Secure Communication in Stochastic Wireless Networks—Part I: Connectivity

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

***Abstract*—The ability to exchange secret information is critical to many commercial, governmental, and military networks. Information-theoretic security—widely accepted as the strictest notion of security—relies on channel coding techniques that exploit the inherent randomness of the propagation channels to strengthen the security of digital communications systems. Motivated by recent developments in the field, we aim to characterize the fundamental secrecy limits of wireless networks. The paper is comprised of two separate parts. In Part I, we define the *intrinsically secure communications graph* ($i\mathcal{S}$-graph), a random graph which describes the connections that can be securely established over a large-scale network. We provide conclusive results for the local connectivity of the Poisson $i\mathcal{S}$-graph, in terms of node degrees and isolation probabilities. We show how the secure connectivity of the network varies with the wireless propagation effects, the secrecy rate threshold of each link, and the noise powers of legitimate nodes and eavesdroppers. We then propose sectorized transmission and eavesdropper neutralization as viable strategies for improving the secure connectivity. Our results help clarify how the spatial density of eavesdroppers can compromise the intrinsic security of wireless networks. In Part II of the paper, we study the achievable secrecy rates and the effect of eavesdropper collusion.**

***Index Terms*—Node degree, physical-layer security, secure connectivity, stochastic geometry, wireless networks.**

I. Introduction

CONTEMPORARY security systems for wireless networks are based on cryptographic primitives that generally ignore two key factors: a) the physical properties of the wireless medium, and b) the spatial configuration of both the legitimate and malicious nodes. These two factors are important since they affect the communication channels between the nodes, which in turn determine the fundamental secrecy limits of a wireless network. In fact, the inherent randomness associated with the wireless medium and the spatial location of the nodes can be leveraged to provide *intrinsic security* of the communications infrastructure at the physical-layer level.[1]

The basis for information-theoretic security, which builds on the notion of perfect secrecy [1], was laid in [2] and later in [3] and [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], cooperative relay networks [12], fading channels [13]–[17], strong secrecy [18], [19], secret key agreement [20]–[23], code design [24]–[27], 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 [28] from a geometrical perspective, and in [29] from an information-theoretic perspective. The scaling laws of the secrecy capacity were presented in [30] and [31].

In this paper, we aim at a mathematical characterization of the secrecy properties of stochastic wireless networks. The main contributions are as follows:

1) *Framework for intrinsic security in stochastic networks*: We propose and define the "intrinsically secure communications graph" ($i\mathcal{S}$-graph), based on the notion of strong secrecy. Our framework considers spatially scattered users and eavesdroppers, subject to generic wireless propagation characteristics.
2) *Local connectivity in the $i\mathcal{S}$-graph*: We provide a complete probabilistic characterization of both in-degree and out-degree of a typical node in the Poisson $i\mathcal{S}$-graph, using fundamental tools of stochastic geometry.
3) *Techniques for communication with enhanced secrecy*: We propose sectorized transmission and eavesdropper neutralization as two techniques for enhancing the secrecy of communication, and quantify their effectiveness in terms of the resulting average node degrees.

In Part II of the paper [32], we study the achievable secrecy rates and the effect of eavesdropper collusion.

This paper is organized as follows. Section II describes the system model. Section III characterizes local connectivity in the

[1]In the literature, the term "security" typically encompasses three different characteristics: *secrecy* (or privacy), *integrity*, and *authenticity*. This paper does not consider the issues of integrity or authenticity, and the terms "secrecy" and "security" are used interchangeably.

Manuscript received February 08, 2011; revised June 13, 2011; accepted August 08, 2011. Date of publication August 22, 2011; date of current version January 13, 2012. This work was supported, in part by the Portuguese Science and Technology Foundation under Grant SFRH-BD-17388-2004, in part by the MIT Institute for Soldier Nanotechnologies, in part by the Office of Naval Research under Presidential Early Career Award for Scientists and Engineers (PECASE) N00014-09-1-0435, and in part by the National Science Foundation under Grant ECS-0636519. This work was presented, in part, at the IEEE International Conference on Communications Systems (ICCS'08) Guangzhou, China, Nov. 2008, and at the IEEE Global Telecommunications Conference, Miami, FL, Dec. 2010. The associate editor coordinating the review of this manuscript and approving it for publication was Prof. Wade Trappe.

P. C. Pinto is with the Swiss Federal Institute of Technology (EPFL), EPFL-IC-LCAV, CH-1015, Lausanne, Switzerland (e-mail: pedro.pinto@epfl.ch).

J. Barros is with DEEC, Faculdade de Engenharia da Universidade do Porto (FEUP), 4200-465 Porto, Portugal (e-mail: jbarros@fe.up.pt).

M. Z. Win is with the Laboratory for Information and Decision Systems (LIDS), Massachusetts Institute of Technology, Cambridge, MA 02139 USA (e-mail: moewin@mit.edu).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TIFS.2011.2165946

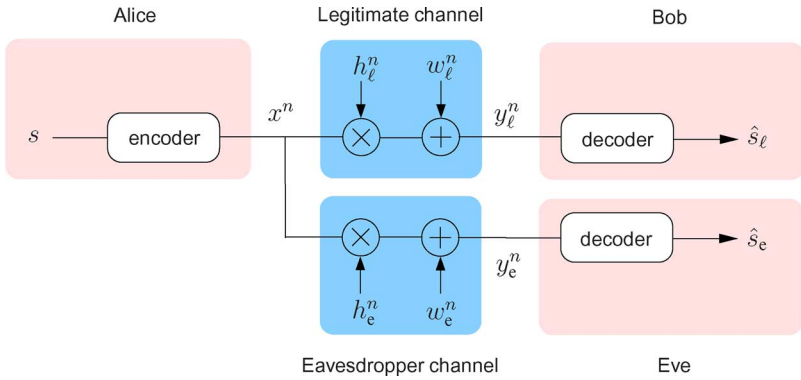

Fig. 1. Wireless wiretap channel.

Poisson $i\mathcal{S}$-graph. Section IV analyzes two techniques for enhancing the secrecy of communication. Section V concludes the paper and summarizes important findings.

II. System Model

We start by describing our system model and defining our measures of secrecy.

A. Wireless Propagation Characteristics

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 $P_{rx}(x_i, x_j)$ associated with the wireless link $\overrightarrow{x_i x_j}$ as

$$P_{rx}(x_i, x_j) = P_\ell \cdot g\left(x_i, x_j, Z_{x_i,x_j}\right) \tag{1}$$

where P_ℓ is the (common) transmit power of the legitimate nodes; and $g(x_i, x_j, Z_{x_i,x_j})$ is the power gain of the link $\overrightarrow{x_i x_j}$, where the random variable (RV) Z_{x_i,x_j} represents the random propagation effects associated with link $\overrightarrow{x_i x_j}$ (such as multipath fading or shadowing). We consider that the $Z_{x_i,x_j}, x_i \neq x_j$ are independent identically distributed (i.i.d.) RVs with common probability density function (pdf) $f_Z(z)$, and that $Z_{x_i,x_j} = Z_{x_j,x_i}$ due to channel reciprocity. The channel gain $g(x_i, x_j, Z_{x_i,x_j})$ is considered constant (quasi-static) throughout the use of the communications channel, which corresponds to channels with a large coherence time. The gain function is assumed to satisfy the following conditions:

1) $g(x_i, x_j, Z_{x_i,x_j})$ depends on x_i and x_j only through the link length $|x_i - x_j|$; with abuse of notation, we can write $g(r, z) \triangleq g(x_i, x_j, z)|_{|x_i - x_j| \to r}$.[2]
2) $g(r, z)$ is continuous and strictly decreasing in r.
3) $\lim_{r\to\infty} g(r, z) = 0$.

The proposed model is general enough to account for common choices of g. One example is the unbounded model where $g(r, z) = z/r^{2b}$. The term $1/r^{2b}$ accounts for the far-field path loss with distance, where the amplitude loss exponent b is environment-dependent and can approximately range from 0.8 (e.g., hallways inside buildings) to 4 (e.g., dense urban environments), with $b = 1$ corresponding to free-space propagation. This model is analytically convenient [33], but since the gain becomes unbounded as the distance approaches zero, it must be used with care for extremely dense networks. Another example is the bounded model where $g(r, z) = z/(1 + r^{2b})$. This model has the same far-field dependence as the unbounded model, but eliminates the singularity at the origin [34]. Unfortunately, it often leads to intractable analytical results. Furthermore, by appropriately choosing of the distribution of Z_{x_i,x_j}, both models can account for various random propagation effects, including Nakagami-m fading, Rayleigh fading, and log-normal shadowing [33].

[2]For notational simplicity, when $Z = 1$ we omit the second argument of the function $g(r, z)$ and simply use $g(r)$.

B. Wireless Information-Theoretic Security

We now define our measure of secrecy more precisely. While our main interest is in the behavior of large-scale networks, we briefly review the setup for a single legitimate link with a single eavesdropper. The results thereof will serve as a basis for the notion of $i\mathcal{S}$-graph to be established later.

Consider the model depicted in Fig. 1, where a legitimate user (Alice) wants to send messages to another user (Bob). Alice encodes a message s, represented by a discrete RV, into a codeword, represented by the complex random sequence of length n, $x^n = (x(1), \ldots, x(n)) \in \mathbb{C}^n$, for transmission over the channel. Bob observes the output of a discrete-time channel (the *legitimate channel*), which at time i is given by

$$y_\ell(i) = h_\ell \cdot x(i) + w_\ell(i), \quad 1 \leq i \leq n$$

where $h_\ell \in \mathbb{C}$ is the quasi-static amplitude gain of the legitimate channel,[3] and $w_\ell(i) \sim \mathcal{N}_c(0, \sigma_\ell^2)$ is AWGN with power σ_ℓ^2 per complex sample.[4] Bob makes a decision $\hat{s}_\ell$ on s based on the output y_ℓ, incurring in an error probability equal to $\mathbb{P}\{\hat{s}_\ell \neq s\}$. A third party (Eve) is also capable of eavesdropping on Alice's transmissions. Eve observes the output of a discrete-time channel (the *eavesdropper's channel*), which at time i is given by

$$y_e(i) = h_e \cdot x(i) + w_e(i), \quad 1 \leq i \leq n$$

[3]The amplitude gain h_ℓ can be related to the power gain in (1) as $g(r_\ell, Z_\ell) = |h_\ell|^2$, where r_ℓ and Z_ℓ are, respectively, the length and random propagation effects of the legitimate link.

[4]We use $\mathcal{N}(\mu, \sigma^2)$ to denote a Gaussian distribution with mean μ and variance σ^2. Furthermore, we use $\mathcal{N}_c(0, \sigma^2)$ to denote a circularly symmetric (CS) complex Gaussian distribution, where the real and imaginary parts are i.i.d. $\mathcal{N}(0, \sigma^2/2)$.

where $h_e \in \mathbb{C}$ is the quasi-static amplitude gain of the eavesdropper channel, and $w_e(i) \sim \mathcal{N}_c(0, \sigma_e^2)$ is AWGN with power σ_e^2 per complex sample. It is assumed that the signals x, h_ℓ, h_e, w_ℓ, and w_e are mutually independent. Each codeword transmitted by Alice is subject to the average power constraint of P_ℓ per complex symbol, i.e., $(1/n)\sum_{i=1}^{n} \mathbb{E}\{|x(i)|^2\} \leq P_\ell$. We define the rate of transmission to be $\mathcal{R} \triangleq (H(s)/n)$, where $H(\cdot)$ denotes the entropy function. Throughout the paper, we use *strong secrecy* as the condition for information-theoretic security, and define it as follows [18].

Definition 2.1 (Strong Secrecy): The rate $\mathcal{R}^*$ is said to be *achievable with strong secrecy* if $\forall \epsilon > 0$, for sufficiently large n, there exists an encoder–decoder pair with rate $\mathcal{R}$ satisfying the following conditions:

$$\begin{aligned} \mathcal{R} &\geq \mathcal{R}^* - \epsilon \\ H\left(s|y_e^n\right) &\geq H(s) - \epsilon \\ \mathbb{P}\{\hat{s}_\ell \neq s\} &\leq \epsilon. \end{aligned}$$

We define the *maximum secrecy rate* (MSR) $\mathcal{R}_s$ of the legitimate channel to be the maximum rate $\mathcal{R}^*$ that is achievable with strong secrecy.[5] If the legitimate link operates at a rate below the MSR $\mathcal{R}_s$, there exists an encoder–decoder pair such that the eavesdropper is unable to obtain additional information about s from the observation y_e^n, in the sense that $H(s|y_e^n)$ approaches $H(s)$ as the codeword length n grows. It was shown in [4] and [16] that for a given realization of the channel gains h_ℓ, h_e, the MSR of the Gaussian wiretap channel is

$$\mathcal{R}_s = \left[\log_2\left(1 + \frac{P_\ell \cdot |h_\ell|^2}{\sigma_\ell^2}\right) - \log_2\left(1 + \frac{P_\ell \cdot |h_e|^2}{\sigma_e^2}\right)\right]^+ \tag{2}$$

in bits per complex dimension, where $[x]^+ = \max\{x, 0\}$.[6] In the next sections, we use these basic results to analyze secrecy in large-scale networks.

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

Consider a wireless network where legitimate nodes and potential eavesdroppers are randomly scattered in space, according to some point process. The $i\mathcal{S}$-graph is a convenient representation of the information-theoretically secure links that can be established on such networks. In the following, we introduce a precise definition of the $i\mathcal{S}$-graph, based on the notion of strong secrecy.

Definition 2.2 ($i\mathcal{S}$-Graph): 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

$$\mathcal{E} = \left\{\overrightarrow{x_i x_j} : \mathcal{R}_s(x_i, x_j) > \varrho\right\} \tag{3}$$

[5]See [19] for a comparison between the concepts of weak and strong secrecy. In the case of Gaussian noise, the MSR is *the same* under the weak and strong secrecy conditions.

[6]Operationally, the MSR $\mathcal{R}_s$ can be achieved if Alice first estimates h_ℓ and h_e (i.e., has full CSI), and then uses a code that achieves MSR in the AWGN channel. Estimation of h_e is possible, for instance, when Eve is another active user in the wireless network, so that Alice can estimate the eavesdropper's channel during Eve's transmissions. As we shall see, the $i\mathcal{S}$-graph model presented in this paper relies on an outage formulation, and therefore does *not* make assumptions concerning availability of full CSI.

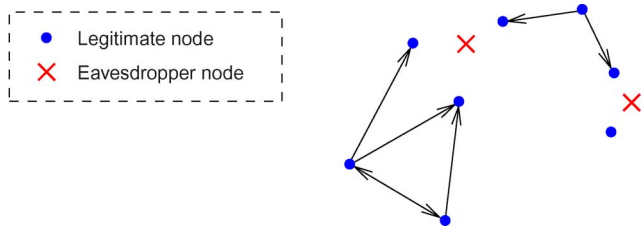

Fig. 2. Example of an $i\mathcal{S}$-graph on $\mathbb{R}^2$.

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 MSR of the link $\overrightarrow{x_i x_j}$ for a given realization of the channel gains, given by

$$\mathcal{R}_s(x_i, x_j) = \left[\log_2\left(1 + \frac{P_{rx}(x_i, x_j)}{\sigma_\ell^2}\right) - \log_2\left(1 + \frac{P_{rx}(x_i, e^*)}{\sigma_e^2}\right)\right]^+ \tag{4}$$

with $e^* = \arg\max_{e_k \in \Pi_e} P_{rx}(x_i, e_k)$.

This definition presupposes that the eavesdroppers are not allowed to *collude* (i.e., they cannot exchange or combine information), and therefore only the eavesdropper with the strongest received signal from x_i determines the MSR between x_i and x_j. The case of colluding eavesdroppers is analyzed in Part II of this paper [32].

The iS-graph admits the following outage interpretation: without access to the channel state information (CSI) of the legitimate nodes and eavesdroppers, the legitimate nodes set a target secrecy rate ϱ at which they *unconditionally* transmit. If this rate is supported by the physical channel (i.e., no secrecy outage), then there is an edge between the two nodes in the $i\mathcal{S}$-graph.

Consider now the particular scenario where the following conditions hold: a) the infimum desired secrecy rate is zero, i.e., $\varrho = 0$; b) the wireless environment introduces only path loss, i.e., $Z_{x_i,x_j} = 1$ in (1); and c) the noise powers of the legitimate users and eavesdroppers are equal, i.e., $\sigma_\ell^2 = \sigma_e^2 = \sigma^2$. 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 if and only if $\mathcal{R}_s(x_i, x_j) > 0$. Under these special conditions, the edge set in (3) simplifies to

$$\mathcal{E} = \left\{\overrightarrow{x_i x_j} : |x_i - x_j| < |x_i - e^*|,\ e^* = \arg\min_{e_k \in \Pi_e} |x_i - e_k|\right\} \tag{5}$$

which corresponds the geometrical model proposed in [28]. Fig. 2 shows an example of such an $i\mathcal{S}$-graph on $\mathbb{R}^2$.

The spatial location of the nodes can be modeled either deterministically or stochastically. However, in many important scenarios, only a statistical description of the node positions is available, and thus a stochastic spatial model is more suitable. In particular, when the node positions are unknown to the network designer *a priori*, we may as well treat them as completely random according to a homogeneous Poisson point process [35].[7] The Poisson process has maximum entropy among all homogeneous

[7]The spatial Poisson process is a natural choice in such situations because, given that a node is inside a region $\mathcal{R}$, the pdf of its position is conditionally uniform over $\mathcal{R}$.

processes, and serves as a simple and useful model for the position of nodes in a network.

Definition 2.3 (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 $\mathbb{R}^2$. We use $\{R_{\ell,i}\}_{i=1}^{\infty}$ and $\{R_{ei}\}_{i=1}^{\infty}$ to denote the ordered random distances between the origin of the coordinate system and the nodes in Π_ℓ and Π_e, respectively, where $R_{\ell,1} \le R_{\ell,2} \le \ldots$ and $R_{e,1} \le R_{e,2} \le \ldots$.

III. Local Connectivity in the Poisson $i\mathcal{S}$-Graph

The node degrees are an important property of a graph, since they describe the connectivity between a node and its immediate neighbors. In a graph, the *in-degree* and *out-degree* of a vertex are, respectively, the number of edges entering and exiting the vertex. Since the $i\mathcal{S}$-graph is a random graph, the in- and out-degrees of the legitimate nodes are RVs. In this section, we provide a complete probabilistic characterization of both in-degree N_{in} and out-degree N_{out} of a typical node in the Poisson $i\mathcal{S}$-graph.[8] We first consider the simplest case of $\varrho = 0$ (the *existence* of secure links), $Z_{x_i,x_j} = 1$ (path loss only), and $\sigma_e^2 = \sigma_\ell^2$ (equal noise powers) in Sections III-A, III-B, and III-C. This scenario leads to an $i\mathcal{S}$-graph with a simple geometric description, thus providing various insights that are useful in understanding more complex cases. Later, in Sections III-D and III-E, we separately analyze how the node degrees are affected by wireless propagation effects other than path loss (e.g., multipath fading), a nonzero secrecy rate threshold ϱ, and unequal noise powers $\sigma_e^2, \sigma_\ell^2$.

A. In-Degree Characterization

The characterization of the in-degree relies on the notion of Voronoi tessellation, which we now introduce. A *planar tessellation* is a collection of disjoint polygons whose closures cover $\mathbb{R}^2$, and which is locally finite (i.e., the number of polygons intersecting any given compact set is finite). Given a generic point process $\Pi = \{x_i\} \subset \mathbb{R}^2$, we define the *Voronoi cell* $\mathcal{C}_{x_i}$ of the point x_i as the set of points of $\mathbb{R}^2$ which are closer to x_i than any other point of Π, i.e.,

$$\mathcal{C}_{x_i} = \left\{ y \in \mathbb{R}^2 : |y - x_i| < |y - x_j|, \forall x_j \neq x_i \right\}.$$

The collection $\{C_{x_i}\}$ of all the cells forms a random *Voronoi tessellation* with respect to the underlying point process Π. Let $\mathcal{C}_0$ denote the *typical Voronoi cell*, i.e., the Voronoi cell associated with a point placed at the origin, according to Slivnyak's theorem. Using the notions just introduced, the following theorem provides a probabilistic characterization of the in-degree of the $i\mathcal{S}$-graph.

[8]In this paper, we analyze the local properties of a *typical node* in the Poisson $i\mathcal{S}$-graph. This notion is made precise in [36, 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 $\mathbb{R}^2$. In this paper, we often omit the word "typical" for brevity.

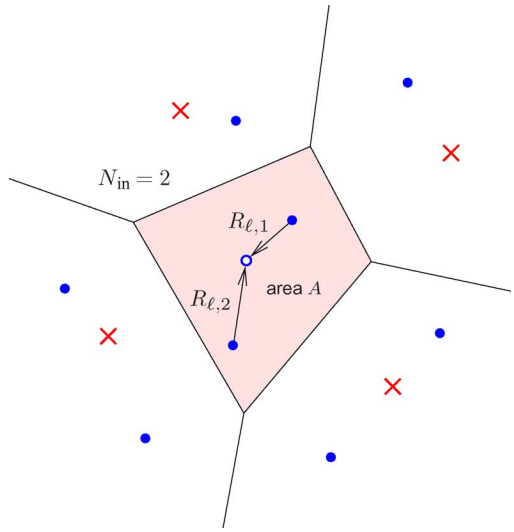

Fig. 3. In-degree of a node. In this example, the node at the origin can receive messages with information-theoretic security from $N_{\text{in}} = 2$ nodes. The RV A is the area of a typical Voronoi cell, induced by the eavesdropper Poisson process Π_e with density λ_e.

Theorem 3.1: The in-degree N_{in} of a typical node in the Poisson $i\mathcal{S}$-graph has the following moment generating function (MGF):

$$M_{N_{\text{in}}}(s) = \mathbb{E}\left\{ \exp\left(\frac{\lambda_\ell}{\lambda_e} \widetilde{A}(e^s - 1) \right) \right\} \tag{6}$$

where $\widetilde{A}$ is the area of a typical Voronoi cell induced by a unit-density Poisson process. Furthermore, all the moments of N_{in} are given by

$$\mathbb{E}\{N_{\text{in}}^n\} = \sum_{k=1}^{n} \left(\frac{\lambda_\ell}{\lambda_e} \right)^k S(n,k) \mathbb{E}\{\widetilde{A}^k\}, \quad n \ge 1 \tag{7}$$

where $S(n,k)$, $1 \le k \le n$, are the Stirling numbers of the second kind [37, Ch. 24].

Proof: Using Slivnyak's theorem [36, Sec. 4.4], we consider the process $\Pi_\ell \cup \{0\}$ obtained by adding a legitimate node to the origin of the coordinate system, and denote the in-degree of the node at the origin by N_{in}. The RV N_{in} corresponds to the number of nodes from the process Π_ℓ that fall inside the typical Voronoi cell $\mathcal{C}_0$ constructed from the process $\Pi_e \cup \{0\}$. This is depicted in Fig. 3. Denoting the random area of such a cell by A, the MGF of N_{in} is given by

$$M_{N_{\text{in}}}(s) = \mathbb{E}\{e^{sN_{\text{in}}}\} = \mathbb{E}\left\{ \exp\left(\lambda_\ell A (e^s - 1) \right) \right\}$$

where we used the fact that conditioned on A, the RV N_{in} is Poisson distributed with parameter $\lambda_\ell A$. If $\widetilde{A}$ denotes the random area of a typical Voronoi cell induced by a *unit-density* Poisson process, then $\widetilde{A} = A\lambda_e$ and (6) follows. This completes the first half of the proof.

To obtain the moments of N_{in}, we use Dobinski's formula

$$\sum_{k=0}^{\infty} k^n \frac{e^{-\mu}\mu^k}{k!} = \sum_{k=1}^{n} \mu^k S(n,k)$$

TABLE I
FIRST FOUR MOMENTS OF THE RANDOM AREA $\widetilde{A}$ OF A TYPICAL VORONOI CELL, INDUCED BY A UNIT-DENSITY POISSON PROCESS

k	1	2	3	4
$\mathbb{E}\{\widetilde{A}^k\}$	1	1.280	1.993	3.650

which establishes the relationship between the nth moment of a Poisson RV with mean μ and the Stirling numbers of the second kind $S(n,k)$. Then,

$$\begin{aligned}\mathbb{E}\{N_{\text{in}}^n\} &= \mathbb{E}\{\mathbb{E}\{N_{\text{in}}^n|A\}\}\\ &= \mathbb{E}\left\{\sum_{k=1}^{n}(\lambda_\ell A)^k S(n,k)\right\}\\ &= \sum_{k=1}^{n}\left(\frac{\lambda_\ell}{\lambda_e}\right)^k S(n,k)\mathbb{E}\{\widetilde{A}^k\}\end{aligned}$$

for $n \geq 1$. This is the result in (7) and the second half of proof is concluded. □

Equation (7) expresses the moments of N_{in} in terms of the moments of $\widetilde{A}$. In general, $\mathbb{E}\{\widetilde{A}^k\}$ cannot be obtained in closed form, except in the case of $k = 1$, which is derived below in (10). For $k = 2$ and $k = 3$, $\mathbb{E}\{\widetilde{A}^k\}$ can be expressed as multiple integrals and then computed numerically [38]. Alternatively, the moments of $\widetilde{A}$ can be determined using Monte Carlo simulation of random Poisson–Voronoi tessellations. The first four moments of $\widetilde{A}$ are given in Table I.

The above theorem can be used to obtain the in-connectivity properties of a node, such as the in-isolation probability, as given in the following corollary.

Corollary 3.1: The average in-degree of a typical node in the Poisson $i\mathcal{S}$-graph is

$$\mathbb{E}\{N_{\text{in}}\} = \frac{\lambda_\ell}{\lambda_e} \tag{8}$$

and the probability that a typical node cannot receive from anyone with positive secrecy rate (in-isolation) is

$$p_{\text{in}-\text{isol}} = \mathbb{E}\left\{e^{-\frac{\lambda_\ell}{\lambda_e}\widetilde{A}}\right\}. \tag{9}$$

Proof: Setting $n = 1$ in (7), we obtain $\mathbb{E}\{N_{\text{in}}\} = (\lambda_\ell/\lambda_e)\mathbb{E}\{\widetilde{A}\}$. Noting that

$$\widetilde{A} = \iint_{\mathbb{R}^2} \mathbb{1}\{z \in \mathcal{C}_0\}dz$$

where $\mathcal{C}_0$ is the typical Voronoi cell induced by a unit-density Poisson process Π, we can write[9]

$$\begin{aligned}\mathbb{E}\{\widetilde{A}\} &= \iint_{\mathbb{R}^2}\mathbb{P}\{z \in \mathcal{C}_0\}dz \qquad (10)\\ &= \iint_{\mathbb{R}^2}\mathbb{P}\left\{\widetilde{\Pi}\left\{\mathcal{B}_z\left(|z|\right)\right\} = 0\right\}dz\\ &= \int_0^{2\pi}\int_0^{\infty} e^{-\pi r^2} r dr d\theta = 1. \qquad (11)\end{aligned}$$

[9]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.

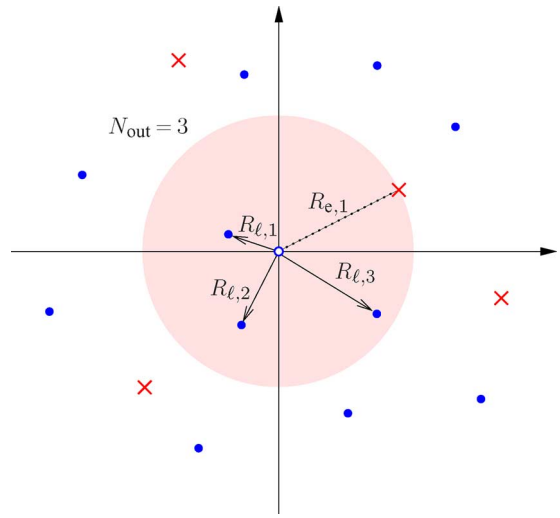

Fig. 4. Out-degree of a node. In this example, the node at the origin can transmit messages with information-theoretic security to $N_{\text{out}} = 3$ nodes.

Equation (10) follows from Fubini's Theorem, while (11) follows from the fact that, for any $z \in \mathbb{R}^2$, the event $\{z \in \mathcal{C}_0\}$ is equivalent to having no points of $\widetilde{\Pi}$ in $\mathcal{B}_z(|z|)$, as depicted in Fig. 5(a). This completes the proof of (8). To derive (9), note that the RV N_{in} conditioned on A is Poisson distributed with parameter $\lambda_\ell A$, and thus $p_{\text{in}-\text{isol}} = p_{N_{\text{in}}}(0) = \mathbb{E}\{p_{N_{\text{in}}|A}(0)\} = \mathbb{E}\{e^{-(\lambda_\ell/\lambda_e)\widetilde{A}}\}$. □

B. Out-Degree Characterization

Theorem 3.2: The out-degree N_{out} of a typical node in the Poisson $i\mathcal{S}$-graph has the following geometric probability mass function (PMF):

$$p_{N_{\text{out}}}(n) = \left(\frac{\lambda_\ell}{\lambda_\ell + \lambda_e}\right)^n\left(\frac{\lambda_e}{\lambda_\ell + \lambda_e}\right), \quad n \geq 0. \tag{12}$$

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 the origin by N_{out}. The RV N_{out} corresponds to the number of nodes from the process Π_ℓ that fall inside the circle with random radius $R_{e,1}$ centered at the origin, i.e., $N_{\text{out}} = \#\{R_{\ell,i} : R_{\ell,i} < R_{e,1}\}$. This is depicted in Fig. 4. To determine the PMF of N_{out}, consider the one-dimensional arrival processes $\widetilde{\Pi}_\ell = \{R_{\ell,i}^2\}_{i=1}^{\infty}$ and $\widetilde{\Pi}_e = \{R_{ei}^2\}_{i=1}^{\infty}$. As can be easily shown using the mapping theorem [35, Sec. 2.3], $\widetilde{\Pi}_\ell$ and $\widetilde{\Pi}_e$ are independent homogeneous Poisson processes with arrival rates $\pi\lambda_\ell$ and $\pi\lambda_e$, respectively. When there is an arrival in the merged process $\widetilde{\Pi}_\ell \cup \widetilde{\Pi}_e$, it comes from process $\widetilde{\Pi}_\ell$ with probability $p = \pi\lambda_\ell/(\pi\lambda_\ell + \pi\lambda_e) = \lambda_\ell/(\lambda_\ell + \lambda_e)$, and from $\widetilde{\Pi}_e$ with probability $1 - p = \lambda_e/(\lambda_\ell + \lambda_e)$, and these events are independent for different arrivals [39]. Since the event $\{N_{\text{out}} = n\}$ is equivalent to the occurrence of n arrivals from $\widetilde{\Pi}_\ell$ followed by one arrival from $\widetilde{\Pi}_e$, then we have the geometric PMF $p_{N_{\text{out}}}(n) = p^n(1-p)$, $n \geq 0$, with parameter $p = \lambda_\ell/(\lambda_\ell + \lambda_e)$. This is the result in (12) and the proof is completed. □

Note that this particular result was also derived in [28]. The above theorem can be used to obtain the out-connectivity properties of a node, such as the out-isolation probability, as given in the following corollary.

Corollary 3.2: The average out-degree of a typical node in the Poisson $i\mathcal{S}$-graph is

$$\mathbb{E}\{N_{\text{out}}\} = \frac{\lambda_\ell}{\lambda_e} \tag{13}$$

and the probability that a typical node cannot transmit to anyone with positive secrecy rate (out-isolation) is

$$p_{\text{out}-\text{isol}} = \frac{\lambda_e}{\lambda_\ell + \lambda_e}. \tag{14}$$

Proof: This follows directly from Theorem 3.2. □

C. General Relationships Between In- and Out-Degree

We have so far considered the probabilistic distribution of the in- and out-degrees in a separate fashion. This section establishes a direct comparison between some characteristics of the in- and out-degrees.

Property 3.1: For the Poisson $i\mathcal{S}$-graph with $\lambda_\ell > 0$ and $\lambda_e > 0$, the average degrees of a typical node satisfy

$$\mathbb{E}\{N_{\text{in}}\} = \mathbb{E}\{N_{\text{out}}\} = \frac{\lambda_\ell}{\lambda_e}. \tag{15}$$

Proof: This follows directly by comparing (8) and (13). □

The property $\mathbb{E}\{N_{\text{in}}\} = \mathbb{E}\{N_{\text{out}}\}$ is valid in general for any directed random graph.

Property 3.2: For the Poisson $i\mathcal{S}$-graph with $\lambda_\ell > 0$ and $\lambda_e > 0$, the probabilities of in- and out-isolation of a typical node satisfy

$$p_{\text{in}-\text{isol}} < p_{\text{out}-\text{isol}}. \tag{16}$$

Proof: Let $\Pi_e\{\mathcal{R}\} \triangleq \#\{\Pi_e \cap \mathcal{R}\}$ denote the number of eavesdroppers inside region $\mathcal{R}$. With this definition, we can rewrite the edge set $\mathcal{E}$ in (5) as

$$\mathcal{E} = \left\{\overrightarrow{x_i x_j} : \Pi_e\left\{\mathcal{B}_{x_i}(|x_i - x_j|\right\} = 0\right\} \tag{17}$$

i.e., x_i is connected to x_j if and only if the ball centered at x_i with radius $|x_i - x_j|$ is free of eavesdroppers. We consider the process $\Pi_\ell \cup \{0\}$ obtained by adding a legitimate node to the origin of the coordinate system. Let $\breve{x}_i$ denote the ordered points in process Π_ℓ of legitimate nodes, such that $|\breve{x}_1| < |\breve{x}_2| < \ldots$. From (17), the node at the origin is out-isolated if and only if $\Pi_e\{\mathcal{B}_0(|\breve{x}_j|)\} \geq 1$ for all $j \geq 1$. This is depicted in Fig. 5(b). Since the balls $\mathcal{B}_0(|\breve{x}_j|)$, $j \geq 1$, are concentric at the origin, we have

$$p_{\text{out}-\text{isol}} = \mathbb{P}\left\{\Pi_e\{\mathcal{B}_0(|\breve{x}_1|)\} \geq 1\right\}.$$

Similarly, we see from (17) that the node at the origin is in-isolated if and only if $\Pi_e\{\mathcal{B}_{\breve{x}_i}(|\breve{x}_i|)\} \geq 1$ for all $i \geq 1$. This is depicted in Fig. 5(c). Then,

$$\begin{aligned} p_{\text{in}-\text{isol}} &= \mathbb{P}\left\{\bigwedge_{i=1}^{\infty} \Pi_e\left\{\mathcal{B}_{\breve{x}_i}\left(|\breve{x}_i|\right)\right\} \geq 1\right\} && (18)\\ &< \mathbb{P}\left\{\Pi_e\left\{\mathcal{B}_{\breve{x}_1}\left(|\breve{x}_1|\right)\right\} \geq 1\right\} && (19)\\ &= \mathbb{P}\left\{\Pi_e\left\{\mathcal{B}_0\left(|\breve{x}_1|\right)\right\} \geq 1\right\} \\ &= p_{\text{out}-\text{isol}}. && (20) \end{aligned}$$

The fact that the inequality in (19) is strict is proved in Appendix A. Equation (20) follows from the spatial invariance of the homogeneous Poisson process Π_e. This concludes the proof. □

Intuitively, out-isolation is *more likely* than in-isolation because out-isolation only requires that one or more eavesdroppers are closer than the nearest legitimate node $\breve{x}_1$. On the other hand, in-isolation requires that *every* ball $\mathcal{B}_{\breve{x}_i}(|\breve{x}_i|)$, $i \geq 1$, has one or more eavesdroppers, which is less likely. Property 3.2 can then be restated in the following way: *it is easier for an individual node to be in-connected than out-connected*.

D. Effect of the Wireless Propagation Characteristics

We have so far analyzed the local connectivity of the $i\mathcal{S}$-graph in the presence of path loss only. However, wireless propagation typically introduces random effects such as multipath fading and shadowing, which are modeled by the RV Z_{x_i,x_j} in (1). In this section, we aim to quantify the impact of such propagation effects on the local connectivity of a node.

Considering $\varrho = 0$, $\sigma_\ell^2 = \sigma_e^2 = \sigma^2$, and arbitrary propagation effects Z_{x_i,x_j} with pdf $f_Z(z)$, we can combine (4) with the general propagation model of (1) and write

$$\begin{aligned} \mathcal{R}_s(x_i, x_j) = \Bigg[\log_2\left(1 + \frac{P_\ell \cdot g\left(|x_i - x_j|, Z_{x_i,x_j}\right)}{\sigma^2}\right) \\ - \log_2\left(1 + \frac{P_\ell \cdot g\left(|x_i - e^*|, Z_{x_i,e^*}\right)}{\sigma^2}\right)\Bigg]^+ \end{aligned} \tag{21}$$

where $e^* = \arg\max_{e_k \in \Pi_e} g(|x_i - e_k|, Z_{x_i,e_k})$. After some algebra, the edge set for the resulting $i\mathcal{S}$-graph can be written as

$$\mathcal{E} = \left\{\overrightarrow{x_i x_j} : g\left(|x_i - x_j|, Z_{x_i,x_j}\right) > g\left(|x_i - e^*|, Z_{x_i,e^*}\right)\right\}. \tag{22}$$

Unlike the case of path-loss only, where the out-connections of a node are determined only by the *closest* eavesdropper, here they are determined by the eavesdropper with the *least attenuated* channel. We start by characterizing the distribution of the out-degree in the following theorem.

Theorem 3.3: For the Poisson $i\mathcal{S}$-graph with propagation effects Z_{x_i,x_j} whose pdf is given by a continuous function $f_Z(z)$, the PMF of the out-degree N_{out} of a typical node is given in (12), and is *invariant* with respect to $f_Z(z)$.

Proof: See Appendix B. □

Intuitively, the propagation environment affects both legitimate nodes and eavesdroppers *in the same way*, such that the PMF of N_{out} is invariant with respect to the particular form of $f_Z(z)$. However, the PMF of N_{in} *does* depend on $f_Z(z)$ in a nontrivial way, although its mean remains the same, as specified in the following corollary.

Corollary 3.3: For the Poisson $i\mathcal{S}$-graph with propagation effects Z_{x_i,x_j} distributed according to $f_Z(z)$, the average node degrees are

$$\mathbb{E}\{N_{\text{in}}\} = \mathbb{E}\{N_{\text{out}}\} = \frac{\lambda_\ell}{\lambda_e} \tag{23}$$

for any distribution $f_Z(z)$.

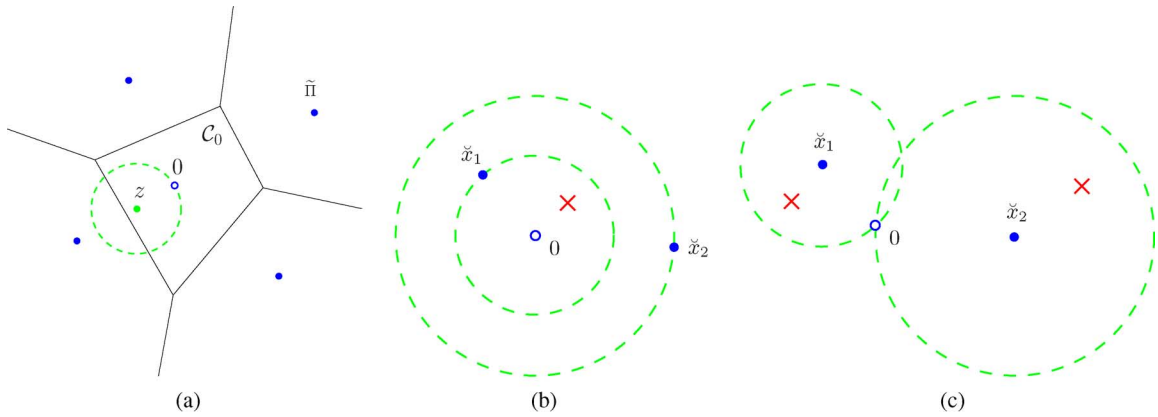

Fig. 5. Auxiliary diagrams. (a) Proof of Corollary 3.1. (b) Proof of Property 3.2. (c) Proof of Property 3.2.

Proof: This follows directly from Theorem 3.3 and the fact that $\mathbb{E}\{N_{\rm in}\} = \mathbb{E}\{N_{\rm out}\}$. □

We thus conclude that the expected node degrees are invariant with respect to the distribution characterizing the propagation effects, and always equal the ratio λ_ℓ/λ_e of spatial densities.

E. Effect of the Secrecy Rate Threshold and Noise Powers

We have so far analyzed the local connectivity of the $i\mathcal{S}$-graph based on the *existence* of positive MSR, by considering a target secrecy rate of zero, i.e., $\varrho = 0$ in (3). We have furthermore considered that the noise powers of the legitimate users and eavesdroppers are equal, i.e., $\sigma_\ell^2 = \sigma_e^2$ in (4). Under these two conditions, the $i\mathcal{S}$-graph reduces to the simple geometric description in (5). In this section, we study the effect of nonzero secrecy rate threshold, i.e., $\varrho > 0$, and unequal noise powers, i.e., $\sigma_\ell^2 \neq \sigma_e^2$, on the $i\mathcal{S}$-graph.

Considering $Z_{x_i,x_j} = 1$ and arbitrary noise powers $\sigma_\ell^2, \sigma_e^2$, we can combine (4) with the general propagation model of (1) and write

$$\mathcal{R}_s(x_i,x_j) = \left[\log_2\left(1+\frac{P_\ell \cdot g\left(|x_i-x_j|\right)}{\sigma_\ell^2}\right) - \log_2\left(1+\frac{P_\ell \cdot g\left(|x_i-e^*|\right)}{\sigma_e^2}\right)\right]^+ \quad (24)$$

where $e^* = \arg\min_{e_k\in\Pi_e} |x_i - e_k|$. We can now replace this expression for $\mathcal{R}_s$ into (3) while allowing an arbitrary threshold ϱ. After some algebra, the edge set for the resulting $i\mathcal{S}$-graph can be written as

$$\mathcal{E} = \left\{\overrightarrow{x_i x_j} : g\left(|x_i-x_j|\right) > \frac{\sigma_\ell^2}{\sigma_e^2}2^\varrho g\left(|x_i-e^*|\right) + \frac{\sigma_\ell^2}{P_\ell}(2^\varrho-1)\right\} \quad (25)$$

with $e^* = \arg\min_{e_k\in\Pi_e} |x_i - e_k|$. By setting $\varrho = 0$ and $\sigma_\ell^2 = \sigma_e^2$ in (25), we obtain the edge set in (5) as a special case. However, for arbitrary parameters $\varrho, \sigma_\ell^2, \sigma_e^2$, the $i\mathcal{S}$-graph can no longer be characterized by the simple geometric description of (5). We now analyze the impact of the secrecy rate threshold ϱ and the noise powers $\sigma_\ell^2, \sigma_e^2$ on the average node degrees, for a general channel gain function $g(r)$.

Property 3.3: For the Poisson $i\mathcal{S}$-graph with edge set in (25) and any channel gain function $g(r)$ satisfying the conditions in Section II-A, the average node degrees $\mathbb{E}\{N_{\rm out}\} = \mathbb{E}\{N_{\rm in}\}$ are decreasing functions of ϱ and σ_ℓ^2, and increasing functions of σ_e^2.

Proof: The result follows in a straightforward manner from a coupling argument [40, Sec. 2.2]. □

In essence, by increasing the secrecy rate threshold ϱ, the requirement $\mathcal{R}_s(x_i,x_j) > \varrho$ for any two nodes x_i, x_j to be securely connected becomes stricter, and thus the local connectivity (as measured by the average node degree) becomes worse. On the other hand, increasing σ_ℓ^2 or decreasing σ_e^2 makes the requirement $\mathcal{R}_s(x_i,x_j) > \varrho$ harder to satisfy for any two legitimate nodes x_i, x_j. As a result, the local connectivity also becomes worse.

The exact dependence of the average node degree on the parameters $\varrho, \sigma_\ell^2, \sigma_e^2$ varies with the function $g(r)$. To gain further insights, we consider the specific channel gain function

$$g(r) = \frac{1}{r^{2b}}, \quad r > 0. \quad (26)$$

This function has been widely used in the literature to model path loss behavior as a function of distance, and satisfies the conditions in Section II-A. For this case, a characterization of the first-order moments of $N_{\rm in}$ and $N_{\rm out}$ is possible, and is provided in the following theorem.

Theorem 3.4: For the Poisson $i\mathcal{S}$-graph with secrecy rate threshold ϱ, noise powers $\sigma_\ell^2, \sigma_e^2$, and channel gain function $g(r) = 1/r^{2b}$, the average node degrees are

$$\mathbb{E}\{N_{\rm in}\} = \mathbb{E}\{N_{\rm out}\} = \pi^2\lambda_\ell\lambda_e \int_0^\infty \frac{x e^{-\pi\lambda_e x}}{\left(\frac{\sigma_\ell^2}{\sigma_e^2}2^\varrho + \frac{\sigma_\ell^2}{P_\ell}(2^\varrho-1)x^b\right)^{1/b}}dx. \quad (27)$$

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 the node at the origin by $N_{\rm out}$. Let $R_{e,1} \triangleq \min_{e_i\in\Pi_e} |e_i|$ be the random distance between the origin and its closest eavesdropper. Define the function

$$\psi(r) \triangleq \frac{r}{\left(\frac{\sigma_\ell^2}{\sigma_e^2}2^\varrho + \frac{\sigma_\ell^2}{P_\ell}(2^\varrho-1)r^{2b}\right)^{1/2b}}, \quad r \geq 0 \quad (28)$$

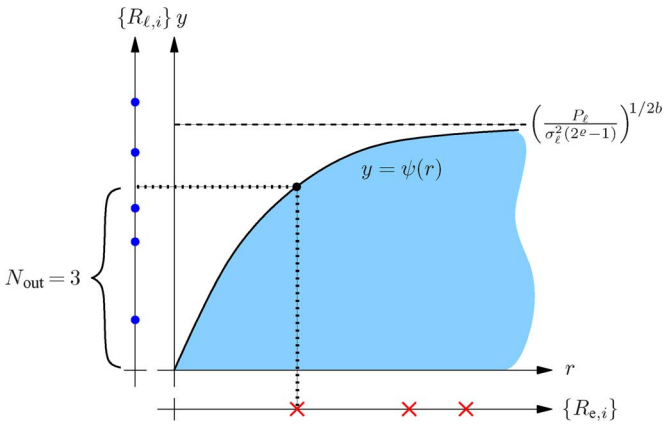

Fig. 6. Effect of nonzero secrecy rate threshold ϱ and unequal noise powers $\sigma_\ell^2, \sigma_e^2$ on the average node degree, for the case of $g(r)=1/r^{2b}$. The function $\psi(r)$ was defined in (28).

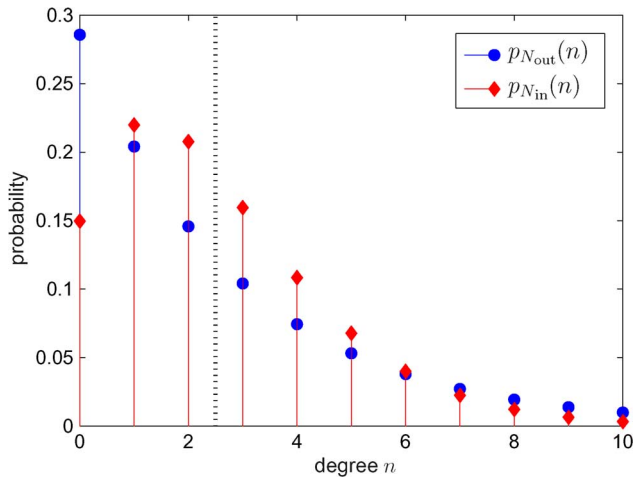

Fig. 7. PMF of the in- and out-degree of a node ($\lambda_e/\lambda_\ell=0.4$). The vertical line marks the average node degrees, $\mathbb{E}\{N_{\text{out}}\}=\mathbb{E}\{N_{\text{in}}\}=\lambda_\ell/\lambda_e=2.5$, in accordance with Property 3.1.

so that (25) can simply be written as $\mathcal{E}=\{\overrightarrow{x_ix_j}:|x_i-x_j|<\psi(|x_i-e^*|)\}$. This function is depicted in Fig. 6. The average out-degree is then given by

$$\begin{aligned}\mathbb{E}\{N_{\text{out}}\}&=\mathbb{E}_{\Pi_\ell,R_{e,1}}\left\{\Pi_\ell\left\{\mathcal{B}_0\left(\psi\left(R_{e,1}\right)\right)\right\}\right\}\\&=\pi\lambda_\ell\mathbb{E}_{R_{e,1}}\left\{\psi^2(R_{e,1})\right\}.\end{aligned}$$

Defining $X\triangleq R_{e,1}^2$, we can write

$$\mathbb{E}\{N_{\text{out}}\}=\pi\lambda_\ell\mathbb{E}_X\left\{\frac{X}{\left(\frac{\sigma_\ell^2}{\sigma_e^2}2^\varrho+\frac{\sigma_\ell^2}{P_\ell}(2^\varrho-1)X^b\right)^{1/b}}\right\}.$$

Using the fact that X is an exponential RV with mean $1/\pi\lambda_e$, we obtain (27). □

F. Numerical Results

Fig. 7 compares the PMFs of the in- and out-degree of a node. We clearly observe that the RV N_{in} does not have a geometric distribution, unlike the RV N_{out}. However, the two RVs have the same mean λ_ℓ/λ_e, according to Property 3.1.

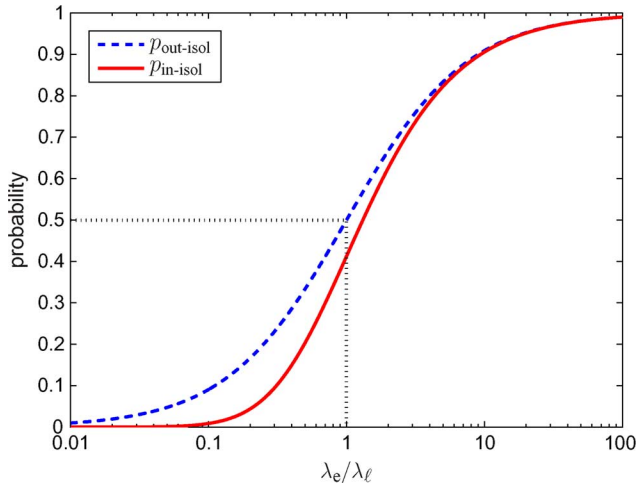

Fig. 8. Probabilities of in- and out-isolation of a node, versus the ratio λ_e/λ_ℓ. Note that $p_{\text{in}-\text{isol}}<p_{\text{out}-\text{isol}}$ for any fixed λ_e/λ_ℓ, as proved in Property 3.2.

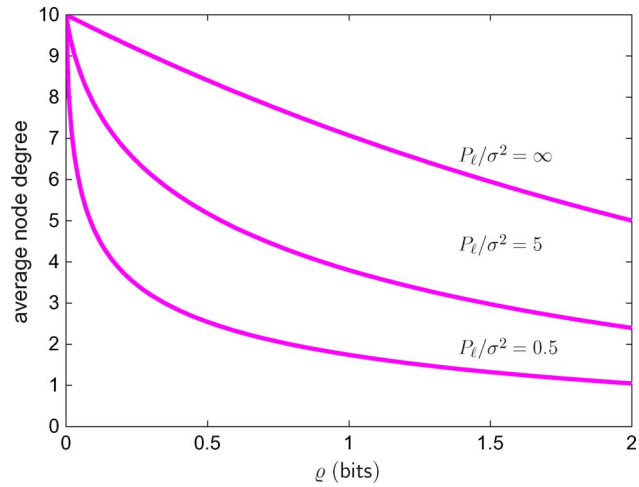

Fig. 9. Average node degree versus the secrecy rate threshold ϱ, for various values of P_ℓ/σ^2 ($\sigma_\ell^2=\sigma_e^2=\sigma^2$, $g(r)=1/r^{2b}$, $b=2$, $\lambda_\ell=1$ m^{-2}, $\lambda_e=0.1$ m^{-2}).

Fig. 8 compares the probabilities of out-isolation and in-isolation of a node for various ratios λ_e/λ_ℓ. The curve for $p_{\text{out}-\text{isol}}$ was plotted using the closed form expression in (14). The curve for $p_{\text{in}-\text{isol}}$ was obtained according to (9) through Monte Carlo simulation of the random area $\widetilde{A}$ of a typical Voronoi cell, induced by a unit-density Poisson process. We observe that $p_{\text{in}-\text{isol}}<p_{\text{out}-\text{isol}}$ for any fixed λ_e/λ_ℓ, as proved in Property 3.2.

Fig. 9 illustrates the effect of the secrecy rate threshold ϱ on the average node degrees. We observe that the average node degree attains its maximum value of $\lambda_\ell/\lambda_e=10$ at $\varrho=0$, and is monotonically decreasing with ϱ. As proved in Property 3.3, such behavior occurs for any function $g(r)$ satisfying the conditions in Section II-A.

IV. Techniques for Communication with Enhanced Secrecy

Based on the results derived in Section III, we observe that even a small density of eavesdroppers is enough to significantly

disrupt connectivity of the $i\mathcal{S}$-graph. For example, if the density of eavesdroppers is half the density of legitimate nodes, then from (15) the average node degree is only $\lambda_\ell/\lambda_e = 2$. In this section, we propose two techniques that achieve an average degree higher than λ_ℓ/λ_e: 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). For each strategy, we characterize the average degree of a typical node in the corresponding enhanced $i\mathcal{S}$-graph. The average degree is a measure of secure connectivity, and is used in this section to quantify and compare the effectiveness of each strategy.

A. Sectorized Transmission

We have so far assumed that the legitimate nodes employ omnidirectional antennas, distributing power equally among all directions. We now consider that each legitimate node is able to 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. With each node $x_i \in \Pi_\ell$, we associate L transmission sectors $\{\mathcal{S}_i^{(l)}\}_{l=1}^{L}$, defined as

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

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 $G_L = \{\Pi_\ell, \mathcal{E}_L\}$ has an edge set given by

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

where

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

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. We start by characterizing the distribution of the out-degree by the following theorem.

Theorem 4.1 (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

$$p_{N_{\text{out}}}(n) = \binom{L+n-1}{L-1} \left(\frac{\lambda_\ell}{\lambda_\ell + \lambda_e}\right)^n \left(\frac{\lambda_e}{\lambda_\ell + \lambda_e}\right)^L \quad (29)$$

for $n \geq 0$.

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 the node at the origin by N_{out}. This is depicted in Fig. 10(a). Let $\mathcal{S}^{(l)}$ denote the lth 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 $\{R_{ei}^{(l)}\}_{i=1}^{\infty}$ for the eavesdroppers falling inside $\mathcal{S}^{(l)}$). Then, $N_{\text{out}} = \sum_{l=1}^{L} N_{\text{out}}^{(l)}$, where $N_{\text{out}}^{(l)} \triangleq \#\{R_{\ell,i}^{(l)} : R_{\ell,i}^{(l)} < \min_k R_{ek}^{(l)}\}$ is the out-degree of node 0 associated with sector l. Furthermore, the RVs $\{N_{\text{out}}^{(l)}\}$ are i.i.d. for different l. To determine the PMF of $N_{\text{out}}^{(l)}$, we use the fact that $\{(R_{\ell,i}^{(l)})^2\}_{i=1}^{\infty}$ and $\{(R_{ei}^{(l)})^2\}_{i=1}^{\infty}$ are homogeneous Poisson processes with rates $\pi\lambda_\ell/L$ and $\pi\lambda_e/L$, respectively (by the mapping theorem [35, Sec. 2.3]). Following the steps analogous to the proof of Theorem 3.2, we can show that each RV $N_{\text{out}}^{(l)}$ has the geometric PMF $p_{N_{\text{out}}^{(l)}}(n) = p^n(1-p)$, $n \geq 0$, with parameter $p = \lambda_\ell/(\lambda_\ell + \lambda_e)$.[10] Now, since the RVs $\{N_{\text{out}}^{(l)}\}$ are i.i.d. in l, the total out-degree N_{out} with L sectors 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 $p = \lambda_\ell/(\lambda_\ell + \lambda_e)$. This is the result in (29) and the proof is completed. □

When $L = 1$, (29) reduces to the PMF without sectorization given in (12), as expected. The following corollary gives the average node degrees as a function of L.

Corollary 4.1: For the Poisson $i\mathcal{S}$-graph G_L with L sectors, the average node degrees are

$$\mathbb{E}\{N_{\text{in}}\} = \mathbb{E}\{N_{\text{out}}\} = L\frac{\lambda_\ell}{\lambda_e}. \quad (30)$$

Proof: From $N_{\text{out}} = \sum_{l=1}^{L} N_{\text{out}}^{(l)}$, we have $\mathbb{E}\{N_{\text{out}}\} = L\mathbb{E}\{N_{\text{out},l}\} = Lp/(1-p)$, with $p = \lambda_\ell/(\lambda_\ell + \lambda_e)$. Since $\mathbb{E}\{N_{\text{in}}\} = \mathbb{E}\{N_{\text{out}}\}$, then (30) follows. □

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. Fig. 10(a) 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 nonoverlapping 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 $\mathcal{S}^{(3)}$.

B. 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. 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.,[11]

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

[10] In other words, each RV $N_{\text{out}}^{(l)}$ has the same distribution as the total out-degree for the case of $L = 1$.

[11] In other fields such as materials science, the points $\{x_i\}$ are also called *germs*, and the sets $\{\Theta_i\}$ are also called *grains* [36].

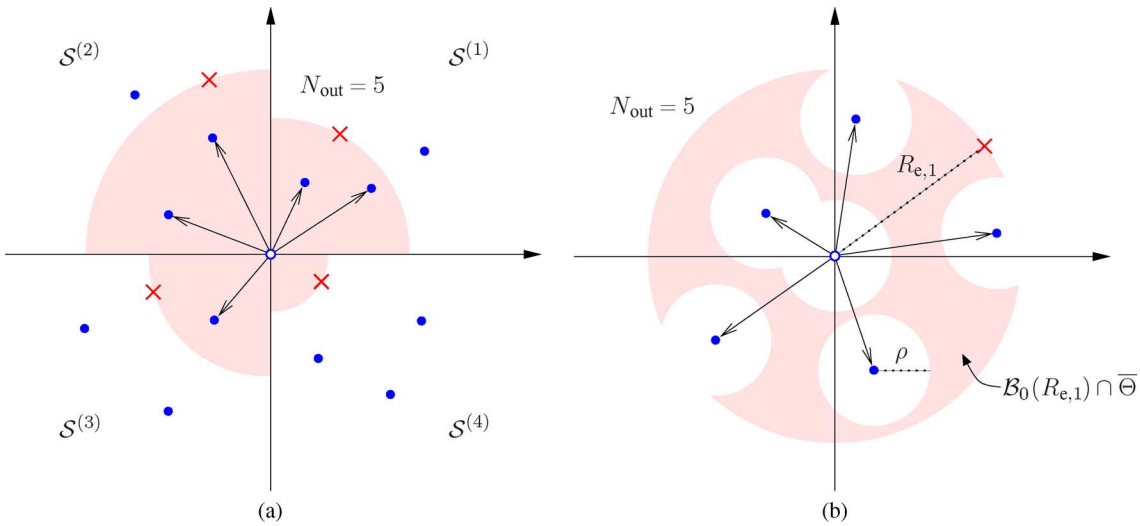

Fig. 10. Techniques for communication with enhanced secrecy. (a) Sectorized transmission. (b) Eavesdropper neutralization.

Since the homogeneous Poisson process Π_ℓ is stationary, it follows that Θ is also stationary, in the sense that its distribution is translation-invariant. Since the eavesdroppers inside Θ have been deactivated, the *effective eavesdropper process* after neutralization is $\Pi_e \cap \overline{\Theta}$, where $\overline{\Theta} \triangleq \mathbb{R}^2 \setminus \Theta$ denotes the complement of Θ.[12] The resulting $i\mathcal{S}$-graph $G_\Theta = \{\Pi_\ell, \mathcal{E}_\Theta\}$ has an edge set given by

$$\mathcal{E}_\Theta = \left\{ \overrightarrow{x_i x_j} : |x_i - x_j| < |x_i - e^*|,\ e^* = \arg\min_{e_k \in \Pi_e \cap \overline{\Theta}} |x_i - e_k| \right\} \tag{31}$$

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*, as shown in Fig. 10(b). We denote the corresponding $i\mathcal{S}$-graph by G_ρ. Even in this simple scenario, the full distributions of the corresponding node degrees N_{in} and N_{out} are difficult to obtain, since the underlying process $\Pi_e \cap \overline{\Theta}$ is quite complex to characterize. However, it is easier to carry out an analysis of the first-order moments, namely of $\mathbb{E}\{N_{\text{out}}\}$. The following theorem provides the desired result.

Theorem 4.1 (Eavesdropper Neutralization): For the enhanced Poisson $i\mathcal{S}$-graph G_ρ with neutralization radius ρ, the average node degrees of a typical node are lower-bounded by

$$\mathbb{E}\{N_{\text{in}}\} = \mathbb{E}\{N_{\text{out}}\} \geq \frac{\lambda_\ell}{\lambda_e} \left(\pi \lambda_e \rho^2 + e^{\pi \lambda_e \rho^2} \right). \tag{32}$$

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 the node at the origin by N_{out}. This is depicted in Fig. 10(b). Let $R_{e,1} \triangleq \min_{e_k \in \Pi_e \cap \overline{\Theta}} |e_k|$ be the random distance between the first nonneutralized eavesdropper and the origin. Noting that

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

we can use Fubini's theorem to write

$$\begin{aligned} \mathbb{E}\{N_{\text{out}}\} &= \lambda_\ell \iint_{\mathbb{R}^2} \mathbb{P}_x\{|x| < R_{e,1}\}\, dx \\ &= \lambda_\ell \pi \rho^2 + \lambda_\ell \iint_{\mathcal{D}(\rho,\infty)} \mathbb{P}_x\{|x| < R_{e,1}\}\, dx \end{aligned} \tag{33}$$

where $\mathcal{D}(a,b) \triangleq \{x \in \mathbb{R}^2 : a \leq |x| \leq b\}$ 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.[13] Appendix C shows that the integrand above satisfies

$$\mathbb{P}_x\{|x| < R_{e,1}\} \geq \exp\left(-\pi \lambda_e e^{-\lambda_\ell \pi \rho^2} \left(|x|^2 - \rho^2 \right) \right). \tag{34}$$

Replacing (34) into (33), we have

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

Rearranging terms and noting that $\mathbb{E}\{N_{\text{in}}\} = \mathbb{E}\{N_{\text{out}}\}$, we obtain the desired result in (32). □

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

[12] In the materials science literature, Θ is typically referred to as the *occupied region*, since it is occupied by grains. In our problem, however, Θ corresponds to a *vacant region*, in the sense that it is free of eavesdroppers. To prevent confusion with the literature, we avoid the use of the terms "occupied" and "vacant" altogether.

[13] 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 [36, Sec. 4.4] for a detailed treatment).

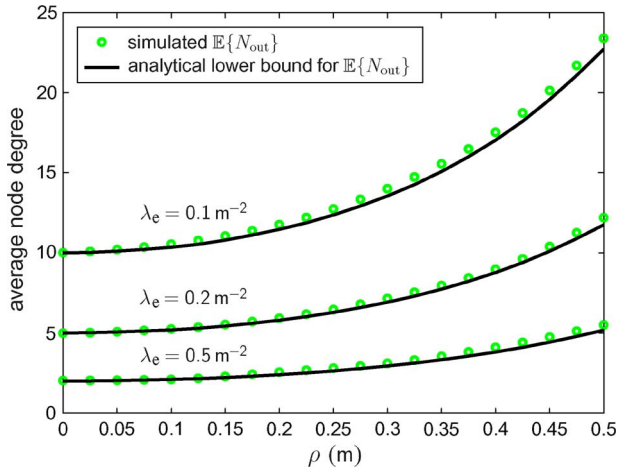

Fig. 11. Average node degree versus the neutralization radius ρ, for various values of λ_e ($\lambda_\ell = 1\ \mathrm{m}^{-2}$).

enhancing the secrecy of communications. Such exponential dependence is intimately tied to the fact that the *fractional area* $p_\Theta = 1 - e^{-\lambda_\ell \pi \rho^2}$ of the neutralization region Θ also approaches 1 exponentially as ρ increases.

C. Numerical Results

Fig. 11 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 $\mathbb{E}\{N_{\rm out}\}$ given in (32) is very close to the actual value of $\mathbb{E}\{N_{\rm out}\}$ 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 (15) we have $\mathbb{E}\{N_{\rm out}\} = \lambda_\ell/\lambda_e$. Since the bound in (32) also equals λ_ℓ/λ_e for $\rho = 0$, it is tight.
2) $\lambda_e \to \infty$: 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, $\mathbb{E}\{N_{\rm out}\}$ 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 (32) also approaches $\lambda_\ell \pi \rho^2$ as $\lambda_e \to \infty$, it is asymptotically tight.

V. Conclusion

Using the notion of strong secrecy, we provided an information-theoretic definition of the $i\mathcal{S}$-graph as a model for intrinsically secure communication in large-scale networks. Fundamental tools from stochastic geometry allowed us to describe in detail how the spatial densities of legitimate and eavesdropper nodes influence various properties of the Poisson $i\mathcal{S}$-graph, such as node degrees and isolation probabilities. In particular, we proved that the average in- and out-degrees equal λ_ℓ/λ_e, and that out-isolation is more probable than in-isolation. In addition, we considered the effect of the wireless propagation on the degree of the legitimate nodes. Surprisingly, the average node degree is invariant with respect to the distribution of the propagation effects (e.g., type of fading or shadowing), and is always equal to the ratio λ_ℓ/λ_e of spatial densities. We then studied the effect of nonzero secrecy rate threshold ϱ and unequal noise powers $\sigma_\ell^2, \sigma_e^2$ on the $i\mathcal{S}$-graph. Specifically, we showed that $\mathbb{E}\{N_{\rm out}\}$ is decreasing in ϱ and σ_ℓ^2, and is increasing in σ_e^2. Furthermore, when the channel gain is of the form $g(r) = 1/r^{2b}$, we obtained expressions for $\mathbb{E}\{N_{\rm out}\}$ as a function of $\varrho, \sigma_\ell^2, \sigma_e^2$, and showed that it decays exponentially with ϱ.

We proposed sectorized transmission and eavesdropper neutralization as two techniques for dramatically enhancing the secrecy of communications. We proved that if each legitimate node is able to transmit independently in L sectors of the plane, then $\mathbb{E}\{N_{\rm out}\}$ increases *linearly* with L. On the other hand, if each legitimate node is able to neutralize all eavesdroppers within a radius ρ, then $\mathbb{E}\{N_{\rm out}\}$ increases *at least exponentially* with ρ.

Perhaps the most interesting insight to be gained from our results is the exact quantification of the impact of the eavesdropper density λ_e on the security of communications provided at the physical layer: even a modest density of scattered eavesdroppers can potentially cause a drastic reduction in secure connectivity. In Part II of the paper [32], we study the achievable secrecy rates and the effect of eavesdropper collusion.

Appendix A
Proof that Inequality (19) is Strict

Define the event $F_i \triangleq \{\Pi_e\{\mathcal{B}_{\breve{x}_i}(|\breve{x}_i|)\} \geq 1\}$ and its complementary event E_i, which denote *full* and *empty*, respectively. Using this notation, we can rewrite (18) as

$$p_{\rm in-isol} = \mathbb{P}\left\{\bigwedge_{i=1}^{\infty} F_i\right\} \leq \mathbb{P}\{F_1 \wedge F_2\}.$$

To prove that $p_{\rm in-isol} < \mathbb{P}\{F_1\}$ as in (19), it is sufficient to show that $\mathbb{P}\{F_1 \wedge F_2\} < \mathbb{P}\{F_1\}$, or equivalently, $\mathbb{P}\{F_1\} - \mathbb{P}\{F_1 \wedge F_2\} = \mathbb{P}\{F_1 \wedge E_2\} > 0$. Define the ball $\mathcal{B}_i \triangleq \mathcal{B}_{\breve{x}_i}(|\breve{x}_i|)$. Then, with reference to the auxiliary diagram in Fig. 5(c), we can write

$$\begin{aligned}&\mathbb{P}\{F_1 \wedge E_2\}\\ &\quad= \mathbb{E}_{\Pi_\ell}\left\{\mathbb{P}\{F_1 \wedge E_2 | \Pi_\ell\}\right\}\\ &\quad= \mathbb{E}_{\Pi_\ell}\left\{\left(1 - e^{-\lambda_e \mathbb{A}\{\mathcal{B}_1 \setminus \mathcal{B}_2\}}\right) \cdot e^{-\lambda_e \mathbb{A}\{\mathcal{B}_2\}}\right\}. \quad (35)\end{aligned}$$

Since $\mathcal{B}_1 \not\subseteq \mathcal{B}_2$ a.s., then $\mathbb{A}\{\mathcal{B}_1 \setminus \mathcal{B}_2\} > 0$ a.s., and the argument inside the expectation in (35) is strictly positive, and thus $\mathbb{P}\{F_1 \wedge E_2\} > 0$. This concludes the proof.

Appendix B
Proof of Theorem 3.3

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 the node at the origin by $N_{\rm out}$. For the legitimate nodes, let the distances to the origin (not necessarily ordered) be $R_{\ell,i} \triangleq |x_i|$, $x_i \in \Pi_\ell$, and the corresponding channel propagation effects be $Z_{\ell,i}$. Similarly, we can define $R_{e,i} \triangleq |e_i|$, $e_i \in \Pi_e$, and $Z_{e,i}$ for the eavesdroppers. Define also the loss function as $l(r,z) \triangleq 1/g(r,z)$. We can now consider the one-dimensional loss processes for the legitimate nodes, $\Lambda_\ell \triangleq$

$\{L_{\ell,i}\}_{i=1}^{\infty}$ with $L_{\ell,i} \triangleq l(R_{\ell,i}, Z_{\ell,i})$, and for the eavesdroppers, $\Lambda_e \triangleq \{L_{e,i}\}_{i=1}^{\infty}$ with $L_{e,i} \triangleq l(R_{e,i}, Z_{e,i})$. Note that loss process $\{L_{\ell,i}\}$ can be interpreted as a stochastic mapping of the distance process $\{R_{\ell,i}\}$, where the mapping depends on the random sequence $\{Z_{\ell,i}\}$ (a similar statement can be made for $\{L_{e,i}\}$, $\{R_{e,i}\}$, and $\{Z_{e,i}\}$). With these definitions, the out-degree of node 0 can be expressed as $N_{\text{out}} = \#\{L_{\ell,i} : L_{\ell,i} < \min_k L_{e,k}\}$, i.e., it is the number of occurrences in the process Λ_ℓ before the *first* occurrence in the process Λ_e. In the remainder of the proof, we first characterize the processes Λ_ℓ and Λ_e; then, using appropriate transformations, we map them into homogeneous processes, where the distribution of N_{out} can be readily determined.

Since the RVs $\{Z_{\ell,i}\}$ are i.i.d. in i and independent of $\{R_{\ell,i}\}$, we know from the marking theorem [35, Sec. 5.2] that the points $\{(R_{\ell,i}, Z_{\ell,i})\}$ form a nonhomogeneous Poisson process on $\mathbb{R}^+ \times \mathbb{R}^+$ with density $2\pi\lambda_\ell r f_Z(z)$, where $f_Z(z)$ is the pdf of $Z_{\ell,i}$. Then, from the mapping theorem [35, Sec. 2.3], $\Lambda_\ell = \{l(R_{\ell,i}, Z_{\ell,i})\}$ is also a nonhomogeneous Poisson process on $\mathbb{R}^+$ with density denoted by $\lambda_{\Lambda_\ell}(l)$.[14] Furthermore, the process Λ_ℓ can be made homogeneous through the transformation $M_{\Lambda_\ell}(t) \triangleq \int_0^t \lambda_{\Lambda_\ell}(l)dl$, such that $M_{\Lambda_\ell}(\Lambda_\ell)$ is a Poisson process with density 1. The homogenizing function $M_{\Lambda_\ell}(t)$ can be calculated as follows:

$$M_{\Lambda_\ell}(t) = \iint\limits_{0<l(r,z)<t} 2\pi\lambda_\ell r f_{Z_\ell}(z)drdz.$$

Using a completely analogous reasoning for the process Λ_e, its homogenizing function $M_{\Lambda_e}(t)$ can be written as

$$M_{\Lambda_e}(t) = \iint\limits_{0<l(r,z)<t} 2\pi\lambda_e r f_{Z_e}(z)drdz.$$

But since $f_{Z_\ell}(z) = f_{Z_e}(z)$, it follows that $M_{\Lambda_\ell}(t) = \lambda_\ell/\lambda_e M_{\Lambda_e}(t)$. The out-degree N_{out} can now be easily obtained in the homogenized domain. Consider that both processes Λ_ℓ and Λ_e are homogenized by the *same* transformation $M_{\Lambda_\ell}(\cdot)$, such that $M_{\Lambda_\ell}(\Lambda_l)$ and $M_{\Lambda_\ell}(\Lambda_e)$ are independent Poisson processes with density 1 and λ_e/λ_ℓ. Furthermore, since $M_{\Lambda_\ell}(\cdot)$ is monotonically increasing, N_{out} can be re-expressed as

$$N_{\text{out}} = \#\left\{L_{\ell,i} : M_{\Lambda_\ell}(L_{\ell,i}) < M_{\Lambda_\ell}(\min_k L_{e,k})\right\}.$$

In this homogenized domain, the propagation effects have disappeared, and the problem is now equivalent to that in Theorem 3.2. Specifically, when there is an arrival in the merged process $M_{\Lambda_\ell}(\Lambda_\ell) \cup M_{\Lambda_\ell}(\Lambda_e)$, it comes from process $M_{\Lambda_\ell}(\Lambda_\ell)$ with probability $p = 1/(1 + \lambda_e/\lambda_\ell) = \lambda_\ell/(\lambda_\ell + \lambda_e)$, and from $M_{\Lambda_\ell}(\Lambda_e)$ with probability $1 - p = \lambda_e/(\lambda_\ell + \lambda_e)$. As a result, N_{out} has exactly the same PMF as the one given in (12), and is, therefore, invariant with respect to the distribution $f_Z(z)$.

[14]In our theorem, the continuity of the function $f_Z(z)$ is sufficient to ensure that Λ_ℓ is a Poisson process. In general, we may allow Dirac impulses in $f_Z(z)$, as long as the distinct points $\{(R_{\ell,i}, Z_{\ell,i})\}$ do not pile on top of one another when forming the process $\Lambda_\ell = \{l(R_{\ell,i}, Z_{\ell,i})\}$.

APPENDIX C
DERIVATION OF (34)

Because Π_ℓ is a Poisson process, the Palm probability $\mathbb{P}_x\{|x| < R_{e,1}\}$ in (33) 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

$$\begin{aligned}
\mathbb{P}_x\{|x| < R_{e,1}\} &= \mathbb{P}_{\Theta,\Pi_e}\left\{\Pi_e\left\{\overline{\Theta} \cap \mathcal{D}(\rho, |x|) \setminus \mathcal{B}_x(\rho)\right\} = 0\right\} \\
&\geq \mathbb{P}_{\Theta,\Pi_e}\left\{\Pi_e\left\{\overline{\Theta} \cap \mathcal{D}(\rho, |x|)\right\} = 0\right\} \\
&= \mathbb{E}_\Theta\left\{\exp(-\lambda_e \mathbb{A}\left\{\overline{\Theta} \cap \mathcal{D}(\rho, |x|)\right\}\right\} \qquad (36) \\
&\geq \exp\left(-\lambda_e \mathbb{E}_\Theta\left\{\mathbb{A}\left\{\overline{\Theta} \cap \mathcal{D}(\rho, |x|)\right\}\right\}\right) \qquad (37)
\end{aligned}$$

where $\mathbb{A}\{\mathcal{R}\}$ denotes the area of the arbitrary region $\mathcal{R}$. Equation (36) follows from conditioning on Θ, and using the fact that Π_e and Θ are independent. Equation (37) follows from Jensen's inequality. The term inside the exponential in (37) corresponds to the average area of a random shape, and can be computed using Fubini's theorem as

$$\begin{aligned}
&\mathbb{E}_\Theta\left\{\mathbb{A}\left\{\overline{\Theta} \cap \mathcal{D}(\rho, |x|)\right\}\right\} \\
&= \mathbb{E}_\Theta\left\{\iint\limits_{\mathbb{R}^2} \mathbb{1}\left\{y \in \overline{\Theta} \cap \mathcal{D}(\rho, |x|)\right\} dy\right\} \\
&= \iint\limits_{\mathcal{D}(\rho,|x|)} \mathbb{P}\{y \in \overline{\Theta}\} dy \\
&= \iint\limits_{\mathcal{D}(\rho,|x|)} \underbrace{e^{-\lambda_\ell \pi \rho^2}}_{\triangleq p_{\overline{\Theta}}} dy \\
&= p_{\overline{\Theta}} \pi\left(|x|^2 - \rho^2\right). \qquad (38)
\end{aligned}$$

Note that $p_{\overline{\Theta}}$ corresponds to the probability that a fixed point y is *outside* the total neutralization region Θ, and does not depend on the coordinates of y due to the stationarity of the process Θ. Replacing (38) into (37), we obtain the desired inequality in (34).

ACKNOWLEDGMENT

The authors would like to thank L. A. Shepp, J. N. Tsitsiklis, V. K. Goyal, Y. Shen, and W. Suwansantisuk for their helpful suggestions.

REFERENCES

[1] C. E. Shannon, "Communication theory of secrecy systems," *Bell Syst. Tech. J.*, vol. 29, pp. 656–715, 1949.
[2] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1367, Oct. 1975.
[3] I. Csiszár and J. Korner, "Broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. IT-24, no. 3, pp. 339–348, May 1978.
[4] S. Leung-Yan-Cheong and M. Hellman, "The Gaussian wire-tap channel," *IEEE Trans. Inf. Theory*, vol. IT-24, no. 4, pp. 451–456, Jul. 1978.
[5] A. Hero, "Secure space-time communication," *IEEE Trans. Inf. Theory*, 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 Conf.*, Dallas, TX, Sep. 2005, vol. 3, pp. 1906–1910.

[7] E. Ekrem and S. Ulukus, "Secrecy capacity region of the gaussian multi-receiver wiretap channel," in *Proc. IEEE Int. Symp. Inf. Theory*, Seoul, Korea, Jun. 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, Jun. 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. Communications, Control, and Computing*, Monticello, IL, Sep. 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] E. Ekrem and S. Ulukus, "Secrecy in cooperative relay broadcast channels," in *Proc. IEEE Int. Symp. Inf. Theory*, Toronto, ON, Jul. 2008, pp. 2217–2221.
[13] P. Parada and R. Blahut, "Secrecy capacity of SIMO and slow fading channels," in *Proc. IEEE Int. Symp. Inf. Theory*, Adelaide, Australia, Sep. 2005, pp. 2152–2155.
[14] P. Gopala, L. Lai, and H. El Gamal, On the Secrecy Capacity of Fading Channels arxiv preprint cs.IT/0610103, 2006.
[15] Z. Li, R. Yates, and W. Trappe, "Secrecy capacity of independent parallel channels," in *Proc. Annu. Allerton Conf. Communication, Control and Computing*, Sep. 2006, pp. 841–848.
[16] 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, Jun. 2008.
[17] Y. Liang, H. V. Poor, and S. Shamai, "Secure communication over fading channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2470–2492, Jun. 2008.
[18] 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, p. 351, 2000.
[19] J. Barros and M. Bloch, "Strong secrecy for wireless channels," in *Proc. Int. Conf. Inf. Theor. Security*, Calgary, Canada, Aug. 2008.
[20] U. Maurer, "Secret key agreement by public discussion from common information," *IEEE Trans. Inf. Theory*, vol. 39, no. 3, pp. 733–742, May 1993.
[21] 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, Jul. 1993.
[22] 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, Mar. 1999.
[23] 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. Inf. Theory*, Seattle, WA, 2006.
[24] A. Thangaraj, S. Dihidar, A. R. Calderbank, S. McLaughlin, and J.-M. Merolla, "On achieving capacity on the wire tap channel using LDPC codes," in *Proc. IEEE Int. Symp. Inf. Theory*, Adelaide, Australia, Sep. 2005, pp. 1498–1502.
[25] 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.
[26] J. Muramatsu, "Secret key agreement from correlated source outputs using low density parity check matrices," *IEICE Trans. Fund. Elec. Commun. Comp.*, vol. E89-A, no. 7, pp. 2036–2046, Jul. 2006.
[27] H. Mahdavifar and A. Vardy, Achieving the Secrecy Capacity of Wiretap Channels Using Polar Codes 2010 [Online]. Available: http://arxiv.org/abs/1001.0210
[28] M. Haenggi, "The secrecy graph and some of its properties," in *Proc. IEEE Int. Symp. Inf. Theory*, Toronto, Canada, Jul. 2008.
[29] P. C. Pinto, J. O. Barros, and M. Z. Win, "Physical-layer security in stochastic wireless networks," in *Proc. IEEE Int. Conf. Commun. Systems*, Guangzhou, China, Nov. 2008, pp. 974–979.
[30] Y. Liang, H. V. Poor, and L. Ying, "Secrecy throughput of MANETs with malicious nodes," in *Proc. IEEE Int. Symp. Inf. Theory*, Jun. 2009, pp. 1189–1193.
[31] O. O. Koyluoglu, C. E. Koksal, and H. E. Gamal, "On secrecy capacity scaling in wireless networks," in *Proc. Inf. Theory and Applications Workshop*, San Diego, CA, Feb. 2010, pp. 1–4.
[32] P. C. Pinto, J. O. Barros, and M. Z. Win, "Secure communication in stochastic wireless networks—Part II: Maximum rate and collusion," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 1, Feb. 2011.
[33] M. Z. Win, P. C. Pinto, and L. A. Shepp, "A mathematical theory of network interference and its applications," *Special Issue on Ultra-Wide Bandwidth (UWB) Technology and Emerging Applications, Proc. IEEE*, vol. 97, no. 2, pp. 205–230, Feb. 2009.
[34] H. Inaltekin, M. Chiang, H. V. Poor, and S. B. Wicker, "The behavior of unbounded path-loss models and the effect of singularity on computed network characteristics," *IEEE J. Sel. Areas Commun.*, vol. 27, no. 7, pp. 1078–1092, Sep. 2009.
[35] J. Kingman, *Poisson Processes*. London, U.K.: Oxford Univ. Press, 1993.
[36] D. Stoyan, W. S. Kendall, and J. Mecke, *Stochastic Geometry and Its Applications*. Hoboken, NJ: Wiley, 1995.
[37] M. Abramowitz and I. A. Stegun, *Handbook of Mathematical Functions*. New York: Dover, 1970.
[38] E. N. Gilbert, "Random subdivisions of space into crystals," *Ann. Math. Statist.*, vol. 33, pp. 958–972, 1962.
[39] D. P. Bertsekas and J. N. Tsitsiklis, *Introduction to Probability*. Belmont, MA: Athena Scientific, 2002.
[40] R. Meester and R. Roy, *Continuum Percolation*. Cambridge, U.K.: Cambridge Univ. Press, 1996.

Pedro C. Pinto (S'04–M'10) received the Licenciatura degree with highest honors in electrical and computer engineering from the University of Porto, Portugal, in 2003, and the M.S. degree in electrical engineering and computer science from the Massachusetts Institute of Technology (MIT), in 2006. Since 2004, he has been with the MIT Laboratory for Information and Decision Systems (LIDS), where he is now a Ph.D. candidate.

His main research interests are in wireless communications and signal processing.

Mr. Pinto was the recipient of the MIT Claude E. Shannon Fellowship in 2007, the Best Student Paper Award at the IEEE International Conference on Ultra-Wideband in 2006, and the Infineon Technologies Award in 2003.

João Barros (M'04) received his undergraduate education in electrical and computer engineering from the Universidade do Porto (UP), Portugal, and Universitaet Karlsruhe, Germany, and the Ph.D. degree in electrical engineering and information technology from the Technische Universitaet Muenchen (TUM), Germany.

He is an Associate Professor of Electrical and Computer Engineering at the University of Porto and the head of the Instituto de Telecomunicações in Porto, Portugal. Since 2008, he has also been a Visiting Professor with the Massachusetts Institute of Technology (MIT). In February 2009, he was appointed National Director of the CMU-Portugal Program, a five-year international partnership with a total budget of 56M Euros, which fosters collaborative research and advanced training among 12 Portuguese universities and research institutes, Carnegie Mellon University, and more than 80 companies. In recent years, he has published more than 120 papers in the fields of information theory, networking and security, with a special focus on network coding, physical-layer security, sensor networks, and intelligent transportation systems.

Dr. Barros was the recipient of the 2010 IEEE Communications Society Young Researcher Award for Europe, the Middle East, and Africa region and of a best teaching award by the Bavarian State Ministry of Sciences, Research and the Arts. Work he coauthored on wireless information-theoretic security received the IEEE Communications Society and Information Theory Society Joint Paper Award, resulting in a book titled *Physical-Layered Security: From Information Theory to Security Engineering* and published by Cambridge University Press in 2011.

Moe Z. Win (S'85–M'87–SM'97–F'04) received the B.S. degree (*magna cum laude*) in electrical engineering from Texas A&M University in 1987, the M.S. degree in electrical engineering from the University of Southern California (USC) in 1989, and both the Ph.D. degree in electrical engineering and the M.S. degree in applied mathematics as a Presidential Fellow from USC in 1998.

He is an Associate Professor at the Massachusetts Institute of Technology (MIT). Prior to joining MIT, he was at AT&T Research Laboratories for five years and at the Jet Propulsion Laboratory for seven years. His research encompasses developing fundamental theory, designing algorithms, and conducting experimentation for a broad range of real-world problems. His current research topics include location-aware networks, time-varying channels, multiple antenna systems, ultra-wide bandwidth systems, optical transmission systems, and space communications systems.

Prof. Win is an IEEE Distinguished Lecturer and elected Fellow of the IEEE, cited for "contributions to wideband wireless transmission." He was honored with the IEEE Eric E. Sumner Award (2006), an IEEE Technical Field Award for "pioneering contributions to ultra-wideband communications science and technology." Together with students and colleagues, his papers have received several awards including the IEEE Communications Society's Guglielmo Marconi Best Paper Award (2008) and the IEEE Antennas and Propagation Society's Sergei A. Schelkunoff Transactions Prize Paper Award (2003). His other recognitions include the Laurea Honoris Causa from the University of Ferrara, Italy (2008), the Technical Recognition Award of the IEEE ComSoc Radio Communications Committee (2008), Wireless Educator of the Year Award (2007), the Fulbright Foundation Senior Scholar Lecturing and Research Fellowship (2004), the U.S. Presidential Early Career Award for Scientists and Engineers (2004), the AIAA Young Aerospace Engineer of the Year (2004), and the Office of Naval Research Young Investigator Award (2003).