Secure Communication in Stochastic Wireless Networks—Part II: Maximum Rate and Collusion

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

***Abstract*—In Part I of this paper, we introduced the *intrinsically secure communications graph* ($i\mathcal{S}$-graph)—a random graph which describes the connections that can be established with strong secrecy over a large-scale network, in the presence of eavesdroppers. We focused on the local connectivity of the $i\mathcal{S}$-graph, and proposed techniques to improve it. In this second part, we characterize the maximum secrecy rate (MSR) that can be achieved between a node and its neighbors. We then consider the scenario where the eavesdroppers are allowed to collude, i.e., exchange and combine information. We quantify exactly how eavesdropper collusion degrades the secrecy properties of the network, in comparison to a noncolluding scenario. Our analysis helps clarify how the presence of eavesdroppers can jeopardize the success of wireless physical-layer security.**

***Index Terms*—Colluding eavesdroppers, physical-layer security, secrecy capacity, stochastic geometry, wireless networks.**

I. Introduction

THE ability to exchange secret information is critical to many commercial, governmental, and military networks. Although much has been achieved in terms of securing the higher layers of the classical protocol stack, protecting the physical layer of wireless networks from one or multiple eavesdroppers remains a formidable task. The theoretical foundation for physical-layer security over noisy channels, which builds on the notion of *perfect secrecy* [1], was laid in [2] and later in [3]. More recently, space–time signal processing techniques for secure communication over wireless links appeared in [4], and the secrecy capacity of various single-input multiple-output (SIMO) fading channels was established in [5]. The concept of outage secrecy capacity of slow fading channels was presented in detail in [6], whereas the ergodic secrecy capacity of fading channels was derived in [7] and [8]. The presence of colluding eavesdroppers is considered in [9], but restricting its attention to a fixed number of eavesdroppers placed at the same spatial location.

In Part I of this paper [10], we introduced 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 focused on the local connectivity of the $i\mathcal{S}$-graph. In this second part, we study the achievable secrecy rates, as well as the effect of eavesdropper collusion on secure connectivity. The main contributions of this paper are as follows:

1) *Maximum secrecy rate (MSR) in the $i\mathcal{S}$-graph:* We provide a complete probabilistic characterization of the MSR between a typical node of the Poisson $i\mathcal{S}$-graph and each of its neighbors. In addition, we derive expressions for the probability of existence of a nonzero MSR, and the probability of secrecy outage.
2) *The case of colluding eavesdroppers:* We provide a characterization of the MSR and average node degrees for scenarios in which the eavesdroppers are allowed to collude. We quantify exactly how eavesdropper collusion degrades the secrecy properties of the legitimate nodes, in comparison to a noncolluding scenario.

This paper is organized as follows. Section II briefly reviews the system model introduced in Part I. Section III considers the MSR between a node and its neighbors. Section IV characterizes the case of colluding eavesdroppers. Section V concludes the paper and summarizes important findings.

II. Model Summary

We briefly review the system model. The $i\mathcal{S}$-graph, introduced in Part I, is a convenient representation of the links that can be established with information-theoretic security in a large-scale network. If $\Pi_\ell = \{x_i\}$ denotes the set of legitimate nodes and $\Pi_e = \{e_i\}$ the set of eavesdroppers, then the edge set of the $i\mathcal{S}$-graph is given by

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

where ϱ is the desired secrecy rate for each communication link; and $\mathcal{R}_s(x_i, x_j)$ is the MSR of the legitimate link $\overrightarrow{x_i x_j}$, given in [10, eq. (4)].

For the purpose of this paper, we can write the received power associated with link $\overrightarrow{x_i x_j}$ as $P_{rx}(r) = P_\ell \cdot g(r)$, where P_ℓ is the transmit power, r is the link length, and g is the channel

Manuscript received February 08, 2011; accepted June 30, 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 Symposium on Information Theory (ISIT'09), Seoul, South Korea, Jun. 2009. The associate editor coordinating the review of this manuscript and approving it for publication was Dr. Wade Trappe.

P. C. Pinto is with the Audiovisual Communications Laboratory, Swiss Federal Institute of Technology, Ecole Polytechnique Fédérale de Lausanne (EPFL), CH-1015, Lausanne, Switzerland (e-mail: pedro.pinto@epfl.ch).

J. Barros is with Departamento de Engenharia Electrotécnica e de Computadores (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.2011.2165947

TABLE I
NOTATION AND SYMBOLS

Symbol	Usage
$\mathbb{E}\{\cdot\}$	Expectation operator
$\mathbb{P}\{\cdot\}$	Probability operator
$*$	Convolution operator
$\dagger$	Conjugate transpose operator
$f_X(x)$	Probability density function of X
$F_X(x)$	Cumulative distribution function of X
$H(X)$	Entropy of X
$\Pi_\ell = \{x_i\}, \Pi_\mathrm{e} = \{e_i\}$	Poisson processes of legitimate nodes and eavesdroppers
$\lambda_\ell, \lambda_\mathrm{e}$	Spatial densities of legitimate nodes and eavesdroppers
$\Pi\{\mathcal{R}\}$	Number of nodes of process Π in region $\mathcal{R}$
$N_\mathrm{in}, N_\mathrm{out}$	In-degree and out-degree of a node
$\mathcal{B}_x(\rho)$	Ball centered at x with radius ρ
$\mathcal{D}(a,b)$	Annular region between radiuses a and b, centered at the origin
$\mathbb{A}\{\mathcal{R}\}$	Area of region $\mathcal{R}$
$R_{\ell,i}$	Distance between $x_i \in \Pi_\ell$ and origin
$R_{\mathrm{e},i}$	Distance between $e_i \in \Pi_\mathrm{e}$ and origin
$\#S$	Number of elements in the set S
$\mathcal{G}(x,\theta)$	Gamma distribution with mean $x\theta$ and variance $x\theta^2$
$\mathcal{N}(\mu,\sigma^2)$	Gaussian distribution with mean μ and variance σ^2
$\mathcal{S}(\alpha,\beta,\gamma)$	Stable distribution with characteristic exponent α, skewness β, and dispersion γ

gain function satisfying the conditions in [10, Sec. II-A]. In the remainder of the paper, we consider that Π_ℓ, Π_e are mutually independent, homogeneous Poisson point processes with densities λ_ℓ and λ_e, respectively. We use $\{R_{\ell,i}\}_{i=1}^{\infty}$ and $\{R_{e,i}\}_{i=1}^{\infty}$ to denote the ordered random distances between the origin of the coordinate system and the nodes in Π_ℓ and Π_e, respectively, where $R_{\ell,1} \le R_{\ell,2} \le \cdots$ and $R_{e,1} \le R_{e,2} \le \cdots$. A summary of the notation and symbols can be found in Table I.

III. MSR IN THE POISSON $i\mathcal{S}$-GRAPH

In Part I of the paper, we characterized *secure connectivity*, i.e., the connections whose MSR $\mathcal{R}_s(x_i,x_j)$ exceed the threshold ϱ in (1). However, we did not provide any characterization of the actual secrecy rate $\mathcal{R}_s(x_i,x_j)$ supported by the link $\overrightarrow{x_ix_j}$. In this section, we analyze the MSR between a node and each of its neighbors, as well as the probability of existence of a nonzero MSR, and the probability of secrecy outage. To obtain additional insights, we consider that the noise powers of legitimate nodes and eavesdroppers are equal ($\sigma_e^2 = \sigma_\ell^2 = \sigma^2$) and that the channel gain is of the form $g(r) = 1/r^{2b}$, 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).

A. Distribution of the MSR

Considering the coordinate system depicted in [10, Fig. 4], the MSR $\mathcal{R}_{s,i}$ between the node at the origin and its ith closest neighbor $i \ge 1$ can be written for a given realization of the node positions Π_ℓ and Π_e as

$$\mathcal{R}_{s,i} = \left[\log_2\left(1+\frac{P_\ell}{R_{\ell,i}^{2b}\sigma^2}\right) - \log_2\left(1+\frac{P_\ell}{R_{e,1}^{2b}\sigma^2}\right)\right]^+ \quad (2)$$

in bits per complex dimension, where $[x]^+ = \max\{x,0\}$. For each instantiation of the random Poisson processes Π_ℓ and Π_e, a realization of the random variable (RV) $\mathcal{R}_{s,i}$ is obtained. The following theorem provides the distribution of this random variable.

Theorem 3.1: The MSR $\mathcal{R}_{s,i}$ between a typical node and its ith closest neighbor $i \ge 1$ is an RV whose cumulative distribution function (cdf) $F_{\mathcal{R}_{s,i}}(\varrho)$ is given by

$$F_{\mathcal{R}_{s,i}}(\varrho) = 1 - \frac{\ln 2(\pi\lambda_\ell)^i}{(i-1)!b}\left(\frac{P_\ell}{\sigma^2}\right)^{i/b}\int_\varrho^{+\infty}\frac{2^z}{(2^z-1)^{1+i/b}} \times \exp\left(-\pi\lambda_\ell\left(\frac{\frac{P_\ell}{\sigma^2}}{2^z-1}\right)^{1/b} - \pi\lambda_e\left(\frac{\frac{P_\ell}{\sigma^2}}{2^{z-\varrho}-1}\right)^{1/b}\right)dz \quad (3)$$

for $\varrho \ge 0$.

Proof: See Appendix A. □

B. Existence and Outage of the MSR

Based on the results of Section III-A, we can now obtain the probability of existence of a nonzero MSR, and the probability of secrecy outage.

Corollary 3.1: Considering the link between a typical node and its ith closest neighbor $i \ge 1$, the probability of *existence* of a nonzero MSR, $p_{\mathrm{exist},i} = \mathbb{P}\{\mathcal{R}_{s,i} > 0\}$, is given by

$$p_{\mathrm{exist},i} = \left(\frac{\lambda_\ell}{\lambda_\ell+\lambda_e}\right)^i \quad (4)$$

and the probability of an *outage* in MSR, $p_{\mathrm{outage},i}(\varrho) = \mathbb{P}\{\mathcal{R}_{s,i} < \varrho\} = F_{\mathcal{R}_{s,i}}(\varrho)$, is given in (3).

Proof: To obtain (4), we note that the event $\{\mathcal{R}_{\ell,i} > \mathcal{R}_e\}$ is equivalent to $\{N_\mathrm{out} \ge i\}$. Thus, we use [10, eq. (12)] to write

$$\begin{aligned} p_{\mathrm{exist},i} &= \mathbb{P}\{\mathcal{R}_{\ell,i} > \mathcal{R}_e\} \\ &= \sum_{n=i}^{\infty}\left(\frac{\lambda_\ell}{\lambda_\ell+\lambda_e}\right)^n\left(\frac{\lambda_e}{\lambda_\ell+\lambda_e}\right) \\ &= \left(\frac{\lambda_\ell}{\lambda_\ell+\lambda_e}\right)^i. \end{aligned}$$

The expression for $p_{\mathrm{outage}}(\varrho)$ follows directly from (3). □

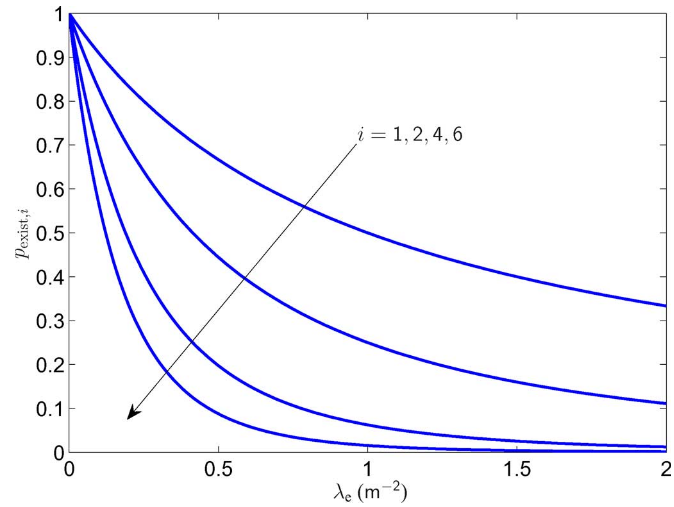

Fig. 1. Probability $p_{\text{exist},i}$ of existence of a nonzero MSR versus the eavesdropper density λ_e, for various values of the neighbor index i ($\lambda_\ell = 1$ m^{-2}, $b = 2$, $P_\ell/\sigma^2 = 10$, $\varrho = 1$ bit).

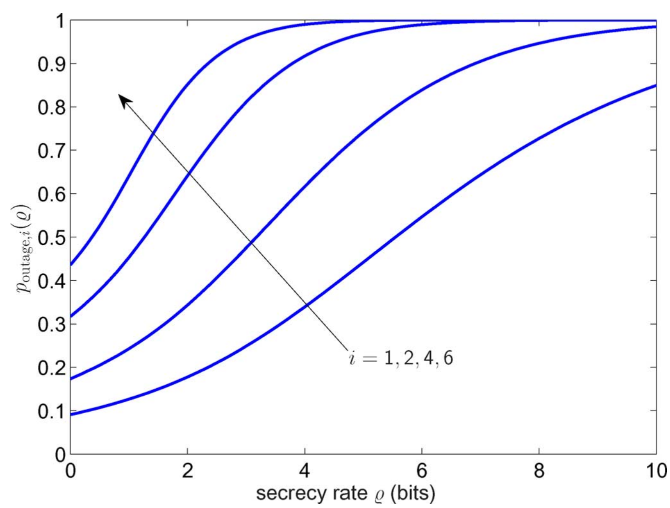

Fig. 2. Probability $p_{\text{outage},i}$ of secrecy outage between a node and its ith closest neighbor, for various values of the neighbor index i ($\lambda_\ell = 1$ m^{-2}, $\lambda_e = 0.1$ m^{-2}, $b = 2$, $P_\ell/\sigma^2 = 10$).

C. Numerical Results

Fig. 1 shows the probability $p_{\text{exist},i}$ of existence of a nonzero MSR from a typical node to its ith neighbor, as a function of the eavesdropper density λ_e. It can be seen that the existence of a nonzero MSR $\mathcal{R}_{s,i}$ to any neighbor i becomes less likely as the value of λ_e increases. Furthermore, since $R_{\ell,1} \leq R_{\ell,2} \leq \cdots$, as the value of i increases, the ith neighbor becomes further away, and the corresponding $p_{\text{exist},i}$ decreases.

Fig. 2 shows the probability $p_{\text{outage},i}$ of secrecy outage of a typical node transmitting to its ith neighbor, as a function of the desired secrecy rate ϱ. As expected, a secrecy outage becomes more likely as we increase the target secrecy rate ϱ set by the transmitter.

IV. The Case of Colluding Eavesdroppers

We now aim to study the effect of colluding eavesdroppers on the secrecy of communications. In Sections IV-A–IV-D, we first consider a *single* legitimate link with deterministic length r_ℓ in the presence of a random process Π_e. Such simplification eliminates the randomness associated with the position of the legitimate nodes. We then consider both random processes Π_ℓ and Π_e in Section IV-E, and characterize the average node degree in the presence of eavesdropper collusion.

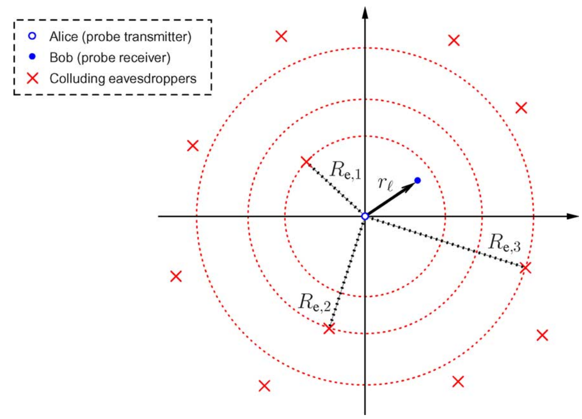

Fig. 3. Communication in the presence of colluding eavesdroppers.

A. MSR of a Single Link

We consider the scenario depicted in Fig. 3, where a legitimate link is composed of two nodes: one transmitter located at the origin (Alice), and one receiver located at a deterministic distance r_ℓ from the origin (Bob). The eavesdroppers have the ability to *collude*, i.e., they can exchange and combine the information received by all the eavesdroppers to decode the secret message. The eavesdroppers are scattered in the two-dimensional plane according to an *arbitrary* spatial process Π_e, and their distances to the origin are denoted by $\{R_{e,i}\}_{i=1}^{\infty}$, where $R_{e,1} \leq R_{e,2} \leq \cdots$.

Since the colluding eavesdroppers may gather the received information and send it to a central processor, the scenario depicted in Fig. 3 can be viewed as the SIMO Gaussian wiretap channel in Fig. 4. Here, the input is the signal transmitted by Alice, and the output of the wiretap channel is the collection of signals received by all the eavesdroppers. We consider that Alice sends a symbol $x \in \mathbb{C}$ with power constraint $\mathbb{E}\{|x|^2\} \leq P_\ell$. The vectors $\mathbf{h}_\ell \in \mathbb{C}^m$ and $\mathbf{h}_e \in \mathbb{C}^n$ represent, respectively, the gains of the legitimate and eavesdropper channels.[1] The noise is represented by the vectors $\mathbf{w}_\ell \in \mathbb{C}^m$ and $\mathbf{w}_e \in \mathbb{C}^n$, which are considered to be mutually independent Gaussian RVs with zero mean and nonsingular covariance matrices $\mathbf{\Sigma}_\ell$ and $\mathbf{\Sigma}_e$, respectively. The system of Fig. 4 can then be summarized as

$$\mathbf{y}_\ell = \mathbf{h}_\ell x + \mathbf{w}_\ell \tag{5}$$
$$\mathbf{y}_e = \mathbf{h}_e x + \mathbf{w}_e. \tag{6}$$

The scenario of interest can be obtained from the SIMO Gaussian wiretap channel in Fig. 4 by appropriate choice of the parameters $\mathbf{h}_\ell$, $\mathbf{h}_e$, $\mathbf{\Sigma}_\ell$, and $\mathbf{\Sigma}_e$, as shown in the following theorem.

[1]We use boldface letters to denote vectors and matrices.

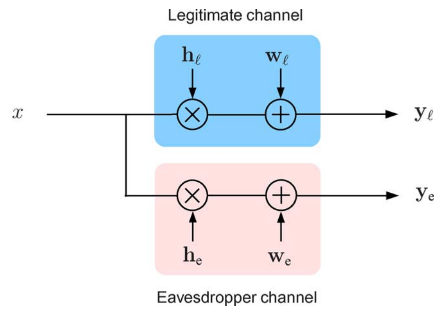

Fig. 4. SIMO Gaussian wiretap channel, which can be used to analyze the scenario of colluding eavesdroppers depicted in Fig. 3.

Theorem 4.1: For a given realization of the arbitrary eavesdropper process Π_e, the MSR of the legitimate link is given by

$$\mathcal{R}_s = \left[\log_2\left(1+\frac{P_\ell \cdot g(r_\ell)}{\sigma_\ell^2}\right) - \log_2\left(1+\frac{P_\ell \sum_{i=1}^{\infty} g(R_{e,i})}{\sigma_e^2}\right)\right]^+ \tag{7}$$

where $P_\ell \sum_{i=1}^{\infty} g(R_{e,i}) \triangleq P_{rx,e}$ is the aggregate power received by all the eavesdroppers.

Proof: For a given realization of the channels $\mathbf{h}_\ell$ and $\mathbf{h}_e$, it can be shown [11] that $\widetilde{y}_\ell = \mathbf{h}_\ell^\dagger \mathbf{\Sigma}_\ell^{-1}\mathbf{y}_\ell$ and $\widetilde{y}_e = \mathbf{h}_e^\dagger \mathbf{\Sigma}_e^{-1}\mathbf{y}_e$ are sufficient statistics to estimate x from the corresponding observations $\mathbf{y}_\ell$ and $\mathbf{y}_e$.[2] Since sufficient statistics preserve mutual information [12], for the purpose of determining the MSR the vector channels in (5) and (6) can be equivalently written in a (complex) scalar form corresponding to the Gaussian wiretap channel introduced in [13]. Thus, the MSR $\mathcal{R}_s$ of the legitimate channel for a given realization of the channels $\mathbf{h}_\ell$ and $\mathbf{h}_e$ is given by

$$\mathcal{R}_s = \left[\log_2\left(\frac{1+\mathbf{h}_\ell^\dagger \Sigma_\ell^{-1}\mathbf{h}_\ell P_\ell}{1+\mathbf{h}_e^\dagger \Sigma_e^{-1}\mathbf{h}_e P_\ell}\right)\right]^+. \tag{8}$$

Setting $\mathbf{h}_\ell = \sqrt{g(r_\ell)}$, $\mathbf{h}_e = \left[\sqrt{g(R_{e,1})}, \sqrt{g(R_{e,2})}, \ldots\right]^T$, $\mathbf{\Sigma}_\ell = \sigma_\ell^2 \mathbf{I}_1$, and $\mathbf{\Sigma}_e = \sigma_e^2 \mathbf{I}_\infty$, where σ_ℓ^2 and σ_e^2 are the noise powers of the legitimate and eavesdropper receivers, respectively, and $\mathbf{I}_n$ is the $n \times n$ identity matrix, then (8) reduces to (7). This concludes the proof. □

B. Distribution of the MSR of a Single Link

Theorem 4.1 is valid for a given realization of the spatial process Π_e. In general, the MSR $\mathcal{R}_s$ of the legitimate link is an RV, since it is a function the random eavesdropper distances $\{R_{e,i}\}_{i=1}^{\infty}$. The following theorem characterizes the distribution of the MSR.

Theorem 4.2: If Π_e is a Poisson process with density λ_e and $g(r) = 1/r^{2b}$, $b > 1$, the MSR $\mathcal{R}_s$ of the legitimate link is an RV whose cdf $F_{\mathcal{R}_s}(\varrho)$ is given by

$$F_{\mathcal{R}_s}(\varrho) = \begin{cases} 0, & \varrho < 0 \\ 1 - F_{\widetilde{P}_{rx,e}}\left(\dfrac{\left(1+\frac{P_\ell}{r_\ell^{2b}\sigma_\ell^2}\right)2^{-\varrho}-1}{(\pi\lambda_e \mathcal{C}_{1/b}^{-1})^b \frac{P_\ell}{\sigma_e^2}}\right), & 0 \le \varrho < \mathcal{R}_\ell \\ 1, & \varrho \ge \mathcal{R}_\ell \end{cases} \tag{9}$$

where $\mathcal{R}_\ell = \log_2\left(1 + P_\ell / r_\ell^{2b}\sigma_\ell^2\right)$ is the capacity of the legitimate channel; $\mathcal{C}_\alpha$ is defined as

$$\mathcal{C}_\alpha \triangleq \frac{1-\alpha}{\Gamma(2-\alpha)\cos\left(\frac{\pi\alpha}{2}\right)} \tag{10}$$

with $\Gamma(\cdot)$ denoting the gamma function; and $F_{\widetilde{P}_{rx,e}}(\cdot)$ is the cdf of a skewed stable RV $\widetilde{P}_{rx,e}$, with parameters[3]

$$\widetilde{P}_{rx,e} \sim \mathcal{S}\left(\alpha = \frac{1}{b},\ \beta = 1,\ \gamma = 1\right). \tag{12}$$

Proof: For $g(r) = 1/r^{2b}$, the MSR $\mathcal{R}_s$ of the legitimate channel in (7) is a function of the total power received by the eavesdroppers, $P_{rx,e} = \sum_{i=1}^{\infty} P_\ell / R_{e,i}^{2b}$. If Π_e is a Poisson process, the characteristic function of $P_{rx,e}$ can be written as [15]

$$P_{rx,e} \sim \mathcal{S}\left(\alpha = \frac{1}{b},\ \beta = 1,\ \gamma = \pi\lambda_e \mathcal{C}_{1/b}^{-1} P_\ell^{1/b}\right) \tag{13}$$

for $b > 1$. Defining the normalized stable RV $\widetilde{P}_{rx,e} \triangleq P_{rx,e}\gamma^{-b}$ with $\gamma = \pi\lambda_e \mathcal{C}_{1/b}^{-1} P_\ell^{1/b}$, we have $\widetilde{P}_{rx,e} \sim \mathcal{S}(1/b, 1, 1)$ from the scaling property [14]. In general, the cdf $F_{\widetilde{P}_{rx,e}}(\cdot)$ cannot be expressed in closed form except in the case where $b = 2$, which is analyzed in Section IV-F. However, the characteristic function of $\widetilde{P}_{rx,e}$ has the simple form of $\phi_{\widetilde{P}_{rx,e}}(w) = \exp\left(-|w|^{1/b}\left[1 - j\,\mathrm{sign}(w)\tan(\pi/2b)\right]\right)$, and thus $F_{\widetilde{P}_{rx,e}}(\cdot)$ can always be expressed in the integral form for numerical evaluation. Using (7), we can now express $F_{\mathcal{R}_s}(\varrho)$ in terms of the cdf of $\widetilde{P}_{rx,e}$, for $0 \le \varrho < \mathcal{R}_\ell$, as

$$\begin{aligned} F_{\mathcal{R}_s}(\varrho) &= \mathbb{P}\{\mathcal{R}_s \le \varrho\} \\ &= 1 - \mathbb{P}\left\{P_{rx,e} \le \sigma_e^2\left[\left(1+\frac{P_\ell}{r_\ell^{2b}\sigma_\ell^2}\right)2^{-\varrho}-1\right]\right\} \\ &= 1 - F_{\widetilde{P}_{rx,e}}\left(\frac{\left(1+\frac{P_\ell}{r_\ell^{2b}\sigma_\ell^2}\right)2^{-\varrho}-1}{(\pi\lambda_e \mathcal{C}_{1/b}^{-1})^b \frac{P_\ell}{\sigma_e^2}}\right). \end{aligned}$$

In addition, $F_{\mathcal{R}_s}(\varrho) = 0$ for $\varrho < 0$ and $F_{\mathcal{R}_s}(\varrho) = 1$ for $\varrho \ge \mathcal{R}_\ell$, since the RV $\mathcal{R}_s$ in (7) satisfies $0 \le \mathcal{R}_s \le \mathcal{R}_\ell$, i.e., the MSR of the legitimate link in the presence of colluding eavesdroppers is a positive quantity which cannot be greater than the MSR of the legitimate link *in the absence of eavesdroppers*. This is the result in (9) and the proof is complete. □

[2]We use † to denote the conjugate transpose operator.

[3]We use $\mathcal{S}(\alpha, \beta, \gamma)$ to denote the distribution of a real stable RV with characteristic exponent $\alpha \in (0, 2]$, skewness $\beta \in$ [-1, 1], and dispersion $\gamma \in [0, \infty)$. The corresponding characteristic function is [14]

$$\phi(w) = \begin{cases} \exp\left(-\gamma|w|^\alpha\left[1 - j\beta\,\mathrm{sign}(w)\tan\left(\frac{\pi\alpha}{2}\right)\right]\right), & \alpha \ne 1 \\ \exp\left(-\gamma|w|\left[1 + j\frac{2}{\pi}\beta\,\mathrm{sign}(w)\ln|w|\right]\right), & \alpha = 1. \end{cases} \tag{11}$$

TABLE II
COMPARISON BETWEEN THE CASES OF NONCOLLUDING AND COLLUDING EAVESDROPPERS, CONSIDERING A SINGLE LEGITIMATE LINK AND A CHANNEL GAIN OF THE FORM $g(r) = 1/r^{2b}$

Non-colluding	Colluding
$P_{\rm rx,e} = \frac{P_1}{R_{e,1}^{2b}}$	$P_{\rm rx,e} = \sum_{i=1}^{\infty} \frac{P_\ell}{R_{e,i}^{2b}}$
$f_{P_{\rm rx,e}}(x) = \frac{\pi\lambda_e}{bx}\left(\frac{P_\ell}{x}\right)^{1/b} \exp\left(-\pi\lambda_e\left(\frac{P_\ell}{x}\right)^{1/b}\right), x \geq 0$	$P_{\rm rx,e} \sim \mathcal{S}\left(\alpha = \frac{1}{b},\ \beta = 1,\ \gamma = \pi\lambda_e \mathcal{C}_{1/b}^{-1} P_\ell^{1/b}\right)$
$F_{\mathcal{R}_s}(c) = 1 - \exp\left(-\pi\lambda_e\left(\frac{\frac{P_\ell}{\sigma_e^2}}{\left(1+\frac{P_\ell}{r_\ell^{2b}\sigma_\ell^2}\right)2^{-\varrho}-1}\right)^{1/b}\right), 0 \leq \varrho < \mathcal{R}_\ell$	$F_{\mathcal{R}_s}(c) = 1 - F_{\widetilde{P}_{\rm rx,e}}\left(\frac{\left(1+\frac{P_\ell}{r_\ell^{2b}\sigma_\ell^2}\right)2^{-\varrho}-1}{(\pi\lambda_e \mathcal{C}_{1/b}^{-1})^b \frac{P_\ell}{\sigma_e^2}}\right), 0 \leq \varrho < \mathcal{R}_\ell$ with $\widetilde{P}_{\rm rx,e} \sim \mathcal{S}\left(\alpha = \frac{1}{b},\ \beta = 1,\ \gamma = 1\right)$
$p_{\rm exist} = \exp\left(-\pi\lambda_e r_\ell^2 \left(\frac{\sigma_\ell^2}{\sigma_e^2}\right)^{1/b}\right)$	$p_{\rm exist} = F_{\widetilde{P}_{\rm rx,e}}\left(\frac{\sigma_e^2}{(\pi\lambda_e r_\ell^2 \mathcal{C}_{1/b}^{-1})^b \sigma_\ell^2}\right)$
$\mathbb{E}\{N_{\rm out}\} = \frac{\lambda_\ell}{\lambda_e}$	$\mathbb{E}\{N_{\rm out}\} = \frac{\lambda_\ell}{\lambda_e}\,\mathrm{sinc}\left(\frac{1}{b}\right)$

C. Existence and Outage of the MSR of a Single Link

Based on the results of Section IV-B, we can now obtain the probability of existence of a nonzero MSR, and the probability of secrecy outage for a single legitimate link in the presence of colluding eavesdroppers. The following corollary provides such probabilities.

Corollary 4.1: If Π_e is a Poisson process with density λ_e and $g(r) = 1/r^{2b}$, $b > 1$, the probability of *existence* of a nonzero MSR in the legitimate link $p_{\rm exist} = \mathbb{P}\{\mathcal{R}_s > 0\}$ is given by

$$p_{\rm exist} = F_{\widetilde{P}_{rx,e}}\left(\frac{\sigma_e^2}{(\pi\lambda_e r_\ell^2 \mathcal{C}_{1/b}^{-1})^b \sigma_\ell^2}\right) \tag{14}$$

and the probability of an *outage* in the MSR of the legitimate link, $p_{\rm outage}(\varrho) = \mathbb{P}\{\mathcal{R}_s < \varrho\}$ for $\varrho > 0$, is given by

$$p_{\rm outage}(\varrho) = \begin{cases} 1 - F_{\widetilde{P}_{rx,e}}\left(\frac{\left(1+\frac{P_\ell}{r_\ell^{2b}\sigma_\ell^2}\right)2^{-\varrho}-1}{(\pi\lambda_e \mathcal{C}_{1/b}^{-1})^b \frac{P_\ell}{\sigma_e^2}}\right), & 0<\varrho<\mathcal{R}_\ell \\ 1, & \varrho \geq \mathcal{R}_\ell \end{cases} \tag{15}$$

where $\mathcal{R}_\ell = \log_2\left(1 + P_\ell/r_\ell^{2b}\sigma_\ell^2\right)$ is the capacity of the legitimate channel; and $F_{\widetilde{P}_{rx,e}}(\cdot)$ is the cdf of the normalized stable RV $\widetilde{P}_{rx,e}$, with parameters given in (12).

Proof: The expressions for $p_{\rm exist}$ and $p_{\rm outage}(\varrho)$ follow directly from (9). □

D. Colluding versus Noncolluding Eavesdroppers for a Single Link

We have so far considered the fundamental secrecy limits of a single legitimate link in the presence of colluding eavesdroppers. According to Theorem 4.1, such a scenario is equivalent to having a single eavesdropper with an array that collects a total power $\widetilde{P}_{rx,e} = \sum_{i=1}^{\infty} P_\ell/R_{e,i}^{2b}$. In particular, when the eavesdroppers are positioned according to an homogeneous Poisson process, Theorem 4.2 shows that the RV $P_{rx,e}$ has a skewed stable distribution.

We can obtain further insights by establishing a direct comparison with the case of a single legitimate link in the presence of *noncolluding eavesdroppers*. In such a scenario, the MSR does not depend on all eavesdroppers, but only on the one with maximum received power (i.e., the closest one, when only path loss is present). Thus, the total eavesdropper power is given by $P_{rx,e} = P_\ell/R_{e,1}^{2b}$. Table II summarizes the differences between the colluding and noncolluding scenarios for a single legitimate link.

E. $i\mathcal{S}$-Graph With Colluding Eavesdroppers

To study the effect of colluding eavesdroppers, we have so far made a simplification concerning the legitimate nodes. Specifically, we considered only a single legitimate link with deterministic length r_ℓ as depicted in Fig. 3, thus eliminating the randomness associated with the position of the legitimate nodes. We now revisit the $i\mathcal{S}$-graph model depicted in [10, Fig. 2], where both legitimate nodes and eavesdroppers are distributed according to Poisson processes Π_ℓ and Π_e. In particular, the following theorem characterizes the effect of collusion in terms of the resulting average node degree in such a graph.

Theorem 4.3: For the Poisson $i\mathcal{S}$-graph with colluding eavesdroppers, secrecy rate threshold $\varrho = 0$, equal noise powers $\sigma_\ell^2 = \sigma_e^2$, and channel gain function $g(r) = 1/r^{2b}$, $b > 1$, the average degrees are given by

$$\mathbb{E}\{N_{\rm in}\} = \mathbb{E}\{N_{\rm out}\} = \frac{\lambda_\ell}{\lambda_e}\,\mathrm{sinc}\left(\frac{1}{b}\right) \tag{16}$$

where $N_{\rm in}$ and $N_{\rm out}$ denote, respectively, the in- and out-degrees of a typical node, and $\mathrm{sinc}(x) \triangleq \sin(\pi x)/\pi x$.

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 $N_{\rm out}$. Using (7), we can write

$$\begin{aligned} N_{\rm out} &= \#\{x_i \in \Pi_\ell : \mathcal{R}_{s,i} > 0\} \\ &= \#\left\{x_i \in \Pi_\ell : R_{\ell,i}^2 < \underbrace{\left(\frac{P_\ell}{P_{rx,e}}\right)^{1/b}}_{\triangleq \nu^2}\right\}. \end{aligned}$$

The average out-degree can be determined as[4]

$$\begin{aligned} \mathbb{E}\{N_{\rm out}\} &= \mathbb{E}_{\Pi_\ell,\Pi_e}\{\Pi_\ell\{\mathcal{B}_0(\nu)\}\} \\ &= \mathbb{E}_{\Pi_e}\{\lambda_\ell \pi \nu^2\} \\ &= \lambda_\ell \pi \mathbb{E}_{\Pi_e}\left\{\left(\frac{P_\ell}{P_{rx,e}}\right)^{1/b}\right\}. \end{aligned} \tag{17}$$

[4]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.

where the RV $P_{rx,e}$ has a stable distribution with parameters given in (13). As before, we define the normalized stable RV $\widetilde{P}_{rx,e} \triangleq P_{rx,e}\gamma^{-b}$ with $\gamma = \pi\lambda_e \mathcal{C}_{1/b}^{-1} P_\ell^{1/b}$, such that $\widetilde{P}_{rx,e} \sim \mathcal{S}(1/b, 1, 1)$. Then, we can rewrite (17) as

$$\mathbb{E}\{N_{\text{out}}\} = \frac{\lambda_\ell}{\lambda_e}\mathcal{C}_{1/b}\mathbb{E}\{\widetilde{P}_{rx,e}^{-1/b}\}. \tag{18}$$

Using the Mellin transform of a stable RV, we show in Appendix B that (18) simplifies to the expression in (16). Noting that $\mathbb{E}\{N_{\text{in}}\} = \mathbb{E}\{N_{\text{out}}\}$, the theorem follows. □

It is insightful to rewrite (16) as

$$\mathbb{E}\{N_{\text{out}}|\text{colluding}\} = \mathbb{E}\{N_{\text{out}}|\text{noncolluding}\} \cdot \eta(b)$$

where $\eta(b) = \text{sinc}(1/b)$, and $\eta(b) < 1$ for $b > 1$. The function $\eta(b)$ can be interpreted as the *degradation factor in average connectivity due to eavesdropper collusion.* In the extreme where $b = 1$ (free-space propagation), we have complete loss of secure connectivity with $\eta(1) = 0$. This is because the series $P_{rx,e} = \sum_{i=1}^{\infty} P_\ell / R_{e,i}^{2b}$ diverges (i.e., the total received eavesdropper power is infinite), so the resulting average node degree is zero. In the other extreme where $b \to \infty$, we achieve the highest secure connectivity with $\eta(\infty) = 1$. This is because the first term $P_\ell / R_{e,1}^{2b}$ in the $P_{rx,e}$ series (corresponding to the noncolluding term) is dominant, so the average node degree in the colluding case approaches the noncolluding one. In conclusion, cluttered environments with larger amplitude loss exponents b are more favorable for secure communication, in the sense that in such environments collusion only provides a marginal performance improvement for the eavesdroppers.

F. Numerical Results

We now illustrate the results obtained in the previous sections with a simple case study. We consider the case where $\sigma_\ell^2 = \sigma_e^2 = \sigma^2$, i.e., the legitimate link and the eavesdroppers are subject to the same noise power, which is introduced by the electronics of the respective receivers. Furthermore, we consider that the amplitude loss exponent is $b = 2$, in which case the cdf of $\widetilde{P}_{rx,e}$ for colluding eavesdroppers can be expressed using the Gaussian Q-function as $F_{\widetilde{P}_{rx,e}}(x) = 2Q(1/\sqrt{x})$, $x \geq 0$. In addition, (14) and (15) reduce, respectively, to

$$p_{\text{exist}} = 2Q\left(\pi\lambda_e r_\ell^2 \mathcal{C}_{1/2}^{-1}\right) \tag{19}$$

and

$$p_{\text{outage}}(\varrho) = \begin{cases} 1 - 2Q\left(\pi\lambda_e\mathcal{C}_{1/2}^{-1}\sqrt{\dfrac{\frac{P_\ell}{\sigma^2}}{\left(1+\frac{P_\ell}{r_\ell^4\sigma^2}\right)2^{-\varrho}-1}}\right), & 0<\varrho<\mathcal{R}_\ell \\ 1, & \varrho \geq \mathcal{R}_\ell. \end{cases} \tag{20}$$

From these analytical results, we observe that of all the following factors lead to a *degradation* of the security of communications: increasing λ_e or r_ℓ, decreasing P_ℓ/σ^2, or allowing the eavesdroppers to collude.

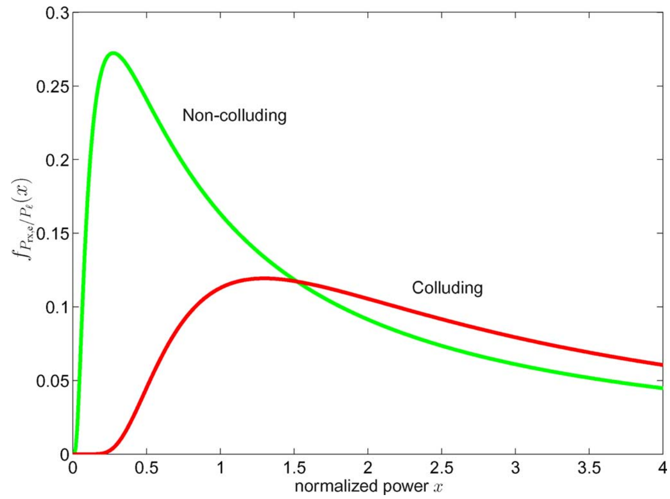

Fig. 5. PDF $f_{P_{rx,e}/P_\ell}(x)$ of the (normalized) received eavesdropper power $P_{rx,e}/P_\ell$, for the cases of colluding and noncolluding eavesdroppers ($b = 2$, $\lambda_e = 0.5$ m^{-2}).

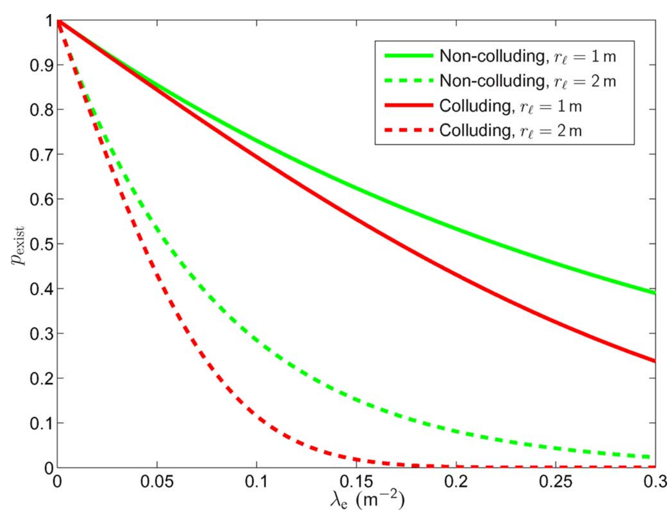

Fig. 6. Probability p_{exist} of existence of a nonzero MSR versus the eavesdropper density λ_e, for the cases of colluding and noncolluding eavesdroppers, and various values of r_ℓ ($b = 2$).

Fig. 5 compares the probability density functions (pdfs) of the (normalized) received eavesdropper power $P_{rx,e}/P_\ell$, for the cases of colluding and noncolluding eavesdroppers. For $b > 1$, it is clear that $\sum_{i=1}^{\infty} 1/R_{e,i}^{2b} > 1/R_{e,1}^{2b}$ a.s., i.e., the received eavesdropper power $P_{rx,e}$ is larger in the colluding case, resulting in a pdf whose mass is more biased towards higher realizations of $P_{rx,e}$.

Fig. 6 plots the probability p_{exist} of existence of a nonzero MSR, given in (19), as a function of the eavesdropper density λ_e, for various values of the legitimate link length r_ℓ. As predicted analytically, the existence of a positive MSR becomes *less likely* by increasing λ_e or r_ℓ. A similar degradation in secrecy occurs by allowing the eavesdroppers to collude, since more signal power from the legitimate user is available to the eavesdroppers, improving their ability to decode the secret message.

Fig. 7 quantifies the probability p_{outage} of secrecy outage, given in (20), as a function of the desired secrecy rate ϱ, for

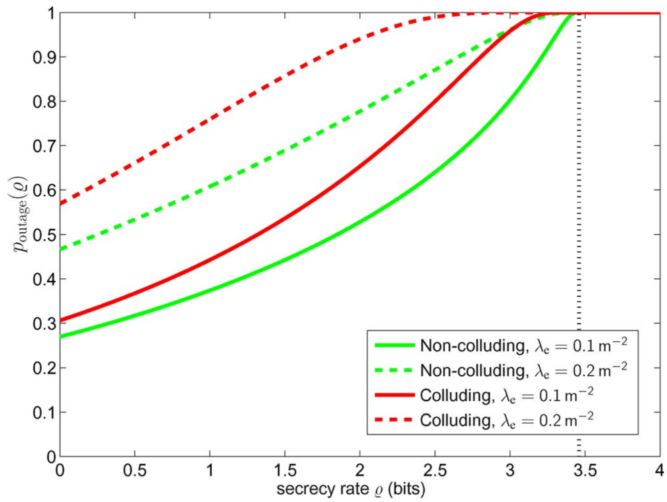

Fig. 7. Probability p_{outage} of secrecy outage for the cases of colluding and noncolluding eavesdroppers, and various densities λ_e of eavesdroppers ($b = 2$, $P_\ell/\sigma^2 = 10$, $r_\ell = 1$ m). The vertical line marks the capacity of the legitimate link, which for these system parameters is $\mathcal{R}_\ell = 3.46$ bits/complex dimension.

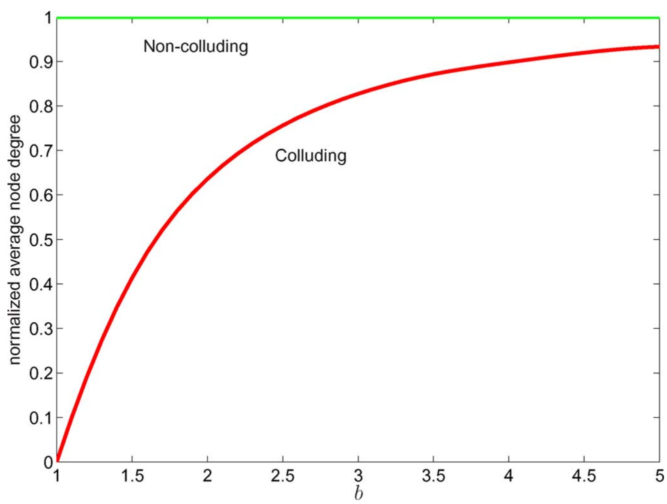

Fig. 8. Normalized average node degree of the $i\mathcal{S}$-graph, $\mathbb{E}\{N_{\mathrm{out}}\}/(\lambda_\ell/\lambda_e)$, versus the amplitude loss exponent b, for the cases of colluding and noncolluding eavesdroppers.

various values of eavesdropper density. The vertical line marks the capacity $\mathcal{R}_\ell$ of the legitimate link, which for the parameters indicated in Fig. 7 is

$$\mathcal{R}_\ell = \log_2\left(1+\frac{P_\ell}{r_\ell^{2b}\sigma_\ell^2}\right) = 3.46 \text{ bits per complex dimension.}$$

As expected, if the target secrecy rate ϱ set by the transmitter exceeds $\mathcal{R}_\ell$, a secrecy outage occurs with probability 1, since the MSR $\mathcal{R}_s$ cannot be greater that the capacity $\mathcal{R}_\ell$ of the legitimate link. In comparison with the noncolluding case, the ability of the eavesdroppers to collude leads to higher probabilities of secrecy outage. A similar degradation in secrecy occurs by increasing the eavesdropper density λ_e.

Fig. 8 quantifies the (normalized) average node degree of the $i\mathcal{S}$-graph, $\mathbb{E}\{N_{\mathrm{out}}\}/(\lambda_\ell/\lambda_e)$, versus the amplitude loss exponent b. The normalizing factor λ_ℓ/λ_e corresponds to the average out-degree in the noncolluding case. As predicted analytically, we observe that in the colluding case, the normalized average out-degree $\eta(b) = \mathbb{E}\{N_{\mathrm{out}}\}/(\lambda_\ell/\lambda_e)$ is strictly increasing with b. Furthermore, $\eta(1) = 0$ because the received eavesdropper power $P_{rx,e}$ is infinite, and $\eta(\infty) = 1$ because the first (noncolluding) term in the $P_{rx,e}$ series dominates the other terms. It is apparent from the figure that cluttered environments with larger amplitude loss exponents b are more favorable for secure communication, as discussed.

V. Conclusion

This two-part paper investigated the secrecy properties of stochastic networks, from an information theoretic perspective. In Part I, we introduced the $i\mathcal{S}$-graph, which captures the connections that can be securely established with strong secrecy over a large-scale network, in the presence of eavesdroppers. We characterized the local connectivity of the $i\mathcal{S}$-graph, and proposed techniques to improve it.

In this second part, we investigated the achievable secrecy rates and the effect of eavesdropper collusion. Specifically, we characterized the pdf of the MSR $\mathcal{R}_{s,i}$ between a legitimate node and its ith neighbor, as well as the probability of existence of a nonzero MSR and the probability of secrecy outage. We quantified how these metrics depend on the densities λ_ℓ, λ_e, the signal-to-noise-ratio P_ℓ/σ^2, and the amplitude loss exponent b.

Then we established the fundamental secrecy limits when the eavesdroppers are allowed to collude, by showing that this scenario is equivalent to an SIMO Gaussian wiretap channel. For an arbitrary spatial process Π_e of the eavesdroppers, we derived the MSR of a legitimate link. Then, for the case where Π_e is a spatial Poisson process and the channel gain is of the form $g(r) = 1/r^{2b}$, we obtained the cdf of MSR of a legitimate link, and the average degree in the $i\mathcal{S}$-graph with colluding eavesdroppers. We concluded that as we increase the density λ_e of eavesdroppers, or allow the eavesdroppers to collude, more power is available to the adversary, improving their ability to decode the secret message, and hence decreasing the MSR of legitimate links. Furthermore, we showed that cluttered environments with large amplitude loss exponent b are more favorable for secure communications, in the sense that in such regime collusion only provides a marginal performance improvement for the eavesdroppers.

Our work has not yet addressed all of the far-reaching implications of the broadcast property of the wireless medium. In the most general scenario, legitimate nodes could, for example, transmit their signals in a cooperative fashion, whereas malicious nodes could use jamming to disrupt all communications. Further work is also necessary to develop practical systems that implement the principles of physical-layer security. Although there has been recent work in that direction [16]–[19], practical codes need to be devised to achieve the secrecy capacity, in the presence of channel randomness and multiple (possibly colluding) eavesdroppers. We hope that further efforts in combining stochastic geometry with information-theoretic principles will lead to a more comprehensive treatment of wireless security.

Appendix A
Proof of Theorem 3.1

The MSR $\mathcal{R}_{s,i}$ in (2) can be expressed as $\mathcal{R}_{s,i} = [\mathcal{R}_{\ell,i} - \mathcal{R}_e]^+$, where $\mathcal{R}_{\ell,i} = \log_2\left(1 + P_\ell/R_{\ell,i}^{2b}\sigma^2\right)$ and $\mathcal{R}_e = \log_2\left(1 + P_\ell/R_{e,1}^{2b}\sigma^2\right)$. The RV $\mathcal{R}_{\ell,i}$ is a transformation of the RV $X_i \triangleq R_{\ell,i}^2$ through the monotonic function $g(x) = \log_2\left(1 + P_\ell/x^b\sigma^2\right)$, and thus its pdf is given by the rule $f_{\mathcal{R}_{\ell,i}}(\varrho) = (1/|g'(x)|) f_{X_i}(x)|_{x=g^{-1}(\varrho)}$. Note that the sequence $\{X_i\}_{i=1}^\infty$ represents Poisson arrivals *on the line* with the constant arrival rate $\pi\lambda_\ell$, as can be easily shown using the mapping theorem [20, Sec. 2.3]. Therefore, the RV X_i has an Erlang distribution of order i with rate $\pi\lambda_\ell$, and its pdf is given by

$$f_{X_i}(x) = \frac{(\pi\lambda_\ell)^i x^{i-1} e^{-\pi\lambda_\ell x}}{(i-1)!}, \quad x \geq 0.$$

Then, applying the above rule, $f_{\mathcal{R}_{\ell,i}}(\varrho)$ can be shown to be

$$f_{\mathcal{R}_{\ell,i}}(\varrho) = \ln 2 \frac{(\pi\lambda_\ell)^i}{(i-1)!b}\left(\frac{P_\ell}{\sigma^2}\right)^{i/b} \frac{2^\varrho}{(2^\varrho - 1)^{1+i/b}} \times \exp\left(-\pi\lambda_\ell\left(\frac{\frac{P_\ell}{\sigma^2}}{2^\varrho - 1}\right)^{1/b}\right) \tag{21}$$

for $\varrho \geq 0$. Replacing λ_ℓ with λ_e and setting $i = 1$, we obtain the pdf of $\mathcal{R}_e$ as

$$f_{\mathcal{R}_e}(\varrho) = \ln 2 \frac{\pi\lambda_e}{b}\left(\frac{P_\ell}{\sigma^2}\right)^{1/b} \frac{2^\varrho}{(2^\varrho - 1)^{1+1/b}} \times \exp\left(-\pi\lambda_e\left(\frac{\frac{P_\ell}{\sigma^2}}{2^\varrho - 1}\right)^{1/b}\right) \tag{22}$$

for $\varrho \geq 0$. Since the sequences $\{R_{\ell,i}\}_{i=1}^\infty$ and $\{R_{e,i}\}_{i=1}^\infty$ are mutually independent, so are the RVs $\mathcal{R}_{\ell,i}$ and $\mathcal{R}_e$. This implies that the cdf of $\mathcal{R}_{s,i} = [\mathcal{R}_{\ell,i} - \mathcal{R}_e]^+$ can be obtained through convolution of $f_{\mathcal{R}_{\ell,i}}(\varrho)$ and $f_{\mathcal{R}_e}(\varrho)$ as

$$\begin{aligned} F_{\mathcal{R}_{s,i}}(\varrho) &= \mathbb{P}\left\{[\mathcal{R}_{\ell,i} - \mathcal{R}_e]^+ \leq \varrho\right\} \\ &= 1 - \int_\varrho^\infty f_{\mathcal{R}_{\ell,i}}(z) * f_{\mathcal{R}_e}(-z)\, dz \end{aligned} \tag{23}$$

for $\varrho \geq 0$. Replacing (21) and (22) into (23), we obtain (3).

Appendix B
Derivation of (16)

Let the Mellin transform of an RV X with pdf $f_X(x)$ be defined as[5]

$$\mathcal{M}_X(s) \triangleq \int_0^\infty x^s f_X(x) dx. \tag{24}$$

If $X \sim \mathcal{S}(\alpha, 1, 1)$ with $0 < \alpha < 1$, then [21, eq. (17)]

$$\mathcal{M}_X(s) = \left(\cos\left(\frac{\pi\alpha}{2}\right)\right)^{-s/\alpha} \frac{\Gamma\left(1 - \frac{s}{\alpha}\right)}{\Gamma(1-s)} \tag{25}$$

for $-1 < \mathrm{Re}\{s\} < \alpha$. Then, since $\widetilde{P}_{rx,e} \sim \mathcal{S}(\alpha, 1, 1)$ with $\alpha = 1/b \in (0, 1)$, we use (25) to write

$$\begin{aligned} \mathbb{E}\{\widetilde{P}_{rx,e}^{-\alpha}\} &= \int_0^\infty x^{-\alpha} f_{\widetilde{P}_{rx,e}}(x) dx \\ &= \mathcal{M}_{\widetilde{P}_{rx,e}}(-\alpha) \\ &= \frac{\cos\left(\frac{\pi\alpha}{2}\right)}{\Gamma(1+\alpha)}. \end{aligned} \tag{26}$$

Using (10) and (26), we expand (18) as

$$\begin{aligned} \mathbb{E}\{N_{\text{out}}\} &= \frac{\lambda_\ell}{\lambda_e}\mathcal{C}_\alpha \mathbb{E}\{\widetilde{P}_{rx,e}^{-\alpha}\} \\ &= \frac{\lambda_\ell}{\lambda_e} \cdot \frac{1-\alpha}{\Gamma(2-\alpha)\Gamma(1+\alpha)} \\ &= \frac{\lambda_\ell}{\lambda_e} \cdot \frac{\sin(\pi\alpha)}{\pi\alpha} \end{aligned}$$

where we used the following properties of the gamma function: $\Gamma(z+1) = z\Gamma(z)$ and $\Gamma(z)\Gamma$

[5]In the literature, the Mellin transform is sometimes defined differently as $\mathcal{M}_X(s) \triangleq \int_0^\infty x^{s-1} f_X(x) dx$. For simplicity, we prefer the definition in (24).

[15] 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.
[16] 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*, 2005.
[17] 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.
[18] 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.
[19] H. Mahdavifar and A. Vardy, Achieving the Secrecy Capacity of Wiretap Channels Using Polar Codes 2010 [Online]. Available: http://arxiv.org/abs/1001.0210
[20] J. Kingman, *Poisson Processes*. London, U.K.: Oxford Univ. Press, 1993.
[21] V. M. Zolotarev, "Mellin-Stieltjes transforms in probability theory," *Theory of Probability and its Applications*, vol. 2, p. 433, 1957.

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).