Techniques for enhanced physical-layer security

Citation: Pinto, P.C., J. Barros, and M.Z. Win. "Techniques for Enhanced Physical-Layer Security." GLOBECOM 2010, 2010 IEEE Global Telecommunications Conference. 2010. 1-5. Copyright © 2010, IEEE

As Published: http://dx.doi.org/10.1109/GLOCOM.2010.5683460

Publisher: Institute of Electrical and Electronics Engineers

Persistent URL: http://hdl.handle.net/1721.1/66197

Version: Final published version: final published article, as it appeared in a journal, conference proceedings, or other formally published context

Techniques for Enhanced Physical-Layer Security

Pedro C. Pinto, *Student Member, IEEE*, João Barros, *Member, IEEE*,
and Moe Z. Win, *Fellow, IEEE*

***Abstract*—Information-theoretic security—widely accepted as the strictest notion of security—relies on channel coding techniques that exploit the inherent randomness of propagation channels to strengthen the security of communications systems. Within this paradigm, we explore strategies to improve secure connectivity in a wireless network. We first consider the *intrinsically secure communications graph* ($i\mathcal{S}$-graph), a convenient representation of the links that can be established with information-theoretic security on a large-scale network. We then propose and characterize two techniques—*sectorized transmission* and *eavesdropper neutralization*—which are shown to dramatically enhance the connectivity of the $i\mathcal{S}$-graph.**

***Index Terms*—Physical-layer security, wireless networks, secure connectivity, stochastic geometry, random graphs, node degree.**

I. Introduction

Wireless communication is particularly susceptible to eavesdropping due to the broadcast nature of the transmission medium. In current systems, security is addressed above the physical layer using cryptographic protocols (e.g., RSA and AES), which assume that an error-free physical link has already been established. In contrast with this paradigm, it is possible to take advantage of physical-layer techniques to significantly strengthen the security of communication systems. This is the basic principle of *information-theoretic security*, widely accepted as the strictest notion of security.[1] It relies on channel coding techniques that exploit the inherent randomness of propagation channels to ensure that the transmitted messages cannot be decoded by a malicious eavesdropper.

The basis for information-theoretic security, which builds on the notion of perfect secrecy [1], was laid in [2] and later in [3], [4]. More recently, there has been a renewed interest in information-theoretic security over wireless channels, from the perspective of space-time communications [5], multiple-input multiple-output communications [6]–[10], eavesdropper collusion [11], [12], cooperative relay networks [13], fading channels [14]–[18], strong secrecy [19], [20], secret key agreement [21]–[25], code design [26]–[28], among other topics. A fundamental limitation of this literature is that it only considers scenarios with a small number of nodes. To account for large-scale networks composed of multiple legitimate and eavesdropper nodes, *secrecy graphs* were introduced in [29] from a geometrical perspective, and in [30] from an information-theoretic perspective. The local connectivity of secrecy graphs was extensively characterized in [31], while the scaling laws of the secrecy capacity were presented in [32], [33]. The feasibility of long-range secure communication was proved in [34], in the context of continuum percolation.

In this paper, we explore strategies to improve secure connectivity in a wireless network. We first consider the *intrinsically secure communications graph* ($i\mathcal{S}$-graph)—a convenient representation of the links that can be established with information-theoretic security on a large network. We then propose two techniques for improving the connectivity of the $i\mathcal{S}$-graph: (i) *sectorized transmission*, whereby each legitimate node transmits independently in multiple sectors of the plane (e.g., using directional antennas); and (ii) *eavesdropper neutralization*, whereby each legitimate node guarantees the absence of eavesdroppers in a surrounding region (e.g., by deactivating such eavesdroppers). We quantify and compare the effectiveness of the proposed techniques in terms of the resulting average node degree.

This paper is organized as follows. Section II describes the system model. Section III proposes and compares techniques for enhancing the secrecy of communication. Section IV provides some numerical results. Section V summarizes important findings.

II. System Model

A. Wireless Propagation

Given a transmitter node $x_i \in \mathbb{R}^d$ and a receiver node $x_j \in \mathbb{R}^d$, we model the received power $P_{\rm rx}(x_i, x_j)$ associated with the wireless link $\overrightarrow{x_i x_j}$ as

$$P_{\rm rx}(x_i, x_j) = P \cdot g(x_i, x_j),$$

where P is the transmit power, and $g(x_i, x_j)$ is the power gain of the link $\overrightarrow{x_i x_j}$. The gain $g(x_i, x_j)$ is considered constant (quasi-static) throughout the use of the communications channel, corresponding to channels with a large coherence time. Furthermore, the function g is assumed to satisfy the following conditions, which are typically observed in practice: i) $g(x_i, x_j)$ depends on x_i and x_j only through the link length $|x_i - x_j|$;[2] ii) $g(r)$ is continuous and strictly decreasing with r; and iii) $\lim_{r\to\infty} g(r) = 0$.

B. $i\mathcal{S}$-Graph

Consider a wireless network where the legitimate nodes and the potential eavesdroppers are randomly scattered in

P. C. Pinto and M. Z. Win are with the Laboratory for Information and Decision Systems (LIDS), Massachusetts Institute of Technology, Room 32-D674, 77 Massachusetts Avenue, Cambridge, MA 02139, USA (e-mail: ppinto@alum.mit.edu, moewin@mit.edu). J. Barros is with Departamento de Engenharia Electrotécnica e de Computadores, Faculdade de Engenharia da Universidade do Porto, Portugal (e-mail: jbarros@fe.up.pt).

This research was supported, in part, by the MIT Institute for Soldier Nanotechnologies, the Office of Naval Research Presidential Early Career Award for Scientists and Engineers (PECASE) N00014-09-1-0435, and the National Science Foundation under grant ECCS-0901034.

[1] Information-theoretic security is also known as *physical-layer security,* or *intrinsic security.* In the literature, the term "security" typically encompasses three different characteristics: *secrecy* (or privacy), *integrity*, and *authenticity*. We do not consider the issues of integrity or authenticity, and use the terms "secrecy" and "security" interchangeably.

[2] With abuse of notation, we write $g(r) \triangleq g(x_i, x_j)|_{|x_i - x_j| \to r}$.

978-1-4244-5638-3/10/$26.00 ©2010 IEEE

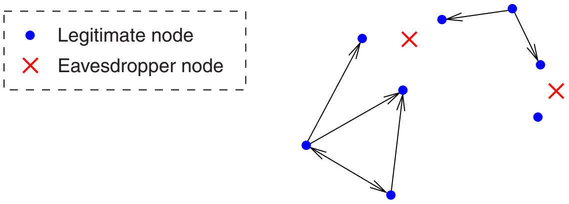

Figure 1. Example of an $i\mathcal{S}$-graph on $\mathbb{R}^2$.

space, according to some point processes. The $i\mathcal{S}$-graph is a convenient representation of the links that can be established with information-theoretic security on such a network.

Definition 2.1 ($i\mathcal{S}$-Graph [31]): Let $\Pi_\ell = \{x_i\}_{i=1}^{\infty} \subset \mathbb{R}^d$ denote the set of legitimate nodes, and $\Pi_e = \{e_i\}_{i=1}^{\infty} \subset \mathbb{R}^d$ denote the set of eavesdroppers. The *$i\mathcal{S}$-graph* is the directed graph $G = \{\Pi_\ell, \mathcal{E}\}$ with vertex set Π_ℓ and edge set

$$\mathcal{E} = \{\overrightarrow{x_i x_j} : \mathcal{R}_s(x_i, x_j) > \varrho\}, \tag{1}$$

where ϱ is a threshold representing the prescribed infimum secrecy rate for each communication link; and $\mathcal{R}_s(x_i, x_j)$ is the *maximum secrecy rate* (MSR) of the link $\overrightarrow{x_i x_j}$, given by

$$\mathcal{R}_s(x_i, x_j) = \left[\log_2\left(1 + \frac{P_{\mathrm{rx}}(x_i, x_j)}{\sigma_\ell^2}\right) - \log_2\left(1 + \frac{P_{\mathrm{rx}}(x_i, e^*)}{\sigma_e^2}\right)\right]^+$$

in bits per complex dimension, where $[x]^+ = \max\{x, 0\}$; $\sigma_\ell^2, \sigma_e^2$ are the noise powers of the legitimate users and eavesdroppers, respectively; and $e^* = \underset{e_k \in \Pi_e}{\operatorname{argmax}}\, P_{\mathrm{rx}}(x_i, e_k)$.[3]

The above definition admits an outage interpretation, in the sense that legitimate nodes set a target secrecy rate ϱ at which they transmit without knowing the channel state information (CSI) of the legitimate nodes and eavesdroppers. In this context, an edge between two nodes in the $i\mathcal{S}$-graph signifies that the corresponding channel is not in secrecy outage.

In the remainder of the paper, we consider the particular scenario where the following conditions hold: (a) the noise powers of the legitimate users and eavesdroppers are equal, i.e., $\sigma_\ell^2 = \sigma_e^2 = \sigma^2$; and (b) the infimum desired secrecy rate is zero, i.e., $\varrho = 0$.[4] Under these special conditions, the edge set in (1) simplifies to

$$\mathcal{E} = \left\{\overrightarrow{x_i x_j} : |x_i - x_j| < |x_i - e^*|, \quad e^* = \underset{e_k \in \Pi_e}{\operatorname{argmin}}\, |x_i - e_k|\right\},$$

which corresponds the geometrical model proposed in [29]. Fig. 1 shows an example of such an $i\mathcal{S}$-graph on $\mathbb{R}^2$.

The spatial location of the legitimate and eavesdropper nodes can be modeled either deterministically or stochastically. In many cases, the node positions are unknown to the network designer a priori, so they may be treated as uniformly random according to a Poisson point process [35], [36].

Definition 2.2 (Poisson $i\mathcal{S}$-Graph): The *Poisson $i\mathcal{S}$-graph* is an $i\mathcal{S}$-graph where $\Pi_\ell, \Pi_e \subset \mathbb{R}^d$ are mutually independent, homogeneous Poisson point processes with densities λ_ℓ and λ_e, respectively.

In the remainder of the paper (unless otherwise indicated), we focus on Poisson $i\mathcal{S}$-graphs on $\mathbb{R}^2$.

III. Techniques for Enhanced Secure Communication

In this section, we first characterize the connectivity of the $i\mathcal{S}$-graph without any enhancement (as introduced in Definition 2.1), and then propose two techniques for improving secure connectivity: sectorized transmission and eavesdropper neutralization. For each strategy, we characterize the *average node degree* of a typical node in the corresponding enhanced $i\mathcal{S}$-graph.[5] The average degree is a measure of secure connectivity, and is used in this paper to quantify and compare the effectiveness of each strategy.

A. Secure Communication Without Enhancement

We start by characterizing secure connectivity in the $i\mathcal{S}$-graph when no particular strategy is used.

Theorem 3.1 (No Enhancement): The out-degree N_{out} of a typical node in the Poisson $i\mathcal{S}$-graph has the following geometric probability mass function (PMF)

$$p_{N_{\mathrm{out}}}(n) = \left(\frac{\lambda_\ell}{\lambda_\ell + \lambda_e}\right)^n \left(\frac{\lambda_e}{\lambda_\ell + \lambda_e}\right), \quad n \geq 0. \tag{2}$$

In particular, the average node degrees are given by

$$\mathbb{E}\{N_{\mathrm{out}}\} = \mathbb{E}\{N_{\mathrm{in}}\} = \frac{\lambda_\ell}{\lambda_e}. \tag{3}$$

Proof: See [29], [30]. □

We observe that in the $i\mathcal{S}$-graph without enhancement, even a small density of eavesdroppers is enough to significantly disrupt connectivity. For example, if the density of eavesdroppers is half the density of legitimate nodes, then the average node degree is only $\frac{\lambda_\ell}{\lambda_e} = 2$. In what follows, we propose techniques that achieve an average degree higher than $\frac{\lambda_\ell}{\lambda_e}$.

B. Secure Communication With Sectorized Transmission

We have so far assumed that the legitimate nodes employ omnidirectional antennas, distributing power equally among all directions in space. We now let each legitimate node transmit independently in L sectors of the plane, with $L \geq 1$. This can be accomplished, for example, through the use of L directional antennas. Our goal is to characterize the impact of the number of sectors L on the local connectivity of the resulting $i\mathcal{S}$-graph.

With each node $x_i \in \Pi_\ell$, we associate L transmission sectors $\{\mathcal{S}_i^{(l)}\}_{l=1}^{L}$, defined as

$$\mathcal{S}_i^{(l)} \triangleq \left\{z \in \mathbb{R}^2 : \phi_i + (l-1)\frac{2\pi}{L} < \angle\overrightarrow{x_i z} < \phi_i + l\frac{2\pi}{L}\right\}$$

[3] This definition uses *strong secrecy* as the condition for information-theoretic security. See [19], [31, Sec. II-B] for more details.

[4] Note that by setting $\varrho = 0$ we are considering the *existence* of secure links, in the sense that an edge $\overrightarrow{x_i x_j}$ is present iff $\mathcal{R}_s(x_i, x_j) > 0$. The general case of non-zero secrecy rate threshold, $\varrho > 0$, and unequal noise powers, $\sigma_\ell^2 \neq \sigma_e^2$, can still be considered (see [31, Sec. III-E] for an analysis) but does not provide as many insights.

[5] We analyze the properties of a *typical node*, a notion which is made precise in [37, Sec. 4.4] using Palm theory. Specifically, Slivnyak's theorem states that the properties observed by a typical legitimate node $x \in \Pi_\ell$ are the same as those observed by node 0 in the process $\Pi_\ell \cup \{0\}$. Informally, a typical node of Π_ℓ is one that is uniformly picked from a finite region expanding to $\mathbb{R}^2$.

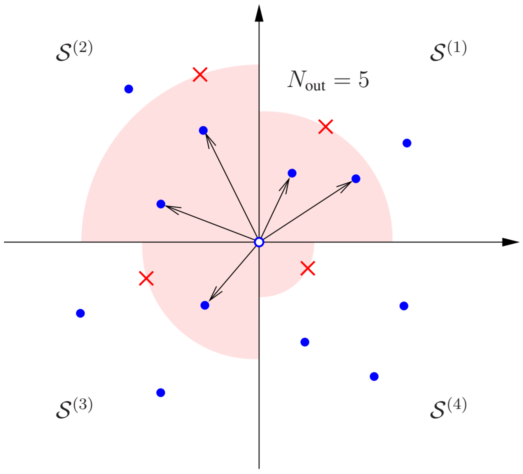

Figure 2. Secure communication with sectorized transmission. In this example with $L = 4$ sectors, the node at the origin can transmit messages with information-theoretic security to $N_{\text{out}} = 5$ nodes.

for $l = 1 \ldots L$, where $\{\phi_i\}_{i=1}^{\infty}$ are random offset angles with an arbitrary joint distribution. The resulting $i\mathcal{S}$-graph with sectorization, $G_L = \{\Pi_\ell, \mathcal{E}_L\}$, has an edge set given by

$$\mathcal{E}_L = \{\overrightarrow{x_i x_j} : |x_i - x_j| < |x_i - e^*|\},$$

where

$$e^* = \underset{e_k \in \Pi_e \cap \mathcal{S}^*}{\operatorname{argmin}} |x_i - e_k|, \qquad \mathcal{S}^* = \left\{\mathcal{S}_i^{(l)} : x_j \in \mathcal{S}_i^{(l)}\right\}.$$

Here, $\mathcal{S}^*$ is the transmission sector of x_i that contains the destination node x_j, and e^* is the eavesdropper inside $\mathcal{S}^*$ that is closest to the transmitter x_i. Then, the secure link $\overrightarrow{x_i x_j}$ exists if and only if x_j is closer to x_i than any other eavesdropper inside the same transmission sector where the destination x_j is located. The following theorem characterizes the distribution of the out-degree.

Theorem 3.2 (Sectorized Transmission): For the enhanced Poisson $i\mathcal{S}$-graph G_L with L sectors, the out-degree N_{out} of a typical node has the following negative binomial PMF

$$p_{N_{\text{out}}}(n) = \binom{L+n-1}{L-1} \left(\frac{\lambda_\ell}{\lambda_\ell + \lambda_e}\right)^n \left(\frac{\lambda_e}{\lambda_\ell + \lambda_e}\right)^L \tag{4}$$

for $n \geq 0$. In particular, the average node degrees are given by

$$\mathbb{E}\{N_{\text{out}}\} = \mathbb{E}\{N_{\text{in}}\} = L\frac{\lambda_\ell}{\lambda_e}. \tag{5}$$

Proof: We consider the process $\Pi_\ell \cup \{0\}$ obtained by adding a legitimate node to the origin of the coordinate system, and denote the out-degree of node 0 by N_{out}, as depicted in Fig. 2. Let $\mathcal{S}^{(l)}$ denote the l-th sector of node 0, where we omitted the subscript 0 for simplicity. Let $\{R_{\ell,i}^{(l)}\}_{i=1}^{\infty}$ be the distances—not necessarily ordered—between the origin and the legitimate nodes falling inside $\mathcal{S}^{(l)}$ (we similarly define $\{R_{e,i}^{(l)}\}_{i=1}^{\infty}$ for the eavesdroppers falling inside $\mathcal{S}^{(l)}$). Then, $N_{\text{out}} = \sum_{l=1}^{L} N_{\text{out}}^{(l)}$, where $N_{\text{out}}^{(l)} \triangleq \#\{R_{\ell,i}^{(l)} : R_{\ell,i}^{(l)} < \min_k R_{e,k}^{(l)}\}$ is the out-degree of node 0 associated with sector l. Furthermore, the random variables (RVs) $\{N_{\text{out}}^{(l)}\}$ are independent identically distributed (IID) for different l.[6] To determine the PMF of $N_{\text{out}}^{(l)}$, we use the fact that $\{(R_{\ell,i}^{(l)})^2\}_{i=1}^{\infty}$ and $\{(R_{e,i}^{(l)})^2\}_{i=1}^{\infty}$ are homogeneous Poisson processes with rates $\frac{\pi\lambda_\ell}{L}$ and $\frac{\pi\lambda_e}{L}$, respectively (by the mapping theorem [35, Sec. 2.3]). Following steps analogous to the proof of [30, Thm. 3.1], it is easy to show that $N_{\text{out}}^{(l)}$ has a geometric PMF given by $p_{N_{\text{out}}^{(l)}}(n) = p^n(1-p)$, $n \geq 0$, with $p = \frac{\lambda_\ell}{\lambda_\ell + \lambda_e}$. Now, since the RVs $\{N_{\text{out}}^{(l)}\}$ are IID in l, the total out-degree N_{out} has a negative binomial PMF with L degrees of freedom and the same parameter p, i.e., $p_{N_{\text{out}}}(n) = \binom{L+n-1}{L-1} p^n (1-p)^L$, $n \geq 0$, with $p = \frac{\lambda_\ell}{\lambda_\ell + \lambda_e}$. This is the result in (4), from which (5) follows trivially. □

We conclude that the average node degree increases *linearly* with the number of sectors L, and hence sectorized transmission is an effective technique for enhancing the secrecy of communications. Figure 2 provides an intuitive understanding of why sectorization works. Specifically, if there was no sectorization, node 0 would be out-isolated, due to the close proximity of the eavesdropper in sector $\mathcal{S}^{(4)}$. However, if we allow independent transmissions in four non-overlapping sectors, that same eavesdropper can only hear the transmissions inside sector $\mathcal{S}^{(4)}$. Thus, even though node 0 is out-isolated with respect to sector $\mathcal{S}^{(4)}$, it may still communicate securely with some legitimate nodes inside sectors $\mathcal{S}^{(1)}$, $\mathcal{S}^{(2)}$, and $\mathcal{S}^{(3)}$. Lastly, note that for $L = 1$ (i.e., no enhancement), Theorem 3.2 reduces to Theorem 3.1 as expected.

C. Secure Communication With Eavesdropper Neutralization

In some scenarios, each legitimate node may be able to physically inspect its surroundings and deactivate the eavesdroppers falling inside some neutralization region. Our goal is to characterize the impact of such region on the local connectivity of the resulting $i\mathcal{S}$-graph.

With each node $x_i \in \Pi_\ell$, we associate a *neutralization region* Θ_i inside which all eavesdroppers have been deactivated. The *total neutralization region* Θ can then be seen as a Boolean model with points $\{x_i\}$ and associated sets $\{\Theta_i\}$, i.e., [37]

$$\Theta = \bigcup_{i=1}^{\infty} (x_i + \Theta_i).$$

Since the eavesdroppers inside Θ have been deactivated, the *effective eavesdropper process* after neutralization is $\Pi_e \cap \overline{\Theta}$, where $\overline{\Theta} \triangleq \mathbb{R}^2 \backslash \Theta$ denotes the complement of Θ. The resulting $i\mathcal{S}$-graph with neutralization, $G_\Theta = \{\Pi_\ell, \mathcal{E}_\Theta\}$, has an edge set given by

$$\mathcal{E}_\Theta = \left\{\overrightarrow{x_i x_j} : |x_i - x_j| < |x_i - e^*|, \quad e^* = \underset{e_k \in \Pi_e \cap \overline{\Theta}}{\operatorname{argmin}} |x_i - e_k|\right\}$$

i.e., the secure link $\overrightarrow{x_i x_j}$ exists if and only if x_j is closer to x_i than any other eavesdropper that has not been neutralized. In the following, we consider the case of a circular neutralization set, i.e, $\Theta_i = \mathcal{B}_0(\rho)$, where ρ is a deterministic *neutralization radius*, and denote the corresponding graph by G_ρ.[7]

Theorem 3.3 (Eavesdropper Neutralization): For the enhanced Poisson $i\mathcal{S}$-graph G_ρ with neutralization radius ρ,

[6] This is because the sectors $\{\mathcal{S}^{(l)}\}_{l=1}^{L}$ correspond to an equipartition of $\mathbb{R}^2$, and the processes Π_ℓ, Π_e are homogeneous Poisson.

[7] We use $\mathcal{B}_x(\rho) \triangleq \{y \in \mathbb{R}^2 : |y - x| \leq \rho\}$ to denote the closed two-dimensional ball centered at point x, with radius ρ.

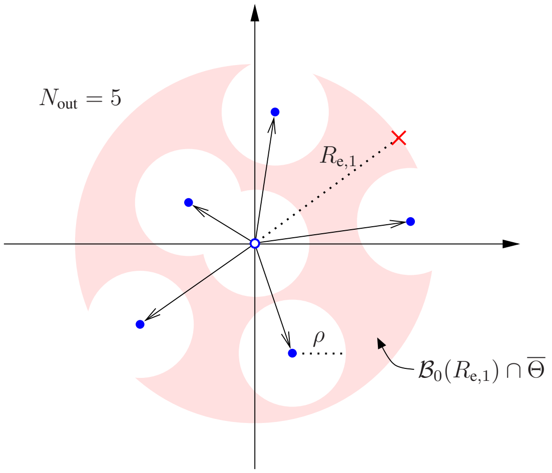

Figure 3. Secure communication with eavesdropper neutralization. In this example, the node at the origin can transmit messages with information-theoretic security to $N_{\mathrm{out}} = 5$ nodes.

the average node degrees of a typical node are lower-bounded by

$$\mathbb{E}\{N_{\mathrm{out}}\} = \mathbb{E}\{N_{\mathrm{in}}\} \ge \frac{\lambda_\ell}{\lambda_{\mathrm{e}}}\left(\pi\lambda_{\mathrm{e}}\rho^2 + e^{\pi\lambda_\ell\rho^2}\right). \tag{6}$$

Proof: We consider the process $\Pi_\ell \cup \{0\}$ obtained by adding a legitimate node to the origin of the coordinate system, and denote the out-degree of node 0 by N_{out}, as depicted in Fig. 3. Let $R_{\mathrm{e},1} \triangleq \min_{e_k \in \Pi_{\mathrm{e}} \cap \overline{\Theta}} |e_k|$ be the random distance between the first non-neutralized eavesdropper and the origin. Noting that

$$N_{\mathrm{out}} = \sum_{x_i \in \Pi_\ell} \mathbb{1}\{|x_i| < R_{\mathrm{e},1}\} = \iint_{\mathbb{R}^2} \mathbb{1}\{|x| < R_{\mathrm{e},1}\}\Pi_\ell(dx),$$

we can use Fubini's theorem to write

$$\begin{aligned}\mathbb{E}\{N_{\mathrm{out}}\} &= \lambda_\ell \iint_{\mathbb{R}^2} \mathbb{P}_x\{|x| < R_{\mathrm{e},1}\}dx \\ &= \lambda_\ell\pi\rho^2 + \lambda_\ell \iint_{\mathcal{D}(\rho,\infty)} \mathbb{P}_x\{|x| < R_{\mathrm{e},1}\}dx, \end{aligned} \tag{7}$$

where $\mathcal{D}(a,b) \triangleq \{x \in \mathbb{R}^2 : a \le |x| \le b\}$ denotes the annulus centered at the origin, with inner radius a and outer radius b; and $\mathbb{P}_x\{\cdot\}$ is the Palm probability associated with point x of process Π_ℓ.[8] Appendix A shows that the integrand above satisfies

$$\mathbb{P}_x\{|x| < R_{\mathrm{e},1}\} \ge \exp\left(-\pi\lambda_{\mathrm{e}}e^{-\lambda_\ell\pi\rho^2}(|x|^2 - \rho^2)\right). \tag{8}$$

Replacing (8) into (7), we have

$$\begin{aligned}\mathbb{E}\{N_{\mathrm{out}}\} &\ge \lambda_\ell\pi\rho^2 + \lambda_\ell \iint_{\mathcal{D}(\rho,\infty)} \exp\left(-\pi\lambda_{\mathrm{e}}e^{-\lambda_\ell\pi\rho^2}(|x|^2 - \rho^2)\right)dx \\ &= \lambda_\ell\pi\rho^2 + \frac{\lambda_\ell}{\lambda_{\mathrm{e}}}e^{\lambda_\ell\pi\rho^2}.\end{aligned}$$

Rearranging terms and noting that $\mathbb{E}\{N_{\mathrm{out}}\} = \mathbb{E}\{N_{\mathrm{in}}\}$, we obtain (6). □

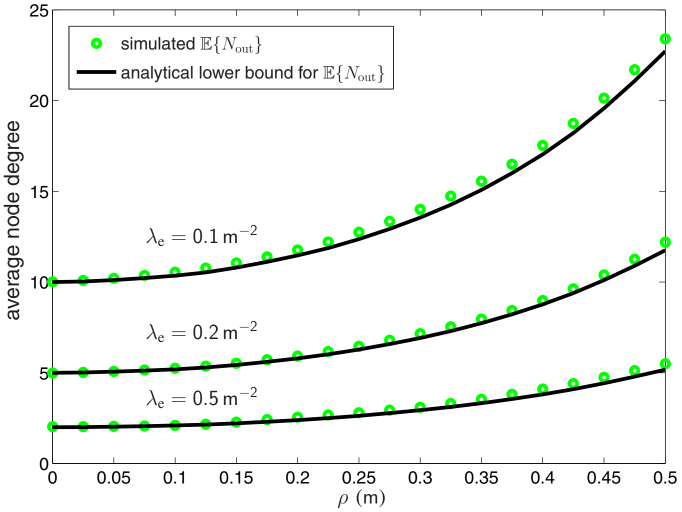

Figure 4. Average node degree versus the neutralization radius ρ, for various values of λ_{e} ($\lambda_\ell = 1\,\mathrm{m}^{-2}$).

We conclude that the average node degree increases at a rate that is at least *exponential* with the neutralization radius ρ, making eavesdropper neutralization an effective technique for enhancing the secrecy of communications.

IV. Numerical Results

Figure 4 illustrates the effectiveness of eavesdropper neutralization in enhancing secure connectivity. In particular, it plots the average node degree versus the neutralization radius ρ, for various values of λ_{e}. We observe that the analytical lower-bound for $\mathbb{E}\{N_{\mathrm{out}}\}$ given in (6) is very close to the actual value of $\mathbb{E}\{N_{\mathrm{out}}\}$ obtained through Monte Carlo simulation. The lower-bound becomes tight in the following two extreme cases:

1) $\rho = 0$: This corresponds to the case of no enhancement, so from (3) we have $\mathbb{E}\{N_{\mathrm{out}}\} = \frac{\lambda_\ell}{\lambda_{\mathrm{e}}}$. Since the bound in (6) also equals $\frac{\lambda_\ell}{\lambda_{\mathrm{e}}}$ for $\rho = 0$, it is tight.
2) $\lambda_{\mathrm{e}} \to \infty$: In the limit, at least one eavesdropper will fall almost surely inside the annulus $\mathcal{D}(\rho, \rho+\epsilon)$, for any $\epsilon > 0$. As a result, $\mathbb{E}\{N_{\mathrm{out}}\}$ approaches the average number of legitimate nodes inside the ball $\mathcal{B}_0(\rho)$, i.e., $\lambda_\ell\pi\rho^2$. Since the bound in (6) also approaches $\lambda_\ell\pi\rho^2$ as $\lambda_{\mathrm{e}} \to \infty$, it is asymptotically tight.

V. Conclusions

In this paper, we proposed two techniques shown to dramatically enhance the connectivity of the $i\mathcal{S}$-graph: *sectorized transmission* and *eavesdropper neutralization*. We proved that if each legitimate node is able to transmit independently in L sectors of the plane, the average node degree increases *linearly* with L. On the other hand, if each legitimate node is able to neutralize all eavesdroppers within a radius ρ, the average degree increases *at least exponentially* with ρ. We are hopeful that further efforts will provide an understanding of how *long-range* secure communication is improved by the two proposed strategies. For example, the effect of L and ρ on the critical densities for continuum percolation is still unknown, as is their effect on the secrecy capacity scaling laws.

[8] Informally, the Palm probability $\mathbb{P}_x\{\cdot\}$ can be interpreted as the conditional probability $\mathbb{P}\{\cdot|x \in \Pi_\ell\}$. Since the conditioning event has probability zero, such conditional probability is ambiguous without further explanation. Palm theory makes this notion mathematically precise (see [37, Sec. 4.4] for a detailed treatment).

APPENDIX A
DERIVATION OF (8)

Because Π_ℓ is a Poisson process, the Palm probability $\mathbb{P}_x\{|x| < R_{\text{e},1}\}$ in (7) can be computed using Slivnyak's theorem by adding a legitimate node at location x to Π_ℓ. For a fixed $x \in \mathcal{D}(\rho, \infty)$, we can thus write

$$\begin{aligned}\mathbb{P}_x\{|x| < R_{\text{e},1}\} &= \mathbb{P}_{\Theta,\Pi_\text{e}}\{\Pi_\text{e}\{\overline{\Theta} \cap \mathcal{D}(\rho, |x|)\backslash\mathcal{B}_x(\rho)\} = 0\} \\ &\geq \mathbb{P}_{\Theta,\Pi_\text{e}}\{\Pi_\text{e}\{\overline{\Theta} \cap \mathcal{D}(\rho, |x|)\} = 0\} \\ &= \mathbb{E}_\Theta\{\exp(-\lambda_\text{e}\mathbb{A}\{\overline{\Theta} \cap \mathcal{D}(\rho, |x|)\}\} \qquad (9) \\ &\geq \exp(-\lambda_\text{e}\mathbb{E}_\Theta\{\mathbb{A}\{\overline{\Theta} \cap \mathcal{D}(\rho, |x|)\}\}), \qquad (10)\end{aligned}$$

where $\mathbb{A}\{\mathcal{R}\}$ to denotes the area of the arbitrary region $\mathcal{R}$. Equation (9) follows from conditioning on Θ, and using the fact that Π_e and Θ are independent. Equation (10) follows from Jensen's inequality. The term inside the exponential in (10) corresponds to the average area of a random shape, and can be computed using Fubini's theorem as

$$\begin{aligned}&\mathbb{E}_\Theta\{\mathbb{A}\{\overline{\Theta} \cap \mathcal{D}(\rho, |x|)\}\} \\ &\qquad = \mathbb{E}_\Theta\left\{\iint_{\mathbb{R}^2} \mathbb{1}\{y \in \overline{\Theta} \cap \mathcal{D}(\rho, |x|)\}dy\right\} \\ &\qquad = \iint_{\mathcal{D}(\rho,|x|)} \mathbb{P}\{y \in \overline{\Theta}\}dy \\ &\qquad = \iint_{\mathcal{D}(\rho,|x|)} \mathbb{P}\{\Pi_\ell\{\mathcal{B}_y(\rho)\} = 0\}dy \\ &\qquad = \iint_{\mathcal{D}(\rho,|x|)} e^{-\lambda_\ell \pi \rho^2}dy \\ &\qquad = \pi(|x|^2 - \rho^2)e^{-\lambda_\ell \pi \rho^2}. \qquad (11)\end{aligned}$$

Replacing (11) into (10), we obtain the desired inequality in (8).

REFERENCES

[1] C. E. Shannon, "Communication theory of secrecy systems," *Bell System Technical Journal*, vol. 29, pp. 656–715, 1949.

[2] A. D. Wyner, "The Wire-Tap Channel," *Bell System Technical Journal*, vol. 54, no. 8, pp. 1355–1367, October 1975.

[3] I. Csiszár and J. Korner, "Broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 24, no. 3, pp. 339–348, 1978.

[4] S. Leung-Yan-Cheong and M. Hellman, "The Gaussian wire-tap channel," *IEEE Trans. Inf. Theory*, vol. 24, no. 4, pp. 451–456, July 1978.

[5] A. Hero, "Secure space-time communication," *IEEE Transactions on Information*, vol. 49, no. 12, pp. 3235–3249, Dec. 2003.

[6] R. Negi and S. Goel, "Secret communication using artificial noise," in *Proc. IEEE Vehicular Technology Conference*, vol. 3, Dallas, TX, Sept. 2005, pp. 1906–1910.

[7] E. Ekrem and S. Ulukus, "Secrecy capacity region of the gaussian multi-receiver wiretap channel," in *Proc. IEEE Int. Symp. on Inf. Theory*, Seoul, Korea, June 2009, pp. 2612–2616.

[8] T. Liu and S. Shamai, "A note on the secrecy capacity of the multiple-antenna wiretap channel," *IEEE Trans. Inf. Theory*, vol. 55, no. 6, pp. 2547–2553, June 2009.

[9] H. Weingarten, T. Liu, S. Shamai, Y. Steinberg, and P. Viswanath, "The capacity region of the degraded multiple-input multiple-output compound broadcast channel," *IEEE Trans. Inf. Theory*, vol. 55, no. 11, pp. 5011–5023, Nov. 2009.

[10] L. Zhang, R. Zhang, Y. Liang, Y. Xin, and S. Cui, "On the relationship between the multi-antenna secrecy communications and cognitive radio communications," in *Proc. Allerton Conf. on Communications, Control, and Computing*, Monticello, IL, Sept. 2009.

[11] S. Goel and R. Negi, "Secret communication in presence of colluding eavesdroppers," in *Proc. Military Commun. Conf.*, Oct. 2005, pp. 1501–1506.

[12] P. C. Pinto, J. O. Barros, and M. Z. Win, "Wireless physical-layer security: The case of colluding eavesdroppers," in *Proc. IEEE Int. Symp. on Inf. Theory*, Seoul, South Korea, July 2009, pp. 2442–2446.

[13] E. Ekrem and S. Ulukus, "Secrecy in cooperative relay broadcast channels," in *Proc. IEEE Int. Symp. on Inf. Theory*, Toronto, ON, July 2008, pp. 2217–2221.

[14] P. Parada and R. Blahut, "Secrecy capacity of SIMO and slow fading channels," in *Proc. IEEE Int. Symp. on Inf. Theory*, Adelaide, Australia, Sept. 2005, pp. 2152–2155.

[15] P. Gopala, L. Lai, and H. El Gamal, "On the Secrecy Capacity of Fading Channels," arxiv preprint cs.IT/0610103, 2006.

[16] Z. Li, R. Yates, and W. Trappe, "Secrecy capacity of independent parallel channels," *Proc. Annu. Allerton Conf. Communication, Control and Computing*, pp. 841–848, Sept. 2006.

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

[18] Y. Liang, H. V. Poor, and S. Shamai, "Secure communication over fading channels," *IEEE Trans. Inf. Theory*, vol. 54, pp. 2470–2492, June 2008.

[19] U. Maurer and S. Wolf, "Information-theoretic key agreement: From weak to strong secrecy for free," *Eurocrypt 2000, Lecture Notes in Computer Science*, vol. 1807, pp. 351+, 2000.

[20] J. Barros and M. Bloch, "Strong secrecy for wireless channels," in *Proc. International Conf. on Inf. Theor. Security*, Calgary, Canada, Aug. 2008.

[21] U. Maurer, "Secret key agreement by public discussion from common information," *IEEE Trans. Inf. Theory*, vol. 39, no. 3, pp. 733–742, May 1993.

[22] R. Ahlswede and I. Csiszar, "Common randomness in information theory and cryptography - Part I: Secret sharing," *IEEE Trans. Inf. Theory*, vol. 39, no. 4, pp. 1121–1132, July 1993.

[23] C. H. Bennett, G. Brassard, C. Crépeau, and U. Maurer, "Generalized privacy amplification," *IEEE Trans. Inf. Theory*, vol. 41, no. 6, pp. 1915–1923, 1995.

[24] U. M. Maurer and S. Wolf, "Unconditionally secure key agreement and intrinsic conditional information," *IEEE Trans. Inf. Theory*, vol. 45, no. 2, pp. 499–514, March 1999.

[25] M. Bloch, A. Thangaraj, S. W. McLaughlin, and J.-M. Merolla, "LDPC-based secret key agreement over the gaussian wiretap channel," in *Proc. IEEE Int. Symp. on Inf. Theory*, Seattle, USA, 2006.

[26] A. Thangaraj, S. Dihidar, A. R. Calderbank, S. W. McLaughlin, and J.-M. Merolla, "Applications of LDPC codes to the wiretap channel," *IEEE Trans. Inf. Theory*, vol. 53, no. 8, pp. 2933–2945, Aug. 2007.

[27] R. Liu, Y. Liang, H. V. Poor, and P. Spasojevic, "Secure nested codes for type II wiretap channels," in *Proc. IEEE Inf. Theory Workshop*, Tahoe City, CA, Sept. 2007, pp. 337–342.

[28] J. Muramatsu, "Secret key agreement from correlated source outputs using low density parity check matrices," *IEICE Trans. on Fund. of Elec. Comm. Comp.*, vol. E89-A, no. 7, pp. 2036–2046, July 2006.

[29] M. Haenggi, "The secrecy graph and some of its properties," in *Proc. IEEE Int. Symp. on Inf. Theory*, Toronto, Canada, July 2008.

[30] P. C. Pinto, J. O. Barros, and M. Z. Win, "Physical-layer security in stochastic wireless networks," in *Proc. IEEE Int. Conf. on Commun. Systems*, Guangzhou, China, Nov. 2008, pp. 974–979.

[31] ——, "Secure communication in stochastic wireless networks," *IEEE Trans. Inf. Theory*, pp. 1–59, 2009, submitted for publication, preprint available on arXiv:1001.3697.

[32] Y. Liang, H. V. Poor, and L. Ying, "Secrecy throughput of MANETs with malicious nodes," in *Proc. IEEE Int. Symp. on Inf. Theory*, June 2009, pp. 1189–1193.

[33] O. O. Koyluoglu, C. E. Koksal, and H. E. Gamal, "On secrecy capacity scaling in wireless networks," in *Inf. Theory and Applications Workshop*, San Diego, CA, Feb. 2010, pp. 1–4.

[34] P. C. Pinto and M. Z. Win, "Continuum percolation in the intrinsically secure communications graph," in *Proc. IEEE Int. Symp. on Inf. Theory and Its Applications*, Taichung, Taiwan, Oct. 2010, pp. 1–6.

[35] J. Kingman, *Poisson Processes*. Oxford University Press, 1993.

[36] M. Haenggi, J. G. Andrews, F. Baccelli, O. Dousse, and M. Franceschetti, "Stochastic geometry and random graphs for the analysis and design of wireless networks," *IEEE J. Sel. Areas Commun.*, vol. 27, no. 7, pp. 1029–1046, 2009.

[37] D. Stoyan, W. S. Kendall, and J. Mecke, *Stochastic geometry and its applications*. John Wiley & Sons, 1995.