

# 國立交通大學

## 網路工程研究所

### 碩士論文

無線隨意網路在具不可靠節點與  
連線環境中之網路連通性

Connectivity of the Wireless Ad Hoc Networks  
with Unreliable Nodes and Links

研究生：林國維

指導教授：易志偉

中華民國九十六年七月

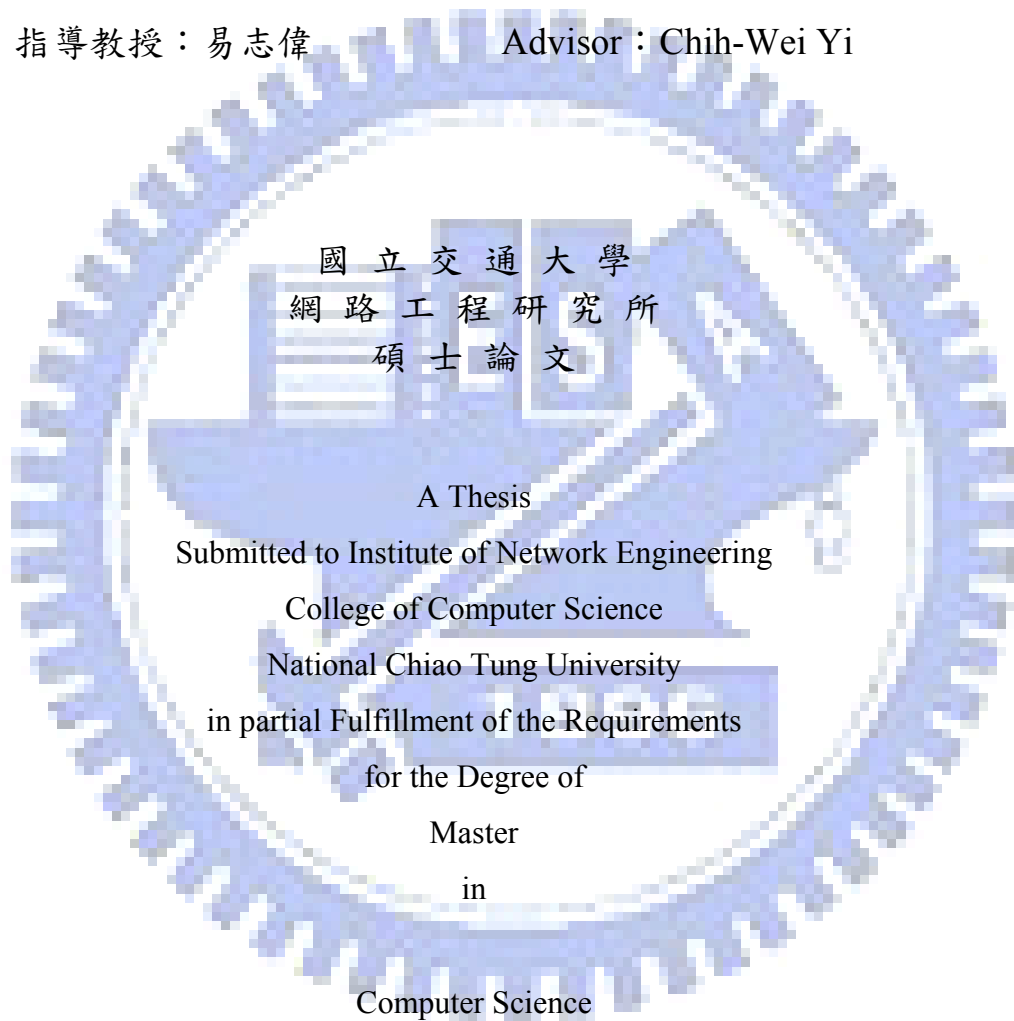
無線隨意網路在具不可靠節點與連線環境中之網路連通性  
Connectivity of the Wireless Ad Hoc Networks  
with Unreliable Nodes and Links

研究生：林國維

Student : Kuo-Wei Lin

指導教授：易志偉

Advisor : Chih-Wei Yi



July 2007

Hsinchu, Taiwan, Republic of China

中華民國九十六年七月

# Connectivity of the Wireless Ad Hoc Networks with Unreliable Nodes and Links

Student: Kuo-Wei Lin      Advisor: Dr. Chih-Wei Yi

Institute of Network Engineering  
National Chiao Tung University

## Abstract

In randomly-deployed wireless ad hoc networks with reliable nodes and links, vanishment of isolated nodes asymptotically implies connectivity of networks. However, in a realistic system, nodes may become inactive, and links may become down. The inactive nodes and down links cannot take part in routing/relaying and thus may affect the connectivity. In this paper, we study the connectivity of a wireless ad hoc network that is composed of unreliable nodes and links by investigating the distribution of the number of isolated nodes in the network. We assume that the wireless ad hoc network consists of  $n$  nodes which are distributed independently and uniformly in an unit-area disk or square. Nodes are active independently with probability  $0 < p_1 \leq 1$ , and links are up independently with probability  $0 < p_2 \leq 1$ . A node is said to be *isolated* if it doesn't have an up link to active nodes. We show that if all nodes have a maximum transmission radius  $r_n = \sqrt{\frac{\ln n + \xi}{\pi p_1 p_2 n}}$  for some constant  $\xi$ , 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 addition, the work can be extended for secure wireless networks which adopt  $m$ -composite key predistribution schemes or multiple-space key predistribution scheme in which a node is said to be *isolated* if it doesn't have a secure link to its neighbor nodes. Let  $p$  denote the probability of the event that two neighbor nodes have a secure link. We show that if all nodes have a maximum transmission radius  $r_n = \sqrt{\frac{\ln n + \xi}{\pi p n}}$  for some constant  $\xi$ , then the total number of isolated nodes is asymptotically Poisson with mean  $e^{-\xi}$ . We also give extensive simulations. The convergence of the asymptotic critical transmission radius was verified by simulations. In our simulations, various network scenarios were considered, and the average and cumulative distribution function of critical transmission radii were investigated.

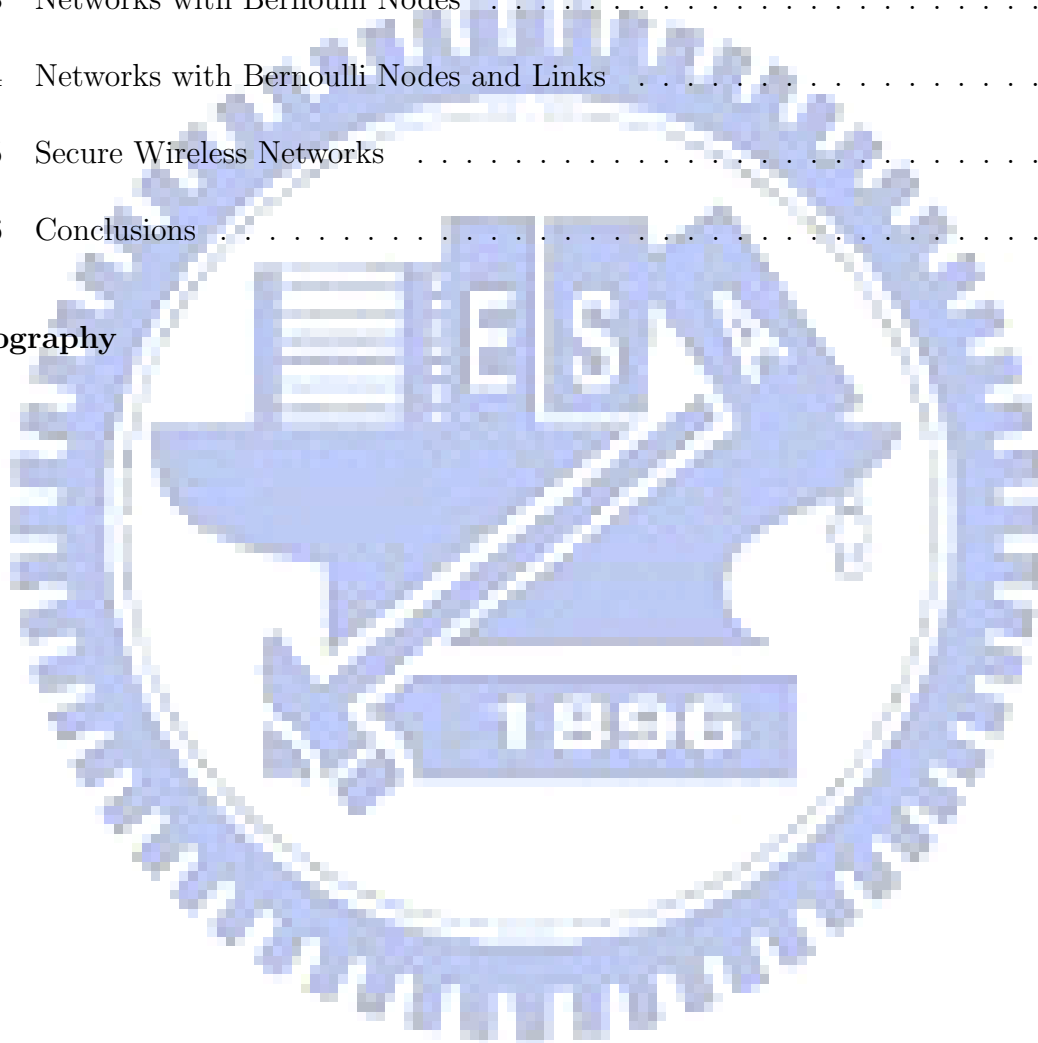
#### **Keywords**

Connectivity, isolated nodes, asymptotic distribution, random geometric graphs, random key predistribution.

# Contents

<b>List of Figures</b>	<b>vii</b>
<b>List of Tables</b>	<b>viii</b>
<b>1 Introduction</b>	<b>1</b>
1.1 What is the Wireless Ad Hoc Network . . . . .	1
1.2 Motivation and Model . . . . .	2
1.3 Related Works . . . . .	3
<b>2 Preliminaries</b>	<b>5</b>
2.1 Geometry of Disks . . . . .	6
2.2 Limits of integrals . . . . .	11
<b>3 Main Results</b>	<b>20</b>
3.1 Wireless Ad Hoc Networks with Bernoulli Model . . . . .	20
3.2 Key Predistribution Scheme . . . . .	23
<b>4 Asymptotic Distribution of The Number of Isolated Nodes</b>	<b>26</b>
4.1 Networks with Bernoulli Nodes and Links . . . . .	27

4.2	Secure Wireless Networks . . . . .	31
<b>5</b>	<b>Simulations and Conclusions</b>	<b>34</b>
5.1	Simulation Setup and Notations . . . . .	34
5.2	Native Models . . . . .	36
5.3	Networks with Bernoulli Nodes . . . . .	38
5.4	Networks with Bernoulli Nodes and Links . . . . .	44
5.5	Secure Wireless Networks . . . . .	52
5.6	Conclusions . . . . .	54
	<b>Bibliography</b>	<b>56</b>



# List of Figures

2.1	The partitions of the unit-area disk $\Omega$ . . . . .	6
2.2	The half-disk and the triangle. . . . .	7
2.3	The area of two intersecting disks. . . . .	8
5.1	The $r$ -disk graph over an unit-area disk. . . . .	36
5.2	The c.d.f. of CTR's of $r$ -disk graphs over an unit-area disk. . . . .	37
5.3	The $r$ -disk graph over an unit-area disk with unreliable nodes. . . . .	38
5.4	The c.d.f. of CTR's over an unit-area disk with unreliable nodes. . . . .	39
5.5	The c.d.f. of CTR's over an unit-area square with unreliable nodes. . . . .	42
5.6	The $r$ -disk graph with waking/sleeping nodes and listening links. . . . .	43
5.7	The c.d.f. of CTR's with waking/sleeping nodes and listening links. . . . .	45
5.8	The $r$ -disk graph with unreliable nodes and links. . . . .	47
5.9	The c.d.f. of CTR's with unreliable nodes and links. . . . .	48
5.10	The c.d.f. of CTR's with waking/sleeping nodes and unreliable links. . . . .	51
5.11	The secure networks with $K = 40$ , $k = 10$ , and $m = 2$ . . . . .	52
5.12	The c.d.f. of CTR's of secure networks. . . . .	53

# List of Tables

5.1	The average CTR's corresponding to Figure 5.2. . . . .	37
5.2	The average CTR's corresponding to Figure 5.4. . . . .	40
5.3	The average CTR's corresponding to Figure 5.5. . . . .	41
5.4	The average CTR's corresponding to Figure 5.7. . . . .	46
5.5	The average CTR's corresponding to Figure 5.8. . . . .	49
5.6	The average CTR's corresponding to Figure 5.10. . . . .	50
5.7	The average CTR's corresponding to Figure 5.12. . . . .	54



# Chapter 1

## Introduction

### 1.1 What is the Wireless Ad Hoc Network

A wireless ad hoc network is composed of a collection of wireless devices distributed over a geographic region. Instead of wired lines, wireless devices transmit/receive data via omnidirectional antennas. 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. Routing is required to be done autonomously by the devices for multi-hop transmission. Due to no need for a fixed infrastructure, wireless ad hoc networks can be flexibly deployed at low cost for various missions. In many applications, wireless devices are deployed in a large volume. The sheer large number of devices deployed coupled with the potential harsh environment often eliminates the possibility of strategic device placement. Consequently, random deployment is often the only viable option.

As wireless ad hoc networks become popular, many related standards have been pro-

posed in the last few years. In 2003, the IEEE 802.15.4 standard [1] was proposed as a MAC and PHY layer standard for low-rate wireless personal area ad hoc networks, and ZigBee specifications [2] were ratified in 2004 as one of the leading standards for wireless ad hoc and sensor networks. J. Zhu and S. Roy (2005) [3] proposed a mesh architecture based on two-radio 802.11 access points (AP's). The IEEE 802.16 standard [4] also known as "WiMAX" was approved in 2004, and the MAC layer supports a primarily point-to-multipoint architecture with an optional mesh topology.

## 1.2 Motivation and Model

The connectivity of wireless ad hoc networks is an essential problem. If a network is not connected, it separates into several disconnected components. There are no communication links between components. So devices in one component can not communicate with devices in other components. Intuitively, there is a tradeoff between the network connectivity and the transmission power of the devices. The larger the transmission power is, the more likely the network is connected. But larger transmission power costs more energy and causes serious interference. In this study, we would like to figure out a balance between network connectivity and transmission power.

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 [5] [6] [7] [8] [9]. 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 (1961) [10] and referred as a *random geometric graph*.

### 1.3 Related Works

A node is said to be *isolated* if it does not have any 1-hop neighbors. The vanishment of isolated nodes in an ad hoc network is a prerequisite of network connectivity. The connectivity of random geometric graphs has been studied by Dette and Henze (1989) [11], Penrose (1997) [12], and others [5] [6] [13] [14]. For an uniform  $n$ -point process over an unit-area square, Dette and Henze (1989) [11] showed that for any constant  $\xi$ , the  $\left(\sqrt{\frac{\ln n + \xi}{\pi n}}\right)$ -disk graph has no isolated nodes with probability  $\exp(-e^{-\xi})$  asymptotically. Later, Penrose (1997) [12] established that if a random geometric graph induced by an uniform point process or Poisson point process has no isolated nodes, then it is almost surely connected.

However, in a realistic system, nodes may become inactive due to, for example, internal breakdown or being in the listening state, and links may become down due to, for example, harsh environment or barriers between nodes. The inactive nodes and down links cannot take part in routing/relaying and thus may affect the connectivity. To model the unreliability of nodes, Wan and Yi et al [6] [14] assume that every nodes independently break down with the same probability  $p$ . They showed that if the maximum transmission radius of every nodes is  $\sqrt{\frac{\ln n + \xi}{\pi p n}}$  for some constant  $\xi$ , the network is connected with probability  $\exp(-pe^{-\xi})$  asymptotically.

Based on the work in [6], we study a more general case of the connectivity of a wireless network with both unreliable nodes and links. We assume nodes are active independently with the same probability  $p_1$  and links are up independently with the same probability  $p_2$ . We show that if all nodes have a maximum transmission radius  $r_n = \sqrt{\frac{\ln n + \xi}{\pi p_1 p_2 n}}$  for some constant  $\xi$ , 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 addition, the work can be extended for secure wireless networks with  $m$ -composite key predistribution schemes [19] [20] [21] [23]. In many applications, the wireless sensor networks are composed of low cost devices. Traditional security schemes and key management algorithms, such as Diffie-Hellman key agreement [17] and RSA signatures [18], are too complex and not feasible for such systems. The  $m$ -composite key predistribution schemes are proposed to offer security for randomly-deployed wireless sensor networks, and are more adaptive to wireless sensor networks. We assume every links have probability  $p$  to be secure independently, and show that if all nodes have a maximum transmission radius  $r_n = \sqrt{\frac{\ln n + \xi}{\pi p n}}$  for some constant  $\xi$ , then the total number of isolated nodes is asymptotically Poisson with mean  $e^{-\xi}$ .

The remaining of this paper is organized as follows. In chapter 2, we present several useful geometric results and integrals. In chapter 3, the main results of the study are given. The distribution of the number of isolated nodes is derived in chapter 4. In chapter 5, we give both simulation results and the conclusions.

# Chapter 2

## Preliminaries

In preparation for our main study, we adopt notations and terminologies used in [6]. For completeness, we give their definitions here. Most lemmas in this chapter can also be found corresponding ones in [6].

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  $S^k$ .  $\|x\|$  is the Euclidean norm of a point  $x \in \mathbb{R}^2$ , and  $|x|$  is the shorthand for 2-dimensional Lebesgue measure (or area) of a measure set  $A \subset \mathbb{R}^2$ . The topological boundary of a set  $A \subset \mathbb{R}^2$  is denoted by  $\partial A$ . 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  $\mathbf{o}$  is denoted by  $\Omega$ . The symbols  $o$  and  $\sim$  always refer to the limit  $n \rightarrow \infty$ . To avoid trivialities, we tacitly assume  $n$  to be sufficiently large if necessary. For simplicity of notation, the dependence of sets and random variables on  $n$  will be frequently suppressed.

Let  $r$  be the transmission radius of the nodes. For any finite set of nodes  $\{x_1, \dots, x_k\}$  in  $\Omega$ , we use  $G_r(x_1, \dots, x_k)$  to denote the  $r$ -disk graph over  $\{x_1, \dots, x_k\}$  in which there is

an edge between two nodes if and only if their Euclidean distance is at most  $r$ . For any positive integers  $k$  and  $m$  with  $1 \leq m \leq k$ , let  $C_{km}$  denote the set of  $(x_1, \dots, x_k) \in \Omega^k$  satisfying that  $G_{2r}(x_1, \dots, x_k)$  has exactly  $m$  connected components.

## 2.1 Geometry of Disks

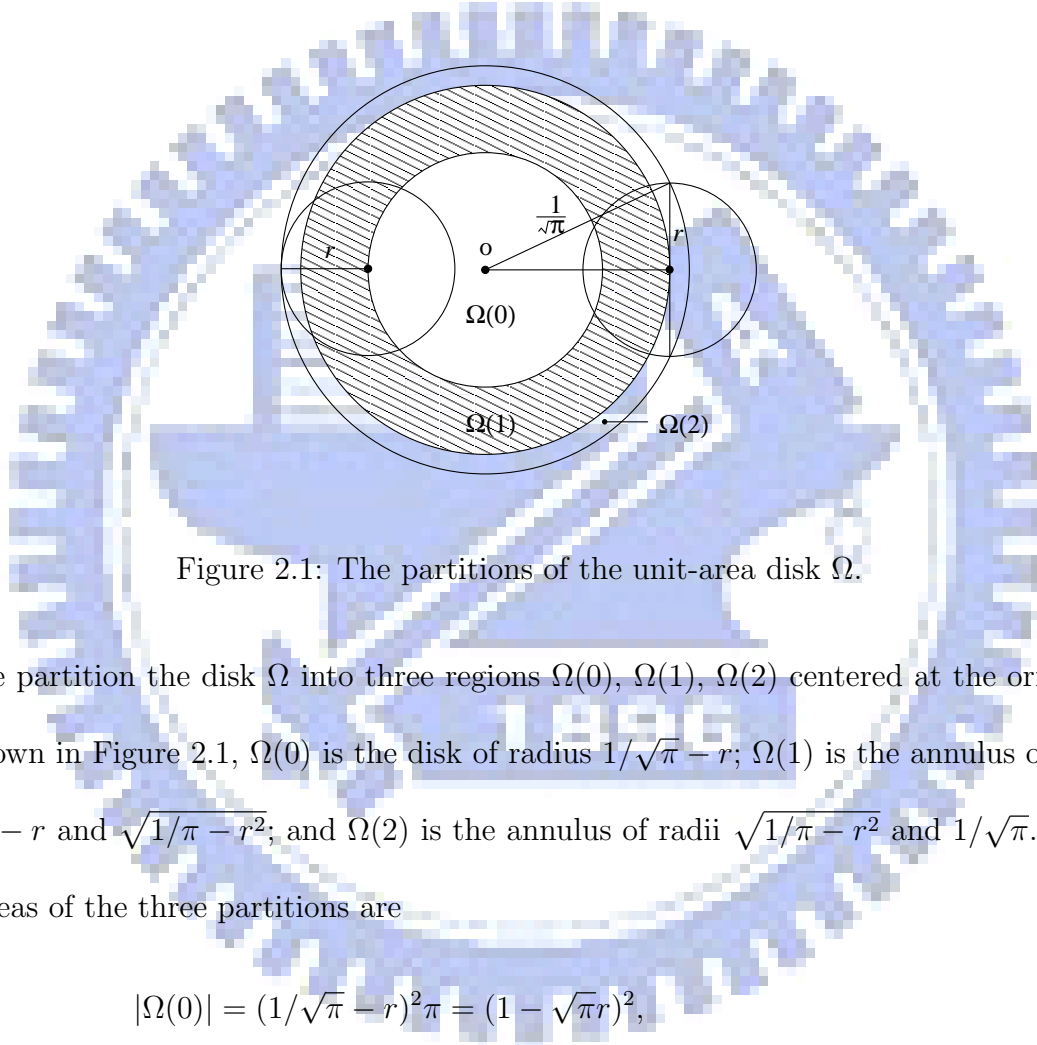


Figure 2.1: The partitions of the unit-area disk  $\Omega$ .

We partition the disk  $\Omega$  into three regions  $\Omega(0)$ ,  $\Omega(1)$ ,  $\Omega(2)$  centered at the origin  $\mathbf{o}$ . As shown in Figure 2.1,  $\Omega(0)$  is the disk of radius  $1/\sqrt{\pi} - r$ ;  $\Omega(1)$  is the annulus of radii  $1/\sqrt{\pi} - r$  and  $\sqrt{1/\pi - r^2}$ ; and  $\Omega(2)$  is the annulus of radii  $\sqrt{1/\pi - r^2}$  and  $1/\sqrt{\pi}$ . Then the areas of the three partitions are

$$\begin{aligned}
 |\Omega(0)| &= (1/\sqrt{\pi} - r)^2 \pi = (1 - \sqrt{\pi}r)^2, \\
 |\Omega(1)| &= (\sqrt{1/\pi - r^2})^2 \pi - (1 - \sqrt{\pi}r)^2 = 2\pi r(1/\sqrt{\pi} - r), \\
 |\Omega(2)| &= \pi r^2.
 \end{aligned}$$

For any set  $S \subseteq \Omega$  and  $r > 0$ , the  $r$ -neighborhood of  $S$  is the set  $\bigcup_{x \in S} B(x, r) \cap \Omega$ . We use  $v_r(S)$  to denote the area of the  $r$ -neighborhood of  $S$ , and sometimes by slightly

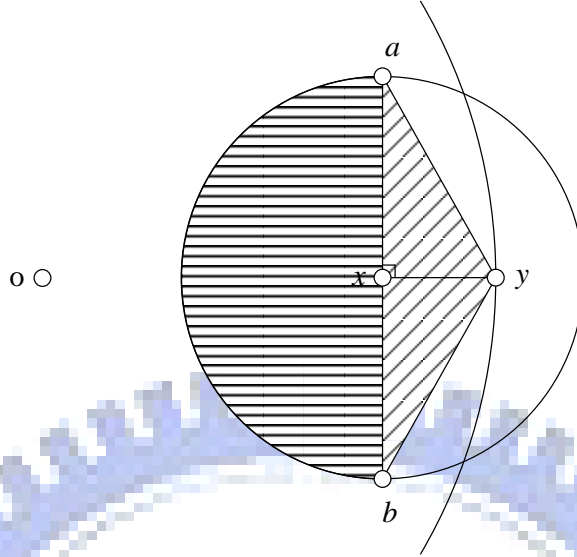


Figure 2.2: The half-disk and the triangle.

abusing the notation, to denote the  $r$ -neighborhood of  $S$  itself. Obviously, for any  $x \in \Omega$ ,  $v_r(x) \geq \pi r^2/3$ . If  $x \in \Omega(0)$ ,  $v_r(x) = \pi r^2$ . If  $x \in \Omega(1)$ , Lemma 1 gives a tighter lower bound on  $v_r(x)$ .

**Lemma 1** For any  $x \in \Omega(1)$ ,

$$v_r(x) \geq \frac{\pi r^2}{2} + \left( \frac{1}{\sqrt{\pi}} - \|x\| \right) r.$$

**Proof.** Intuitively, the transmission radius of  $\Omega = \|y\| = 1/\sqrt{\pi}$ . Let  $y$  be the point in  $\partial\Omega$  such that  $\|y - x\| = \frac{1}{\sqrt{\pi}} - \|x\|$ , and  $ab$  be the diameter of  $B(x, r)$  perpendicular to  $xy$  (see Figure 2.2). Then  $v_r(x)$  contains a half-disk of  $B(x, r)$  to the side of  $ab$  opposite to  $y$ , and the triangle  $aby$ . Since the area of the triangle  $aby$  is exactly  $\left( \frac{1}{\sqrt{\pi}} - \|x\| \right) r$ , the lemma follows. ■

**Lemma 2** Assume that

$$r \leq \frac{1/\sqrt{\pi}}{12/\pi + \pi/12} \approx 0.245/\sqrt{\pi}.$$

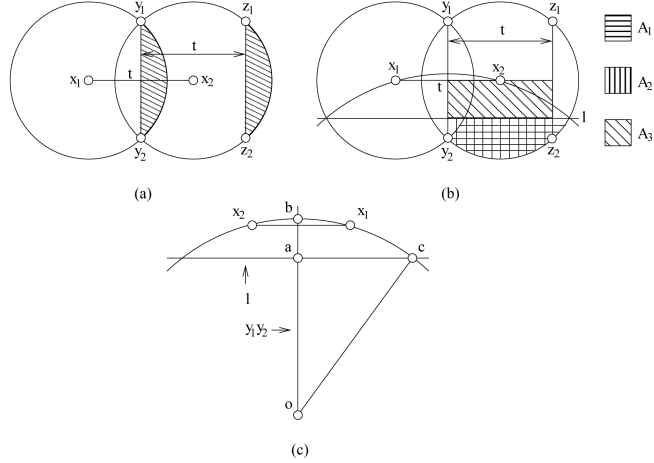


Figure 2.3: The area of two intersecting disks.

Let  $x_1, \dots, x_k$  be a sequence of  $k \geq 2$  nodes in  $\Omega$  such that  $x_1$  has the largest norm, and  $\|x_i - x_j\| \leq 2r$  if and only if  $|i - j| \leq 1$ . then

$$v_r(x_1, \dots, x_k) \geq v_r(x_1) + \frac{\pi}{12} r \sum_{i=1}^{k-1} \|x_{i+1} - x_i\|.$$

**Proof.** We prove the lemma by induction on  $k$ . When  $k = 2$ , let  $t = \|x_2 - x_1\|$  and  $f(t) = |B(x_2, r) \cap B(x_1, r)|$ . First, we show that  $f(t) \geq (\pi/2)rt$ . As shown in Figure 2.3(a), let  $y_1y_2$  be the common chord of  $\partial B(x_1, r)$  and  $\partial B(x_2, r)$ , and  $z_1z_2$  be another chord of  $\partial B(x_2, r)$  that is parallel to  $y_1y_2$  and has the same length as  $y_1y_2$ . Then  $f(t)$  is also equal to the area of the portion of  $B(x_2, r)$  between the two chords  $y_1y_2$  and  $z_1z_2$ . Thus,  $f'(t) = \|y_1y_2\|$ , which is decreasing over  $[0, 2r]$ . Therefore,  $f(t)$  is concave over  $[0, 2r]$ . Since  $f(0) = 0$  and  $f(2r) = \pi r^2$ , we have  $f(t) \geq (\pi/2)rt$ .

Now we are ready to prove the lemma for  $k = 2$ . If  $x_1 \in \Omega(0)$ , then  $v_r(x_1, x_2) - v_r(x_1)$  is exactly  $f(t)$ , and thus the lemma follows immediately from  $f(t) \geq (\pi/2)rt$ . So we assume that  $x_1 \notin \Omega(0)$ . Note that for the same distance  $t$ ,  $v_r(x_1, x_2) - v_r(x_1)$  achieves



its minimum when both  $x_1$  and  $x_2$  are in  $\partial\Omega$ . It is sufficient to prove the lemma for  $x_1, x_2 \in \partial\Omega$ . As shown in Figure 2.3(b), let  $y_1y_2$  and  $z_1z_2$  be the two chords of  $\partial B(x_2, r)$  as above with  $y_2 \in \Omega$ , and  $\ell$  be the line through the two intersection points between  $\partial\Omega$  and  $\partial(B(x_1, r) \cup B(x_2, r))$ .  $A_1$  denotes the portion of  $B(x_2, r) \setminus B(x_1, r)$  which lies in the same side of  $\ell$  as  $y_2$ ;  $A_2$  denotes the portion of  $B(x_2, r)$  which is surrounded by  $y_1y_2$ ,  $z_1z_2$ ,  $\ell$ , and the short arc between  $y_2$  and  $z_2$ ; and  $A_3$  denotes the rectangle surrounded by  $y_1y_2$ ,  $z_1z_2$ ,  $\ell$ , and the line through  $x_1$  and  $x_2$ . Intuitively,  $|A_1| = |A_2|$ . Then

$$v_r(x_1, x_2) - v_r(x_1) \geq |A_1| = |A_2| = f(t)/2 - |A_3|.$$

An upper bound on  $|A_3|$  can be obtained as follows. Let  $a$  be the intersection point between  $y_1y_2$  and  $\ell$ ,  $b$  be the intersection point between  $y_1y_2$  and  $\partial\Omega$ , and  $c$  be the intersection point between  $\ell$  and  $\partial\Omega$ . See Figure 2.3(c). Then  $\|ac\| \leq 2r$ , and

$$\|oa\| = \sqrt{\|oc\|^2 - \|ac\|^2} \geq \sqrt{\frac{1}{\pi} - (2r)^2}.$$

Hence,

$$\begin{aligned} \|ab\| &= \|ob\| - \|oa\| \\ &\leq \frac{1}{\pi} - \sqrt{\frac{1}{\pi} - (2r)^2} \\ &= \frac{4r^2}{\frac{1}{\pi} + \sqrt{\frac{1}{\pi} - (2r)^2}} \end{aligned}$$

Note that one side of  $A_3$  is exactly  $t$  and the other side is at most  $\|ab\|$ . Thus

$$|A_3| \leq \frac{4r^2}{\frac{1}{\pi} + \sqrt{\frac{1}{\pi} - (2r)^2}}$$

As  $f(t) \geq (\pi/2)rt$ , we have

$$\begin{aligned} v_r(x_1, x_2) - v_r(x_1) &\geq f(t)/2 - |A_3| \\ &= \left( \frac{\pi}{4} - \frac{4r}{\frac{1}{\pi} + \sqrt{\frac{1}{\pi} - (2r)^2}} \right) rt \end{aligned}$$

It is straightforward to verify that if

$$r \leq \frac{1/\sqrt{\pi}}{12/\pi + \pi/12} \approx 0.245/\sqrt{\pi},$$

then

$$\frac{\pi}{4} - \frac{4r}{\frac{1}{\pi} + \sqrt{\frac{1}{\pi} - (2r)^2}} \geq \frac{\pi}{12}$$

and thereby the lemma for  $k = 2$  follows.

In the next, we assume the lemma is true for at most  $k - 1$  nodes. We shall show that the lemma is true for  $k$  nodes. If  $k = 3$ , then

$$\begin{aligned} v_r(x_1, x_2, x_3) &\geq v_r(x_1) + v_r(x_3) \\ &\geq v_r(x_1) + \frac{\pi r^2}{3} \\ &= v_r(x_1) + \frac{\pi}{12} r \cdot 2 \cdot 2r \\ &\geq v_r(x_1) + \frac{\pi}{12} \sum_{i=1}^2 \|x_{i+1} - x_i\|. \end{aligned}$$

If  $k > 3$ , then by the induction hypothesis

$$\begin{aligned} v_r(x_1, \dots, x_k) &\geq v_r(x_1, \dots, x_{k-2}) + v_r(x_k) \\ &\geq v_r(x_1) + \frac{\pi}{12} \sum_{i=1}^{k-3} \|x_{i+1} - x_i\| + \frac{\pi}{12} r \cdot 4r \\ &\geq v_r(x_1) + \frac{\pi}{12} \sum_{i=1}^{k-1} \|x_{i+1} - x_i\| \end{aligned}$$

Therefore, the lemma is true by the induction. ■

**Corollary 3** *Assume that*

$$r \leq \frac{1/\sqrt{\pi}}{12/\pi + \pi/12} \approx 0.245/\sqrt{\pi}.$$

*Then for any  $(x_1, \dots, x_k) \in C_{k1}$  with  $x_1$  being the one of the largest norm among  $x_1, \dots, x_k$ ,*

$$v_r(x_1, \dots, x_k) \geq v_r(x_1) + \frac{\pi}{12} r \max_{2 \leq i \leq k} \|x_i - x_1\|.$$

**Proof.** Without loss of generality, we assume that  $\|x_k - x_1\|$  achieves  $\max_{2 \leq i \leq k} \|x_i - x_1\|$ . Let  $P$  be a path between  $x_1$  and  $x_k$  with minimum hop counts in  $G_{2r}(x_1, x_2, \dots, x_k)$  and  $t$  be the total length of  $P$ . Then every pair of nodes in  $P$  that does not establish a link (not adjacent) are separated by a distance of more than  $2r$ . Thus by applying Lemma 2 to the nodes in  $P$ , we obtain

$$v_r(\{x_i \mid x_i \in P\}) \geq v_r(x_1) + \frac{\pi}{12} r t.$$

Since  $v_r(x_1, \dots, x_k) \geq v_r(\{x_i \mid x_i \in P\})$  and  $t \geq \|x_k - x_1\|$ , we have

$$\begin{aligned} v_r(x_1, \dots, x_k) &\geq v_r(\{x_i \mid x_i \in P\}) \\ &\geq v_r(x_1) + \frac{\pi}{12} r \|x_k - x_1\| \\ &\geq v_r(x_1) + \frac{\pi}{12} r \max_{2 \leq i \leq k} \|x_i - x_1\|, \end{aligned}$$

and the corollary follows. ■

## 2.2 Limits of integrals

In the remaining of this chapter, we give the limits of several integrals which is useful for chapter 4. Similar lemmas can be found in [6].

**Lemma 4** For any  $z \in [0, \frac{1}{2}]$ ,

$$e^{-z-z^2} \leq 1 - z \leq e^{-z}.$$

**Proof.** For any  $z \geq 0$ ,  $1 - z \leq e^{-z} \leq 1 - z + \frac{z^2}{2}$ .

If  $z \in [0, \frac{1}{2}]$ , then

$$\begin{aligned} e^{z-z^2} &\leq \left(1 - z + \frac{z^2}{2}\right) \left(1 - z^2 + \frac{z^4}{2}\right) \\ &= 1 - z - z^2 \left(\frac{1}{2} - z\right) - \frac{1}{4}z^5(2 - z) \\ &\leq 1 - z, \end{aligned}$$

and the lemma follows. ■

**Lemma 5** If  $\lim_{n \rightarrow \infty} p \ln n = \infty$  and  $r = \sqrt{\frac{\ln n + \xi}{\pi p n}}$  for some constant  $\xi$ , then

$$\begin{aligned} n \int_{\Omega} e^{-npv_r(x)} dx &\sim e^{-\xi}, \\ n \int_{\Omega} (1 - pv_r(x))^{n-1} dx &\sim e^{-\xi}. \end{aligned}$$

**Proof.** By Lemma 4,  $e^{-pv_r(x) - (pv_r(x))^2} \leq 1 - pv_r(x) \leq e^{-pv_r(x)}$ . Then

$$e^{-npv_r(x) - n(pv_r(x))^2} \leq (1 - pv_r(x))^n \leq e^{-npv_r(x)}.$$

Therefore,

$$\begin{aligned} e^{-npv_r(x) - n(pv_r(x))^2} &= e^{-npv_r(x)} \cdot e^{-npv_r(x)^2} \\ &= e^{-npv_r(x)} \cdot e^{-\frac{c \ln^2 n}{n}} \\ &= e^{-npv_r(x)}. \end{aligned}$$

Note that  $npv_r(x) = c \ln n$ ,  $\frac{1}{3} \leq c \leq 1$ . Thus,

$$\begin{aligned} n(pv_r(x))^2 &= \frac{(npv_r(x))^2}{n} \\ &= \frac{c^2 \ln^2 n}{n} \sim 0. \end{aligned}$$

By the squeeze theorem, we have

$$n \int_{\Omega} (1 - pv_r(x))^{n-1} dx \sim n \int_{\Omega} e^{-npv_r(x)} dx,$$

and the second equality would follow from the first one. We only have to give the proof of the first asymptotic equality. First we calculate the integration over  $\Omega(0)$ .

$$\begin{aligned} n \int_{\Omega(0)} e^{-npv_r(x)} dx &\leq ne^{-np\pi r^2} |\Omega(0)| \\ &\sim ne^{-np\pi r^2} = e^{-\xi}. \end{aligned}$$

Next, we calculate the integration over  $\Omega(2)$ .

$$\begin{aligned} n \int_{\Omega(2)} e^{-npv_r(x)} dx &\leq ne^{-\frac{1}{3}np\pi r^2} |\Omega(2)| \\ &= n\pi r^2 e^{-\frac{1}{3}np\pi r^2} = o(1). \end{aligned}$$

Now we calculate the integration over  $\Omega(1)$ . By Lemma 1,

$$\begin{aligned}
n \int_{\Omega(1)} e^{-npv_r(x)} dx &\leq ne^{-\frac{np\pi r^2}{2}} n \int_{\Omega(1)} e^{-npr\left(\frac{1}{\sqrt{\pi}} - \|x\|\right)} dx \\
&= 2\pi ne^{-\frac{np\pi r^2}{2}} \int_{\frac{1}{\sqrt{\pi}} - r}^{\sqrt{\frac{1}{\pi} - r^2}} pe^{-npr\left(\frac{1}{\sqrt{\pi}} - \rho\right)} d\rho \\
&\leq 2\pi ne^{-\frac{np\pi r^2}{2}} \int_{\frac{1}{\sqrt{\pi}} - r}^{\frac{1}{\sqrt{\pi}}} pe^{-npr\left(\frac{1}{\sqrt{\pi}} - \rho\right)} d\rho \\
&\leq 2\sqrt{\pi} ne^{-\frac{np\pi r^2}{2}} \int_{\frac{1}{\sqrt{\pi}} - r}^{\frac{1}{\sqrt{\pi}}} e^{-npr\left(\frac{1}{\sqrt{\pi}} - \rho\right)} d\rho \\
&= 2\sqrt{\pi} ne^{-\frac{np\pi r^2}{2}} \int_0^r e^{-nprt} dt \\
&\leq \frac{2\sqrt{\pi}}{p} \frac{1}{r} e^{-\frac{np\pi r^2}{2}} \\
&= O(1) (\ln n)^{-\frac{1}{2}} = o(1).
\end{aligned}$$

Therefore,

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

■

**Lemma 6** *If  $\lim_{n \rightarrow \infty} p \ln n = \infty$  and  $r = \sqrt{\frac{\ln n + \xi}{\pi p n}}$  for some constant  $\xi$ , then for any fixed integer  $k \geq 2$ ,*

$$\begin{aligned}
n^k \int_{C_{k1}} e^{-npv_r(x_1, x_2, \dots, x_k)} \prod_{i=1}^k dx_i &= o(1), \\
n^k \int_{C_{k1}} (1 - pv_r(x_1, x_2, \dots, x_k))^{n-k} \prod_{i=1}^k dx_i &= o(1).
\end{aligned}$$

**Proof.** Since

$$(1 - pv_r(x_1, x_2, \dots, x_k))^{n-k} \leq \frac{e^{-npv_r(x_1, x_2, \dots, x_k)}}{(1 - pk\pi r^2)^k},$$

the second equality would follow from the first one. Hence, we only have to prove the first one. Let  $S$  denote the set of  $(x_1, x_2, \dots, x_k) \in C_{k1}$  satisfying that  $x_1$  is the one with largest norm among  $x_1, \dots, x_k$  and  $x_2$  is the one with longest distance from  $x_1$  among  $x_2, \dots, x_k$ .

Then

$$n^k \int_{C_{k1}} e^{-npv_r(x_1, x_2, \dots, x_k)} \prod_{i=1}^k dx_i \leq k(k-1) n^k \int_S e^{-npv_r(x_1, x_2, \dots, x_k)} \prod_{i=1}^k dx_i.$$

It suffices to prove

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

Note that for any  $(x_1, x_2, \dots, x_k) \in S$ ,

$$\begin{aligned} v_r(x_1) + cr \|x_2 - x_1\| &\leq v_r(x_1, x_2, \dots, x_k) \\ &\leq k\pi r^2 \end{aligned}$$

for some constant  $c$ , and

$$\begin{aligned} x_i &\in B(x_1, \|x_2 - x_1\|), 3 \leq i \leq k; \\ x_2 &\in B(x_1, 2(k-1)r). \end{aligned}$$

Thus,

$$\begin{aligned}
& n^k \int_S e^{-npv_r(x_1, x_2, \dots, x_k)} \prod_{i=1}^k dx_i \\
& \leq n^k \int_S e^{-np(v_r(x_1) + cr\|x_2 - x_1\|)} \prod_{i=1}^k dx_i \\
& \leq n^k \int_{\Omega} e^{-npv_r(x_1)} dx_1 \int_{B(x_1, 2(k-1)r)} e^{-npcr\|x_2 - x_1\|} dx_2 \prod_{i=3}^k \int_{B(x_1, \|x_2 - x_1\|)} dx_i \\
& = n^k \int_{\Omega} e^{-npv_r(x_1)} dx_1 \int_{B(x_1, 2(k-1)r)} e^{-npcr\|x_2 - x_1\|} (\pi \|x_2 - x_1\|^2)^{k-2} dx_2 \\
& = 2\pi^{k-1} \left( n^k \int_{\Omega} e^{-npv_r(x_1)} dx_1 \right) \left( n^{k-1} \int_0^{2(k-1)r} e^{-npcr\rho} \rho^{2k-3} d\rho \right) \\
& < 2\pi^{k-1} \left( n^k \int_{\Omega} e^{-npv_r(x_1)} dx_1 \right) \left( n^{k-1} \int_0^{\infty} e^{-npcr\rho} \rho^{2k-3} d\rho \right) \\
& = \frac{(2k-3)! 2\pi^{k-1} n^{k-1}}{(npcr)^{2k-2}} \left( n^k \int_{\Omega} e^{-npv_r(x_1)} dx_1 \right) \\
& = O(1) \frac{n^k \int_{\Omega} e^{-npv_r(x_1)} dx_1}{(\ln n)^{k-1}} = o(1),
\end{aligned}$$

where the last equality follows from Lemma 5. ■

**Lemma 7** *Let  $\lim_{n \rightarrow \infty} p \ln n = \infty$  and  $r = \sqrt{\frac{\ln n + \xi}{\pi p n}}$  for some constant  $\xi$ . Then for any fixed integers  $2 \leq m < k$ .*

$$\begin{aligned}
& n^k \int_{C_{km}} e^{-npv_r(x_1, x_2, \dots, x_k)} \prod_{i=1}^k dx_i = o(1), \\
& n^k \int_{C_{km}} (1 - pv_r(x_1, x_2, \dots, x_k))^{n-k} \prod_{i=1}^k dx_i = o(1).
\end{aligned}$$

**Proof.** Since

$$(1 - pv_r(x_1, x_2, \dots, x_k))^{n-k} \leq \frac{e^{-npv_r(x_1, x_2, \dots, x_k)}}{(1 - pk\pi r^2)^k},$$

the second equality would follow from the first one, and thus we only have to prove the first one. For any  $m$ -partition  $\Pi = \{K_1, K_2, \dots, K_m\}$  of  $\{1, 2, \dots, k\}$ , let  $\Omega^k(\Pi)$  denote the



set of  $(x_1, x_2, \dots, x_k) \in \Omega^k$  such that for any  $1 \leq j \leq m$ , the nodes  $\{x_i : i \in K_j\}$  form a connected component of  $G_{2r}(x_1, x_2, \dots, x_k)$ . Then  $C_{km}$  is the union of  $\Omega^k(\Pi)$  over all  $m$ -partitions  $\Pi$  of  $\{1, 2, \dots, k\}$ . So it is sufficient to show that for any  $m$ -partition  $\Pi$  of  $\{1, 2, \dots, k\}$ ,

$$n^k \int_{\Omega^k(\Pi)} e^{-npv_r(x_1, x_2, \dots, x_k)} \prod_{i=1}^k dx_i = o(1).$$

Now fix a  $m$ -partition  $\Pi = \{K_1, K_2, \dots, K_m\}$  of  $\{1, 2, \dots, k\}$ , and let  $l_j = |K_j|$  for  $1 \leq j \leq m$ . Then,

$$\Omega^k(\Pi) \subseteq \prod_{j=1}^m C_{l_j, 1},$$

and for any  $(x_1, x_2, \dots, x_k) \in \Omega^k(\Pi)$ ,

$$v_r(x_1, x_2, \dots, x_k) = \sum_{i=1}^m v_r(\{x_i \mid i \in K_j\}).$$

Thus,

$$\begin{aligned} & n^k \int_{\Omega^k(\Pi)} e^{-npv_r(x_1, x_2, \dots, x_k)} \prod_{i=1}^k dx_i \\ &= n^k \int_{\Omega^k(\Pi)} e^{-np \sum_{j=1}^m v_r(\{x_i \mid i \in K_j\})} \prod_{i=1}^k dx_i \\ &= n^k \int_{\Omega^k(\Pi)} \prod_{i=1}^m e^{-npv_r(\{x_i \mid i \in K_j\})} \prod_{i=1}^k dx_i \\ &\leq n^k \prod_{i=1}^m \int_{C_{l_j, 1}} e^{-npv_r(\{x_i \mid i \in K_j\})} \prod_{i \in K_j} dx_i \\ &= \prod_{i=1}^m \left( n^{l_j} \int_{C_{l_j, 1}} e^{-npv_r(\{x_i \mid i \in K_j\})} \prod_{i \in K_j} dx_i \right) \\ &= o(1), \end{aligned}$$

where the last equality follows from Lemma 6 and the fact that at least one  $l_j \geq 2$ . ■

**Lemma 8** Let  $\lim_{n \rightarrow \infty} p \ln n = \infty$  and  $r = \sqrt{\frac{\ln n + \xi}{\pi p n}}$  for some constant  $\xi$ . Then for any fixed integer  $k \geq 2$ ,

$$n^k \int_{C_{kk}} e^{-npv_r(x_1, x_2, \dots, x_k)} \prod_{i=1}^k dx_i \sim e^{-k\xi},$$

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

**Proof.** We again only give the proof of the first asymptotic equality and remark that the second one can be proved in the similar manner together with the inequalities in Lemma 4. For any  $(x_1, x_2, \dots, x_k) \in C_{kk}$ ,

$$v_r(x_1, x_2, \dots, x_k) = \sum_{i=1}^k v_r(x_i).$$

Thus,

$$\begin{aligned} & n^k \int_{C_{kk}} e^{-npv_r(x_1, x_2, \dots, x_k)} \prod_{i=1}^k dx_i \\ &= n^k \int_{C_{kk}} e^{-np \sum_{i=1}^k v_r(x_i)} \prod_{i=1}^k dx_i \\ &= n^k \int_{\Omega^k} e^{-np \sum_{i=1}^k v_r(x_i)} \prod_{i=1}^k dx_i - n^k \int_{\Omega^k \setminus C_{kk}} e^{-np \sum_{i=1}^k v_r(x_i)} \prod_{i=1}^k dx_i. \end{aligned}$$

We show the first term is asymptotically equal to  $e^{-k\xi}$ , and the second term is asymptotically negligible. Indeed,

$$\begin{aligned} n^k \int_{\Omega^k} e^{-np \sum_{i=1}^k v_r(x_i)} \prod_{i=1}^k dx_i &= n^k \int_{\Omega^k} \prod_{i=1}^k e^{-npv_r(x_i)} \prod_{i=1}^k dx_i \\ &= \prod_{i=1}^k \left( n^k \int_{\Omega} e^{-npv_r(x_i)} dx_i \right) \sim e^{-k\xi}, \end{aligned}$$

where the last equality follows from Lemma 5. Note that for any  $(x_1, x_2, \dots, x_k) \in \Omega^k \setminus C_{kk}$ ,

$$v_r(x_1, x_2, \dots, x_k) \leq \sum_{i=1}^k v_r(x_i).$$

Thus,

$$\begin{aligned} n^k \int_{\Omega^k \setminus C_{kk}} e^{-np \sum_{i=1}^k v_r(x_i)} \prod_{i=1}^k dx_i &\leq n^k \int_{\Omega^k \setminus C_{kk}} e^{-np v_r(x_1, x_2, \dots, x_k)} \prod_{i=1}^k dx_i \\ &= \sum_{m=1}^{k-1} n^k \int_{C_{km}} e^{-np v_r(x_1, x_2, \dots, x_k)} \prod_{i=1}^k dx_i \\ &= o(1), \end{aligned}$$

where the last equality follows from Lemma 6 and 7. ■



# Chapter 3

## Main Results

### 3.1 Wireless Ad Hoc Networks with Bernoulli Model

In 802.11 wireless networks, two basic service sets (BSS) are defined: infrastructure BSS and independent BSS. In infrastructure BSS, access points (AP's) which are similar to the base stations in mobile networks are connected to the Internet directly. AP accounts for all the communications in the network. To gain the ability to access the network, devices with a wireless card can only connect to the access point. In independent BSS, devices in ad hoc mode only do one-hop transmission with another device, and multi-hop communication is not allowed. An instance is the most common wireless networks with 802.11b [15] and 802.11g [16] protocols nowadays.

As we mentioned in chapter 1, wireless ad hoc networks show another concept. A wireless ad hoc network is composed of a collection of mobile devices with wireless communication ability, such as laptops, PDAs, and smartphones. Devices in wireless ad hoc networks have the responsibility to relay packets for others, and multi-hop communica-

tion can be achieved. There are several characteristics:

- **Mobility:** Every devices in the network may move at anytime in any direction independently without breaking down the network. The capability to tolerate mobility is necessary for a wireless ad hoc network.
- **Self-organization:** No fixed infrastructure is needed in a wireless ad hoc network. The devices in the network can automatically forms a network topology by either distributed or centralized schemes.
- **Scalability:** Some applications of ad hoc networks require large amount of devices, e.g. pollution monitoring in industrial estates and adversary investigation on battlefields. Besides, devices with mobility will join and leave the network dynamically and frequently. Scalibility is an essential consideration.
- **Security:** Wireless communications via radio are easily eavesdropped if links are not protected by security schemes. In addition, wireless ad hoc networks can also be jammed or spoofed by packet replicas. Security is an important issue of wireless ad hoc networks.

To simplify the analysis of probability distribution in the following chapter, we make some assumptions first. The wireless ad hoc network is represented by an uniform point process or Poission point process with mean  $n$  over an unit-area region  $\Omega$ . All nodes in the network are homogeneous, and are associated with a maximum transmission radius  $r$  which is a function of  $n$ . Two nodes may have a link if the distance between them is at most  $r$ . The approach used in this study is based on the method used in [6].

We study the connectivity of a wireless network with both unreliable nodes and links by investigating the number of isolated nodes. To model unreliable nodes and links in ad hoc networks, we introduce the Bernoulli model: assume nodes are active independently with the same probability  $p_1$  and inactive with probability  $1 - p_1$  for  $0 < p_1 \leq 1$ ; and links are up independently with the same probability  $p_2$  and down with probability  $1 - p_2$  for  $0 < p_2 \leq 1$ . Here  $p_1$  and  $p_2$  can be constants or functions of  $n$ . Depending on the meaning of the "inactive" nodes, there 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 adjacent to at least one active node. In both cases, a node is said to be *isolated*, if it doesn't have up links with active nodes. We shall prove that the number of isolated nodes is with asymptotic Poisson distributions.

We have the following theorem about the total number of isolated (active) nodes in wireless ad hoc networks. It will be proved in chapter 4.

**Theorem 9** *Suppose that  $\lim_{n \rightarrow \infty} p_1 p_2 \ln n = \infty$  and nodes have the same maximum transmission radius  $r = \sqrt{\frac{\ln n + \xi}{n p_1 p_2 \pi}}$  for some constant  $\xi$ . 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  $p_1 e^{-\xi}$ .*

So we are able to estimate the transmission radius of nodes in a wireless ad hoc network for good connectivity. For instance, assume the deployment region of nodes is known in a pollution monitoring application. By proper scaling, we can estimate the number of nodes to be deployed according to the maximum transmission radius of nodes.

## 3.2 Key Predistribution Scheme

The study can be extended for secure wireless networks which adopt the  $m$ -composite key predistribution schemes. The  $m$ -composite key predistribution scheme is a key-management scheme for wireless sensor networks composed of large number of microsensors. Different from mobile devices like laptops and handheld devices, microsensors only have limited power resource (usually batteries), memory storage, computation power, and transmission bandwidth. With such strict hardware limitations, a security scheme shall be less complicated on encryption/decryption computation, but still be strong enough against attacks.

In the  $m$ -composite key predistribution schemes [19] [21], a 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 deployed, each node randomly loads  $k$  distinct keys drawn from the key pool, which is called a key ring, into its memory. After deployed, 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 task.

Whether a security scheme is qualified or not can be judged by certain criteria:

- Resilience against node capture: After deployment, we assume the adversary can reach and capture microsensors easily. The adversary may decompose the hardware and steal the secret informations from the memory storage. We say the resilience is great if the leaked information from one sensor does not compromise the other secure links.

- Revocation: When a node is detected to be captured or falsified by the adversary, the node should be revoked rapidly. The keys and other secret data are removed dynamically from the network.
- Scalability: There are often a large number of sensors in the network. To adapt to this characteristic, the security scheme must be scalable, too.

Due to the  $m$ -composite key predistribution scheme, every nodes have the capability for self-revocation without network-wide broadcast messages. Revocation of the keys is simple and fast for each captured node due to the small size of the key ring. The scalability is also great. Both the key pre-distribution and shared-key discovery are simple.

To strengthen the resilience, Du, Deng, Han, and Varshney proposed the multiple-space key predistribution scheme [23] using multiple key spaces. We first constructed  $\omega$  key spaces using Blom's scheme [24], and each node randomly selects  $\tau$  ( $2 \leq \tau < \omega$ ) spaces. If two nodes select a common key space, they can compute their pairwise secret key. These two nodes within each other's transmission range can establish a secure link via the pairwise key. In the analysis of the global connectivity of secure networks, we found the similarity between the  $m$ -composite key predistribution scheme and the multiple-space key predistribution scheme. The  $\omega$  key spaces in the multiple-space key predistribution scheme can be treated as the key pool size  $K$  in the  $m$ -composite key predistribution scheme, and the  $\tau$  key spaces in the multiple-space key predistribution scheme can be treated as the key ring size  $k$  in the  $m$ -composite key predistribution scheme.

Similarly, we shall prove that the number of isolated nodes in the secure wireless network have asymptotic Poisson distributions. Hence, the secure wireless network is the



graph in which two nodes have an edge if their distance is at most  $r$  and they have at least  $m$  common keys in their key rings. A node is said to be isolated, if it doesn't 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,

$$\begin{aligned} q &= q_0 + q_1 + \cdots + q_{m-1} \\ p &= 1 - q \end{aligned} \tag{3.1}$$

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

**Theorem 10** *In  $m$ -composite key predistribution schemes, let  $p$  be given by Eq. (3.1). If  $\lim_{n \rightarrow \infty} p \ln n = \infty$  and nodes have the same maximum transmission radius  $r = \sqrt{\frac{\ln n + \xi}{\pi p n}}$  for some constant  $\xi$ , then the total number of isolated nodes is asymptotically Poisson with mean  $e^{-\xi}$ .*

## Chapter 4

# Asymptotic Distribution of The Number of Isolated Nodes

Theorem 9 and 10 will be proved by using *Brun's sieve* in the form described, for example, in [22], chapter 8, which is an implication of the Bonferroni inequalities.

**Theorem 11** *Let  $B_1, \dots, B_n$  be events and  $Y$  be the number of  $B_i$  that hold. Suppose that for any set  $\{i_1, \dots, i_k\} \subseteq \{1, \dots, n\}$*

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

*and there is a constant  $\mu$  so that for any fixed  $k$*

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

*Then  $Y$  is also asymptotically Poisson with mean  $\mu$ .*

## 4.1 Networks with Bernoulli Nodes and Links

In the Bernoulli model, for applying Theorem 11, 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  $B'_i$  that hold. Then  $Y'$  is exactly the number of isolated active nodes. Obviously, for any set  $\{i_1, \dots, i_k\} \subseteq \{1, \dots, n\}$ ,

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

$$\Pr(B'_{i_1} \wedge \dots \wedge B'_{i_k}) = \Pr(B'_1 \wedge \dots \wedge B'_k).$$

In addition,

$$\Pr(B'_1 \wedge \dots \wedge B'_k) = (p_1)^k \Pr(B_1 \wedge \dots \wedge B_k).$$

Thus, in order to prove Theorem 9, it suffices to show that if  $r = \sqrt{\frac{\ln n + \xi}{\pi p_1 p_2 n}}$  for some constant  $\xi$ , then for any fixed  $k$ ,

$$n^k \Pr(B_1 \wedge \dots \wedge B_k) \sim e^{-k\xi}. \quad (4.1)$$

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 12** *For any  $x \in \Omega$ ,*

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

**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  $X_2, \dots, X_n$  within  $v_r(X_1)$  respectively. There are exactly  $N_1$

links between  $X_1$  and those  $N_1$  active nodes. If  $X_1$  are isolated, all of those  $N_1$  links must be down. So

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

and

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

Thus

$$\begin{aligned} & \Pr(B_1 \mid X_1 = x) \\ &= \sum_{i+j=0}^{n-1} \frac{\Pr(B_1 \mid N_1 = i, N_2 = j)}{\Pr(N_1 = i, N_2 = j \mid X_1 = x)} \\ &= \sum_{i+j=0}^{n-1} \frac{(q_2)^i \binom{n-1}{i, j} (1 - v_r(x))^{n-1-i-j}}{(p_1 v_r(x))^i (q_1 v_r(x))^j} \\ &= (1 - p_1 p_2 v_r(x))^{n-1}. \end{aligned}$$

Therefore, the lemma is proved. ■

**Lemma 13** For any  $k \geq 2$  and  $(x_1, \dots, x_k) \in \Omega^k$ ,

$$\begin{aligned} & \Pr(B_1 \wedge \dots \wedge B_k \mid X_i = x_i, 1 \leq i \leq k) \\ & \leq (1 - p_1 p_2 v_r(x_1, \dots, x_k))^{n-k}. \end{aligned}$$

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

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

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

Thus,

$$\begin{aligned} & \Pr(B_1 \wedge \dots \wedge B_k | X_i = x_i, 1 \leq i \leq k) \\ &= \sum_{i+j=0}^{n-k} \Pr(B_1 \wedge \dots \wedge B_k | N_1 = i, N_2 = j) \cdot \\ & \quad \Pr(N_1 = i, N_2 = j | X_i = x_i \text{ for } 1 \leq i \leq k) \\ &\leq \sum_{i+j=0}^{n-k} (q_2)^i \binom{n-k}{i,j} (1 - v_r(x_1, \dots, x_k))^{n-k-i-j} \cdot \\ & \quad (p_1 v_r(x_1, \dots, x_k))^i (q_1 v_r(x_1, \dots, x_k))^j \\ &= (1 - p_1 p_2 v_r(x_1, \dots, x_k))^{n-k}. \end{aligned}$$

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

$$\begin{aligned}
& \Pr(B_1 \wedge \dots \wedge B_k \mid X_i = x_i, 1 \leq i \leq k) \\
&= \Pr \left( \begin{array}{l} \forall 1 \leq i \leq k, X_i \text{ has no up links} \\ \text{to active nodes of } X_{k+1}, \dots, X_n \end{array} \right) \\
&= \sum_{\substack{m_1 + \dots + m_k = 0 \\ m'_1 + \dots + m'_k = 0}}^{n-k} \Pr \left( \begin{array}{l} \forall 1 \leq i \leq k, v_r(x_i) \text{ contains} \\ m_i \text{ active nodes, } m'_i \text{ inactive} \\ \text{nodes, and links of } X_i \text{ to} \\ \text{active nodes are down} \end{array} \right) \\
&= \sum_{\substack{m_1 + \dots + m_k + \\ m'_1 + \dots + m'_k = 0}}^{n-k} \binom{n-k}{m_1, \dots, m_k, m'_1, \dots, m'_k} \\
&\quad \cdot \left( \prod_{i=1}^k (q_2 p_1 v_r(x_i))^{m_i} \right) \left( \prod_{i=1}^k (q_1 v_r(x_i))^{m'_i} \right) \\
&\quad \cdot (1 - v_r(x_1, \dots, x_k))^{n-k - \sum_{i=1}^k (m_i + m'_i)} \\
&= (1 - p_1 p_2 v_r(x_1, \dots, x_k))^{n-k}.
\end{aligned}$$

Therefore, the lemma is proved.  $\blacksquare$

Now we are ready to prove the asymptotic equality (4.1). From Lemma 12 and Lemma 5,

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

So the asymptotic equality (4.1) is true for  $k = 1$ . Now we fix  $k \geq 2$ . From Lemma 13, Lemma 6 and Lemma 7,

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

>From Lemma 13 and Lemma 8,

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

Thus, the asymptotic equality (4.1) is also true for any fixed  $k \geq 2$ . This completes the proof of Theorem 9.

## 4.2 Secure Wireless Networks

In secure wireless networks, for applying Theorem 11, 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. Obviously, for any set  $\{i_1, \cdots, i_k\} \subseteq \{1, \cdots, n\}$ ,

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

Thus, in order to prove Theorem 10, it suffices to show that if  $r = \sqrt{\frac{\ln n + \xi}{\pi p n}}$  for some constant  $\xi$ , then for any fixed  $k$ ,

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

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 14** For any  $x \in \Omega$ ,

$$\Pr(B_1 | X_1 = x) = (1 - pv_r(x))^{n-1}.$$

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

$$\begin{aligned} \Pr(B_1 | X_1 = x) &= \sum_{i=0}^{n-1} \Pr(X_1 \text{ is isolated} | N = i) \Pr(N = i | X_1 = x) \\ &= \sum_{i=0}^{n-1} q^i \binom{n-1}{i} (1 - v_r(x))^{n-1-i} v_r(x)^i \\ &= (1 - v_r(x) + qv_r(x))^{n-1} = (1 - pv_r(x))^{n-1}. \end{aligned}$$

Therefore, the lemma is proved. ■

**Lemma 15** For any  $k \geq 2$  and  $(x_1, \dots, x_k) \in \Omega^k$ ,

$$\begin{aligned} \Pr(B_1 \wedge \dots \wedge B_k | X_i = x_i, 1 \leq i \leq k) \\ \leq (1 - pv_r(x_1, \dots, x_k))^{n-k}. \end{aligned}$$

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

**Proof.** For any  $(x_1, \dots, x_k) \in \Omega^k$ , let  $N$  denote the number of nodes of  $X_{k+1}, \dots, X_n$  within  $v_r(X_1, \dots, X_k)$ . Each of those  $N$  nodes is neighbor to at least one of  $X_1, \dots, X_k$ ,



but the link is not secured. Therefore, we have  $\Pr(B_1 \wedge \cdots \wedge B_k \mid N = i) \leq q^i$ . Thus,

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

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

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

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 12 and 13 by Lemma 14 and 15. Thus, we complete the proof of Theorem 10.

# Chapter 5

## Simulations and Conclusions

In chapter 1, we already introduced several different models of connectivity of wireless ad hoc networks. In the general case, the vanishment of isolated nodes in wireless ad hoc networks is a necessary but not sufficient condition for network connectivity. That is to say, the critical transmission radius (CTR) for connectivity is at least as large as the critical transmission radius for without isolated nodes. In this chapter, the difference between the two CTR's and our theoretical CTR will be investigated by running extensive simulations. To verify the correctness of the theory, first we will give the simulation result of the native model, and then the results of the other models.

### 5.1 Simulation Setup and Notations

In the simulation, the locations of wireless ad hoc devices are generated by a uniform point process over an unit-area region with node density  $n = 100$ ,  $n = 400$ , and  $n = 1600$ . Both unit-area disk and square will be considered. 800 sets of random points are generated

for each network scenario. Each scenario will simulate for 800 times with different sets of random points generated independently. To maintain the consistency of our notations, we assume each node has probability  $p_1$  to be active independently, and each link has probability  $p_2$  to be up independently.

In the network with unreliable nodes, each node has probability  $p_1$  to be active and probability  $1 - p_1$  to be inactive independently. The inactive nodes break down and are out of function. So there is no need to put them in consideration of network connectivity. In addition, we consider another meaning of inactive nodes. Each node has two states: (1) nodes in waking state can do jobs but consumes more power, (2) nodes in sleeping state only listen to the channels and save energy.

For convenience, let  $R_{iso}$  be the CTR for without isolated nodes,  $R_{con}$  be the CTR for connectivity, and  $R_{th}$  be the theoretical CTR. The cumulative distribution functions (c.d.f.) of critical transmission radii will be illustrated. In these figures, including Figure 5.2, Figure 5.4, Figure 5.5, Figure 5.7, Figure 5.9, Figure 5.10, and Figure 5.12,  $x$ -axis presents the transmission radius, and  $y$ -axis presents the probability. In each figure, there are three sets of curves, from right to left, for  $n = 100$ ,  $n = 400$ , and  $n = 1600$ , respectively. In each set, the green curve is the c.d.f. of  $R_{th}$ , the black one is of  $R_{iso}$ , and the red one is of  $R_{con}$ .

To compare the difference between asymptotic theoretical value and simulation outcomes, we calculate the inaccuracy by the following formulas:

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

To show clear view of our results, we will list the average CTR's and the inaccuracies of

$DR_{iso}$ ,  $DR_{iso}$  in tables.

## 5.2 Native Models

For the sake of comparison, we first consider the network model in which neither node failure nor link failure occurs. This is exactly a special case of  $p_1 = 1$  and  $p_2 = 1$ . Actually, this is the most case discussed in literature. Figure 5.1 is two  $r$ -disk graphs over the same 200 random nodes but with different value of  $r$ 's deployed in an unit-area disk. Black

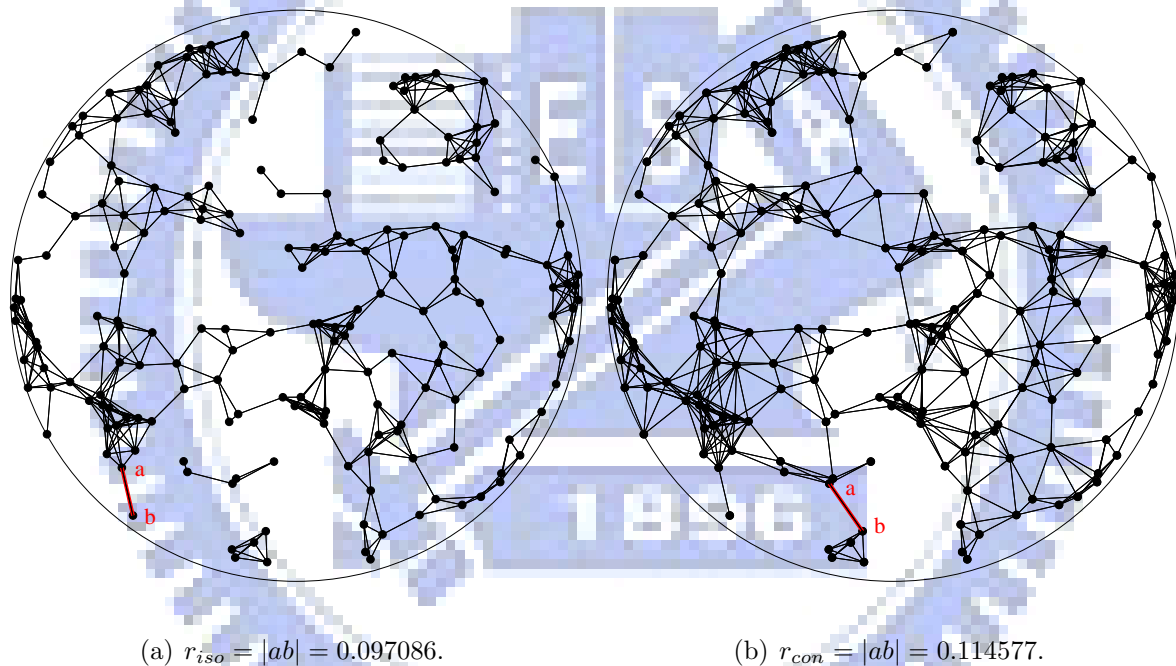


Figure 5.1: The  $r$ -disk graph over an unit-area disk.

nodes represent devices in the network, and solid lines are communication links between two devices. Figure 5.1(a) is the network without isolated nodes, and  $ab$  is the longest edge and with length 0.097086 that is corresponding to the CTR for without isolated nodes, and the  $r$ -disk graph is plotted with  $r = \|a - b\|$ . Figure 5.1(b) is the network with connectivity, and  $ab$  is the longest edge and with length 0.114577 that is corresponding

to the CTR for connectivity, and the  $r$ -disk graph is plotted with  $r = \|a - b\|$ . In this instance, obviously two CTR's are different. Figure 5.2 illustrates the c.d.f. of the CTR of this model. In Table 5.1, the average CTR and inaccuracies are listed. The inaccuracy

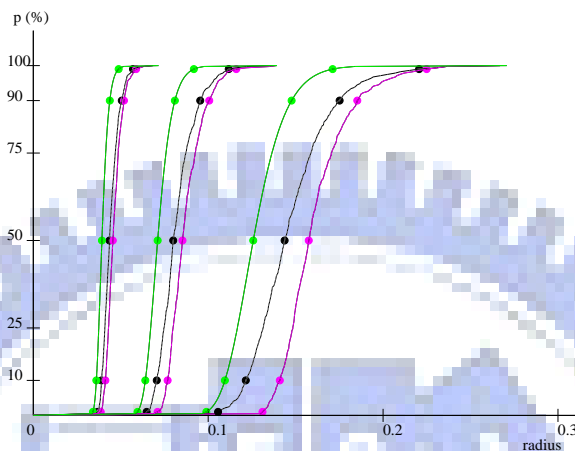


Figure 5.2: The c.d.f. of CTR's of  $r$ -disk graphs over an unit-area disk.

$DR_{iso}$  drops from 15.08% to 11.63%, and  $DR_{con}$  drops from 26.27% to 16.32%. We can see that three CTR's converge as the network size increases.

Table 5.1: The average CTR's corresponding to Figure 5.2.

$n$	$R_{iso}$	$R_{con}$	$R_{th}$	$DR_{iso}$	$DR_{con}$
100	0.1469	0.1612	0.1277	15.08%	26.27%
400	0.0821	0.0872	0.0721	13.95%	21.07%
1600	0.0443	0.0462	0.0340	11.63%	16.32%

### 5.3 Networks with Bernoulli Nodes

Next, we consider the network with unreliable nodes but with reliable links, i.e.  $0 \leq p_1 < 1$  and  $p_2 = 1$ . This is the same model discussed in [6] and [14] in which nodes may break down with probability  $1 - p_1$  independently after deployed. Figure 5.3 is two networks over the same 200 random nodes but with different value of  $r$ 's deployed in an unit-area disk. Similar to the  $r$ -disk graphs in Figure 5.1, black nodes represent active

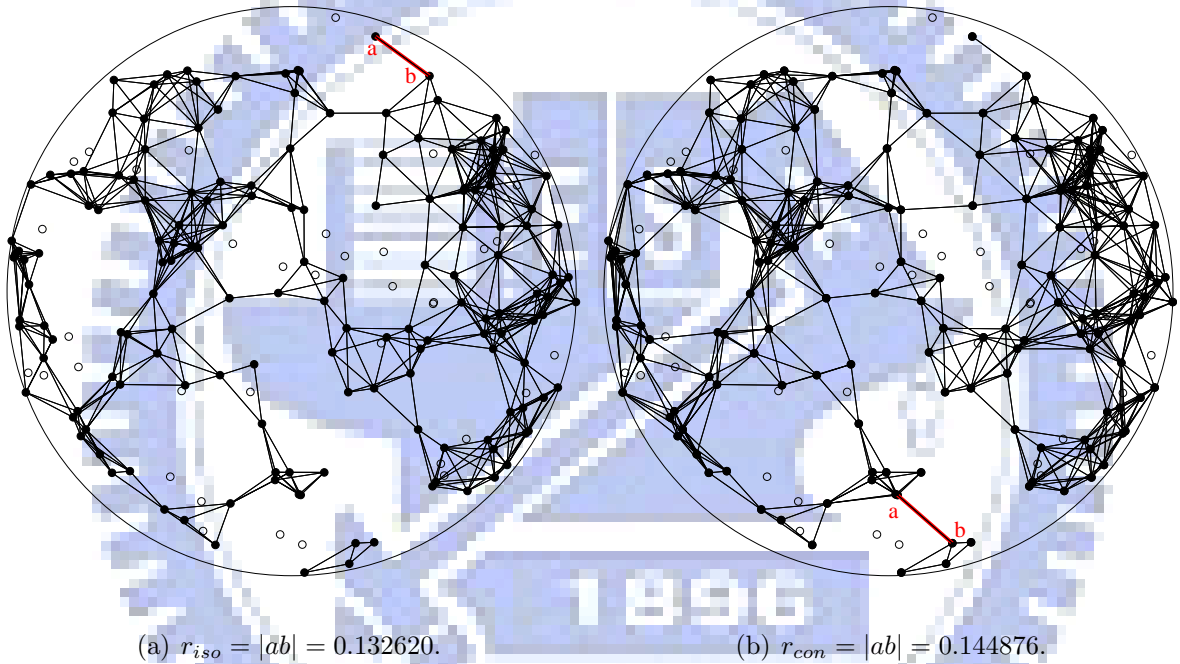
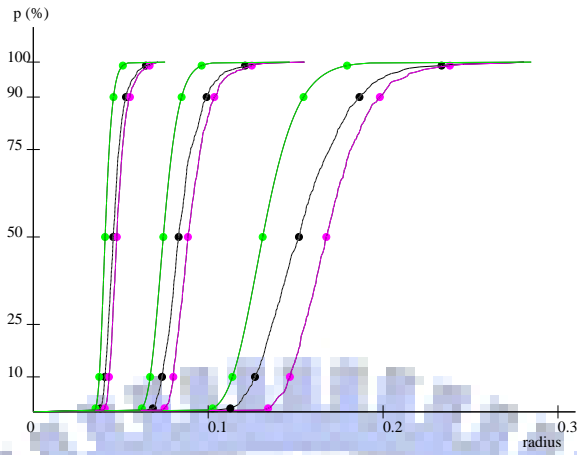
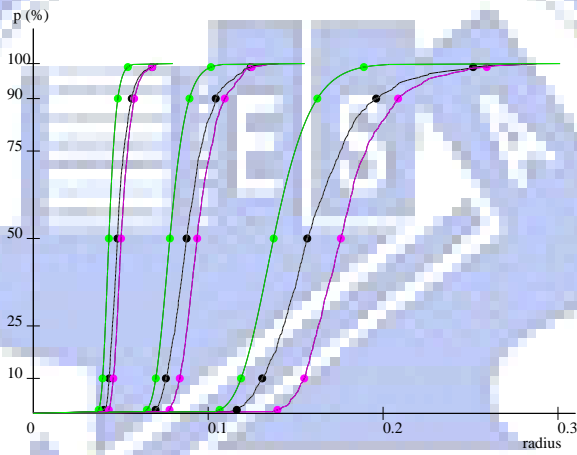


Figure 5.3: The  $r$ -disk graph over an unit-area disk with unreliable nodes.

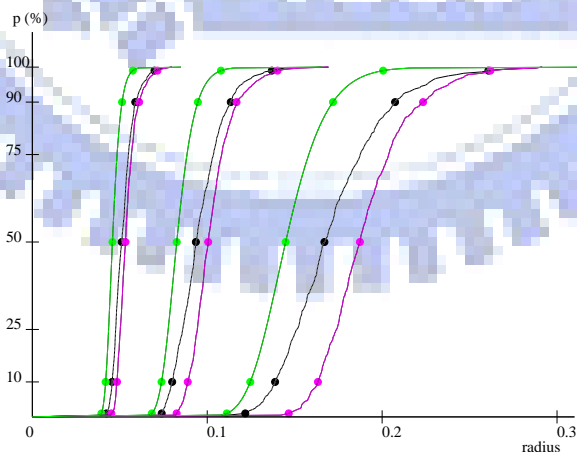
nodes, and solid lines are links between two nodes. Moreover, the white nodes represent the broken nodes. Figure 5.3(a) is the network without isolated nodes, and  $ab$  is the CTR for without isolated nodes and with length 0.132620. Figure 5.3(b) is the network with connectivity, and  $ab$  is the CTR for connectivity and with length 0.144876. Figure 5.4 illustrates the c.d.f. corresponding to  $p_1 = 0.9$ ,  $p_1 = 0.8$ , and  $p_1 = 0.7$ , respectively. The average CTRs and inaccuracies of  $R_{iso}$ ,  $R_{con}$ , and  $R_{th}$  are listed in Table 5.2.



(a)  $p_1 = 0.9$  and  $p_2 = 1$ .



(b)  $p_1 = 0.8$  and  $p_2 = 1$ .



(c)  $p_1 = 0.7$  and  $p_2 = 1$ .

Figure 5.4: The c.d.f. of CTR's over an unit-area disk with unreliable nodes.

Table 5.2: The average CTR's corresponding to Figure 5.4.

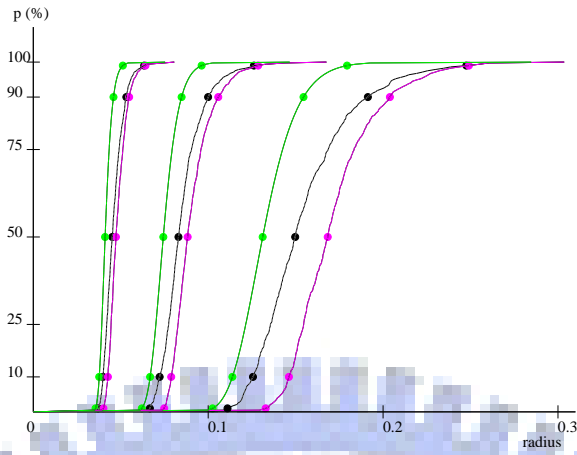
Figure 5.4(a): $p_1 = 0.9, p_2 = 1$					
$n$	$R_{iso}$	$R_{con}$	$R_{th}$	$DR_{iso}$	$DR_{con}$
100	0.1548	0.1706	0.1332	16.22%	28.12%
400	0.0853	0.0907	0.0753	13.23%	20.41%
1600	0.0466	0.0487	0.0416	12.13%	17.26%
Figure 5.4(b): $p_1 = 0.8, p_2 = 1$					
$n$	$R_{iso}$	$R_{con}$	$R_{th}$	$DR_{iso}$	$DR_{con}$
100	0.1617	0.1795	0.1396	15.87%	28.60%
400	0.0895	0.0955	0.0792	13.04%	20.69%
1600	0.0492	0.0513	0.0437	12.35%	17.22%
Figure 5.4(c): $p_1 = 0.7, p_2 = 1$					
$n$	$R_{iso}$	$R_{con}$	$R_{th}$	$DR_{iso}$	$DR_{con}$
100	0.1714	0.1905	0.1471	16.50%	29.47%
400	0.0957	0.1025	0.0837	14.33%	22.41%
1600	0.0519	0.0542	0.0464	12.04%	16.78%



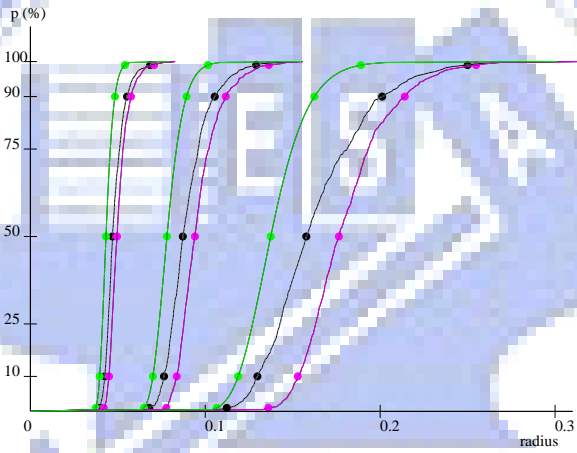
Besides generating points over an unit-area disk, we also run similar simulations over an unit-area square. The c.d.f. corresponding to  $p_1 = 0.9$ ,  $p_1 = 0.8$ , and  $p_1 = 0.7$  are illustrated by Figure 5.5. The average CTR's and inaccuracies of  $R_{iso}$ ,  $R_{con}$ , and  $R_{th}$  are listed in Table 5.3. Basically, the results are similar to results of random point sets over an unit-area disk, and our theory still keeps the accuracy.

Table 5.3: The average CTR's corresponding to Figure 5.5.

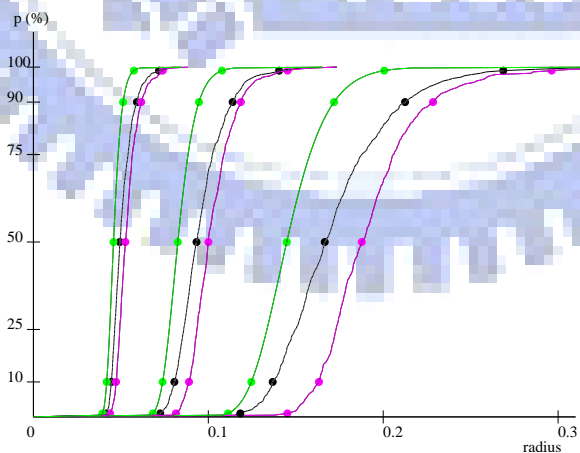
Figure 5.5(a): $p_1 = 0.9, p_2 = 1$					
$n$	$R_{iso}$	$R_{con}$	$R_{th}$	$DR_{iso}$	$DR_{con}$
100	0.1549	0.1720	0.1332	16.29%	29.15%
400	0.0853	0.0908	0.0753	13.20%	20.58%
1600	0.0461	0.0483	0.0416	10.82%	16.20%
Figure 5.5(b): $p_1 = 0.8, p_2 = 1$					
$n$	$R_{iso}$	$R_{con}$	$R_{th}$	$DR_{iso}$	$DR_{con}$
100	0.1631	0.1805	0.1396	16.88%	29.30%
400	0.0897	0.0962	0.0792	13.27%	21.56%
1600	0.0483	0.0506	0.0437	10.34%	15.62%
Figure 5.5(c): $p_1 = 0.7, p_2 = 1$					
$n$	$R_{iso}$	$R_{con}$	$R_{th}$	$DR_{iso}$	$DR_{con}$
100	0.1721	0.1928	0.1471	16.96%	31.06%
400	0.0957	0.1025	0.0837	14.30%	22.48%
1600	0.0509	0.0538	0.0464	09.80%	16.10%



(a)  $p_1 = 0.9$  and  $p_2 = 1$ .



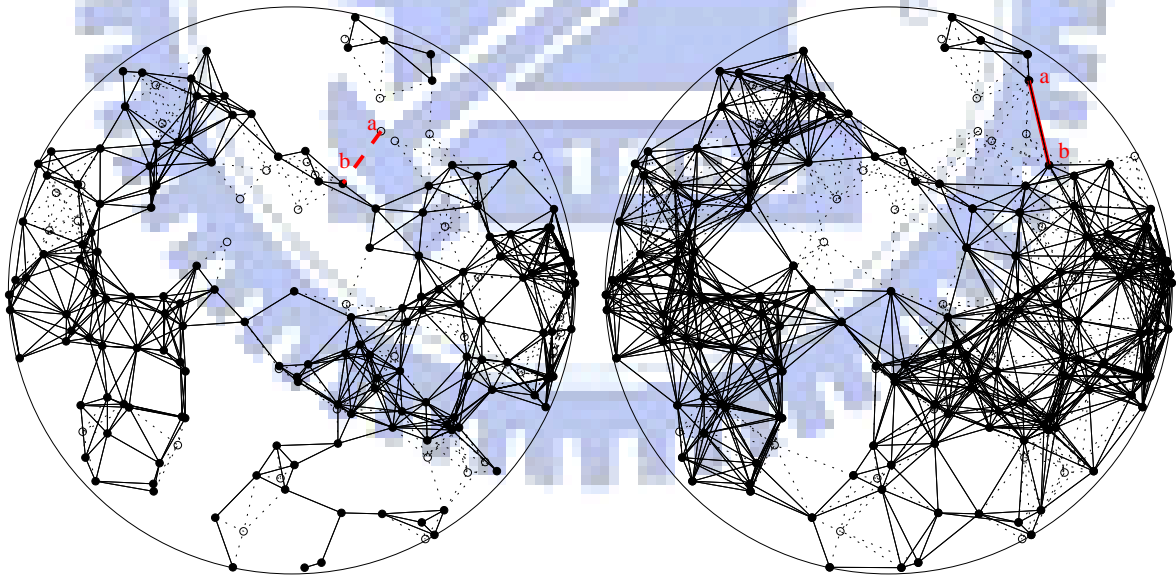
(b)  $p_1 = 0.8$  and  $p_2 = 1$ .



(c)  $p_1 = 0.7$  and  $p_2 = 1$ .

Figure 5.5: The c.d.f. of CTR's over an unit-area square with unreliable nodes.

In addition, we consider another scenario. Each node has probability  $p_1$  to stay in waking state, and may switch to sleeping state independently with probability  $1 - p_1$ . Nodes only do jobs in waking state, such as sending/receiving data, or being a member of the virtual backbone and relaying packet for other nodes. When in sleeping state, they do nothing but monitor a particular broadcasting channel, e.g. beacons in ZigBee networks [2]. Moreover, nodes in sleeping state need to have at least one waking neighbor to prevent from being isolated in the networks. For such networks, a node is isolated if it doesn't have waking neighbors, and a network is connected if every nodes have at least one waking neighbors. Figure 5.6 shows two networks over the same 200 random nodes with different value of  $r$ 's deployed in an unit-area disk. Black nodes represent nodes in waking state, and white nodes represent nodes in sleeping state. Dotted lines are the listening links of white nodes to black nodes.



(a)  $r_{iso} = |ab| = 0.129692$ .

(b)  $r_{con} = |ab| = 0.172918$ .

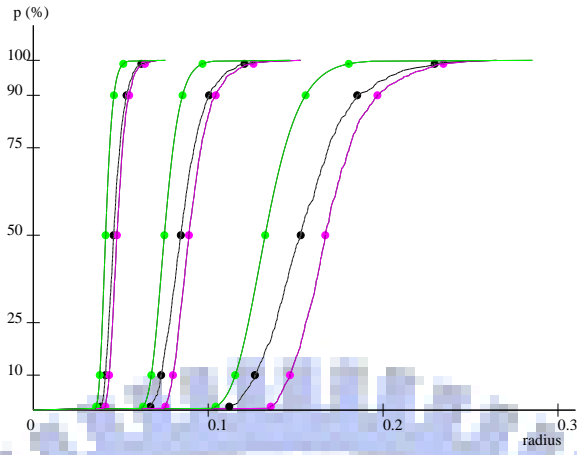
Figure 5.6: The  $r$ -disk graph with waking/sleeping nodes and listening links.

Figure 5.6(a) is the network without isolated nodes, and  $ab$  is the longest edge and with length 0.129692 that is corresponding to the CTR for without isolated nodes, and the  $r$ -disk graph is plotted with  $r = \|a - b\|$ . Figure 5.6(b) is the network with connectivity, and  $ab$  is the longest edge and with length 0.172918 that is corresponding to the CTR for connectivity, and the  $r$ -disk graph is plotted with  $r = \|a - b\|$ . Note that the CTR can be contributed by a dotted line. The c.d.f. corresponding to  $p_1 = 0.9$ ,  $p_1 = 0.8$  and  $p_1 = 0.7$  are illustrated by Figure 5.7.

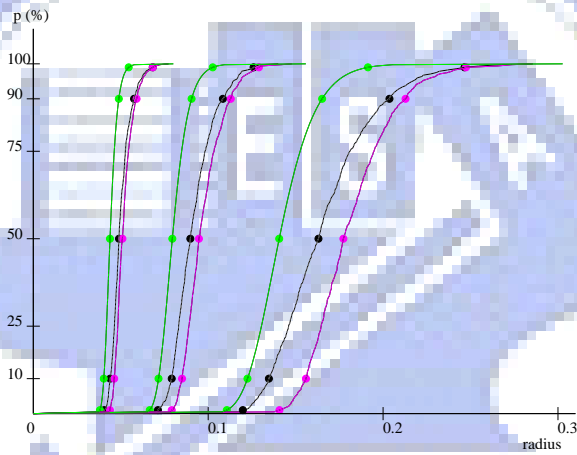
The average CTR's and inaccuracies of  $R_{iso}$ ,  $R_{con}$ , and  $R_{th}$  are listed in Table 5.4. The results are similar to those of the former scenario.

## 5.4 Networks with Bernoulli Nodes and Links

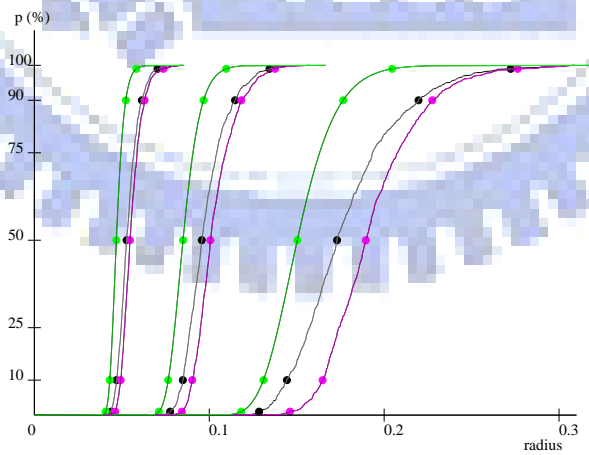
In the real world, wireless signals may be blocked or reflected by geographic barriers and buildings, and interfered by other signals. Thus, communication links is not available everytime. So, besides unreliable nodes, we consider networks with unreliable links. Assume nodes may break down independently with probability  $1 - p_1$ , and links may be down independently with probability  $1 - p_2$ . Figure 5.8 shows the instance of two networks over the same 200 nodes but with different value of  $r$ 's deployed in an 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. Edges denoted by solid lines between black nodes are up links, and edges denoted by dash lines are down links. Figure 5.8(a) is the network without isolated nodes, and  $ab$  is the longest edge and with length 0.097235 that is corresponding to the CTR such that every black nodes have at least one solid edge, and the graph is plotted



(a)  $p_1 = 0.9$  and  $p_2 = 1$ .



(b)  $p_1 = 0.8$  and  $p_2 = 1$ .

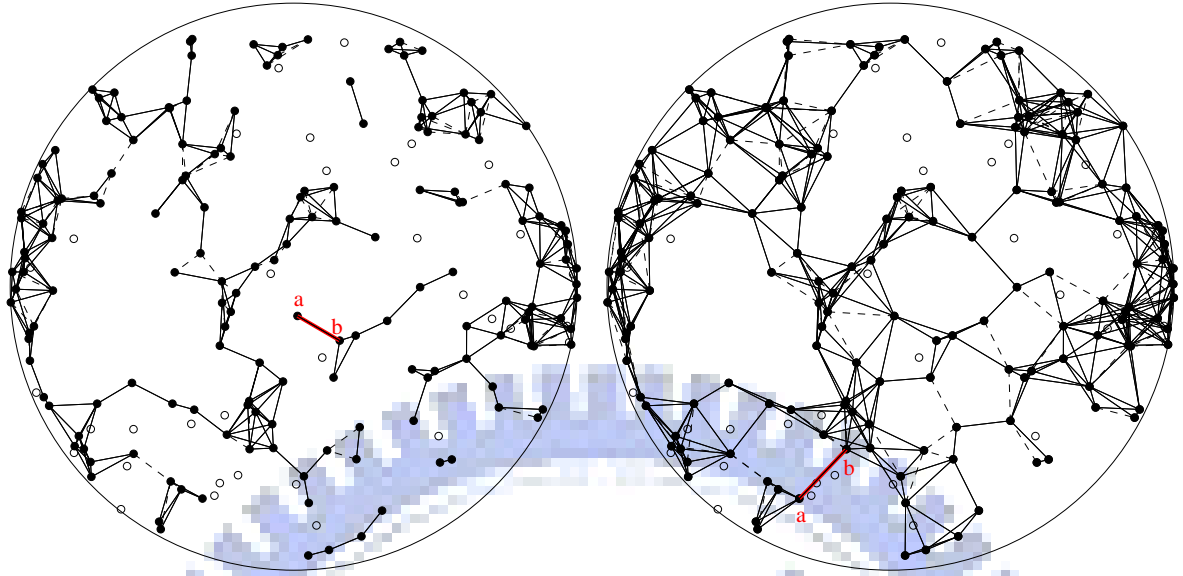


(c)  $p_1 = 0.7$  and  $p_2 = 1$ .

Figure 5.7: The c.d.f. of CTR's with waking/sleeping nodes and listening links.

Table 5.4: The average CTR's corresponding to Figure 5.7.

Figure 5.7(a): $p_1 = 0.9, p_2 = 1$					
$n$	$R_{iso}$	$R_{con}$	$R_{th}$	$DR_{iso}$	$DR_{con}$
100	0.1557	0.1704	0.1346	15.71%	26.62%
400	0.0860	0.0910	0.0759	13.28%	19.83%
1600	0.0468	0.0486	0.0418	11.86%	16.24%
Figure 5.7(b): $p_1 = 0.8, p_2 = 1$					
$n$	$R_{iso}$	$R_{con}$	$R_{th}$	$DR_{iso}$	$DR_{con}$
100	0.1662	0.1815	0.1427	16.42%	27.15%
400	0.0918	0.0972	0.0806	13.93%	20.70%
1600	0.0501	0.0519	0.0444	12.95%	16.98%
Figure 5.7(c): $p_1 = 0.7, p_2 = 1$					
$n$	$R_{iso}$	$R_{con}$	$R_{th}$	$DR_{iso}$	$DR_{con}$
100	0.1786	0.1936	0.1526	17.06%	26.88%
400	0.0980	0.1032	0.0861	13.81%	19.81%
1600	0.0537	0.0557	0.0474	13.20%	17.34%



(a)  $r_{iso} = |ab| = 0.097235$ .

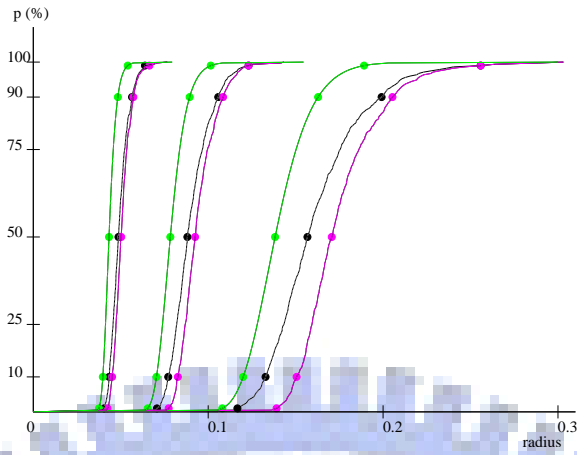
(b)  $r_{con} = |ab| = 0.135864$ .

Figure 5.8: The  $r$ -disk graph with unreliable nodes and links.

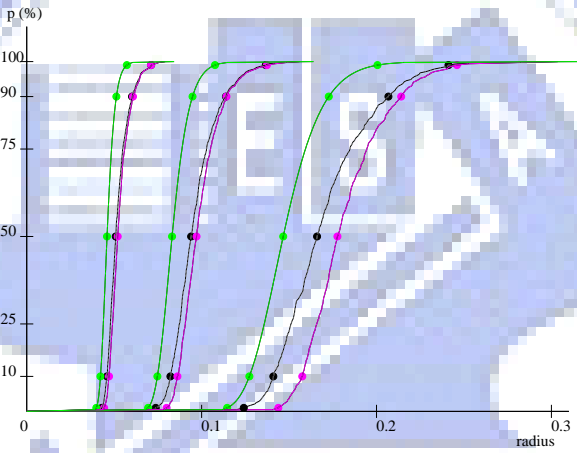
with  $r = \|a - b\|$ . Figure 5.8(b) is the network with connectivity, and  $ab$  is the longest edge and with length 0.135864 that is corresponding to the CTR such that black nodes and solid edges form a connected graph, and the graph is plotted with  $r = \|a - b\|$ . Figure 5.9 illustrates the c.d.f. of CTR's corresponding to  $p_1 = 0.9$ , and respectively  $p_2 = 0.9$ ,  $p_2 = 0.8$ , and  $p_2 = 0.7$ .

The average CTR's and inaccuracies of  $R_{iso}$ ,  $R_{con}$ , and  $R_{th}$  are listed in Table 5.5.

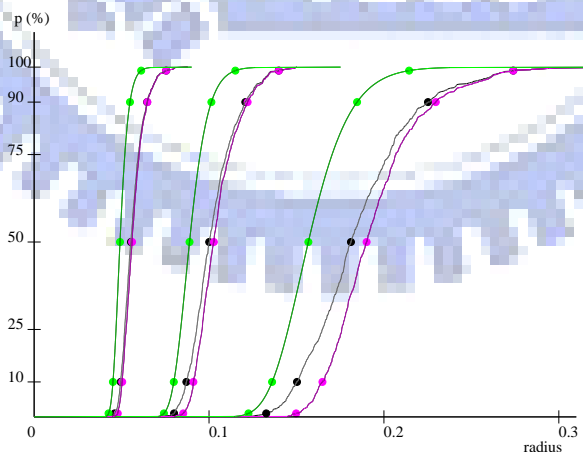
In addition, we consider another scenario in which every nodes independently stay in waking state with probability  $p_1$  and in sleeping state with probability  $1 - p_1$ , instead of breaking down. For such networks, a node is isolated if it doesn't have an up link connecting to black node, and a network is connected if awake nodes are connected by solid edge and every sleeping nodes have at least one solid edge. Figure 5.10 illustrates the c.d.f. of CTR's corresponding to  $p_1 = 0.9$ , and respectively  $p_2 = 0.9$ ,  $p_2 = 0.8$ , and



(a)  $p_1 = 0.9$  and  $p_2 = 1$ .



(b)  $p_1 = 0.8$  and  $p_2 = 1$ .



(c)  $p_1 = 0.7$  and  $p_2 = 1$ .

Figure 5.9: The c.d.f. of CTR's with unreliable nodes and links.



Table 5.5: The average CTR's corresponding to Figure 5.8.

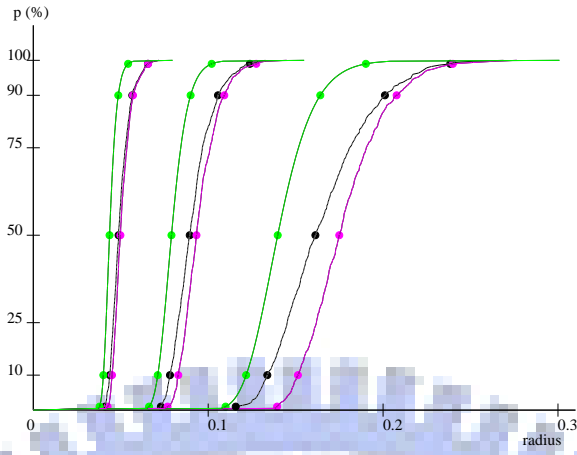
Figure 5.9(a): $p_1 = 0.9, p_2 = 0.9$					
$n$	$R_{iso}$	$R_{con}$	$R_{th}$	$DR_{iso}$	$DR_{con}$
100	0.1619	0.1753	0.1404	15.33%	24.88%
400	0.0902	0.0943	0.0794	13.58%	18.78%
1600	0.0494	0.0509	0.0438	12.81%	16.10%
Figure 5.9(b): $p_1 = 0.9, p_2 = 0.8$					
$n$	$R_{iso}$	$R_{con}$	$R_{th}$	$DR_{iso}$	$DR_{con}$
100	0.1704	0.1823	0.1489	14.43%	22.42%
400	0.0963	0.0991	0.0842	14.33%	17.69%
1600	0.0522	0.0532	0.0465	12.30%	14.50%
Figure 5.9(c): $p_1 = 0.9, p_2 = 0.7$					
$n$	$R_{iso}$	$R_{con}$	$R_{th}$	$DR_{iso}$	$DR_{con}$
100	0.1859	0.1945	0.1592	16.79%	22.22%
400	0.1024	0.1048	0.0900	13.71%	16.44%
1600	0.0563	0.0570	0.0497	13.43%	14.68%

$p_2 = 0.7$ .

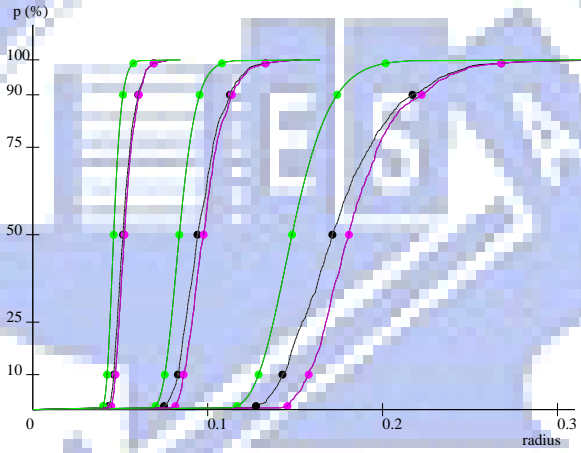
The average CTR's and inaccuracies of  $R_{iso}$ ,  $R_{con}$ , and  $R_{th}$  are listed in Table 5.6.

Table 5.6: The average CTR's corresponding to Figure 5.10.

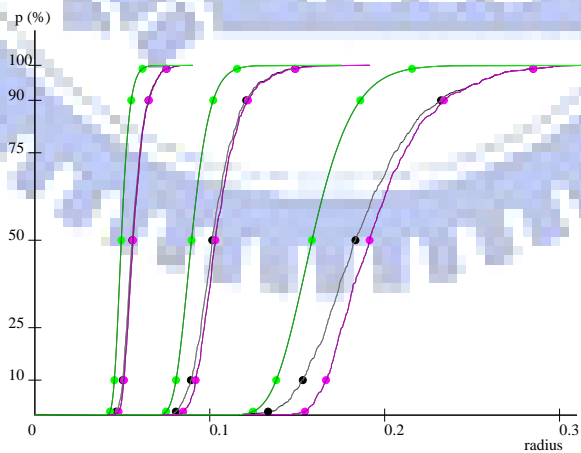
Figure 5.10(a): $p_1 = 0.9, p_2 = 0.9$					
$n$	$R_{iso}$	$R_{con}$	$R_{th}$	$DR_{iso}$	$DR_{con}$
100	0.1651	0.1778	0.1419	16.41%	25.35%
400	0.0911	0.0950	0.0801	13.74%	18.62%
1600	0.0497	0.0507	0.0441	12.63%	14.98%
Figure 5.10(b): $p_1 = 0.9, p_2 = 0.8$					
$n$	$R_{iso}$	$R_{con}$	$R_{th}$	$DR_{iso}$	$DR_{con}$
100	0.1765	0.1856	0.1505	17.32%	23.35%
400	0.0964	0.0991	0.0849	13.55%	16.73%
1600	0.0525	0.0534	0.0468	12.30%	14.07%
Figure 5.10(c): $p_1 = 0.9, p_2 = 0.7$					
$n$	$R_{iso}$	$R_{con}$	$R_{th}$	$DR_{iso}$	$DR_{con}$
100	0.1889	0.1966	0.1609	17.43%	22.21%
400	0.1039	0.1057	0.0908	14.44%	16.49%
1600	0.0568	0.0573	0.0500	13.60%	14.59%



(a)  $p_1 = 0.9$  and  $p_2 = 1$ .



(b)  $p_1 = 0.8$  and  $p_2 = 1$ .



(c)  $p_1 = 0.7$  and  $p_2 = 1$ .

Figure 5.10: The c.d.f. of CTR's with waking/sleeping nodes and unreliable links.

## 5.5 Secure Wireless Networks

The last simulations are for the  $m$ -composite key predistribution scheme [19] [20] [21]. 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. For example, Figure 5.11 is two secure networks over the same 200 random nodes but with different value of  $r$ 's.

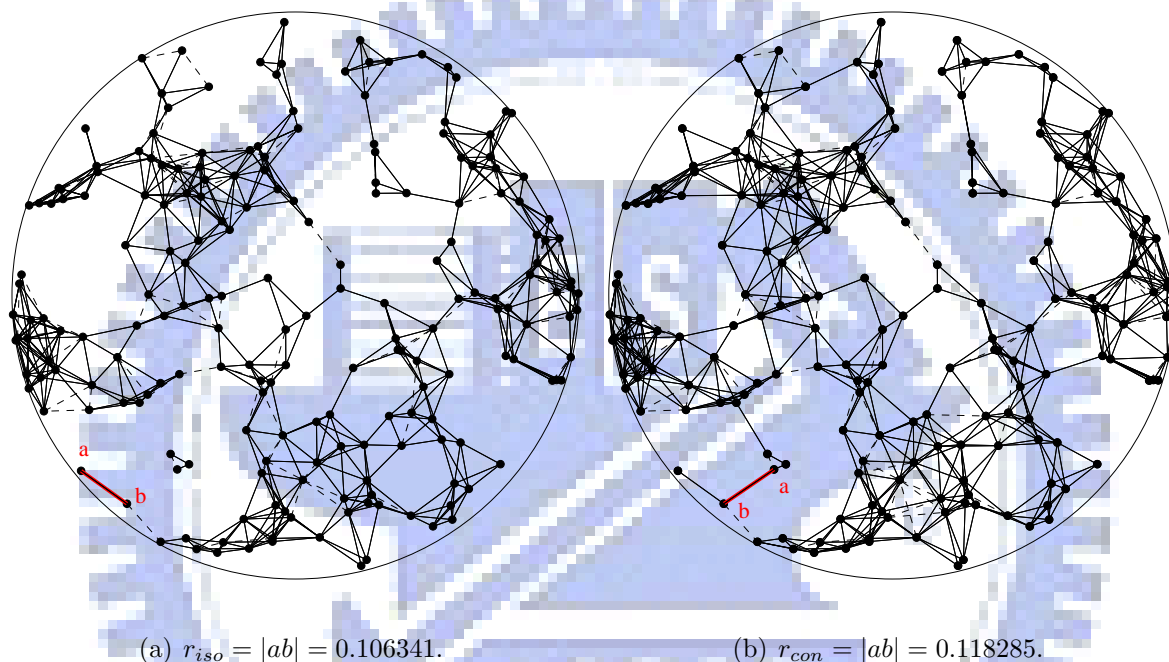
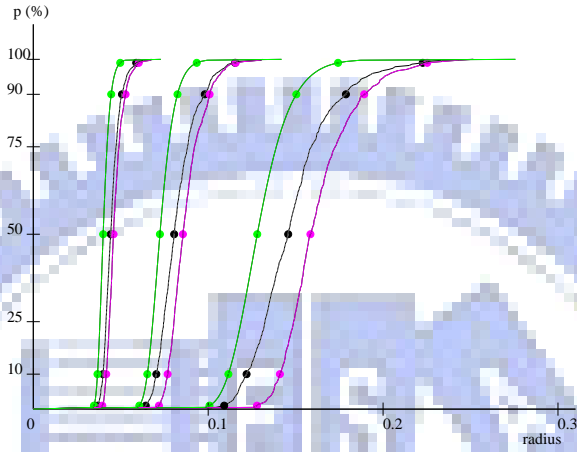
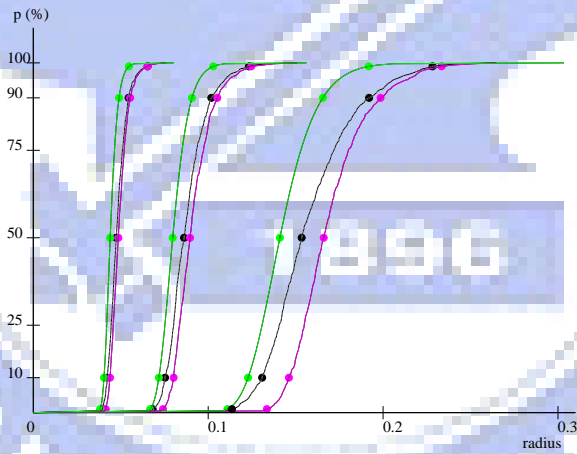


Figure 5.11: The secure networks with  $K = 40$ ,  $k = 10$ , and  $m = 2$ .

Two nodes at the same position in Figure 5.11(a) and Figure 5.11(b) respectively own the same key ring which are randomly drawn from the key pool. Solid lines are secured links, and dashed lines are unsecured links. The edge  $ab$  marked by red line is corresponding to the CTR of each network. In the simulations, we assume  $K = 40$  and  $k = 10$ . To focus our attention on the effect of the key predistribution scheme, we assume all nodes are active, i.e.  $p_1 = 1$ . Figure 5.12 illustrates the c.d.f. of CTR's corresponding to  $m = 1$  and  $m = 2$ , respectively.



(a)  $m = 1$ .



(b)  $m = 2$ .

Figure 5.12: The c.d.f. of CTR's of secure networks.

Table 5.7 shows the average CTRs and inaccuracies of  $R_{iso}$ ,  $R_{con}$ ,  $R_{th}$ . Note that

Table 5.7: The average CTR's corresponding to Figure 5.12.

Figure 5.12(a): $K = 40, k = 10, m = 1$					
$n$	$R_{iso}$	$R_{con}$	$R_{th}$	$DR_{iso}$	$DR_{con}$
100	0.1482	0.1627	0.1300	13.97%	25.15%
400	0.0824	0.0874	0.0734	12.34%	19.18%
1600	0.0449	0.0467	0.0404	11.03%	15.57%
Figure 5.12(b): $K = 40, k = 10, m = 2$					
$n$	$R_{iso}$	$R_{con}$	$R_{th}$	$DR_{iso}$	$DR_{con}$
100	0.1580	0.1698	0.1431	10.42%	18.62%
400	0.0879	0.0915	0.0808	08.83%	13.28%
1600	0.0482	0.0493	0.0445	08.31%	10.88%

$K = 40, k = 10$ , and  $m = 1$  is equivalent to  $p = 0.964555$ ; and  $K = 40, k = 10$ , and  $m = 2$  is equivalent to  $p = 0.795771$ .

## 5.6 Conclusions

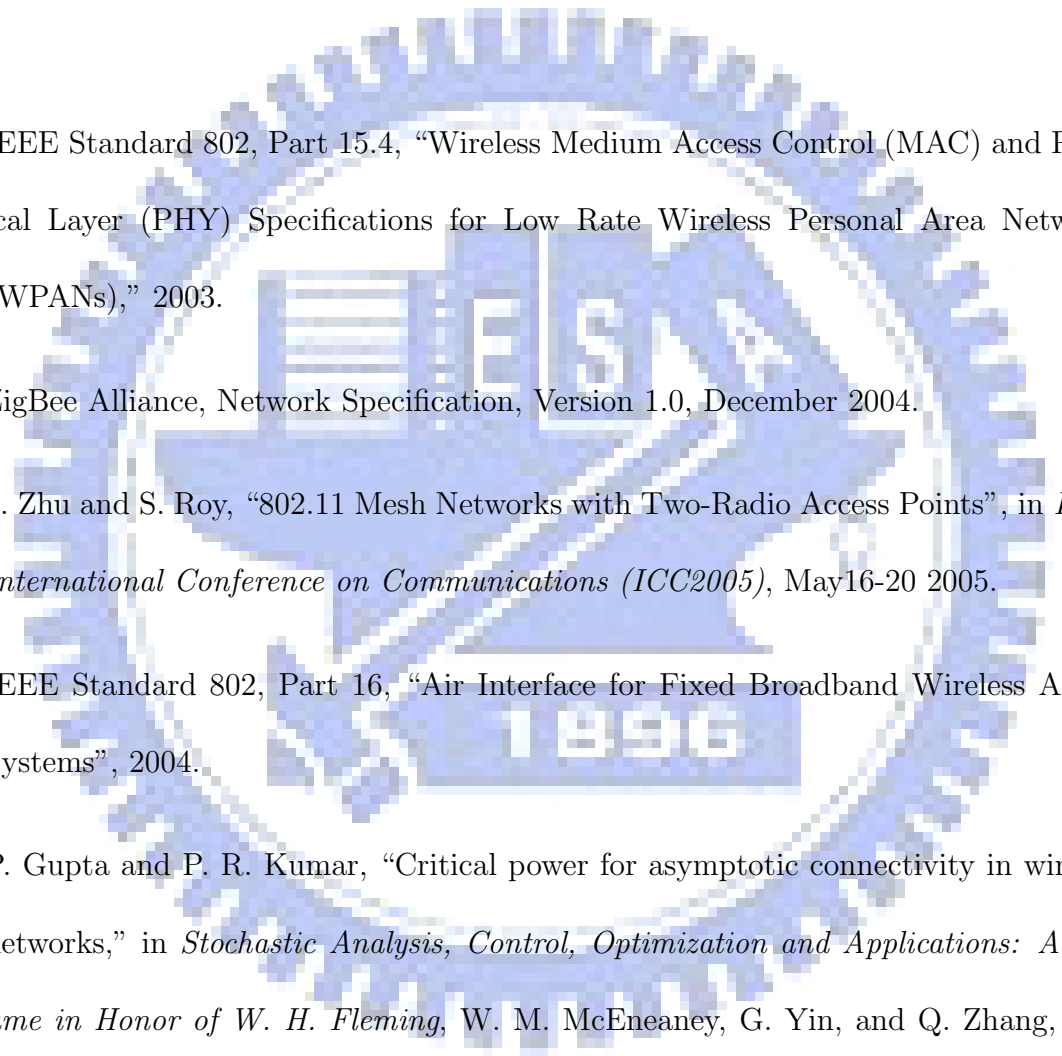
The connectivity of wireless networks in which nodes and links are not reliable is investigated in this study by the distribution of the number of isolated nodes in the networks. We assume a wireless network is composed of a collection of wireless devices represented by an uniform point process or Poisson 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 result 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  $\xi$ , 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  $\xi$ , 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. Different network models were considered, and the average and c.d.f. of CTR's were investigated. The problem whether vanishment of isolated nodes almost surely implies connectivity of networks or not is still open.

# Bibliography

- 
- [1] IEEE Standard 802, Part 15.4, “Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low Rate Wireless Personal Area Networks (WPANs),” 2003.
- [2] ZigBee Alliance, Network Specification, Version 1.0, December 2004.
- [3] J. Zhu and S. Roy, “802.11 Mesh Networks with Two-Radio Access Points”, in *IEEE International Conference on Communications (ICC2005)*, May16-20 2005.
- [4] IEEE Standard 802, Part 16, “Air Interface for Fixed Broadband Wireless Access Systems”, 2004.
- [5] 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.
- [6] 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,” in *IEEE*



*Wireless Communications and Networking Conference (WCNC 2003)*, March 16-20 2003.

- [7] H. Zhang and J. Hou, “On deriving the upper bound of  $\alpha$ -lifetime for large sensor networks,” in *Proceedings of the 5th ACM International Symposium on Mobile Ad Hoc Networking and Computing*, May 24-26 2004, pp. 121–132.
- [8] 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.
- [9] 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*, May 22-25 2006, pp. 25–36.
- [10] E. N. Gilbert, “Random plane networks,” *Journal of the Society for Industrial and Applied Mathematics*, vol. 9, no. 4, pp. 533–543, December 1961.
- [11] 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, pp. 67–80, 1989.
- [12] M. D. Penrose, “The longest edge of the random minimal spanning tree,” *The annals of applied probability*, vol. 7, no. 2, pp. 340–361, 1997.
- [13] 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*, May 24-26 2004, pp. 1–8.

- [14] —, “Asymptotic critical transmission ranges for connectivity in wireless ad hoc networks with Bernoulli nodes,” in *IEEE Wireless Communications and Networking Conference (WCNC 2005)*, March 13-17 2005.
- [15] IEEE Standard 802, Part 11, “Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: Higher-Speed Physical Layer Extension in the 2.4 GHz Band, 1999.
- [16] IEEE Standard 802, Part 11, “Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications Amendment 4: Further Higher Data Rate Extension in the 2.4 GHz Band,” 2003.
- [17] W. Diffie and M. E. Hellman, “New directions in cryptography,” *IEEE Transactions on Information Theory*, IT-22: pp. 644–654, November 1976.
- [18] Ronald L. Rivest, Adi Shamir, and Leonard M. Adleman, “A method for obtaining digital signatures and public-key cryptosystems,” *Communications of the ACM*, 21(2): pp. 120–126, 1978.
- [19] 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*, May 11-14 2003, pp. 197–213.
- [20] 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)*, October 25 2004.

- [21] 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*, November 18-22 2002, pp. 41–47.
- [22] N. Alon and J. H. Spencer, *The Probabilistic Method*, 2nd ed. New York, USA: Wiley, March 2000.
- [23] W. Du, J. Deng, Y. S. Han, and P. K. Varshney, “A Pairwise Key Pre-distribution Scheme for Wireless Sensor Networks,” in *Proceedings of the 10th ACM Conference on Computer and Communications Security (CCS2003)*, October, 2003, pp. 42–51.
- [24] R. Blom. An optimal class of symmetric key generation systems. *Advances in Cryptology: Proceedings of EUROCRYPT 84 (Thomas Beth, Norbert Cot, and Ingemar Ingemarsson, eds.)*, *Lecture Notes in Computer Science*, Springer-Verlag, 209: pp. 335–338, 1985.
- [25] IEEE Standard 802, Part 15.3, “Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for High Rate Wireless Personal Area Networks (WPANs),” 2003.
- [26] C. Bisdikian, S. Bouet, J. Inouye, R. Mettala, et al, “Bluetooth Protocol Architecture - Version 1.0,” Bluetooth White Paper - Bluetooth Special Interest Group, 1999.