k}\right) = \Pr\left(B_1 \wedge \cdots \wedge B_k\right).$$

Thus, in order to prove Theorem 2.2, it suffices to show that if $r = \sqrt{\frac{\ln n + \xi}{\pi p n}}$ for some constant ξ, then for any fixed k,

$$n^k \Pr\left(B_1 \wedge \cdots \wedge B_k\right) \sim e^{-k\xi}. \tag{4.2}$$

The proof of this asymptotic equality will use the following two lemmas. For convenience, let $q = 1 - p$. (Here p is the probability of the event that two key rings have at least m common keys.)

Lemma 4.4. *For any $x \in \Omega$,*

$$\Pr\left(B_1 \mid X_1 = x\right) = \left(1 - p\nu_r\left(x\right)\right)^{n-1}.$$

Proof. For any $x \in \Omega$, let N denote the number of nodes of $X_2, \cdots, X_n$ within $\nu_r\left(X_1\right)$. If X_1 is isolated, all X_1's neighbors may have at most $m-1$ keys that are also in the key ring of X_1. For X_1's neighbors, the event is independent and identical. Thus,

$$\begin{aligned}
&\Pr\left(B_1 \mid X_1 = x\right) \\
&= \sum_{i=0}^{n-1} \Pr\left(X_1 \text{ is isolated} \mid N = i\right) \cdot \\
&\quad \Pr\left(N = i \mid X_1 = x\right) \\
&= \sum_{i=0}^{n-1} q^i \binom{n-1}{i} \left(1 - \nu_r\left(x\right)\right)^{n-1-i} \nu_r\left(x\right)^i \\
&= \left(1 - \nu_r\left(x\right) + q\nu_r\left(x\right)\right)^{n-1} = \left(1 - p\nu_r\left(x\right)\right)^{n-1}.
\end{aligned}$$

Therefore, the lemma is proved. □

Lemma 4.5. *For any $k \geq 2$ and $(x_1, \cdots, x_k) \in \Omega^k$,*

$$\begin{aligned}
&\Pr\left(B_1 \wedge \cdots \wedge B_k \mid X_i = x_i, 1 \leq i \leq k\right) \\
&\leq \left(1 - p\nu_r\left(x_1, \cdots, x_k\right)\right)^{n-k}.
\end{aligned}$$

In addition, the equality is achieved for $(x_1, \cdots, x_k) \in C_{kk}$.

Proof. For any $(x_1, \cdots, x_k) \in \Omega^k$, let N denote the number of nodes of $X_{k+1}, \cdots, X_n$ within $\nu_r(X_1, \cdots, X_k)$. Each of those N nodes is neighbor to at least one of $X_1, \cdots, X_k$, but the link is not secured. Therefore, we have $\Pr(B_1 \wedge \cdots \wedge B_k \mid N = i) \leq q^i$. Thus,

$$\begin{aligned}
&\Pr(B_1 \wedge \cdots \wedge B_k \mid X_i = x_i, 1 \leq i \leq k) \\
&= \sum_{i=0}^{n-k} \Pr(B_1 \wedge \cdots \wedge B_k \mid N = i) \cdot \\
&\quad \Pr(N = i \mid X_i = x_i \text{ for } 1 \leq i \leq k) \\
&\leq \sum_{i=0}^{n-k} q^i \binom{n-k}{i} (1 - v_r(x_1, \cdots, x_k))^{n-k-i} \\
&\quad v_r(x_1, \cdots, x_k)^i \\
&= (1 - v_r(x_1, \cdots, x_k) + q v_r(x_1, \cdots, x_k))^{n-k} \\
&= (1 - p v_r(x_1, \cdots, x_k))^{n-k}.
\end{aligned}$$

For any $(x_1, \cdots, x_k) \in C_{kk}$, each of those N nodes has exactly one neighbor among $X_1, \cdots, X_k$. Therefore, we have $\Pr(B_1 \wedge \cdots \wedge B_k \mid N = i) = q^i$ and

$$\begin{aligned}
&\Pr(B_1 \wedge \cdots \wedge B_k \mid X_i = x_i, 1 \leq i \leq k) \\
&= (1 - p \nu_r(x_1, \cdots, x_k))^{n-k}.
\end{aligned}$$

Therefore, the lemma is proved. □

The asymptotic equality (4.2) can be proved by applying the same argument used for the Bernoulli model but replacing Lemma 4.2 and 4.3 by Lemma 4.4 and 4.5. Thus, we complete the proof of Theorem 2.2.

5. Network Scenarios and Simulation Results

For the sake of convenience, we introduce an acronym CTR, the critical transmission radius. For an instance of point sets, the smallest transmission radius r such that the induced r-disk graph over the point set has no isolated nodes is called the *CTR for no isolated nodes*; the smallest transmission radius r such that the induced r-disk graph over the point set is connected is called the *CTR for connectivity*. For random point processes, CTRs are random variables.

In the general case, the inexistence of isolated nodes in wireless ad hoc networks is a necessary condition (but not sufficient) for network connectivity. That is to say, the CTR for connectivity is at least as large as the CTR for no isolated nodes. But in large-scale randomly deployed wireless ad hoc networks, the two CTRs are asymptotically the same in probability. In this section, the difference between the two CTRs and our theoretical CTR will be investigated by running extensive simulations over different network sizes.

Table 1. The average CTRs of native random geometric graph model.

n	R_{iso}	R_{con}	R_{th}	DR_{iso}	DR_{con}
100	0.1469	0.1612	0.1277	0.1508	0.2627
400	0.0821	0.0872	0.0721	0.1395	0.2107
1600	0.0443	0.0462	0.0397	0.1163	0.1632

In our simulation, the locations of wireless ad hoc devices are generated by a uniform point process over a unit-area disk or square with node density $n = 100$, $n = 400$, and $n = 1600$, and 800 sets of random points are generated for each case. The cumulative distribution functions of CTRs will be illustrated. In these figures (including Fig. 3, 4, and 5), the x-axis represents the transmission radius, and the y-axis represents the probability. In each figure, there are three sets of curves, from left to right, for $n = 1600$, $n = 400$, and $n = 100$, respectively. In each set of curves, the blue curve is the c.d.f. of the theoretical CTR for no isolated nodes, the black one is of the CTR for no isolated nodes, and the red one is of the CTR for connectivity. For convenience, let R_{iso} be the CTR for no isolated nodes, R_{con} be the CTR for connectivity, and R_{th} be the theoretical CTR. To show the difference between the theoretical values and simulation outcomes, we calculate the inaccuracy by following formulas

$$DR_{iso} = \frac{R_{iso} - R_{th}}{R_{iso}} \text{ and } DR_{con} = \frac{R_{con} - R_{th}}{R_{con}}.$$

5.1. *Native Models*

For comparison, we first consider the network model in which neither node failure nor link failure occurs. This is exactly a special case with $p_1 = 1$ and $p_2 = 1$, and actually, this is also the most popular model discussed in literature. Table 1 shows average CTRs, and we can see that the average CTRs converge in percentage as the network size increases. The DR_{iso} and DR_{iso} should be close to 0 as n approaches infinity. However, the gap may be associated with the boundary effect. The sensor nodes near the boundary have a higher chance of having fewer neighbors.

5.2. *Networks with Bernoulli Nodes*

Next, we consider the network with unreliable nodes but with reliable links, i.e., $p_1 < 1$ and $p_2 = 1$. This is the same model discussed in [10,5] in which nodes may break down with probability $1 - p_1$ independently after deployed.

In addition, we consider another scenario. Each node independently has probability p_1 to stay in waking mode, and probability $1 - p_1$ in sleeping mode. Nodes only do jobs in waking mode, such as sending/receiving data, or being a member of the virtual backbone and relaying packet for other nodes. In sleeping mode, they do

Table 2. The average CTRs of the Bernoulli node model.

$p_1 = 0.8$ (active/inactive), $p_2 = 1$					
n	R_{iso}	R_{con}	R_{th}	DR_{iso}	DR_{con}
100	0.1617	0.1795	0.1396	0.1587	0.2860
400	0.0895	0.0955	0.0792	0.1304	0.2069
1600	0.0492	0.0513	0.0437	0.1235	0.1722
$p_1 = 0.8$ (awake/sleeping), $p_2 = 1$					
n	R_{iso}	R_{con}	R_{th}	DR_{iso}	DR_{con}
100	0.1662	0.1815	0.1427	0.1642	0.2715
400	0.0918	0.0972	0.0806	0.1393	0.2070
1600	0.0501	0.0519	0.0444	0.1295	0.1698

nothing but monitor a particular broadcasting channel, e.g. beacons in ZigBee networks. Moreover, nodes in sleeping mode need to have at least one waking neighbor to prevent being isolated from the network. For such networks, a node is called isolated if it does not have waking neighbors, and a network is connected if all waking nodes form a connected network and every sleeping node has at least one waking neighbor. Note that CTRs here can be contributed by a listening link between a pair of waking and sleeping nodes.

The average CTRs for R_{iso}, R_{con}, and R_{th} corresponding to previous two network scenarios are listed in Table 2. Beside a unit-area disk, we also run simulations for random point sets over a unit-area square. Basically, the results are similar to the results of random point sets over a unit-area disk. Due to the similarity and the constraint on the number of figures and tables, we do not give related simulation data here.

5.3. *Networks with Bernoulli Nodes and Links*

In the real world, wireless signals may be blocked and reflected by geographic barriers as well as buildings and interfered by other signals. Thus, communication links may not be available anytime. So, besides unreliable nodes, we consider networks with unreliable links. Assume nodes may break down independently with probability $1-p_1$, and links may be down independently with probability $1-p_2$. Fig. 1 and 2 are instances of networks with 200 nodes in a unit-area disk with $p_1 = 0.8$ and $p_2 = 0.8$.

Black nodes represent well-functioned devices, and white nodes represent failed ones. The edges denoted by solid lines between black nodes are up-links, and the edges denoted by dash lines are down links. In Fig. 1, ab with length 0.097235 is the longest edge and corresponds to the CTR such that every black node has at least one solid edge. In Fig. 2, ab with length 0.135864 is the longest edge and corresponds to the CTR such that black nodes and solid edges form a connected graph. Fig. 3

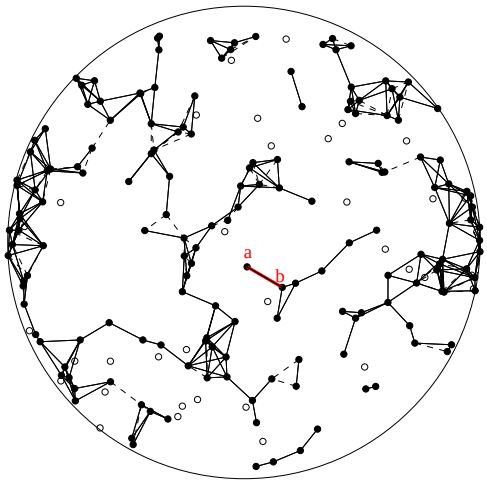

Fig. 1. A network with unreliable nodes and links in which $p_1 = 0.8$ is the probability for nodes being well-functioned and $p_2 = 0.8$ is the probability for links being up. 200 nodes are deployed in a unit-area disk. The edge ab marked by red line is corresponding to the CTR for no isolated nodes. The figure is plotted with $r = \|a - b\| = 0.097235$.

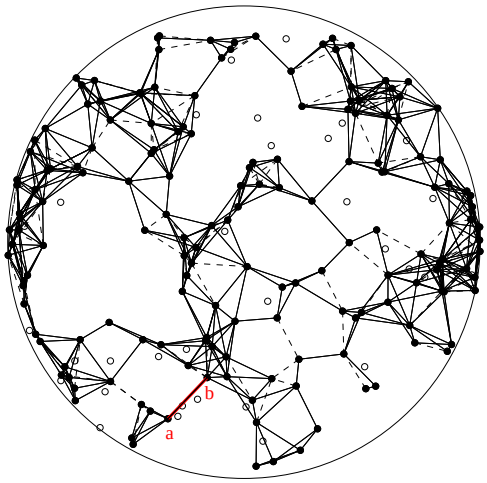

Fig. 2. A network with unreliable nodes and links in which $p_1 = 0.8$ is the probability for nodes being well-functioned and $p_2 = 0.8$ is the probability for links being up. 200 nodes are deployed in a unit-area disk. The edge ab marked by red line is corresponding to the CTR for connectivity. The figure is plotted with $r = \|a - b\| = 0.135864$.

illustrates the c.d.f. of CTRs corresponding to $p_1 = 0.9$ and $p_2 = 0.8$.

In addition, we consider another scenario in which every node independently stays in waking mode with probability p_1 and in sleeping mode with probability $1 - p_1$, instead of breaking down. For such networks, a node is isolated if it does

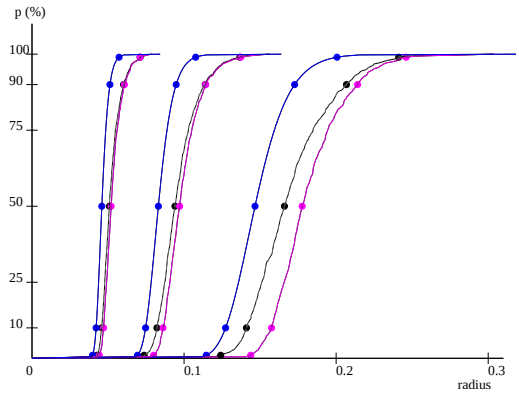

Fig. 3. The c.d.f. of CTRs of networks composed of Bernoulli nodes (well-functioned/breaking down mode) with $p_1 = 0.9$ and Bernoulli links with $p_2 = 0.8$. Nodes are distributed over a unit-area disk.

not have any solid edge connecting to black node, and a network is connected if all black nodes and solid edges form a connected graph and every white node has at least one solid edge. Fig. 4 illustrates the c.d.f. of CTRs corresponding to $p_1 = 0.9$ and $p_2 = 0.8$.

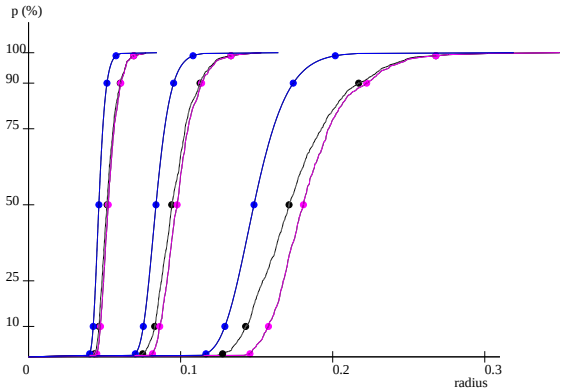

Fig. 4. The c.d.f. of CTRs of networks composed of Bernoulli nodes (awake/sleeping mode) with $p_1 = 0.9$ and Bernoulli links with $p_2 = 0.8$. Nodes are distributed over a unit-area disk.

The average CTRs for R_{iso}, R_{con}, and R_{th} corresponding to previous two network scenarios are listed in Table 3.

As the network size increases, qualitatively, we see the c.d.f. curves become closer to each other in Fig. 3 and 4, and in addition, quantitatively, we see that the average CTRs converge in percentage in Table 3.

Table 3. The average CTRs of the Bernoulli node and link model.

$p_1 = 0.9$ (active/inactive), $p_2 = 0.8$ (Fig. 3)					
n	R_{iso}	R_{con}	R_{th}	DR_{iso}	DR_{con}
100	0.1704	0.1823	0.1489	0.1443	0.2242
400	0.0963	0.0991	0.0842	0.1433	0.1769
1600	0.0522	0.0532	0.0465	0.1230	0.1450
$p_1 = 0.9$ (awake/sleeping), $p_2 = 0.8$ (Fig. 4)					
n	R_{iso}	R_{con}	R_{th}	DR_{iso}	DR_{con}
100	0.1765	0.1856	0.1505	0.1732	0.2335
400	0.0964	0.0991	0.0849	0.1355	0.1673
1600	0.0525	0.0534	0.0468	0.1230	0.1407

5.4. *Secure Wireless Networks*

The last simulation result is for the m-composite key predistribution scheme. In secure networks with key pool size K and key ring size k, at least m common keys are required for each pair of nodes to establish secured links. In the simulation, we use $K = 40$ and $k = 10$. For simplicity, we assume all nodes are active, i.e., $p_1 = 1$. Fig. 5 illustrates the c.d.f. of CTRs corresponding to $m = 2$. Table 4 shows average CTRs for R_{iso}, R_{con}, R_{th} corresponding to $K = 40$, $k = 10$, and $m = 2$. Note that $p = 0.795771$ for $K = 40$, $k = 10$, and $m = 2$.

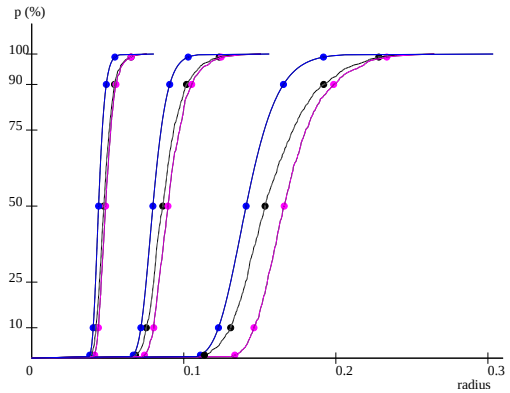

Fig. 5. The c.d.f. of CTRs of secured networks composed of nodes distributed over a unit-area disk with $K = 40$, $k = 10$, and $m = 2$. The corresponding p is 0.795771.

Table 4. The average CTRs corresponding to $K = 40$, $k = 10$, and $m = 1$ and 2, respectively.

$K = 40, k = 10, m = 1$					
n	R_{iso}	R_{con}	R_{th}	DR_{iso}	DR_{con}
100	0.1482	0.1627	0.1300	0.1397	0.2515
400	0.0824	0.0874	0.0734	0.1234	0.1918
1600	0.0449	0.0467	0.0404	0.1103	0.1557
$K = 40, k = 10, m = 2$ (Fig. 5)					
n	R_{iso}	R_{con}	R_{th}	DR_{iso}	DR_{con}
100	0.1580	0.1698	0.1431	0.1042	0.1862
400	0.0879	0.0915	0.0808	0.0883	0.1328
1600	0.0482	0.0493	0.0445	0.0831	0.1088

6. Conclusions

In this paper, the connectivity of wireless networks in which nodes and links are not reliable was investigated by the distribution of the number of isolated nodes in the networks. We assume a wireless network is composed of a collection of wireless sensors represented by a uniform n-point process over the unit-area disk or square. In the Bernoulli model, nodes are active independently with probability $0 < p_1 \leq 1$, and links are up independently with probability $0 < p_2 \leq 1$. We show that, if all nodes have the same transmission radius $r_n = \sqrt{\frac{\ln n + \xi}{\pi p_1 p_2 n}}$ for some constant ξ, then the total number of isolated nodes is asymptotically Poisson with mean $e^{-\xi}$ and the total number of isolated active nodes is also asymptotically Poisson with mean $p_1 e^{-\xi}$. In the m-composite key predistribution schemes, let p denote the probability of the event that two neighbor nodes have a secure link. We show that, if all nodes have the same transmission radius $r_n = \sqrt{\frac{\ln n + \xi}{\pi p n}}$ for some constant ξ, then the total number of isolated nodes is asymptotically Poisson with mean $e^{-\xi}$. The convergence of the asymptotic CTR was verified by extensive simulations. The average and c.d.f. of CTRs were investigated under different network scenarios. The problem whether or not the inexistence of isolated nodes almost surely implies connectivity of networks is still open.

Acknowledgments

This work of Dr. Wan is supported in part by NSF Grant No. CCF-0515088 of USA. This work of Dr. Yi is supported in part by NSC under Grant No. NSC97-2221-E-009-052-MY3 and NSC98-2218-E-009-023, by MoEA under Grant No. 98-EC-17-A-02-S2-0048, by ITRI under Grant No. 99-EC-17-A-05-01-0626, and by the MoE ATU plan.

References

[1] P. Gupta and P. R. Kumar, "Critical power for asymptotic connectivity in wireless networks," in *Stochastic Analysis, Control, Optimization and Applications: A Volume in Honor of W. H. Fleming*, W. M. McEneaney, G. Yin, and Q. Zhang, Eds. Birkhauser, March 1998, pp. 547–566.

[2] H. Zhang and J. Hou, "On deriving the upper bound of α-lifetime for large sensor networks," in *Proceedings of the 5th ACM International Symposium on Mobile Ad Hoc Networking and Computing*, 24-26 May 2004, pp. 121–132.

[3] P.-J. Wan, C.-W. Yi, F. Yao, and X. Jia, "Asymptotic critical transmission radius for greedy forward routing in wireless ad hoc networks," in *Proceedings of the 7th ACM International Symposium on Mobile Ad Hoc Networking and Computing*, 22-25 May 2006, pp. 25–36.

[4] P.-J. Wan and C.-W. Yi, "Coverage by randomly deployed wireless sensor networks," *IEEE Transactions on Information Theory*, vol. 52, no. 6, pp. 2658–2669, June 2006.

[5] C.-W. Yi, P.-J. Wan, X.-Y. Li, and O. Frieder, "Asymptotic distribution of the number of isolated nodes in wireless ad hoc networks with Bernoulli nodes," *IEEE Transactions on Communications*, vol. 54, no. 3, pp. 510–517, March 2006.

[6] E. N. Gilbert, "Random plane networks," *Journal of the Society for Industrial and Applied Mathematics*, vol. 9, no. 4, pp. 533–543, December 1961.

[7] H. Dette and N. Henze, "The limit distribution of the largest nearest-neighbour link in the unit d-cube," *Journal of Applied Probability*, vol. 26, no. 1, pp. 67–80, March 1989.

[8] M. D. Penrose, "The longest edge of the random minimal spanning tree," *The Annals of Applied Probability*, vol. 7, no. 2, pp. 340–361, May 1997.

[9] P.-J. Wan and C.-W. Yi, "Asymptotic critical transmission radius and critical neighbor number for k-connectivity in wireless ad hoc networks," in *Proceedings of the 5th ACM International Symposium on Mobile Ad Hoc Networking and Computing*, 24-26 May 2004, pp. 1–8.

[10] ——, "Asymptotic critical transmission ranges for connectivity in wireless ad hoc networks with Bernoulli nodes," in *IEEE Wireless Communications and Networking Conference (WCNC '05)*, 13-17 March 2005.

[11] R. Meester and R. Roy, *Continuum Percolation*. New York, NY, USA: Cambridge University Press, 1996.

[12] H. M. Ammari and S. K. Das, "Critical density for coverage and connectivity in three-dimensional wireless sensor networks using continuum percolation," *IEEE Transactions on Parallel Distributed Systems*, vol. 20, no. 6, pp. 872–885, June 2009.

[13] M. Franceschetti and R. Meester, "Critical node lifetimes in random networks via the Chen-Stein method," *IEEE Transactions on Information Theory*, vol. 52, no. 6, pp. 2831–2837, June 2006.

[14] L. Eschenauer and V. D. Gligor, "A key-management scheme for distributed sensor networks," in *Proceedings of the 9th ACM Conference on Computer and Communications Security*, 18-22 November 2002, pp. 41–47.

[15] H. Chan, A. Perrig, and D. Song, "Random key predistribution schemes for sensor networks," in *Proceedings of the 2003 IEEE Symposium on Security and Privacy*, 11-14 May 2003, pp. 197–213.

[16] R. D. Pietro, L. Mancini, A. Mei, A. Panconesi, and J. Radhakrishnan, "Connectivity properties of secure wireless sensor networks," in *Proceedings of the 2004 ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN '04)*, 25 October 2004, pp. 53–58.

[17] N. Alon and J. H. Spencer, *The Probabilistic Method*, 2nd ed. New York, USA:

Wiley, March 2000.