Connectivity of Wireless Information-Theoretic Secure Networks

Tao Yang[1], Guoqiang Mao[2,3] and Wei Zhang[4]
[1]School of Electrical and Information Engineering, The University of Sydney
[2]School of Computing and Communications, University of Technology Sydney
[3]National ICT Australia
[4]School of Electrical Engineering and Telecommunications, The University of New South Wales

***Abstract*—Connectivity is one of the most fundamental properties of wireless multi-hop networks. This paper studies the connectivity of large wireless networks with secrecy constraint, i.e. a pair of nodes can communicate securely against eavesdropping. Specifically, we consider a network with a mixture of legitimate nodes and eavesdroppers that are distributed according to two independent Poisson point processes on a $\sqrt{n} \times \sqrt{n}$ square. Assuming that legitimate nodes can generate artificial noise, which is shown in the literature to be an effective way of suppressing eavesdropping, we provide sufficient conditions on the transmission power and the noise generation power required for a network with known intensity of eavesdroppers to be asymptotically almost surely connected with secrecy constraint as $n \to \infty$, considering the cases of both non-colluding and colluding eavesdroppers.**

***Index Terms*—Connectivity; Information-theoretic secure network; CSMA**

I. Introduction

Wireless multi-hop networks are being increasingly used in military and civilian applications. Connectivity is a prerequisite in wireless multi-hop networks for providing many network functions, such as routing, localization and topology control. A networks is said to be *connected* if there is a (multi-hop) path between any pair of nodes. The scaling behavior of the connectivity is of particular interest when the network becomes sufficiently large.

The broadcast nature of wireless communications makes it susceptible to malicious eavesdropping. Accordingly, communication secrecy has recently drawn intensive attention [1]–[8]. Traditionally, security is viewed as an independent feature addressed using techniques above the physical layer. Almost all widely used cryptographic protocols are designed and implemented assuming that the physical link has already been established and is not involved in securing the communication [1]. Cryptographic methods can be broadly classified into public-key and private-key protocols [3]. The former approach assumes that the eavesdroppers have a limited computational power, and the latter approach assumes that a random key is shared among legitimate users. However, due to the rapid growth of computational power, the costs in distributing key among legitimate users and the advancement of decoding technology, cryptography becomes increasingly more challenging as the network size grows significantly. To avoid the aforementioned limitations in cryptographic methods, this work investigates the use of physical layer techniques to secure the communication and adopts an *information-theoretic security* [1] framework where eavesdroppers are assumed to have infinite computational power and the idealistic assumption of pre-distributed keys is relaxed.

The notion of information-theoretic secrecy was first introduced by Shannon to study secure communication over point-to-point noiseless channels [9] and was later extended by Wyner [10] to noisy channels. To model large-scale networks operating in the presence of eavesdroppers, Haenggi [11] and Pinto *et al*. [5] introduced the so called *secrecy graph* which represents a large-scale random wireless network where legitimate nodes and eavesdroppers are distributed in $\Re^2$ following two independent Poisson point processes. The secrecy graph includes only edges that can be *securely* established. Particularly, a *directed and secure* connection from a legitimate node to another legitimate node in the secrecy graph is established in the following way. Assume that all legitimate nodes transmit with the same power P and let $\boldsymbol{x}_k$, $k \in \Gamma$ be the location of node k, where Γ represents the set of indices of all legitimate nodes in the network. A node j can receive the transmitted signal from a node i securely (i.e. node j *is securely connected to* node i) iff (if and only if) the secrecy rate is above a prescribed threshold ϱ, i.e.,

$$\mathcal{R}_s\left(\boldsymbol{x}_i \to \boldsymbol{x}_j\right) > \varrho; \tag{1}$$

and $\mathcal{R}_s\left(\boldsymbol{x}_i \to \boldsymbol{x}_j\right)$ is the Maximum Secrecy Rate (MSR) of the transmission, given by

$$\begin{aligned}&\mathcal{R}_s\left(\boldsymbol{x}_i \to \boldsymbol{x}_j\right)\\ &= \left[\log_2\left(1+\frac{P\ell\left(\boldsymbol{x}_i,\,\boldsymbol{x}_j\right)}{N_0}\right) - \log_2\left(1+\frac{P\ell\left(\boldsymbol{x}_i,\,e^*\right)}{N_0}\right)\right]^+\end{aligned} \tag{2}$$

where $[x]^+ = \max\{x, 0\}$, $e^* = \arg\max_{e_k \in \mathcal{E}} P\ell\left(\boldsymbol{x}_i,\, e_k\right)$ and $\mathcal{E}$ represents the set of indices of all eavesdroppers respectively, N_0 is the background noise power and the function $\ell\left(\boldsymbol{x}_i,\, \boldsymbol{x}_j\right)$ is the power attenuation from $\boldsymbol{x}_i$ to $\boldsymbol{x}_j$. By setting $\varrho = 0$, the *existence* of secure links are considered. A secrecy graph is said to be *connected* if there exists a path from any legitimate node to any other legitimate node where all (directed) links along the path can be securely established. It is shown in [11]

This research is funded by ARC Discovery projects: DP110100538 and DP120102030.

that even a small density of eavesdroppers has a drastic impact on the connectivity of the secrecy graph.

Since [11], the connectivity of the secrecy graph has received extensive attention in the literature. In [5], using stochastic geometry tools, Pinto *et al*. studied secrecy connectivity by providing statistical characterizations of node degree and isolation probability of a typical node in a secrecy graph defined on an infinite plane. In another work [4], Pinto *et al*. studied connectivity of the secrecy graph from the percolation perspective. They proved the existence of an unbounded connected component as the density of legitimate nodes increases. Furthermore, the paper [4] studied the secrecy connectivity of a typical legitimate node of a secrecy graph in a finite region, i.e., the probability that a typical legitimate node is fully out- and fully in-connected. A legitimate node is said to be *fully out-connected* if there exists a directed and secure path from the node to every other legitimate node in the network. A node is said to be *fully in-connected* if there exists a directed and secure path from every other legitimate node in the network to the node. In [12], Zhou *et al*. studied secrecy connectivity from the perspective of existence of secure connections from a typical legitimate transmitter to the legitimate receivers, and showed that the secrecy connectivity can be improved by using two antenna array techniques, namely directional antenna or eigen-beamforming.

Existing research on secrecy connectivity has mainly focused on either local connectivity of the network, which is characterized by the node degree of a *typical* node, or percolation in an infinite secrecy network. Further note that, when defining secure connections in the aforementioned secrecy graph using (1) and (2), the mutual interference among legitimate nodes and between legitimate nodes and eavesdroppers has not been taken into consideration.

In this paper, we analyze the secrecy connectivity of large-scale wireless networks considering the impact of mutual interference. Specifically we consider a network with legitimate nodes randomly distributed on a $\sqrt{n} \times \sqrt{n}$ square following a Poisson point process with unit intensity. Furthermore, eavesdroppers are distributed following another Poisson process, independently of legitimate nodes. Each legitimate node is capable of performing carrier sense operation. Considering that it is difficult to obtain some priori information such as location information of eavesdroppers, especially in large-scale wireless networks, different from some previous work in the field, we assume such information is unknown to legitimate nodes. Following the lead of [13] and [7], we assume that a legitimate node can generate artificial noise to suppress eavesdropping and has the capability of canceling interference caused by its own signal. The importance of these capabilities to ensure connectivity of secrecy graph becomes clear in our later analysis.

Our main contributions are summarized as follows.

1) We study secrecy connectivity in two scenarios: colluding case where eavesdroppers can only decode legitimate node's transmission individually, and non-colluding case where eavesdroppers can collaborate to exchange and combine the received information by all the eavesdroppers to decode legitimate node's transmission.
2) In both scenarios, we show that the maximum secrecy rate of a legitimate transmission is lower bounded by a positive constant as $n \to \infty$, by exploiting artificial noise generation and self-interference cancellation capabilities to suppress eavesdropping.
3) Based on the above results, we provide sufficient conditions on the transmission power and the noise generation power required for a network with known intensity of eavesdroppers to be asymptotically almost surely (a.a.s.) connected as $n \to \infty$, in both colluding and non-colluding scenarios.

The remainder of this paper is organized as follows: in Section II, we review related work in the field; Section III gives a formal definition of the network model considered in this paper; Section IV first presents a discussion on the impact of intensity of eavesdroppers on secrecy connectivity, then presents sufficient conditions for the network to be a.a.s. connected as $n \to \infty$ in non-colluding scenario; Section V presents sufficient conditions for the network to be a.a.s. connected as $n \to \infty$ in colluding scenarios; finally Section VI concludes the paper.

II. Related work

The literature is rich in studying connectivity of wireless multi-hop networks using the well-known *random geometric graph* and the *unit disk model*, which is usually obtained by randomly and uniformly distributing n nodes in a given area and connecting any two nodes iff their Euclidean distance is smaller than or equal to a certain threshold $r(n)$, known as the *transmission range*. Significant outcomes have been achieved [14], [15]. Particularly, Penrose [15] and Gupta and Kumar [14] proved that under the unit disk model and on a disk of unit area, the above network with a transmission range of $r(n) = \sqrt{\frac{\log n + c(n)}{\pi n}}$ is *a.a.s.* connected as $n \to \infty$ iff $c(n) \to \infty$. An event ξ_n depending on n is said to occur *a.a.s.* if its probability tends to one as $n \to \infty$. There is also work studying the asymptotic connectivity of random networks under the log-normal shadowing connection model [16], the more general random connection model [17], [18] and the SINR connection model [19]–[21].

Despite the importance of considering secrecy constraint in wireless networks, limited work exists on investigating the secrecy connectivity problem. The two papers [11] and [4] discussed in Section I studied the connectivity of secrecy graph from the percolation perspective, while references [12] and [5] studied secrecy connectivity from the perspective of a typical legitimate node, e.g., the node degree and isolation probability of a typical legitimate node. Goel *et al.* [22] considered the impact of uncertainty in the knowledge of eavesdroppers' location on the secrecy connectivity.

Some other work exists on analyzing the capacity of secrecy networks [3], [5], [6], [8]. Vasudevan *et al*. [6] studied the secrecy capacity of large-scale networks. Specifically, they introduced helper nodes around transmitters to generate noise to degrade eavesdroppers' channels and utilize channel fading gain of receivers to enhance secure communications. In the work of Koylouglu *et al*. [3] and Zhou *et al*. [8], they assumed

that there is a guard zone around each legitimate transmitters in which no eavesdroppers exist and on that basis, they analyzed the secrecy capacity of large-scale networks. In [7], Zhang *et al.* proposed using artificial noise generated by legitimate nodes to suppress eavesdroppers' channels. They analyzed the secrecy capacity considering two scenarios, namely, non-colluding and colluding eavesdroppers.

III. Network model

In this paper, we consider a network in which both legitimate nodes and eavesdroppers are randomly distributed on the plane following two independent homogeneous Poisson point process. We are mainly concerned with the secrecy connectivity of the network G_n formed by the legitimate nodes in a $\sqrt{n} \times \sqrt{n}$ box $B_n \subset \Re^2$.

Legitimate nodes are distributed following a Poisson point process with unit intensity, denoted by Π. Furthermore, following the lead of [13] and [7], we assume that legitimate nodes have self-interference cancelation capability. More precisely, each legitimate node is equipped with three antennas. When a legitimate node acts as a receiver, one antenna is used for reception while the other two antennas are used to generate artificial noise to suppress eavesdropping. The distances between the receiving antenna and the two transmitting antennas should be different by at least half a wavelength. The interference caused by the two transmitting antennas at the receiving antenna can then be eliminated using the self-interference cancelation technique proposed in [13].

Eavesdroppers are also distributed following a Poisson point process with λ_{e}, denoted by Π_{e}. We assume that eavesdroppers always keep silent since they will be easily detected if active. Furthermore, differently from some previous work which considers that the location of eavesdroppers is known to the legitimate nodes, we assume that location information of eavesdroppers is *unknown* to legitimate nodes.

We consider that a uniform signal transmission power P and a uniform noise generation power P_r are used at every legitimate node. Let Γ be the set of indices of all legitimate nodes in the network. We use $\boldsymbol{x}_i$ to denote the location of node i. The SINR at node j is given by [7], [23]

$$\mathrm{SINR}\left(\boldsymbol{x}_i \to \boldsymbol{x}_j\right) = \frac{P\ell\left(\boldsymbol{x}_i,\, \boldsymbol{x}_j\right)}{N_0 + \sum\limits_{k\in\mathcal{T}_i} P\ell\left(\boldsymbol{x}_k,\, \boldsymbol{x}_j\right) + \sum\limits_{k\in\mathcal{U}_j} P_r\ell\left(\boldsymbol{x}_k,\, \boldsymbol{x}_j\right)} \tag{3}$$

where $\mathcal{T}_i \subseteq \Gamma$ denotes the set of simultaneous transmitters as node i, not including node i itself, $\mathcal{U}_i \subseteq \Gamma$ denotes the set of simultaneous receivers, whose antennas are generating aitifical noise, as node j, *including node j itself*, and N_0 denotes the power of the background noise. The function $\ell\left(\boldsymbol{x}_i,\, \boldsymbol{x}_j\right)$ is the power attenuation from $\boldsymbol{x}_i$ to $\boldsymbol{x}_j$. As commonly done in the field, we consider that the attenuation function ℓ only depends on the Euclidean distance and is a power-law function, i.e.,

$$\ell\left(\boldsymbol{x}_i,\, \boldsymbol{x}_j\right) = \min\left\{1,\, \left\|\boldsymbol{x}_i - \boldsymbol{x}_j\right\|^{-\alpha}\right\}, \tag{4}$$

where $\alpha > 2$ is the path-loss exponent. Furthermore, *to reflect the self-interference cancellation capability of legitimate nodes*, we let $\ell\left(\boldsymbol{x}_i,\, \boldsymbol{x}_j\right) = 0$ whenever $\left\|\boldsymbol{x}_i - \boldsymbol{x}_j\right\| = 0$.

Similarly the SINR at an eavesdropper located at $\boldsymbol{e}_t$, $t \in \mathcal{E}$, where $\mathcal{E}$ represents the set of indices of all eavesdroppers, is given by

$$\mathrm{SINR}\left(\boldsymbol{x}_i \to \boldsymbol{e}_t\right) = \frac{P\ell\left(\boldsymbol{x}_i,\, \boldsymbol{e}_t\right)}{N_0 + \sum\limits_{k\in\mathcal{T}_i} P\ell\left(\boldsymbol{x}_k,\, \boldsymbol{e}_t\right) + \sum\limits_{k\in\mathcal{U}_j} P_r\ell\left(\boldsymbol{x}_k,\, \boldsymbol{e}_t\right)} \tag{5}$$

Node j can *securely* receive signals transmitted from node i (i.e., node j is directly and securely connected to node i) if the secrecy rate is above a prescribed threshold ϱ, i.e. inequality (1) is met.

When the eavesdroppers do not collude, the Maximum Secrecy Rate (MSR) of the transmission, denoted by $\mathcal{R}_s\left(\boldsymbol{x}_i \to \boldsymbol{x}_j\right)$, is given by

$$\begin{aligned}\mathcal{R}_s\left(\boldsymbol{x}_i \to \boldsymbol{x}_j\right) \;=\; &\left[\log_2\left(1 + \mathrm{SINR}\left(\boldsymbol{x}_i \to \boldsymbol{x}_j\right)\right)\right. \\ &-\;\left.\log_2\left(1 + \mathrm{SINR}\left(\boldsymbol{x}_i \to \boldsymbol{e}^*\right)\right)\right]^+\end{aligned} \tag{6}$$

where $[x]^+ = \max\{x, 0\}$; $e^* = \arg\max\limits_{e_k\in\mathcal{E}} \mathrm{SINR}\left(\boldsymbol{x}_i \to e_k\right)$.

When the eavesdroppers collude, the MSR of the transmission, denoted by $\mathcal{R}_{sc}\left(\boldsymbol{x}_i \to \boldsymbol{x}_j\right)$, is given by

$$\begin{aligned}\mathcal{R}_{sc}\left(\boldsymbol{x}_i \to \boldsymbol{x}_j\right) \;=\; &\left[\log_2\left(1 + \mathrm{SINR}\left(\boldsymbol{x}_i \to \boldsymbol{x}_j\right)\right)\right. \\ &-\;\left.\log_2\left(1 + \sum_{t\in\mathcal{E}} \mathrm{SINR}\left(\boldsymbol{x}_i \to \boldsymbol{e}_t\right)\right)\right]^+\end{aligned} \tag{7}$$

To avoid excessive interference, we consider that each legitimate node is capable of carrier-sensing operation. Therefore a CSMA network is considered. We further assume that legitimate nodes are capable of distinguishing signals from the artificially generated noise.

In CSMA networks, two nodes located at $\boldsymbol{x}_i$ and $\boldsymbol{x}_j$ respectively can transmit simultaneously iff they can not detect each other's transmission, i.e. both $P\ell\left(\boldsymbol{x}_i,\, \boldsymbol{x}_j\right)$ and $P\ell\left(\boldsymbol{x}_j,\, \boldsymbol{x}_i\right)$ in (3) and (5) are below a pre-designated detection threshold P_{th}. It then follows from Equation (4) that the carrier-sensing range R_c, which determines the *minimum* Euclidean distance between two concurrent transmitters, is given by

$$R_c = \left(P/P_{\mathrm{th}}\right)^{1/\alpha} \tag{8}$$

IV. Non-colluding eavesdroppers

In this section, eavesdroppers are assumed to be operating individually, i.e., they do not collaborate by sharing their observations.

A. The impact of λ_e on network connectivity

Now we discuss the impact of λ_{e}, i.e., the intensity of eavesdroppers, on network connectivity in the non-colluding scenario. Particularly, we will show that in a network where eavesdroppers are not able to collaborate, the probability that the network is securely connected is smaller than or equal to a positive value that is independent of λ_{e}.

First, observe that a necessary condition for a network to be connected is that the network has no isolated node. A

legitimate node is *isolated* iff there is no other legitimate node that is securely *connected to* it. Let us temporarily consider a case where $\varrho = 0$ and $P_r = 0$, i.e., legitimate nodes do not generate artificial noises. It can be shown that if a node is isolated when $\varrho = 0$, then it is also isolated when $\varrho > 0$. Consider a *randomly* selected eavesdropper $\boldsymbol{e}_t \in \mathcal{E}$ and its closest legitimate node i. We can write

$$\begin{aligned} & \Pr\{G_n \text{ is securely connected}\} \\ \leq\ & \Pr\{\text{There is no isolated node in } G_n\} \\ =\ & 1 - \Pr\{\text{There exist isolated nodes in } G_n\} \\ \leq\ & 1 - \Pr\{\text{The legitimate node } i \text{ is isolated}\}. \end{aligned} \quad (9)$$

If there is no node that can receive from node i securely, then it is isolated. Let $I_{\min}$ be the *minimum* interference that could possibly be experienced by a potential receiver of node i in the network. Let d be the Euclidean distance between node i and its receiver. By equation (5), it follows that *only* when $\frac{Pd^{-\alpha}}{N_0+I_{\min}} > \frac{P\|\boldsymbol{x}_i-\boldsymbol{e}_t\|^{-\alpha}}{N_0+I_{\boldsymbol{e}_t}}$, where $I_{\boldsymbol{e}_t}$ denotes the interference at eavesdropper $\boldsymbol{e}_t$, the transmission from node i to its receiver could *possibly* be successful. In other words, if there is no other legitimate node within a Euclidean distance of $\|\boldsymbol{x}_i - \boldsymbol{e}_t\| \left(\frac{N_0+I_{\min}}{N_0+I_{\boldsymbol{e}_t}}\right)^{-\frac{1}{\alpha}}$ to node i, then node i is isolated. Because Π is a Poisson point process with unit intensity, we have

$$\begin{aligned} & \Pr\{\text{The legitimate node } i \text{ is isolated}\} \\ \geq\ & \exp\left(-\pi\left(\frac{N_0+I_{\min}}{N_0+I_{\boldsymbol{e}_t}}\right)^{-\frac{2}{\alpha}}\|\boldsymbol{x}_i-\boldsymbol{e}_t\|^2\right) \\ =\ & \int_0^\infty \exp\left(-\pi\left(\frac{N_0+I_{\min}}{N_0+I_{\boldsymbol{e}_t}}\right)^{-\frac{2}{\alpha}}x\right)\times\pi\exp\left(-\pi x\right)\mathrm{d}x \\ =\ & \frac{1}{\left(\frac{N_0+I_{\boldsymbol{e}_t}}{N_0+I_{\min}}\right)^{\frac{2}{\alpha}}+1}. \end{aligned} \quad (10)$$

By (10) and (9), conclusion follows that $\Pr\{\text{The network is connected}\} \leq 1 - \frac{1}{\left(\frac{N_0+I_{\boldsymbol{e}_t}}{N_0+I_{\min}}\right)^{\frac{2}{\alpha}}+1}$.

The above discussion shows that in the case of non-colluding eavesdroppers, given that an eavesdropper exists in B_n, the legitimate node nearest to this eavesdropper is isolated with a probability that can not be made arbitrarily small by reducing λ_e. On the other hand, if the ratio of $\frac{N_0+I_{\boldsymbol{e}_t}}{N_0+I_{\min}}$ do not goes to infinity, the probability that the network is securely connected will be upper bounded by a small positive constant. Therefore, to improve secure connectivity of the network, it is necessary that legitimate nodes generate artificial noise to suppress eavesdropping.

B. A sufficient condition

Since we have established the necessity of having legitimate nodes generating artificial noise to improve secrecy connectivity, in this subsection we establish sufficient conditions on the transmission power and the noise generating power required for the network to be securely connected a.a.s..

A major challenge of the secrecy connectivity analysis is that the existence of a connection between a pair of legitimate nodes depends on both the locations and activities of other legitimate nodes and eavesdroppers. To solve the difficulty caused by this correlation on theoretical analysis, we resort to the coupling technique [15]. Specifically, we first establish an upper bound on the interference at any legitimate receiver, then we derive a lower bound on the secrecy rate between any two legitimate nodes, and finally we obtain a sufficient condition for a.a.s. secrecy connectivity by resorting to the coupling between the secrecy connection model and the unit disk model.

The following lemma establishes an upper bound on the interference at any legitimate receiver in the network.

Lemma 1. *Denote by r_0 the Euclidean distance between a receiver and its intended transmitter in the network, which is also the intended transmitter for the receiver. When $r_0 < R_c$, the maximum interference at the receiver is smaller than or equal to $I(r_0)$, where*

$$\begin{aligned} I(r_0) &= 6P(R_c - r_0)^{-\alpha} + 6P_r \\ &+ \frac{8P\left(\frac{3\sqrt{3}}{4}R_c - r_0\right)^{1-\alpha}\left(\frac{3\sqrt{3}}{4}(\alpha-1)R_c - r_0\right)}{R_c^2(\alpha-1)(\alpha-2)} \\ &+ \frac{8P_r\left(\frac{3\sqrt{3}-4}{4}R_c - r_0\right)^{1-\alpha}\left(\frac{1}{4}\left(3\sqrt{3}\alpha - 3\sqrt{3} - 4\right)R_c - r_0\right)}{R_c^2(\alpha-1)(\alpha-2)} \end{aligned} \quad (11)$$

Remark 2. In the proof of Lemma 1, it is assumed that each legitimate node communicate with other nodes located no further than a distance of R_c. This assumption is valid in most wireless systems which not only require the SINR to be above a threshold but also require the received signal to be of sufficiently good quality.

Proof: Consider that an arbitrary legitimate node, say node i, is transmitting to a legitimate node at a Euclidean distance of r_0 away. Note that the distance between any two concurrent transmitters is at least R_c. Draw a circle of radius $R_c/2$ centered at each transmitter. Then the two circles centered at two closest transmitters cannot overlap except at a single point. Pack these equal-radius non-overlapping circles in the densest way around node i, which is done by placing the circle centers at the vertices of a hexagonal lattice [24]. Group the vertices of the hexagonal lattice into tiers of increasing distances from the origin. The six vertices of the first tier are within a Euclidean distance R_c to the origin. The $6m$ vertices of the m^{th} tier are located at distances within $((m-1)R_c, mR_c]$ from the origin. By (4), the interference at the intended receiver due to the six closest transmitters and associated receivers is smaller than or equal to $6P(R_c - r_0)^{-\alpha} + 6P_r$; the interference at the intended receiver due to the $6m$ transmitters the m^{th} tier and their associated receivers is smaller than or equal to $6mP\left(\frac{\sqrt{3}}{2}mR_c - r_0\right)^{-\alpha} + 6mP_r\left(\frac{\sqrt{3}}{2}mR_c - R_c - r_0\right)^{-\alpha}$. Taking into account the interference generated by all of the concurrent transmitters and receivers, the interference at the intended receiver can be upper bounded as follows:

$$I(r_0) \leq 6P(R_c - r_0)^{-\alpha} + 6P_r + \sum_{m=2}^{\infty} 6mP\left(\frac{\sqrt{3}}{2}mR_c - r_0\right)^{-\alpha}$$

$$+\sum_{m=2}^{\infty} 6mP_r \left(\frac{\sqrt{3}}{2}mR_c - R_c - r_0\right)^{-\alpha} \quad (12)$$

Look at the first summation in (12). Let $U_m, m = 2, \ldots, \infty$, be random variables uniformly and i.i.d. in $[m - 1/2,\ m + 1/2]$. It follows from the convexity of $6mP\left(\frac{\sqrt{3}}{2}mR_c - r_0\right)^{-\alpha}$ and Jensen's inequality (used in the second step) that

$$\begin{aligned}
&\sum_{m=2}^{\infty} 6mP \left(\frac{\sqrt{3}}{2}mR_c - r_0\right)^{-\alpha} \\
= &\sum_{m=2}^{\infty} 6\mathrm{E}\left[U_m\right] P \left(\frac{\sqrt{3}}{2}\mathrm{E}\left[U_m\right] R_c - r_0\right)^{-\alpha} \\
\leq &\sum_{m=2}^{\infty} \mathrm{E}\left[6mP \left(\frac{\sqrt{3}}{2}mR_c - r_0\right)^{-\alpha}\right] \\
= &\frac{8P\left(\frac{3\sqrt{3}}{4}R_c - r_0\right)^{1-\alpha}\left(\frac{3\sqrt{3}}{4}\left(\alpha-1\right)R_c - r_0\right)}{R_c^2\left(\alpha-1\right)\left(\alpha-2\right)} \quad (13)
\end{aligned}$$

Likewise, we also have

$$\begin{aligned}
&\sum_{m=2}^{\infty} 6mP_r \left(\frac{\sqrt{3}}{2}mR_c - R_c - r_0\right)^{-\alpha} \\
\leq &\frac{8P_r\left(\frac{3\sqrt{3}-4}{4}R_c - r_0\right)^{1-\alpha}\left(\frac{1}{4}\left(3\sqrt{3}\alpha - 3\sqrt{3} - 4\right)R_c - r_0\right)}{R_c^2\left(\alpha-1\right)\left(\alpha-2\right)} \quad (14)
\end{aligned}$$

Combining (13), (13) and (14), the Lemma is proved. ■

Using Lemma 1, the following result can be obtained.

Lemma 3. *For any legitimate transmitter-receiver pair that is separated by an Euclidean distance of r_0 and $r_0 < R_c$, the secrecy rate between them is lower bounded by*

$$\mathcal{R}_s(r_0) = \left[\log_2\left(1 + \frac{Pr_0^{-\alpha}}{N_0 + I\left(r_0\right)}\right) - \log_2\left(1 + \frac{P}{P_r}\left(1 + r_0\right)^{\alpha}\right)\right]^+ \quad (15)$$

where $I\left(r_0\right)$ is given by (11).

Proof: First we derive an upper bound on the maximum rate that an eavesdropper can obtain. Consider an arbitrary eavesdropper $\boldsymbol{e}_t$ who is overhearing the transmission from legitimate node i to legitimate node j. Let $r_0 = \|\boldsymbol{x}_i - \boldsymbol{x}_j\|$, $r_1 = \|\boldsymbol{x}_i - \boldsymbol{e}_t\|$ and $r_2 = \|\boldsymbol{x}_j - \boldsymbol{e}_t\|$. Using equation (5), we have

$$\begin{aligned}
&\mathrm{SINR}\left(\boldsymbol{x}_i \to \boldsymbol{e}_t\right) \\
= &\frac{P\left\|\boldsymbol{x}_i - \boldsymbol{e}_t\right\|^{-\alpha}}{N_0 + \sum\limits_{k\in\mathcal{T}_i} P\left\|\boldsymbol{x}_k - \boldsymbol{e}_t\right\|^{-\alpha} + \sum\limits_{k\in\mathcal{U}_j} P_r\left\|\boldsymbol{x}_k - \boldsymbol{e}_t\right\|^{-\alpha}} \\
\leq &\frac{Pr_1^{-\alpha}}{P_r r_2^{-\alpha}} \quad (16) \\
\leq &\frac{Pr_1^{-\alpha}}{P_r\left(r_0 + r_1\right)^{-\alpha}} = \frac{P}{P_r}\left(1 + \frac{r_0}{r_1}\right)^{\alpha}. \quad (17)
\end{aligned}$$

The $\mathrm{SINR}\left(\boldsymbol{x}_i \to \boldsymbol{e}_t\right)$ depends critically on r_1. Consider the following two cases, namely when $r_1 \geq 1$ and $r_1 < 1$. When $r_1 \geq 1$, it is straightforward that RHS of (17) is less than or equal to $\frac{P}{P_r}\left(1 + r_0\right)^{\alpha}$. When $r_1 < 1$, it follows from (16) and (4) that $\frac{Pr_1^{-\alpha}}{P_r r_2^{-\alpha}} = \frac{P}{P_r r_2^{-\alpha}} \leq \frac{P}{P_r}\left(r_1 + r_0\right)^{\alpha} < \frac{P}{P_r}\left(1 + r_0\right)^{\alpha}$. Therefore, the maximum SINR that any eavesdropper can have by overhearing a transmission between two legitimate nodes spaced by an Euclidean distance r_0 is upper bounded by

$$\frac{P}{P_r}\left(1 + r_0\right)^{\alpha} \triangleq \mathrm{SINR}_e^u. \quad (18)$$

Combining (6) with Lemma 1, the proof is completed. ■

Remark 4. The lower bound in (15) does not depend on the intensity of eavesdroppers. Due to (4), even if an eavesdropper is very close to a legitimate transmitter, the received signal is still less than or equal to P. Hence, non-colluding eavesdroppers can not achieve arbitrarily high rate simply by increasing their intensity.

The following lemma is a ready consequence of Lemma 3.

Lemma 5. *Assume that the threshold of secrecy rate is ϱ. Let the noise generation power $P_r = PR_c^{\alpha}$. There exists a secrecy transmission range R_s such that a pair of legitimate nodes are securely connected if their Euclidean distance is smaller than or equal to R_s, given implicitly by*

$$\log_2\left(1 + \frac{PR_s^{-\alpha}}{N_0 + I\left(R_s\right)}\right) - \log_2\left(1 + R_c^{-\alpha}\left(1 + R_s\right)^{\alpha}\right) = \varrho. \quad (19)$$

Proof: Lemma 3 establishes that the secrecy rate from a legitimate transmitter to its receiver at a distance r_0 is lower bounded by $\mathcal{R}_s\left(r_0\right)$. Note that, for $r_0 < R_c$, $\mathcal{R}_s\left(r_0\right)$ is decreasing with r_0. Hence, using (15) the secrecy rate of a legitimate receiver at $r_0 \leq R_s$ from its transmitter meets $\mathcal{R}_s\left(r_0\right) \geq \mathcal{R}_s\left(R_s\right) \geq \varrho$. By symmetry, when the transmission occurs in the opposite direction, the secrecy rate is also lower bounded by $\mathcal{R}_s\left(R_s\right)$. Therefore, the secrecy rate is also greater than or equal to ϱ.

The existence of a unique solution to (19) can be proved by noting that $\mathcal{R}_s\left(r_0\right) \to \infty$ as $r_0 \to 0$, $\mathcal{R}_s\left(r_0\right) \to \log\frac{1}{1+\left(1+\frac{1}{R_c}\right)^{\alpha}} < 0$ as $r_0 \to R_c^-$ and that $\mathcal{R}_s\left(r_0\right)$ is monotonically decreasing with r_0. ■

We define $\beta_{\mathrm{e}} = 2^{\varrho}$ such that node j is directly connected to node i if $\frac{1+\mathrm{SINR}(\boldsymbol{x}_i \to \boldsymbol{x}_j)}{1+\mathrm{SINR}(\boldsymbol{x}_i \to \boldsymbol{e}^*)} \geq \beta_{\mathrm{e}}$. Based on (19), Figure 1 shows the ratio of $\frac{R_c}{R_s}$ as a function of β_{e}, and Figure 2 shows the ratio of $\frac{R_c}{R_s}$ as a function of ϱ, for different choices of α. It can be seen from Figure 2 that the required transmission power for achieving a moderate level of security, i.e., a small ϱ, is low, however the transmission power must be increased significantly to achieve a high level of security.

The following result is obtained, based on the secrecy transmission range R_s derived in Lemma 5.

Theorem 6. *Let $P_r = PR_c^{\alpha}$. The legitimate network G_n is a.a.s. connected if the transmission power*

$$P = P_{th}R_c'^{\alpha},$$

where R_c' is the solution to $\mathcal{R}_s\left(r\left(n\right)\right) = \varrho$, $r\left(n\right) = \sqrt{\frac{\log n + c(n)}{\pi}}$, $c\left(n\right) = o\left(\log n\right)$ and $c\left(n\right) \to \infty$ as $n \to \infty$.

Proof: Under the unit disk model, a pair of nodes are directly connected iff their Euclidean distance is smaller than

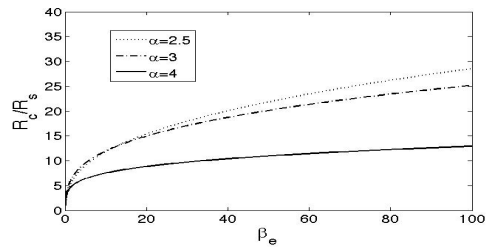

Figure 1. Variation of the ratio $\frac{R_c}{R_s}$ with $\beta_{\mathrm{e}} = 2^{\varrho}$ when the path loss exponent α equals to 2.5, 3 and 4, respectively.

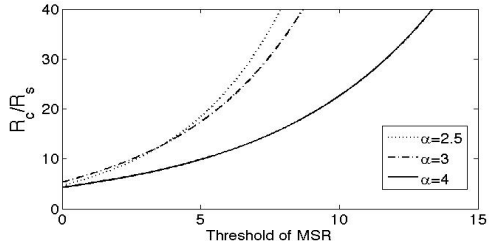

Figure 2. Variation of the ratio $\frac{R_c}{R_s}$ with the threshold of MSR ϱ when the path loss exponent α equals to 2.5, 3 and 4, respectively.

or equal to a given threshold $r(n)$. Based on the secrecy transmission range R_s derived in Lemma 5, coupling the secrecy connection model with the unit disk model and letting $r(n) = R_s$, if a pair of legitimate nodes are connected under the unit disk model, then they will also be securely connected under the secrecy connection model.

The results in [18] show that for a network formed by Poisson nodes with unit intensity located in a $\sqrt{n}\times\sqrt{n}$ square and using unit disk model, the network is a.a.s. connected as $n\to\infty$ iff $r(n) = \sqrt{\frac{\log n + c(n)}{\pi}}$ where $c(n)\to\infty$ as $n\to\infty$. Using this result, combining $R_s = r(n)$, $P_r = PR_c^{\alpha}$ and (8), and solving (19) for R_c, the result in the theorem follows. ■

V. Colluding eavesdroppers

In this section, it is assumed that eavesdroppers have the ability to collude, i.e., they can collaborate to exchange and combine the received information by all the eavesdroppers to decode the secret messages. We assume that the maximum ratio combining [7] is used by eavesdroppers to maximize their SINR. In this case, MSR of a transmission from $\boldsymbol{x}_i$ to $\boldsymbol{x}_j$ is given by (7).

It can be seen from (7) that the intensity of eavesdroppers has a critical impact on MSR through the summation item in (7). The following lemma shows that with the constraint on the intensity of eavesdroppers, i.e., $\lambda_{\mathrm{e}} = O(n^{-\rho})$ and $\rho > 0$, the secrecy rate of any legitimate transmission can be lower bounded. This result will later be used to derive a sufficient condition on transmission power and noise generating power for network connectivity in the case of colluding eavesdroppers.

Lemma 7. *Suppose the eavesdroppers are Poissonly distributed with intensity $\lambda_e = O(n^{-\rho})$ and $\rho > 0$. In the case of colluding eavesdroppers, for any legitimate transmitter-receiver pair that is separated by an Euclidean distance of r_0, the secrecy rate between them is greater than or equal to*

$$\begin{aligned}\mathcal{R}_{sc}(r_0) &= \left[\log_2\left(1+\frac{Pr_0^{-\alpha}}{N_0+I(r_0)}\right)\right.\\ &- \left.\log_2\left(\bar{\eta}\frac{P}{P_r}(1+r_0)^{\alpha}+\bar{\eta}\frac{P}{N_0}\frac{2}{\alpha-2}\left(\frac{a}{\pi}\right)^{-\frac{\alpha}{2}}\right)\right]^{+}\end{aligned}$$

where $I(r_0)$ is given by (11) , and $\bar{\eta} = \left\lceil\frac{1}{\rho}\right\rceil + 1$, and a is a constant such that $a\lambda_e < 1$.

Proof: Considering an arbitrary pair of legitimate nodes $\boldsymbol{x}_i$ and $\boldsymbol{x}_j$, we partition the network into disjoint concentric annulus centered at the transmitter $\boldsymbol{x}_i$. Each concentric annulus is of the same constant size of a. Let r_k be the external diameter of the kth ring and $a = \pi r_1^2 = \pi\left(r_k^2 - r_{k-1}^2\right)$ for $k > 1$. Next, we first show that the number of eavesdroppers inside each annulus is less than or equal to $\bar{\eta} = \left\lceil\frac{1}{\rho}\right\rceil + 1$ a.a.s. as $n\to\infty$, then we show that the accumulated SINR at all eavesdroppers in the network is upper bounded.

Denote by η_k the number of eavesdroppers in the kth ring and $1 \le k < \frac{n}{a}$. Let η be the expected value of η_k. The value of a can be easily chosen in a way such that $\eta = a\lambda_{\mathrm{e}} < 1$ and it follows that

$$\begin{aligned}\Pr[\eta_k \ge \bar{\eta}] &= \sum_{k=\bar{\eta}}^{\infty}\frac{\eta^k}{k!}e^{-\eta} \le \frac{e^{-\eta}}{\bar{\eta}!}\sum_{k=\bar{\eta}}^{\infty}\eta^k = \frac{e^{-\eta}\eta^{\bar{\eta}}}{\bar{\eta}!}\sum_{k=0}^{\infty}\eta^k\\ &= \frac{e^{-\eta}\eta^{\bar{\eta}}}{\bar{\eta}!}\times\frac{1}{1-\eta} = \frac{e^{-a\lambda_{\mathrm{e}}}}{1-a\lambda_{\mathrm{e}}}\times\frac{(a\lambda_{\mathrm{e}})^{\bar{\eta}}}{\bar{\eta}!}\to 0\end{aligned}$$

as $n\to\infty$. Next we use the union bound on all rings and obtain

$$\begin{aligned}&\Pr\left[\bigcup_{i=1}^{\frac{n}{a}}\eta_k \ge \bar{\eta}\right]\\ \le\ & \frac{n}{a}\times\frac{e^{-\eta}\eta^{\bar{\eta}}}{\bar{\eta}!}\times\frac{1}{1-\eta} = n\eta^{\bar{\eta}}\frac{e^{-\eta}}{a\times\bar{\eta}!\times(1-\eta)}\\ \le\ & n\left(an^{-\rho}\right)^{\bar{\eta}}\frac{e^{-\eta}}{a\times\bar{\eta}!\times(1-\eta)}\\ =\ & n^{1-\rho\left\lceil\frac{1}{\rho}\right\rceil-\rho}\frac{e^{-\eta}a^{\bar{\eta}-1}}{\bar{\eta}!\times(1-\eta)}\to 0\end{aligned}$$

as $n\to\infty$. Hence, the number of eavesdroppers in each ring is less than or equal to $\bar{\eta}$ a.a.s. as $n\to\infty$.

Note that the distance from the legitimate transmitter to an eavesdropper in the kth ring is at least r_{k-1}. Let $\mathcal{E}_k$ denote the set of indices of all eavesdroppers in the kth ring. With the upper bound on the SINR at any individual eavesdropper, given by (18), we calculate the accumulated SINR at all eavesdroppers as

$$\begin{aligned}&\sum_{t\in\mathcal{E}}\mathrm{SINR}(\boldsymbol{x}_i\to e_t) \le \sum_{k=1}^{\infty}\sum_{t\in\mathcal{E}_k}\mathrm{SINR}(\boldsymbol{x}_i\to e_t)\\ \le\ & \bar{\eta}\mathrm{SINR}_e^u +\\ & \sum_{k=2}^{\infty}\sum_{t\in\mathcal{E}_k}\frac{P\left\|\boldsymbol{x}_i-\boldsymbol{e}_t\right\|^{-\alpha}}{N_0+\sum\limits_{h\in\mathcal{T}_i}P\left\|\boldsymbol{x}_h-\boldsymbol{e}_t\right\|^{-\alpha}+\sum\limits_{h\in\mathcal{U}_j}P_r\left\|\boldsymbol{x}_h-\boldsymbol{e}_t\right\|^{-\alpha}}\end{aligned}$$

$$\leq \bar{\eta}\mathrm{SINR}_e^u + \sum_{k=2}^{\infty} \bar{\eta}\frac{Pr_{k-1}^{-\alpha}}{N_0}$$
$$= \bar{\eta}\left(\frac{P}{P_r}(1+r_0)^{\alpha} + \sum_{k=2}^{\infty}\frac{Pr_{k-1}^{-\alpha}}{N_0}\right)$$

Since $a = \pi r_1^2 = \pi\left(r_k^2 - r_{k-1}^2\right)$ for $k > 1$, we have $r_k = \sqrt{k}r_1$. We continue to write

$$\begin{aligned}
&\sum_{t\in\mathcal{E}} \mathrm{SINR}\left(\boldsymbol{x}_i \to e_t\right) \\
\leq\ & \bar{\eta}\left(\frac{P}{P_r}(1+r_0)^{\alpha} + \frac{P}{N_0}\sum_{k=1}^{\infty}\left(\sqrt{k}r_1\right)^{-\alpha}\right) \\
=\ & \bar{\eta}\left(\frac{P}{P_r}(1+r_0)^{\alpha} + \frac{P}{N_0}r_1^{-\alpha}\sum_{k=1}^{\infty}k^{-\frac{\alpha}{2}}\right) \\
\leq\ & \bar{\eta}\left(\frac{P}{P_r}(1+r_0)^{\alpha} + \frac{P}{N_0}\frac{2r_1^{-\alpha}}{\alpha-2}\right) \\
=\ & \bar{\eta}\frac{P}{P_r}(1+r_0)^{\alpha} + \bar{\eta}\frac{P}{N_0}\frac{2}{\alpha-2}\left(\frac{a}{\pi}\right)^{-\frac{\alpha}{2}}.
\end{aligned}$$

Therefore, the secrecy rate between any pair of legitimate nodes is greater than or equal to

$$\begin{aligned}
\mathcal{R}_{sc}(r_0) =\ & \log_2\left(1+\frac{Pr_0^{-\alpha}}{I(r_0)}\right) \\
& -\log_2\left(\bar{\eta}\frac{P}{P_r}(1+r_0)^{\alpha} + \bar{\eta}\frac{P}{N_0}\frac{2}{\alpha-2}\left(\frac{a}{\pi}\right)^{-\frac{\alpha}{2}}\right).
\end{aligned}$$

The proof is completed. ∎

Theorem 8. *Suppose the eavesdroppers are Poissonly distributed with intensity $\lambda_e = O(n^{-\rho})$ and $\rho > 0$. Let $P_r = PR_c^{\alpha}$. The legitimate network G_n is a.a.s. connected if the transmission power $P = P_{th}R_{cc}^{\prime\alpha}$, where $R_{cc}^{\prime}$ is the solution to $\mathcal{R}_{sc}(r(n)) = \varrho$, $r(n) = \sqrt{\frac{\log n + c(n)}{\pi}}$, $c(n) = o(\log n)$ and $c(n) \to \infty$ as $n \to \infty$.*

Proof: Following the same argument used in Lemma 5, in the case of colluding eavesdroppers, there exists a transmission range R_{sc} such that a pair of legitimate nodes are securely connected if their Euclidean distance is smaller than or equal to R_{sc}, given implicitly by $\mathcal{R}_{sc}(R_{sc}) = \varrho$. Letting $R_{sc} = r(n)$ and solving $\mathcal{R}_{sc}(r(n)) = \varrho$ for R_c, the result in the theorem follows. ∎

VI. Conclusions

In this work, we studied the secrecy connectivity of large-scale wireless multi-hop networks. It was shown that the intensity of eavesdroppers has a critical impact on the secrecy connectivity in the colluding scenario, but comparatively less impact in the non-colluding scenario. Considering the scenarios of both non-colluding and colluding eavesdroppers, we provide sufficient conditions on the transmission power and the noise generation power required for a network with known intensity of eavesdroppers to be a.a.s. connected with secrecy constraint as $n \to \infty$. The results suggest that the required transmission power for achieving a moderate level of security is low, while the transmission power must be increased significantly to achieve a high level of security.

References

[1] M. Bloch, J. Barros, M. R. D. Rodrigues, and S. W. McLaughlin, "Wireless information-theoretic security," *IEEE Transactions on Information Theory*, vol. 54, no. 6, pp. 2515–2534, 2008.

[2] I. Csiszar and J. Korner, "Broadcast channels with confidential messages," *IEEE Transactions on Information Theory*, vol. 24, no. 3, pp. 339–348, 1978.

[3] O. O. Koyluoglu, C. E. Koksal, and H. E. Gamal, "On secrecy capacity scaling in wireless networks," *IEEE Transactions on Information Theory*, vol. 58, no. 5, pp. 3000–3015, 2012.

[4] P. C. Pinto and M. Z. Win, "Percolation and connectivity in the intrinsically secure communications graph," *IEEE Transactions on Information Theory*, vol. 58, no. 3, pp. 1716–1730, 2012.

[5] P. C. Pinto, J. Barros, and M. Z. Win, "Secure communication in stochastic wireless networks–part i: Connectivity," *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 1, pp. 125–138, 2012.

[6] S. Vasudevan, D. Goeckel, and D. F. Towsley, "Security-capacity trade-off in large wireless networks using keyless secrecy," in *Proceedings of ACM Mobihoc*. Chicago, Illinois, USA: ACM, 2010, pp. 21–30.

[7] J. Zhang, L. Fu, and X. Wang, "Asymptotic analysis on secrecy capacity in large-scale wireless networks," *IEEE/ACM Transactions on Networking*, vol. PP, no. 99, pp. 1–1, 2013.

[8] X. Zhou, R. K. Ganti, J. G. Andrews, and A. Hjorungnes, "On the throughput cost of physical layer security in decentralized wireless networks," *IEEE Transactions on Wireless Communications*, vol. 10, no. 8, pp. 2764–2775, 2011.

[9] C. E. Shannon, "Communication theory of secrecy systems," *Bell System Technical Journal*, vol. 28, no. 4, pp. 656–715, 1949.

[10] A. D. Wyner, "The wire-tap channel," *The Bell System Technical Journal*, vol. 54, pp. 1355–1387, 1975.

[11] M. Haenggi, "The secrecy graph and some of its properties," in *Proceedings of ISIT*, 2008, pp. 539–543.

[12] X. Zhou, R. K. Ganti, and J. G. Andrews, "Secure wireless network connectivity with multi-antenna transmission," *IEEE Transactions on Wireless Communications*, vol. 10, no. 2, pp. 425–430, 2011.

[13] J. I. Choi, M. Jain, K. Srinivasan, P. Levis, and S. Katti, "Achieving single channel full duplex wireless communication," in *Proceedings of ACM Mobicom*. Chicago, Illinois, USA: ACM, 2010, pp. 1–12.

[14] P. Gupta and P. R. Kumar, "Critical power for asymptotic connectivity," in *IEEE Conference on Decision and Control, 1998*, vol. 1, 1998, pp. 1106–1110 vol.1.

[15] M. Penrose, *Random Geometric Graphs*, 1st ed. New York: Oxford University Press, 2003.

[16] C. Bettstetter and C. Hartmann, "Connectivity of wireless multihop networks in a shadow fading environment," *Wireless Networks*, vol. 11, no. 5, pp. 571–579, 2005.

[17] G. Mao and B. D. O. Anderson, "Connectivity of large wireless networks under a general connection model," *IEEE Transactions on Information Theory*, vol. 59, no. 3, pp. 1761–1772, 2013.

[18] M. Franceschetti and R. Meester, *Random Networks for Communication from Statistical Physics to Information Systems*. Cambridge University Press, 2007.

[19] O. Dousse, F. Baccelli, and P. Thiran, "Impact of interferences on connectivity in ad hoc networks," *IEEE/ACM Transactions on Networking*, vol. 13, no. 2, pp. 425–436, 2005.

[20] O. Dousse, M. Franceschetti, N. Macris, R. Meester, and P. Thiran, "Percolation in the signal to interference ratio graph," *Journal of Applied Probability*, vol. 43, no. 2, pp. 552–562, 2006.

[21] T. Yang, G. Mao, and W. Zhang, "Connectivity of large-scale csma networks," *IEEE Transactions on Wireless Communications*, vol. 11, no. 6, pp. 2266–2275, 2012.

[22] S. Goel, V. Aggarwal, A. Yener, and A. R. Calderbank, "The effect of eavesdroppers on network connectivity: A secrecy graph approach," *IEEE Transactions on Information Forensics and Security*, vol. 6, no. 3, pp. 712–724, 2011.

[23] P. C. Pinto, J. Barros, and M. Z. Win, "Secure communication in stochastic wireless networks–part ii: Maximum rate and collusion," *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 1, pp. 139–147, 2012.

[24] J. H. Conway and N. J. A. Sloane, *Sphere Packings, Lattices and Groups*, 3rd ed. New York: Springer, 1999.