Wireless Network Intrinsic Secrecy

Alberto Rabbachin, *Member, IEEE*, Andrea Conti, *Senior Member, IEEE*, and Moe Z. Win, *Fellow, IEEE*

***Abstract*—Wireless secrecy is essential for communication confidentiality, health privacy, public safety, information superiority, and economic advantage in the modern information society. Contemporary security systems are based on cryptographic primitives and can be complemented by techniques that exploit the intrinsic properties of a wireless environment. This paper develops a foundation for design and analysis of wireless networks with secrecy provided by intrinsic properties such as node spatial distribution, wireless propagation medium, and aggregate network interference. We further propose strategies that mitigate eavesdropping capabilities, and we quantify their benefits in terms of network secrecy metrics. This research provides insights into the essence of wireless network intrinsic secrecy and offers a new perspective on the role of network interference in communication confidentiality.**

***Index Terms*—Network secrecy, wireless networks, stochastic geometry, interference exploitation, fading channels.**

Fig. 1. Hall Pompeiana of Massimo Theater at Palermo (Foto Studio Camera Palermo).

I. Introduction

INFORMATION society largely benefits from the ability to transfer confidential information, to guarantee privacy, and to authenticate users in communication networks. Contemporary security systems are based on cryptographic primitives that rely on the computational intractability of solving certain numeric-theoretic problems [1]. Security in wireless systems is challenging due to the broadcast nature of the channel, which facilitates the interception of radio communications. Wireless security schemes have typically evolved from those developed for traditional wireline applications [2], [3]; these schemes do not consider physical properties of the wireless channels.

The idea of exploiting physical properties of the environment for providing communication confidentiality dates back several centuries. For example, the Hall Pompeiana of Massimo Theater, shown in Fig. 1, was designed to make conversations in the proximity of its center indecipherable in any other parts of the hall. This was achieved by creating intentional echoes generated by the shape of the hall, thus giving credence to the idea that interference can be exploited to provide confidentiality.

The concept of communication secrecy is built on the information-theoretic notion of perfect secrecy [4]. Based on this concept, the wire-tap channel is introduced in [5] to investigate scenarios in which the eavesdropper attempts to intercept the information by tapping the legitimate link in the presence of noisy observations. As shown for a discrete memoryless wire-tap channel [5] and for a Gaussian wire-tap channel [6], the secrecy capacity depends on the difference between the capacity of the legitimate link and that of the eavesdropping link.[1] In wireless environments, the propagation medium plays an important role in communication confidentiality; specifically, the secrecy capacity in fading channels is investigated in [11]–[13]. Secrecy capacity has been further studied in the context of multiple-access channels [14]–[16], broadcast channels [17]–[19], artificial noise [20], eavesdropper collusion [21]–[23], point-to-point diversity communications [24]–[27], and cooperative communications [28]. The generation of secret keys at the physical layer using common sources, such as reciprocal wireless channels, is addressed in [29]–[33].

In a network setting, spatial distribution of nodes plays an important role, and the Poisson point process (PPP) is used to investigate wireless networks with secrecy [34]–[39].[2] We advocate the exploitation of wireless network intrinsic properties (e.g., network interference) to strengthen communication secrecy. While interference is conventionally considered deleterious for communications [58]–[60], we envision that interference can be beneficial for *network secrecy* [61]–[63]. Therefore, it is important to characterize the effects of network

Manuscript received August 24, 2012; revised July 14, 2013; accepted November 07, 2013; approved by IEEE/ACM TRANSACTIONS ON NETWORKING Editor Y.-C. Hu. Date of publication February 05, 2014; date of current version February 12, 2015. This work was supported in part by the European Commission Marie Curie International Outgoing Fellowship under Grant 2010-272923, the FP7 European project CONCERTO under Grant 288502, the Copernicus Fellowship, the National Science Foundation under Grant CCF-1116501, the Office of Naval Research under Grant N00014-11-1-0397, and the MIT Institute for Soldier Nanotechnologies. The material in this paper was presented in part at the IEEE International Conference on Communications (ICC), Ottawa, ON, Canada, June 10–15, 2012, and at the IEEE ICC, Budapest, Hungary, June 9–13, 2013.

A. Rabbachin was with the Wireless Communications and Network Science Laboratory, Massachusetts Institute of Technology, Cambridge, MA 02139 USA. He is now with the European Commission, 1000 Brussels, Belgium (e-mail: a.rabbachin@ieee.org).

A. Conti is with the Engineering Department (ENDIF), University of Ferrara, 44122 Ferrara, Italy (e-mail: a.conti@ieee.org).

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/TNET.2013.2297339

[1]For a discrete memoryless channel, polar codes have been shown to achieve strong secrecy [7]–[10].

[2]The PPP [40] has been used extensively to model node positions in various studies of wireless networks [41]–[57].

interference at both legitimate receivers and eavesdroppers. From this, competitive strategies can be devised for elevating the secrecy of the network to a new level.

In this paper, we establish foundations for the design and analysis of wireless networks with intrinsic secrecy. In particular, we develop a framework accounting for: 1) the spatial distributions of legitimate, eavesdropping, and interfering nodes; 2) the physical properties of the wireless propagation medium; and 3) the characteristics of aggregate network interference. Our approach is based on stochastic geometry, probability theory, and communication theory. The key contributions of the paper can be summarized as follows:

- introduction of the concept of network secrecy and new metrics for characterizing intrinsic wireless secrecy in scenarios composed by legitimate, eavesdropping, and interfering nodes;
- development of a framework for design and analysis of wireless networks with intrinsic secrecy that accounts for node spatial distribution, physical propagation medium, and aggregate network interference;
- characterization of the received signal-to-interference ratios (SIRs) in legitimate and eavesdropping networks for different destination selection techniques;
- quantification of the network secrecy performance provided by legitimate network strategies that mitigate the capabilities of the eavesdropping network.

This research shows that the intrinsic properties of wireless networks can provide a new level of secrecy, paving the way to the design of wireless networks with enhanced intrinsic secrecy.

The remaining sections are organized as follows. Section II presents the scenarios for legitimate, eavesdropping, and interfering networks. Section III introduces metrics for assessing wireless network secrecy. Sections IV and V provide the statistical characterization of SIRs for different fading channels. In Section VI, competitive strategies for enhancing network secrecy are proposed and analyzed. Numerical results and final remarks are provided in Sections VII and VIII, respectively.

II. Network Scenarios

We now present the scenarios for legitimate, eavesdropping, and interfering networks. We first introduce the network scenarios and then present the wireless-tap channel within the considered network setting.

A. Network Secrecy Scenarios

Consider three different overlaid networks as described in the following (see Fig. 2).

1) The *legitimate network* is composed of nodes that aim to exchange confidential information. This network is described by the point process $\mathbf{\Pi}_\ell$ with spatial density λ_ℓ.[3] $\mathbf{\Pi}_\ell$ is composed of point processes $\mathbf{\Pi}_{\rm tx}$ and $\mathbf{\Pi}_{\rm rx}$ with spatial densities $\lambda_{\rm tx}$ and $\lambda_{\rm rx}$ corresponding to the legitimate transmitters and the legitimate receivers, respectively. Thus, $\lambda_\ell = \lambda_{\rm tx} + \lambda_{\rm rx}$ and
$$\alpha \triangleq \frac{\gamma_{\rm tx}}{\gamma_{\rm tx} + \gamma_{\rm rx}} \tag{1}$$
is defined such that $\lambda_{\rm tx} = \alpha\lambda_\ell$ and $\lambda_{\rm rx} = (1-\alpha)\lambda_\ell$ with $\alpha \in (0,1)$.

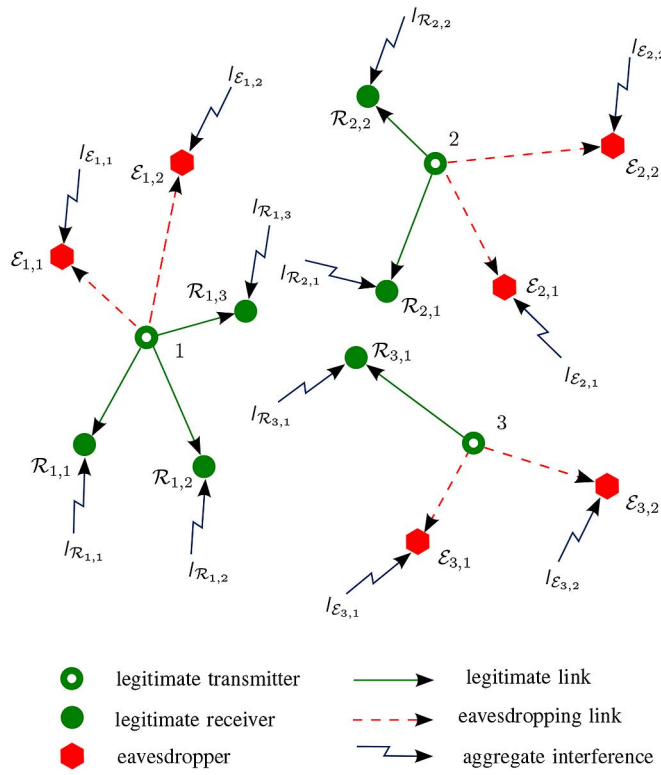

Fig. 2. Network scenario considered in the paper.

2) The *eavesdropping network* is composed of nodes that attempt to intercept the confidential information flowing through the legitimate network. This network is described by the point process $\mathbf{\Pi}_{\rm e}$ with spatial density $\lambda_{\rm e}$.
3) The *interfering network* is composed of nodes that interfere with both legitimate receivers and eavesdroppers. Each legitimate receiver experiences the unintentional interference generated by the legitimate transmitters that intend to communicate with other receivers. On the other hand, each eavesdropper is affected by unintentional and intentional interference generated by the legitimate transmitters and the intentional interferers, respectively.[4] The network of intentional interferers is described by the point process $\mathbf{\Pi}_{\rm jx}$ with spatial density $\lambda_{\rm jx}$. The quantities $\lambda_{\rm ir} = \lambda_{\rm tx}$ and $\lambda_{\rm ie} = \lambda_{\rm tx} + \lambda_{\rm jx}$ represent the total spatial density of nodes interfering the legitimate network and the eavesdropping network, respectively.

Legitimate transmitters, legitimate receivers, eavesdroppers, and intentional interferers are spatially scattered in an n-dimensional Euclidian space $\mathbb{R}^n$ according to the homogeneous spatial PPPs $\mathbf{\Pi}_{\rm tx}$, $\mathbf{\Pi}_{\rm rx}$, $\mathbf{\Pi}_{\rm e}$, and $\mathbf{\Pi}_{\rm jx}$, respectively. Let $\mathcal{T}$ and $\mathcal{J}$ denote the index sets of legitimate transmitters and of intentional interferers, respectively. Consider a bounded set $\mathcal{A} \subset \mathbb{R}^n$. For the jth legitimate transmitter in $\mathcal{A}$:[5]

- $\mathcal{R}_j$ denotes the index set of potential legitimate receivers for the jth transmitter, and

[3]Spatial densities are measured in nodes per unit volume (UV). For a two-dimensional plane, spatial densities are given in node/m^2.

[4]Networks of intentional interferers are especially effective if they have the knowledge of legitimate receivers' positions (see for example, Section VI).

[5]Hereafter, the jth node refers to the node with index j in the network.

- $\mathcal{E}_j$ denotes the index set of eavesdroppers attempting to intercept the confidential information from the jth transmitter.

Note, the probability that there are no transmitters in $\mathcal{A}$ is $e^{-\lambda_{\rm tx}|\mathcal{A}|}$ where $|\mathcal{A}|$ is the volume of $\mathcal{A}$.

B. Wireless-Tap Channel in Network Setting

Based on the network scenarios described in Section II-A, we introduce the wireless-tap channel composed of a legitimate transmitter with index j, a legitimate receiver with index $\mathcal{R}_{j,k} \in \mathcal{R}_j$ (i.e., the kth potential legitimate receiver among those of the jth transmitter), and an eavesdropper with index $\mathcal{E}_{j,i} \in \mathcal{E}_j$ (i.e., the ith eavesdropper among those of the jth transmitter) attempting to intercept the transmission of confidential information. A key feature of the wireless-tap channel in a network setting is the network interference, which will be described in the following.

At a given instant, the received signal at a node with index v from the uth transmitter is given by

$$Y_{u,v}^{(\square)} = \sqrt{P_{\rm T}} \frac{H_{u,v}}{D_{u,v}^{b}} S_u + \widetilde{W}_v \tag{2}$$

where, for the jth legitimate transmitter

$$v \in \begin{cases} \mathcal{R}_j & \text{for } \square = \ell \\ \mathcal{E}_j & \text{for } \square = e \end{cases} \tag{3}$$

with ℓ or e denoting the legitimate link or eavesdropping link, respectively. In (2), $P_{\rm T}$ is the signal power at the reference distance d_0 from the transmitter; $H_{u,v} \in \mathbb{C}$ is the quasi-static channel gain; $D_{u,v} = \|\mathbf{X}_u - \mathbf{X}_v\|/d_0$ is the normalized Euclidian distance between the transmitter and the receiver at the random positions $\mathbf{X}_u$ and $\mathbf{X}_v$, respectively; S_u is a transmitted symbol; b is the amplitude path-loss exponent; and $\widetilde{W}_v$ is the disturbance composed of the network interference and the receiver noise. Specifically

$$\widetilde{W}_v = \sqrt{P_{\rm T}} \sum_{q \in \mathcal{I}_v} \frac{H_{q,v}}{D_{q,v}^{b}} S_q + W_v \tag{4}$$

where $\mathcal{I}_v$ is the index set of nodes causing interference to the receiver v, i.e.,

$$\mathcal{I}_v = \begin{cases} \mathcal{T} \setminus \{j\} & \text{for } v \in \mathcal{R}_j \\ \mathcal{J} \bigcup \mathcal{T} \setminus \{j\} & \text{for } v \in \mathcal{E}_j \end{cases} \tag{5}$$

in which $W_v \sim \mathcal{N}_{\rm c}(0, \sigma_v^2)$ is the addictive white Gaussian noise (AWGN).[6]

The variation of distances $\{D_{q,v}\}$ and channel gains $\{H_{q,v}\}$ affects the behavior of $\widetilde{W}_v$. Therefore, $\mathbf{\Phi}_{\rm tj}$ is introduced to denote the set of $\mathbf{\Pi}_{\rm tj}$ and channel gains from transmitters to receivers. In particular, $\mathbf{\Pi}_{\rm tj}$ is equal to $\mathbf{\Pi}_{\rm tx}$ or $\mathbf{\Pi}_{\rm tx} \cup \mathbf{\Pi}_{\rm jx}$ depending on whether v is a legitimate receiver or an eavesdropper, respectively. To maximize the mutual information over legitimate links and to maximize the entropy over interfering links, all transmitters employ signaling schemes such that the resulting disturbance conditioned on the PPP $\mathbf{\Phi}_{\rm tj}$ is complex Gaussian [64]–[67]

$$\widetilde{W}_v \overset{|\mathbf{\Phi}_{\rm tj}}{\sim} \mathcal{N}_{\rm c}\left(0, \mathbb{V}\{S\} P_{\rm T} I_v + \sigma_v^2\right) \tag{6}$$

where $\mathbb{V}\{S\}$ is the variance of a transmitted complex symbol S and I_v is the normalized network interference power given by

$$I_v = \sum_{q \in \mathcal{I}_v} \frac{|H_{q,v}|^2}{D_{q,v}^{2b}}. \tag{7}$$

Note that since I_v in (7) depends on $\mathbf{\Phi}_{\rm tj}$, it can be seen as a random variable taking different values for each realization of the $\mathbf{\Phi}_{\rm tj}$. In particular, for nodes in $\mathbb{R}^2$, the randon variable (RV) I_v follows a Stable distribution [41], [42], [48][7]

$$I_v \sim \mathcal{S}\left(\frac{1}{b}, 1, \lambda_{\rm i}^{(\square)} \gamma\right) \tag{8}$$

where

$$\lambda_{\rm i}^{(\square)} = \begin{cases} \lambda_{\rm ir} & \text{for } \square = \ell \\ \lambda_{\rm ie} & \text{for } \square = e \end{cases} \tag{9a}$$

$$\gamma = \pi B_{\frac{1}{b}}^{-1} \mathbb{E}\left\{|H_{u,v}|^{\frac{2}{b}}\right\} \tag{9b}$$

$$B_x = \begin{cases} \frac{1-x}{\Gamma(2-x)\cos\left(\frac{\pi x}{2}\right)} & x \neq 1 \\ \frac{2}{\pi} & x = 1. \end{cases} \tag{9c}$$

III. Network Secrecy Metrics

We now introduce new metrics for assessing intrinsic secrecy in wireless networks.

A. Maximum Secrecy Rate of a Wireless-Tap Channel

We first review the maximum secrecy rate (MSR) of a Gaussian wire-tap channel [6]. We then extend it to scenarios with network interference.[8]

1) Absence of Network Interference: Conditioned on $\mathring{\Psi}_{u,v_\ell}^{(\ell)}$ and $\mathring{\Psi}_{u,v_e}^{(e)}$ with $\mathring{\Psi}_{u,v}^{(\square)} = \{H_{u,v}, D_{u,v}\}$, the wireless-tap channel reduces to the Gaussian wire-tap channel. Specifically, the conditional MSR in the absence of interference is given by[9]

$$\mathring{R}_{u,v_\ell,v_e} = \left[C\left(\mathring{\Psi}_{u,v_\ell}^{(\ell)}\right) - C\left(\mathring{\Psi}_{u,v_e}^{(e)}\right)\right]^+. \tag{10}$$

The term

$$C\left(\mathring{\Psi}_{u,v}^{(\ell)}\right) = c(\mathring{Z}_{u,v}) \tag{11}$$

is the conditional capacity[10] of the legitimate link ($\square = \ell$) or eavesdropping link ($\square = e$) in the absence of network interference with

$$\mathring{Z}_{u,v} = \frac{|H_{u,v}|^2 P_{\rm T}}{D_{u,v}^{2b} \sigma_v^2}. \tag{12}$$

2) Presence of Network Interference: Conditioned on $\Psi_{u,v_\ell}^{(\ell)}$ and $\Psi_{u,v_e}^{(e)}$ with $\Psi_{u,v}^{(\square)} = \{H_{u,v}, D_{u,v}, I_v\}$, the MSR in the

[6]The notation $\mathcal{N}_{\rm c}(\mu, \sigma^2)$ denotes a circularly symmetric complex Gaussian distribution with mean μ and variance $\sigma^2/2$ per dimension.

[7]In a space with more than two dimensions, the RV still follows a skewed stable distribution with different parameters [68].

[8]Hereafter, consider a network scenario composed of multiple legitimate and eavesdropping links with receivers that treat interference as noise.

[9]$[x]^+ = \max\{x, 0\}$, and the unit of the MSR is confidential information bits (cib) per second per Hertz (cib/s/Hz).

[10]For notational convenience, define $c(x) \triangleq \log_2(1+x)$ bits/s/Hz.

presence of interference is given by

$$R_{u,v_\ell,v_e}\left[C\left(\Psi^{(\ell)}_{u,v_\ell}\right)-C\left(\Psi^{(e)}_{u,v_e}\right)\right]^+. \tag{13}$$

The term

$$C\left(\Psi^{(\square)}_{u,v}\right)=c(Z_{u,v}) \tag{14}$$

is the conditional capacity[11] of the legitimate link ($\square=\ell$) or eavesdropping link ($\square=e$) in the presence of network interference, where

$$Z_{u,v}=\frac{|H_{u,v}|^2P_{\mathrm{T}}}{D^{2b}_{u,v}\left(P_{\mathrm{T}}I_v+\sigma^2_v\right)}. \tag{15}$$

The MSR of the legitimate link from the jth transmitter to the kth receiver, conditioned on $\Psi^{(\ell)}_{j,\mathcal{R}_{j,k}}$ and $\{\Psi^{(e)}_{j,\mathcal{E}_{j,i}}\}_{i\in\mathcal{E}_j}$, is determined by the minimum MSR over all possible eavesdroppers in the network attempting to intercept the confidential information as

$$R_{j,\mathcal{R}_{j,k},\mathcal{E}_{j,\check{\imath}}}=\left[c(Z_{j,\mathcal{R}_{j,k}})-c(\eta_{j,\mathcal{E}_j})\right]^+ \tag{16}$$

where $\eta_{j,\mathcal{E}_j}\triangleq Z_{j,\mathcal{E}_{j,\check{\imath}}}$ with $\check{\imath}\triangleq\arg\max_{i\in\mathcal{E}_j}\{Z_{j,\mathcal{E}_{j,i}}\}$.

B. Network Secrecy Rate Density

To characterize the successful transmission of confidential information originated from legitimate nodes in a bounded set $\mathcal{A}$, define the conditional network secrecy rate as

$$R_{\mathrm{ns}}(\Omega_{\mathcal{A}})=\sum_{j\in\mathcal{T}}\mathbb{1}_{\mathcal{A}}(\mathbf{X}_j)\,R_{j,\mathcal{R}_{j,\bar{k}},\mathcal{E}_{j,\check{\imath}}} \tag{17}$$

where $\Omega_{\mathcal{A}}=\Omega^{(\ell)}_{\mathcal{A}}\cup\Omega^{(e)}_{\mathcal{A}}$ with

$$\Omega^{(\ell)}_{\mathcal{A}}\triangleq\left\{\Psi^{(\ell)}_{j,\mathcal{R}_{j,\bar{k}}}:\mathbf{X}_j\in\mathcal{A},\ \mathcal{R}_{j,\bar{k}}\in\mathcal{R}_j\right\} \tag{18a}$$

$$\Omega^{(e)}_{\mathcal{A}}\triangleq\left\{\Psi^{(e)}_{j,\mathcal{E}_{j,\check{\imath}}}:\mathbf{X}_j\in\mathcal{A},\ \mathcal{E}_{j,\check{\imath}}\in\mathcal{E}_j\right\}. \tag{18b}$$

In (17), $\mathbb{1}_{\mathcal{A}}(\mathbf{X}_j)$ accounts for the legitimate transmitters in $\mathcal{A}$ according to

$$\mathbb{1}_{\mathcal{A}}(\mathbf{X}_j)=\begin{cases}1 & \text{if }\mathbf{X}_j\in\mathcal{A}\\ 0 & \text{otherwise}\end{cases}$$

and $\mathcal{R}_{j,\bar{k}}=\mathbb{S}\{\mathcal{R}_j\}$ is the index of the selected receiver for the jth transmitter.[12] The network secrecy rate density is defined as the limit over $\mathcal{A}$ and can be expressed as

$$\rho_{\mathrm{ns}}=\lim_{t\to\infty}\frac{R_{\mathrm{ns}}\left(\Omega_{\mathcal{A}_t}\right)}{|\mathcal{A}_t|} \tag{19}$$

where $\{\mathcal{A}_t\}$ is a convex averaging sequence with $\mathcal{A}_1\subset\mathcal{A}_2\subset\cdots\subset\mathbb{R}^n$. It is demonstrated in Appendix A that if $\sup\{r:\mathcal{B}(r)\subseteq\mathcal{A}_t\}\to\infty$ as $t\to\infty$, then[13]

$$\rho_{\mathrm{ns}}=\lambda_{\mathrm{tx}}R \tag{20}$$

where $R\triangleq\mathbb{E}_{\mathbf{o}}\{R_{0,\mathcal{R}_{0,\bar{k}},\mathcal{E}_{0,\check{\imath}}}\}$ is the average MSR of a typical link in the network [69] and over the channel gains.[14,15] When $I_{\mathcal{R}_{0,\bar{k}}}$ and $I_{\mathcal{E}_{0,\check{\imath}}}$ are statistically independent, the average MSR can be written as

$$\begin{aligned}R&=\mathbb{E}_{Z_{0,\mathcal{R}_{0,\bar{k}}}}\left\{\mathbb{E}_{\eta_{0,\mathcal{E}_0}}\left\{\left[c\left(Z_{0,\mathcal{R}_{0,\bar{k}}}\right)-c(\eta_{0,\mathcal{E}_0})\right]^+\right\}\right\}\\&=\int_0^\infty c(y)F_{\eta_{0,\mathcal{E}_0}}(y)f_{Z_{0,\mathcal{R}_{0,\bar{k}}}}(y)dy\\&\quad-\int_0^\infty\int_0^y c(x)f_{\eta_{0,\mathcal{E}_0}}(x)f_{Z_{0,\mathcal{R}_{0,\bar{k}}}}(y)dxdy\end{aligned} \tag{21}$$

where $f_X(\cdot)$ and $F_X(\cdot)$ are the probability density function (PDF) and the cumulative distribution function (CDF) of the RV X, respectively.

Remark: The PDF of $Z_{0,\mathcal{R}_{0,\bar{k}}}$, and thus the average MSR of a typical link, depends on the destination selection strategy.

C. Network Secrecy Rate Outage Density

Now, define a network secrecy metric to account for the legitimate links that are in outage, i.e., the legitimate links with MSR below a target MSR. Specifically, for a given target MSR $R^\star$ and for transmitters in $\mathcal{A}$, the number of legitimate links in outage is

$$K_{\mathrm{nso}}(\Omega_{\mathcal{A}},R^\star)=\sum_{j\in\mathcal{T}}\mathbb{1}_{\mathcal{A}}(\mathbf{X}_j)\mathbb{1}_{[0,R^\star]}\left(R_{j,\mathcal{R}_{j,\bar{k}},\mathcal{E}_{j,\check{\imath}}}\right). \tag{22}$$

Following the approach used in Section III-B, the density of transmitting nodes that are in outage is obtained as

$$\kappa_{\mathrm{nso}}(R^\star)=\lim_{t\to\infty}\frac{K_{\mathrm{nso}}(\Omega_{\mathcal{A}_t},R^\star)}{|\mathcal{A}_t|}. \tag{23}$$

The density of transmitting nodes in outage (23) results in

$$\kappa_{\mathrm{nso}}(R^\star)=\lambda_{\mathrm{tx}}P_{\mathrm{lso}}(R^\star) \tag{24}$$

where $P_{\mathrm{lso}}(R^\star)$ is the probability that a legitimate link is in outage given by

$$P_{\mathrm{lso}}(R^\star)=\left[1-\int_{2^{R^\star}-1}^\infty F_{\eta_{0,\mathcal{E}_0}}\left(\frac{y+1}{2^{R^\star}}-1\right)f_{Z_{0,\mathcal{R}_{0,\bar{k}}}}(y)dy\right]. \tag{25}$$

Remark: To achieve the MSR, the transmitter has to know the signal-to-interfernce-plus-noise ratios (SINRs) at the selected receiver and that at each eavesdropper. The latter requirement is challenging to devise techniques for achieving the MSR. Therefore, in Section III-D, the concept of network secrecy throughput is introduced to characterize the confidential information flowing through the legitimate network.

[11]Conditioned on $\Psi^{(\square)}_{u,v}$, the instantaneous amplitude of the aggregate interference is Gaussian distributed [64]–[67], and the capacity of the legitimate and eavesdropping links is expressed using $c(\cdot)$.

[12]The network secrecy depends on the destination selection strategy that will be described in Sections IV and V. The $\mathbb{S}\{\mathcal{R}_j\}$ is the selection operator that selects the index of the destination among the potential receiver indexes $\mathcal{R}_j$ for the jth transmitter. For brevity, in the notation of the MSR, its dependence on $\mathbb{S}\{\mathcal{R}_j\}$ will be omitted.

[13]$\mathcal{B}(r)$ denotes a ball in $\mathbb{R}^n$ with radius r.

[14]The expectation $\mathbb{E}_{\mathbf{o}}\{\cdot\}$ is over the point processes for which the legitimate transmitter is located in the origin.

[15]We consider a typical link of the network with transmitter index $j=0$.

D. Probability to Transmit Information With Secrecy

We first generalize the secrecy outrage probability (SOP) of [13] to account for the presence of multiple eavesdroppers and multiple interferers as[16]

$$P_{\rm so} = \mathbb{P}\left\{c(\eta_{j,\mathcal{E}_j}) > R_j^{(\ell)} - R_{\rm s}|\mathcal{M}_{\mathcal{I}}\right\} \tag{26}$$

where $R_j^{(\ell)}$ is the transmission rate of a legitimate link associated with the jth transmitter, $R_{\rm s}$ is the desired rate of confidential information, and $\mathcal{M}_{\mathcal{I}}$ indicates the event that a confidential information message is transmitted.[17] When a confidential message is not transmitted, various strategies can be employed for mitigating the capabilities of the eavesdropping network. In particular, we propose to transmit no-information messages over low-quality links to increase network interference. In this setting, the jth legitimate transmitter sends a no-information message when $Z_{j,\mathcal{R}_{j,\bar{k}}}$ for a selected receiver is below a minimum required value μ; otherwise, a confidential information message is transmitted. Therefore, the probability of confidential message transmission is

$$P_{\rm it}(\mu) \triangleq \mathbb{P}\{\mathcal{M}_{\mathcal{I}}\} = \mathbb{P}\left\{Z_{j,\mathcal{R}_{j,\bar{k}}} > \mu\right\}. \tag{27}$$

The minimum required SINR value of μ is related to the secrecy rate $R_{\rm s}$ according to $\mu > 2^{R_{\rm s}} - 1$. Note also from (26) that the network secrecy outage is reduced by increasing $R_j^{(\ell)}$. Since $R_j^{(\ell)} = c(Z_{j,\mathcal{R}_{j,\bar{k}}}) - \epsilon$ for any $\epsilon > 0$, the SOP results in

$$\begin{aligned} P_{\rm so}(\mu) &= \mathbb{P}\left\{c(\eta_{j,\mathcal{E}_j}) > c(Z_{j,\mathcal{R}_{j,\bar{k}}}) - R_{\rm s}|Z_{j,\mathcal{R}_{j,\bar{k}}} > \mu\right\} \\ &= \frac{\mathbb{P}\left\{\mu < Z_{j,\mathcal{R}_{j,\bar{k}}} < 2^{R_{\rm s}}\left(1+\eta_{j,\mathcal{E}_j}\right) - 1\right\}}{\mathbb{P}\left\{Z_{j,\mathcal{R}_{j,\bar{k}}} > \mu\right\}} \\ &= \frac{1}{1 - F_{Z_{j,\mathcal{R}_{j,\bar{k}}}}(\mu)} \\ &\quad \times \left[F_{Z_{j,\mathcal{R}_{j,\bar{k}}}}(\mu) F_{\eta_{j,\mathcal{E}_j}}\left(\frac{\mu+1}{2^{R_{\rm s}}} - 1\right) - F_{Z_{j,\mathcal{R}_{j,\bar{k}}}}(\mu)\right. \\ &\quad \left. + \int_{\frac{\mu+1}{2^{R_{\rm s}}-1}}^{\infty} F_{Z_{j,\mathcal{R}_{j,\bar{k}}}}\left(2^{R_{\rm s}}(1+y) - 1\right) f_{\eta_{j,\mathcal{E}_j}}(y) dy\right]. \end{aligned} \tag{28}$$

For a given secrecy rate $R_{\rm s}$ and a maximum tolerable SOP $P_{\rm so}^{\star}$, we define the *secrecy protection ratio* $\mu^{\star}$ as

$$\mu^{\star} = \arg\max_{\mu \in \mathcal{M}} P_{\rm it}(\mu) \tag{29}$$

where $\mathcal{M} = \{\mu : P_{\rm so}(\mu) \leq P_{\rm so}^{\star}\}$.

E. Network Secrecy Throughput Density

For a given $R_{\rm s}$ and $P_{\rm so}^{\star}$, the secrecy throughput of the legitimate link associated with the jth transmitter, conditioned on $\Psi_{j,\mathcal{R}_{j,\bar{k}}}^{(\ell)}$, is given by

$$T_{j,\mathcal{R}_{j,\bar{k}}} = R_{\rm s} \mathbb{1}_{[\mu^{\star},\infty]}\left(Z_{j,\mathcal{R}_{j,\bar{k}}}\right). \tag{30}$$

[16]The outage probability is a metric largely used in wireless communication systems requiring inverse performance expressions (see, e.g., [70]–[75]). Similarity with network secrecy is in evaluating the probability that the desired secrecy rate is not achieved when confidential information is transmitted.

[17]The transmission of a confidential message can be based on the SINR at the intended receiver.

Similar to the conditional network secrecy rate defined in Section III-B, the conditional network secrecy throughput originated from the legitimate nodes in a bounded set $\mathcal{A}$ is defined as

$$T_{\rm ns}\left(\Omega_{\mathcal{A}}^{(\ell)}\right) = \sum_{j \in \mathcal{T}} \mathbb{1}_{\mathcal{A}}(\mathbf{X}_j) T_{j,\mathcal{R}_{j,\bar{k}}}. \tag{31}$$

Then, the network secrecy throughput density is given by

$$\tau_{\rm ns} = \lim_{t\to\infty} \frac{T_{\rm ns}\left(\Omega_{\mathcal{A}_t}^{(\ell)}\right)}{|\mathcal{A}_t|} \tag{32}$$

which results in

$$\tau_{\rm ns} = \lambda_{\rm tx} T. \tag{33}$$

In (33), $T = \mathbb{E}_{\mathbf{o}}\{T_{0,\mathcal{R}_{0,\bar{k}}}\}$ is the average secrecy throughput of a typical link in the network with the legitimate transmitter placed in the origin. Specifically, we can write[18]

$$T = P_{\rm it}(\mu^{\star}) R_{\rm s}. \tag{34}$$

The evaluation of network secrecy metrics, given by (20), (24), and (33), requires the statistical characterization of $Z_{0,\mathcal{R}_{0,\bar{k}}}$ and $\eta_{0,\mathcal{E}_0}$, whose CDF and PDF are derived in the following.

IV. Statistical Characterization of SIRs in Generic Fading Channels

Various strategies for selecting destinations can be employed to establish the legitimate links in wireless networks. Specifically, we consider the destination selection strategies where confidential information is sent to: 1) the kth closest receiver, or 2) the receiver with the maximum SIR. We consider interference limited conditions and characterize the SIRs at the kth legitimate receiver and at the ith eavesdropper, which are respectively given by

$$Z_{0,\mathcal{R}_{0,k}} \simeq \frac{|H_{0,\mathcal{R}_{0,k}}|^2}{D_{0,\mathcal{R}_{0,k}}^{2b} I_{\mathcal{R}_{0,k}}} \tag{35}$$

and

$$Z_{0,\mathcal{E}_{0,i}} \simeq \frac{|H_{0,\mathcal{E}_{0,i}}|^2}{D_{0,\mathcal{E}_{0,i}}^{2b} I_{\mathcal{E}_{0,i}}}. \tag{36}$$

A. SIRs in the Legitimate Network

We now characterize the SIR at a legitimate receiver selected from $\mathcal{R}_0$ using different selection strategies.

1) kth Closest Legitimate Receiver: Consider all legitimate receivers of the network with index set $\mathcal{R}_0$. To characterize the SIR at the receiver selected based on distances from the transmitter, consider the ordered index set of legitimate receivers $\{\mathcal{R}_{0,(k)}\}$ where the ordering is based on distances, i.e., $D_{0,\mathcal{R}_{0,(k)}} \leq D_{0,\mathcal{R}_{0,(k+1)}}\ \forall k$. The CDF $F_{Z_{0,\mathcal{R}_{0,(k)}}}(x)$ is given by

$$F_{Z_{0,\mathcal{R}_{0,(k)}}}(x) = \mathbb{P}\left\{\frac{|H_{0,\mathcal{R}_{0,(k)}}|^2}{D_{0,\mathcal{R}_{0,(k)}}^{2b} I_{\mathcal{R}_{0,(k)}}} \leq x\right\} \tag{37}$$

$$= \mathbb{P}\left\{G_{0,\mathcal{R}_{0,(k)}} \leq 0\right\} \tag{38}$$

[18]Note that the network secrecy throughput density in (33) has a double dependency on both $\lambda_{\rm tx}$ and $R_{\rm s}$ since $P_{\rm it}(\mu)$ also depends on the density of transmitters and the secrecy rate.

where $G_{0,\mathcal{R}_{0,(k)}} = |H_{0,\mathcal{R}_{0,(k)}}|^2 - xD_{0,\mathcal{R}_{0,(k)}}^{2b} I_{\mathcal{R}_{0,(k)}}$. Using the inversion theorem [76]

$$F_{Z_{0,\mathcal{R}_{0,(k)}}}(x) = g_{G_{0,\mathcal{R}_{0,(k)}}}(x) \tag{39}$$

where[19]

$$g_G(x) \triangleq \frac{1}{2} + \frac{1}{\pi}\int_0^\infty \Re\left\{\frac{\psi_G(\jmath\omega)}{\jmath\omega}\right\} d\omega \tag{40}$$

and $\psi_G(\cdot)$ is the characteristic function CF of the RV G.[20] In Appendix B, the CF $\psi_{G_{0,\mathcal{R}_{0,(k)}}}(\jmath\omega)$ is derived as

$$\psi_{G_{0,\mathcal{R}_{0,(k)}}}(\jmath\omega) = \psi_{|H_{0,\mathcal{R}_{0,(k)}}|^2}(\jmath\omega) \times \left(1 + \frac{\lambda_{\rm ir}}{\pi\lambda_{\rm rx}}\gamma x^{\frac{1}{b}}|\omega|^{\frac{1}{b}}\left[1 + \frac{\jmath\omega}{|\jmath\omega|}\tan\left(\frac{\pi}{2b}\right)\right]\right)^{-k}. \tag{41}$$

Equation (39), together with (40) and (41), gives the CDF of $Z_{0,\mathcal{R}_{0,(k)}}$.

Remark: The CF (41) and therefore the CDF (39) depend on the ratio between densities of legitimate transmitters and receivers $\lambda_{\rm ir}/\lambda_{\rm rx} = \lambda_{\rm tx}/\lambda_{\rm rx} = (1/\alpha - 1)^{-1}$.

2) Maximum SIR Legitimate Receiver: Consider all legitimate receivers, with index set $\mathcal{R}_0$, in a bounded set $\mathcal{A}_\mathcal{R}$. The CDF of $\eta_{0,\mathcal{R}_0} \triangleq \max_{k\in\mathcal{R}_0}\{Z_{0,\mathcal{R}_{0,k}}\}$ can be expressed as (see derivation in Appendix C)

$$F_{\eta_{0,\mathcal{R}_0}}(x) = e^{\left[F_{Z_{0,\mathcal{R}_{0,k}}}(x)-1\right]\lambda_{\rm rx}|\mathcal{A}_\mathcal{R}|} \tag{42}$$

where

$$F_{Z_{0,\mathcal{R}_{0,k}}}(x) = g_{G_{0,\mathcal{R}_{0,k}}}(x) \tag{43}$$

with $g_G(\cdot)$ defined in (40). The CF $\psi_{G_{0,\mathcal{R}_{0,k}}}(\jmath\omega)$ is given by (68) and (69), except that $D_{0,\mathcal{R}_{0,(k)}}$ is replaced by $D_{0,\mathcal{R}_{0,k}}$.

For a two-dimensional circular region $\mathcal{A}_\mathcal{R}$ centered at the legitimate transmitter with radius $d_{\rm Mr}$, $|\mathcal{A}_\mathcal{R}| = \pi d_{\rm Mr}^2$ and the squared distances $D_{\mathcal{R}_0,k}^2$ for various k's are independent and identically distributed (i.i.d.) with uniform distribution in $[0, d_{\rm Mr}^2]$.[21] Therefore, the CF of $G_{0,\mathcal{R}_{0,k}}$ becomes

$$\psi_{G_{0,\mathcal{R}_{0,k}}}(\jmath\omega) = \psi_{|H_{0,\mathcal{R}_{0,k}}|^2}(\jmath\omega) \times \frac{e^{-\lambda_{\rm ir}\gamma x^{\frac{1}{b}}|\omega|^{\frac{1}{b}}\left[1+\frac{\jmath\omega}{|\jmath\omega|}\tan\left(\frac{\pi}{2b}\right)\right]d_{\rm Mr}^2} - 1}{-\lambda_{\rm ir}\gamma x^{\frac{1}{b}}|\omega|^{\frac{1}{b}}\left[1 + \frac{\jmath\omega}{|\jmath\omega|}\tan\left(\frac{\pi}{2b}\right)\right]d_{\rm Mr}^2}. \tag{44}$$

B. SIR in the Eavesdropping Network

Consider all the eavesdroppers, with index $\mathcal{E}_0$, in a bounded set $\mathcal{A}_\mathcal{E}$. Recall that the eavesdropper with the maximum SIR $\eta_{0,\mathcal{E}_0}$ determines the secrecy performance. The CDF of $\eta_{0,\mathcal{E}_0}$ can be obtained following similar derivation as in Section IV-A.2 as

$$F_{\eta_{0,\mathcal{E}_0}}(x) = e^{\left[F_{Z_{0,\mathcal{E}_{0,i}}}(x)-1\right]\lambda_{\rm e}|\mathcal{A}_\mathcal{E}|}. \tag{45}$$

[19]Note that the right side of (39) is written explicitly as a function of x to emphasize the dependence of $G_{0,\mathcal{R}_{0,(k)}}$ on x.

[20]The notation $\Re\{\cdot\}$ indicates the real part of its argument, $\jmath = \sqrt{-1}$, and $\psi_G(\jmath\omega) \triangleq \mathbb{E}\{e^{+\jmath\omega G}\}$.

[21]Note that the CDF expression derived for a finite area will be useful in Section VI when competitive strategies for network secrecy will be proposed and analyzed.

Using the fact that $I_{\mathcal{E}_{0,i}}$ is a Stable RV according to (8), we obtain the CF $\psi_{G_{0,\mathcal{E}_{0,i}}}(\jmath\omega)$ as in (68) and (69), except that the parameters of the legitimate receivers are replaced by those of the eavesdroppers.

For a two-dimensional circular region $\mathcal{A}_\mathcal{E}$ centered at the legitimate transmitter with radius $d_{\rm Me}$, the CDF $F_{\eta_{0,\mathcal{E}_0}}(x)$ is given by (43)–(45), except: $\mathcal{R}_{0,k}$ is replaced by $\mathcal{E}_{0,i}$ in (43), and $\mathcal{R}_{0,k}$, $\lambda_{\rm ir}$, and $d_{\rm Mr}$ are replaced by $\mathcal{E}_{0,i}$, $\lambda_{\rm ie}$, and $d_{\rm Me}$ in (44).

For some fading distributions, the CDF of the SIR for both legitimate and eavesdropping networks can be obtained in closed form. Specifically, Section V provides closed-form expressions for Nakagami-m fading channels.

V. Statistical Characterization of SIRs in Nakagami Fading Channels

Based on the results obtained in Section IV, we now characterize the SIR at the selected legitimate receivers and at the eavesdroppers in Nakagami-m fading channels.[22]

A. SIRs in the Legitimate Network

1) kth Closest Legitimate Receiver: The CDF of the SIR at the legitimate receiver selected based on distances from the transmitter can be derived using the chain rule of conditional expectation as

$$F_{Z_{0,\mathcal{R}_{0,(k)}}}(x) = \mathbb{E}_{D_{0,\mathcal{R}_{0,(k)}}}\left\{F_{Z_{0,\mathcal{R}_{0,(k)}}|D_{0,\mathcal{R}_{0,(k)}}}(x)\right\} \tag{46}$$

where

$$F_{Z_{0,\mathcal{R}_{0,k}}|D_{0,\mathcal{R}_{0,(k)}}}(x) = \mathbb{E}_{I_{\mathcal{R}_{0,(k)}}|D_{0,\mathcal{R}_{0,(k)}}}\left\{F_{Z_{0,\mathcal{R}_{0,k}}|D_{0,\mathcal{R}_{0,(k)}},I_{\mathcal{R}_{0,(k)}}}(x)\right\}. \tag{47}$$

In Appendix D, the CDF $F_{Z_{0,\mathcal{R}_{0,(k)}}}(x)$ for Nakagami-m fading channels is derived as

$$F_{Z_{0,\mathcal{R}_{0,(k)}}}(x) = 1 - \sum_{i=0}^{m-1}\frac{(-1)^i}{i!}\left[\frac{d^i}{ds^i}\left(1 + \frac{(mxs)^{\frac{1}{b}}\lambda_{\rm ir}\gamma}{\cos\left(\frac{\pi}{2b}\right)\pi\lambda_{\rm rx}}\right)^{-k}\right]_{s=1}. \tag{48}$$

Finally, by differentiating (48) with respect to x, we obtain the PDF of $Z_{0,\mathcal{R}_{0,(k)}}$ as

$$f_{Z_{0,\mathcal{R}_{0,(k)}}}(x) = \sum_{i=0}^{m-1}\frac{(-1)^i}{i!} \times \left[\frac{d^i}{ds^i}\frac{(\pi\lambda_{\rm rx})^k (ms)^{\frac{1}{b}} k\lambda_{\rm ir}\frac{\gamma}{\cos\left(\frac{\pi}{2b}\right)}x^{\frac{1}{b}-1}}{b\left(\pi\lambda_{\rm rx} + \frac{\gamma}{\cos\left(\frac{\pi}{2b}\right)}(msx)^{\frac{1}{b}}\lambda_{\rm ir}\right)^{k+1}}\right]_{s=1}. \tag{49}$$

2) Maximum SIR Legitimate Receiver: The CDF of the SIR at the legitimate receiver, selected based on the maximum SIR, is given by (42) in terms of $F_{Z_{0,\mathcal{R}_{0,k}}}(x)$. The CDF of of $Z_{0,\mathcal{R}_{0,k}}$ can be written as

$$F_{Z_{0,\mathcal{R}_{0,k}}}(x) = \mathbb{E}_{D_{0,\mathcal{R}_{0,k}}}\left\{F_{Z_{0,\mathcal{R}_{0,k}}|D_{0,\mathcal{R}_{0,k}}}(x)\right\} \tag{50}$$

[22]Integer values for fading severity m are considered.

where the conditional CDF $F_{Z_{0,\mathcal{R}_{0,k}}|D_{0,\mathcal{R}_{0,k}}}(x)$ for Nakagami-m fading channels is given by (72), except that $D_{0,\mathcal{R}_{0,(k)}}$ is replaced by $D_{0,\mathcal{R}_{0,k}}$. To carry out the expectation in (50), we consider a two-dimensional circular region $\mathcal{A}_{\mathcal{R}}$ centered at the legitimate transmitter with radius d_{Mr}. The expectation over $D_{0,\mathcal{R}_{0,k}}$ results in

$$F_{Z_{0,\mathcal{R}_{0,k}}}(x) = 1 - \sum_{i=0}^{m-1} \frac{(-1)^i}{i!} \left[\frac{d^i}{ds^i} - 10000 fil\left(\lambda_{\mathrm{ir}}, \frac{\gamma}{\cos\left(\frac{\pi}{2b}\right)}, x, s, 0, d_{\mathrm{Mr}}\right)\right]_{s=1} \quad (51)$$

for $x > 0$, and 0 otherwise, where

$$-10000 fil\left(\lambda, \gamma, x, s, d_{\mathrm{m}}, d_{\mathrm{M}}\right) \triangleq \frac{e^{-(msx)^{\frac{1}{b}}\lambda\gamma d_{\mathrm{m}}^2} - e^{-(msx)^{\frac{1}{b}}\lambda\gamma d_{\mathrm{M}}^2}}{\lambda\gamma (msx)^{\frac{1}{b}} \left(d_{\mathrm{M}}^2 - d_{\mathrm{m}}^2\right)}. \quad (52)$$

Substituting (51) into (42), the CDF for the maximum SIR $F_{\eta_{0,\mathcal{R}_0}}(x)$ is obtained. To complete the derivation, we take the limit as $d_{\mathrm{Mr}} \to \infty$, resulting in

$$F_{\eta_{0,\mathcal{R}_0}}(x) = \exp\left(- \sum_{i=0}^{m-1} \frac{(-1)^i}{i!} \frac{\lambda_{\mathrm{rx}}}{\lambda_{\mathrm{ir}}} \left[\frac{d^i}{ds^i} \frac{\pi \cos\left(\frac{\pi}{2b}\right)}{(mxs)^{\frac{1}{b}}\gamma} \right]_{s=1} \right). \quad (53)$$

Differentiating (53) with respect to x yields the PDF of the maximum SIR for the legitimate receivers. Note that the distribution of the maximum SIR depends on the ratio $\lambda_{\mathrm{rx}}/\lambda_{\mathrm{ir}}$.

B. SIR in the Eavesdropping Network

By following the approach in Section IV-B for the case of general fading and using the derivations in Section V-A.2, the CDF of $\eta_{0,\mathcal{E}_0}$ can be expressed as in (45) where, for Nakagami-m fading, $F_{Z_{0,\mathcal{E}_{0,i}}}(x)$ is given by

$$F_{Z_{0,\mathcal{E}_{0,i}}}(x) = 1 - \sum_{i=0}^{m-1} \frac{(-1)^i}{i!} \left[\frac{d^i}{ds^i} - 10000 fil\left(\lambda_{\mathrm{ie}}, \frac{\gamma}{\cos\left(\frac{\pi}{2b}\right)}, x, s, 0, d_{\mathrm{Me}}\right)\right]_{s=1} \quad (54)$$

for $x > 0$ and 0 otherwise. Letting $d_{\mathrm{Me}} \to \infty$, we obtain the CDF of $\eta_{0,\mathcal{E}_0}$ given by (53) except $\eta_{0,\mathcal{R}_0}$, λ_{rx}, and λ_{ir} are replaced by $\eta_{0,\mathcal{E}_0}$, λ_{e}, and λ_{ie}, respectively. Note that the distribution of the maximum SIR depends on the ratio $\lambda_{\mathrm{e}}/\lambda_{\mathrm{ie}}$.

VI. Competitive Strategies for Network Secrecy

As observed in Sections IV and V, intrinsic properties, such as aggregate network interference and nodes spatial distribution, affect network secrecy. Therefore, both legitimate and eavesdropping nodes can employ competitive strategies exploiting these intrinsic properties for preserving or disrupting information confidentiality, respectively. In particular, we propose and analyze competitive strategies for: 1) neutralizing eavesdropping capabilities; 2) reducing network interference at the legitimate receiver; 3) reducing network interference at the eavesdroppers; and 4) controlling the network interference injected into the legitimate and the eavesdropping networks.[23] These strategies are presented for networks in a two-dimensional plane.

A. Nearby Eavesdropping Region Neutralization

The nearby eavesdropping region neutralization (NERN) strategy aims to deny capabilities of eavesdroppers around the legitimate transmitter. This strategy is based on the observation that eavesdroppers close to the transmitter are likely to have high SIR; therefore, they are primary culprits for reducing the level of network secrecy. Specifically, when NERN is employed, all eavesdroppers within a distance d_{me} from the transmitter are neutralized.[24] In this case, the squared distances $D_{0,\mathcal{E}_{0,i}}^2$ of the remaining eavesdroppers are i.i.d. and follow a uniform distribution in $[d_{\mathrm{me}}^2, d_{\mathrm{Me}}^2]$. Therefore, the CDF of $Z_{0,\mathcal{E}_{0,i}}$ becomes

$$F_{Z_{0,\mathcal{E}_{0,i}}}(x) = 1 - \sum_{i=0}^{m-1} \frac{(-1)^i}{i!} \times \left[\frac{d^i}{ds^i} - 10000 fil\left(\lambda_{\mathrm{ie}}, \frac{\gamma}{\cos\left(\frac{\pi}{2b}\right)}, x, s, d_{\mathrm{me}}, d_{\mathrm{Me}}\right)\right]_{s=1}. \quad (55)$$

Letting $d_{\mathrm{Me}} \to \infty$, the CDF of the maximum SIR becomes

$$F_{\eta_{0,\varepsilon_0}}(x) = \exp\left(- \sum_{i=0}^{m-1} \frac{(-1)^i}{i!} \frac{\lambda_{\mathrm{e}}}{\lambda_{\mathrm{ie}}} \times \left[\frac{d^i}{ds^i} \frac{\pi \cos\left(\frac{\pi}{2b}\right) e^{-\gamma x^{\frac{1}{b}} d_{\mathrm{me}}^2}}{(mxs)^{\frac{1}{b}}\gamma} \right]_{s=1} \right). \quad (56)$$

Using (56) together with the results in Section V, the network secrecy rate density (20), the network secrecy rate outage density (24), and the network secrecy throughput density (33) are obtained for the case of NERN strategy.

B. Eavesdropping Network Interference Suppression

The eavesdropping network interference suppression (ENIS) strategy aims to reduce the effects of network interference on the eavesdroppers. This strategy is based on the observation that the eavesdroppers with higher SIR have better capabilities for eavesdropping the confidential information. Specifically, when ENIS is employed, the network interference at each eavesdropper can be reduced, for example, by narrowing the angle from which radio signals are received via beamforming.

Consider the ENIS strategy where eavesdroppers employ antennas with aperture angle θ_{e} radians, in which case the effective density of interferers $\breve{\lambda}_{\mathrm{ie}}$ affecting the eavesdroppers is

$$\breve{\lambda}_{\mathrm{ie}} = \frac{\theta_{\mathrm{e}}}{2\pi}(\lambda_{\mathrm{tx}} + \lambda_{\mathrm{jx}}). \quad (57)$$

Such strategy also affects the density of the eavesdroppers capable of intercepting the confidential information, whose effective density $\breve{\lambda}_{\mathrm{e}}$ is given by

$$\breve{\lambda}_{\mathrm{e}} = \lambda_{\mathrm{e}} \quad (58a)$$

or

$$\breve{\lambda}_{\mathrm{e}} = \frac{\theta_{\mathrm{e}}}{2\pi}\lambda_{\mathrm{e}} \quad (58b)$$

[23] For brevity, the performance of these strategies is analyzed in the case of Nakagami-m fading channel. However, the analysis can be carried out for other fading distributions using the results of Section IV.

[24] Consider that eavesdroppers within the neutralization region of transmitter j are still capable of eavesdropping other transmitters.

depending on whether the eavesdroppers have or do not have the knowledge of legitimate transmitter positions.[25]

Replacing $\lambda_{\rm e}$ and $\lambda_{\rm ie}$ with $\breve{\lambda}_{\rm e}$ and $\breve{\lambda}_{\rm ie}$, and using the results in Section V, the network secrecy rate density (20), the network secrecy rate outage density (24), and the network secrecy throughput density (33) are obtained for the ENIS strategy.

C. Legitimate Network Interference Suppression

The legitimate network interference suppression (LNIS) strategy aims to reduce the effects of network interference on the legitimate receivers. This strategy is based on the observation that the legitimate receivers with higher SIR have better capabilities for receiving confidential information. Specifically, when LNIS is employed, the network interference at each legitimate receiver can be reduced, for example, by narrowing the angle from which the radio signals are received or by narrowing the transmission antenna pattern via beamforming.

Consider first the LNIS strategy where the legitimate receivers employ antennas with aperture angles $\theta_{\rm r}$ radians, in which case the effective density of interferers $\breve{\lambda}_{\rm ir}$ affecting the legitimate receivers is

$$\breve{\lambda}_{\rm ir} = \frac{\theta_{\rm r}}{2\pi}\lambda_{\rm tx}. \tag{59}$$

Such strategy also affects the density of the legitimate receivers capable of listening the confidential information, whose effective density $\breve{\lambda}_{\rm rx}$ is given by

$$\breve{\lambda}_{\rm rx} = \lambda_{\rm rx} \tag{60a}$$

or

$$\breve{\lambda}_{\rm rx} = \frac{\theta_{\rm r}}{2\pi}\lambda_{\rm rx} \tag{60b}$$

depending on whether the legitimate receivers have or do not have the knowledge of legitimate transmitter positions.

Consider next the LNIS strategy where legitimate transmitters employ antennas with aperture angle $\theta_{\rm t}$ radians, in which case the effective density $\breve{\lambda}_{\rm e}$ of the eavesdroppers capable of intercepting the confidential information is

$$\breve{\lambda}_{\rm e} = \frac{\theta_{\rm t}}{2\pi}\lambda_{\rm e}. \tag{61}$$

Such strategy also affects the densities of nodes interfering the legitimate receivers and the eavesdroppers, whose effective densities $\breve{\lambda}_{\rm ir}$ and $\breve{\lambda}_{\rm ie}$ are given by

$$\breve{\lambda}_{\rm ir} = \frac{\theta_{\rm t}}{2\pi}\lambda_{\rm tx} \tag{62}$$

$$\breve{\lambda}_{\rm ie} = \frac{\theta_{\rm t}}{2\pi}\lambda_{\rm tx} + \lambda_{\rm jx}. \tag{63}$$

Now, consider the LNIS strategy where both the legitimate transmitters and receivers employ antennas with aperture angles $\theta_{\rm t}$ and $\theta_{\rm r}$, respectively, in which case the effective density $\breve{\lambda}_{\rm ir}$ of interferers affecting the legitimate receivers is

$$\breve{\lambda}_{\rm ir} = \frac{\theta_{\rm t}\theta_{\rm r}}{4\pi^2}\lambda_{\rm tx}. \tag{64}$$

Replacing $\lambda_{\rm rx}$, $\lambda_{\rm e}$, $\lambda_{\rm ir}$, and $\lambda_{\rm ie}$ with $\breve{\lambda}_{\rm rx}$, $\breve{\lambda}_{\rm e}$, $\breve{\lambda}_{\rm r}$, and $\breve{\lambda}_{\rm ie}$, depending on the specific LNIS strategy, and using the results in Section V, the network secrecy rate density (20), the network secrecy rate outage density (24), and the network secrecy throughput density (33) are obtained for the LNIS strategy.

D. Asymmetric Network Interference Generation

The asymmetric network interference generation (ANIG) strategy aims to control the amount of network interference injected into the legitimate network and the eavesdropping networks. This strategy is based on the observation that intrinsic secrecy can be enhanced by increasing the SIR at the legitimate receivers or decreasing those at the eavesdroppers. This can be accomplished, for example, by nulling the emission in the direction of unintended legitimate receivers via beamforming.

Consider a legitimate network with a fraction $\xi \in [0,1]$ of legitimate transmitters having emission nulling capabilities. In this case, the effective density of interferers $\breve{\lambda}_{\rm ir}$ affecting the legitimate receivers is

$$\breve{\lambda}_{\rm ir} = (1-\xi)\lambda_{\rm tx}. \tag{65}$$

Replacing $\lambda_{\rm ir}$ with $\breve{\lambda}_{\rm ir}$, and using the results in Section V, the network secrecy rate density (20), the network secrecy rate outage density (24), and the network secrecy throughput density (33) are obtained for the ANIG strategy.

VII. Numerical Results

This section presents the secrecy performance of a large wireless network. In particular, the impact of the destination selection, propagation environment, network configuration, and various competitive strategies on network secrecy are quantified.[26]

A. Destinations Selection

Fig. 3 shows the network secrecy rate density $\rho_{\rm ns}$ in cib/s/Hz/m^2 as a function of α when the kth closest receivers are selected in the legitimate network for different values of k. It can be observed that $\rho_{\rm ns}$ decreases significantly as k increases. This behavior can be attributed to the fact that the network secrecy rate is limited by the capacity of legitimate links, which decreases as the distance between legitimate transmitters and receivers increases. It can also be observed that an optimal value of α maximizing $\rho_{\rm ns}$ exists. This is due to the fact that the network interference affects both legitimate and eavesdropping networks, therefore it can be either beneficial or harmful for network secrecy. Fig. 3 also shows results obtained by two levels of Monte Carlo simulations. Low-level simulation results (black cross markers) are obtained by generating node positions of the legitimate and eavesdropping networks according to the PPPs, accounting for possible spatial correlation of the network interference. High-level simulation results (black triangle markers) are obtained by assuming independent network interference. In addition to agreeing with the analytical results, these simulation results confirm that the independence assumption for network interference is sufficient for evaluating network secrecy metrics in large wireless networks.

[25]Various localization techniques can be employed for determining the positions of nodes in the network [77]–[84].

[26]In the following, consider a two-dimensional network and (unless otherwise stated) Rayleigh fading, infinite $d_{\rm Me}$ and $d_{\rm Mr}$, and $d_0 = 1$ m. Although the analysis of the network secrecy metrics accounts for the presence of intentional interfering nodes, consider (unless otherwise stated) $\lambda_{\rm jx} = 0$ as a worst case for network secrecy.

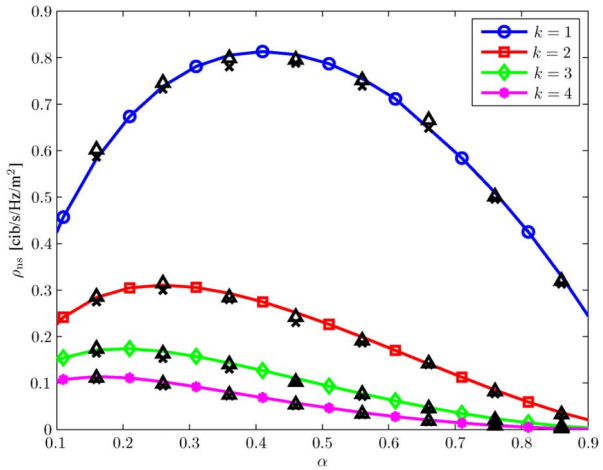

Fig. 3. Network secrecy rate density as a function of α when the kth closest legitimate receivers are selected for $b = 2$, $\lambda_\ell = 1$ [node/m^2], and $\lambda_{\rm e}/\lambda_\ell = 0.1$. Lines represent analytical results. Black crosses and triangles represent the Monte Carlo simulations done for the case when interferer distances depend on the placement of the transmitters and for the case when interferer distances are generated independently, respectively.

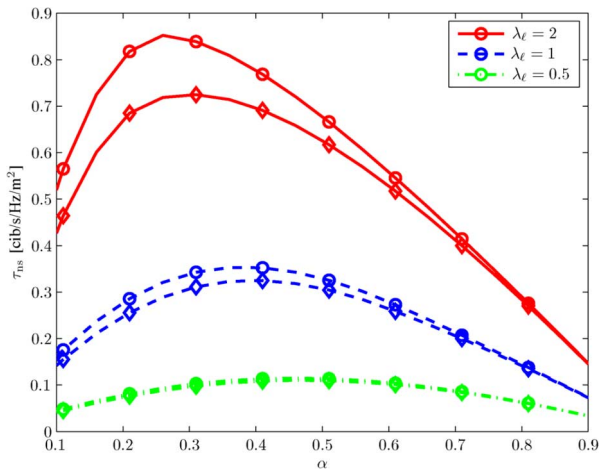

Fig. 4. Network secrecy throughput density as a function of α when the closest legitimate receivers ($k = 1$) are selected (diamonds) and when the receivers with highest SIR ($\eta_{0,\mathcal{R}_0}$) are selected (circles) for $b = 2$, $P^*_{\rm so} = 0.1$, $R_{\rm s} = 4$ [cib/s/Hz], and $\lambda_{\rm e} = 0.1$ [node/m^2].

Fig. 4 shows the network secrecy throughput density $\tau_{\rm ns}$ in cib/s/Hz/m^2 as a function of α for different values of λ_ℓ when the receivers closest to the transmitters or those with the maximum SIR are selected. It can be observed that $\tau_{\rm ns}$ increases with λ_ℓ. It can also be observed that an optimal value of α maximizing $\tau_{\rm ns}$ exists. This again is due to the fact that the network interference affects both legitimate and eavesdropping networks. Note that the selection based on the maximum SIR provides better performance. This behavior is noticeable particularly for large λ_ℓ, while for small λ_ℓ, the legitimate receiver with maximum SIR is often the one closest to the legitimate transmitter.

B. Propagation Environment and Network Configuration

Fig. 5 shows the network secrecy throughput density $\tau_{\rm ns}$ as a function of α, when the closest legitimate receivers are selected as a destination, for different values of fading severity parameter m and amplitude-loss coefficient b. It can be observed that $\tau_{\rm ns}$ is insensitive to variations in m, whereas it is affected more significantly by b. This behavior is due to the fact that b significantly affects the average received power of the useful and interfering signals in the network. It can also be observed that the optimal value of α shifts toward higher values as b increases.

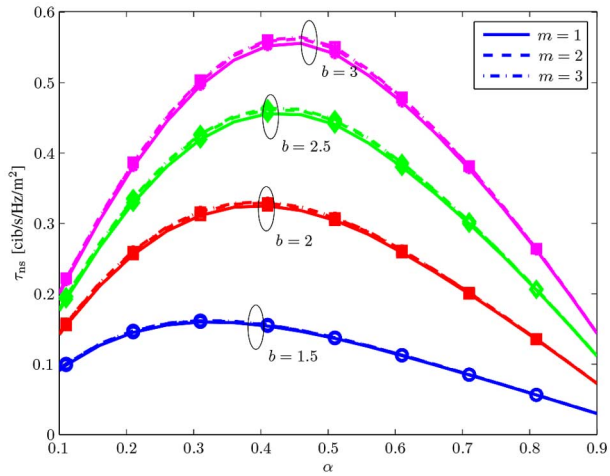

Fig. 5. Network secrecy throughput density as a function of α when the closest legitimate receivers are selected for $P^*_{\rm so} = 0.1$, $R_{\rm s} = 4$ [cib/s/Hz], $\lambda_\ell = 1$ [node/m^2], $\lambda_{\rm e} = 0.1$ [node/m^2], different values of b, and different values of m.

Fig. 6(a) and (b), respectively, shows the contours of network secrecy throughput density $\tau_{\rm ns}$ as a function of α and $R_{\rm s}$, when the closest legitimate receivers are selected, for $\lambda_\ell = 2$ and 0.5 node/m^2. It can be observed that $\tau_{\rm ns}$ scales with λ_ℓ.[27] It can also be seen that the maximum throughput density region shifts toward lower $R_{\rm s}$ and higher α for a lower value of λ_ℓ. These results show that for a lower legitimate node density, a higher fraction of transmitters among the legitimate nodes is preferable for enhancing the network secrecy. Note that this observation is consistent with that of Fig. 4.

Fig. 7 shows the network secrecy throughput density $\tau_{\rm ns}$ as a function of α for different values of $\lambda_{\rm e}$ when the closest legitimate receivers are selected. As expected, $\tau_{\rm ns}$ decreases as the density of eavesdroppers increases. It can also be observed that the optimal α shifts toward higher values as $\lambda_{\rm e}$ increases. This behavior can be attributed to the fact that, for a higher $\lambda_{\rm e}$, a larger amount of network interference is needed to mitigate the eavesdropper capabilities.

Fig. 8 shows the network secrecy throughput density $\tau_{\rm ns}$ as a function of $\lambda_{\rm jx}/\lambda_\ell$ (i.e., the ratio between densities of intentional interferers and legitimate nodes) for different values of α when the closest legitimate receivers are selected. It can be observed that $\tau_{\rm ns}$ increases as $\lambda_{\rm jx}/\lambda_\ell$ increases, showing the benefits of intentional interference on network secrecy. This behavior can be attributed to the fact that intentional interference mitigates the eavesdropping capabilities. It can also be observed that $\tau_{\rm ns}$ approaches the asymptotic values, corresponding to the absence of eavesdroppers. Note that the asymptotic value of $\tau_{\rm ns}$ depends on α according to the number of legitimate links and the amount of network interference.

[27] Note that, for a fixed α, a higher density of legitimate receivers corresponds to a lower average link distance.

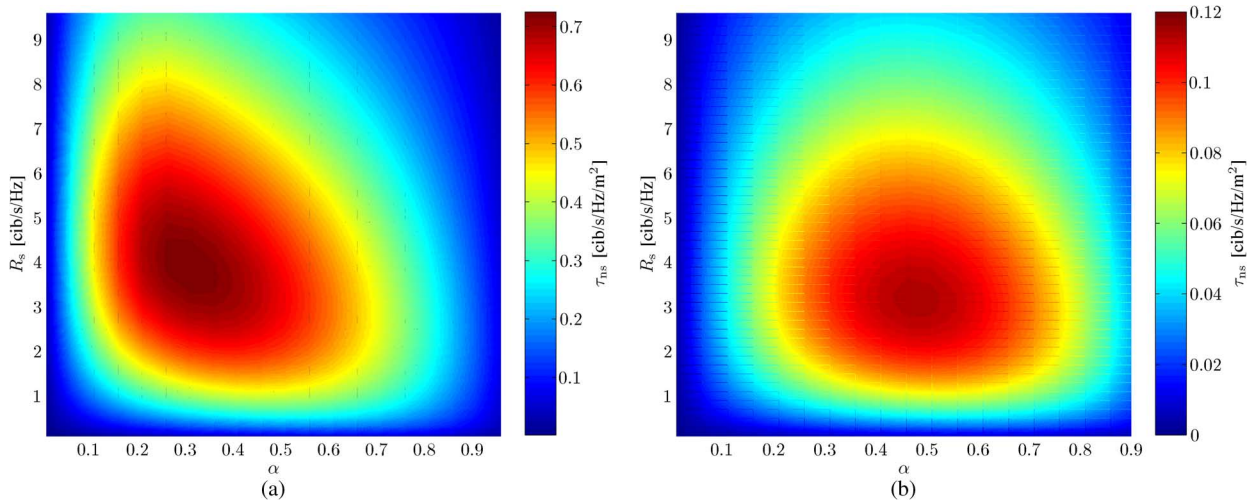

Fig. 6. Network secrecy throughput density as a function of α and R_s when the closest legitimate receivers are selected for $b = 2$, $P_{so}^* = 0.1$, $\lambda_e = 0.1$ [node/m^2], and $\lambda_\ell = 2$ or 0.5 [node/m^2]. (a) $\lambda_\ell = 2$[node/m^2]. (b) $\lambda_\ell = 0.5$[node/m^2]

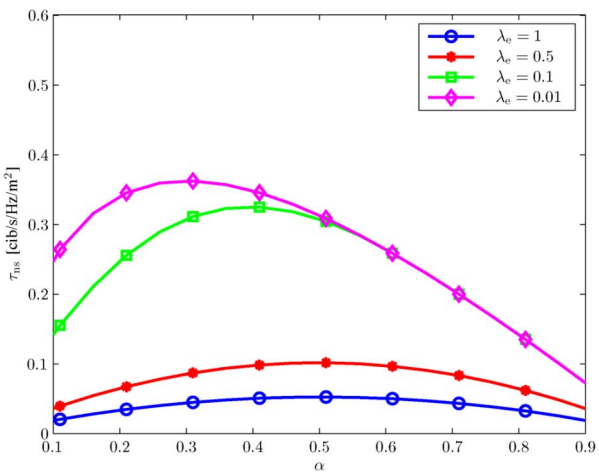

Fig. 7. Network secrecy throughput density as a function of α when the closest legitimate receivers are selected for $b = 2$, $P_{so}^* = 0.1$, $R_s = 4$ [cib/s/Hz], $\lambda_\ell = 1$ [node/m^2], and different values of λ_e.

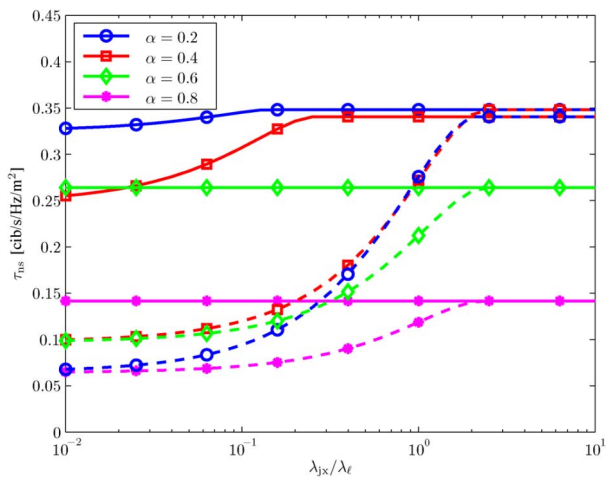

Fig. 8. Network secrecy throughput density as a function of $\lambda_{jx}/\lambda_\ell$ when the closest legitimate receivers are selected, intentional interferers are active, $b = 2$, $P_{so}^* = 0.1$, $\lambda_\ell = 1$ [node/m^2], $R_s = 4$ [cib/s/Hz], and $\lambda_e = 0.1$ (continuous lines) or $\lambda_e = 0.5$ [node/m^2] (dashed lines).

Note also that the asymptotic values are reached by lower values of $\lambda_{jx}/\lambda_\ell$ for lower λ_e.

C. Competitive Strategies for Network Secrecy

Fig. 9 shows the network secrecy throughput density τ_{ns} as a function of d_{me} for different values of α when NERN is employed (note that $d_{me} = 0$ corresponds to the absence of NERN). It can be observed that τ_{ns} increases with d_{me} and approaches the asymptotic values corresponding to the absence of eavesdroppers. This behavior can be attributed to the fact that a higher d_{me} corresponds to the neutralization of a larger number of nearby eavesdroppers, therefore improving the network secrecy. Note that the asymptotic values are consistent with those of Fig. 8 as expected.

Fig. 10 shows the network secrecy throughput density τ_{ns} as a function of antenna aperture angles for different values of α and λ_e when ENIS and LNIS are employed. It can be observed that LNIS can successfully counteract ENIS. In fact, note that when nodes have the same beamforming capability ($\theta_e = \theta_r = \theta_t = \theta$), the τ_{ns} increases as θ decreases.

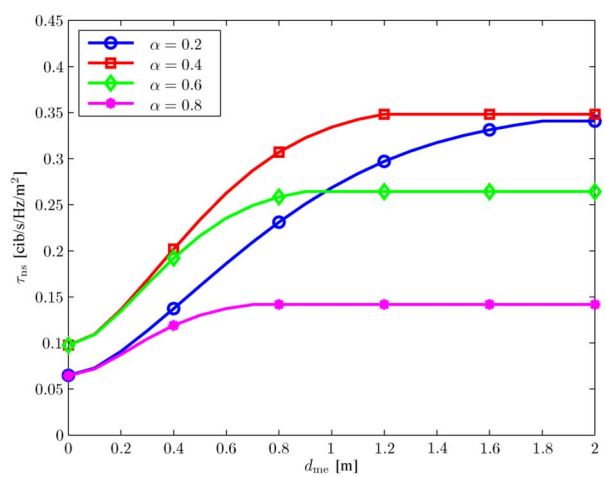

Fig. 9. Network secrecy throughput density as a function of d_{me} when the closest legitimate receivers are selected in the presence of NERN for $b = 2$, $P_{so}^* = 0.1$, $R_s = 4$ [cib/s/Hz], $\lambda_\ell = 1$ [node/m^2], and $\lambda_e = 0.5$ [node/m^2].

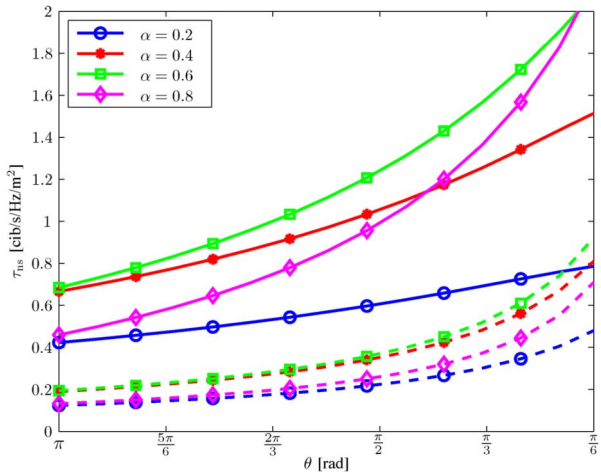

Fig. 10. Network secrecy throughput density as a function of $\theta_{\rm e} = \theta_{\rm r} = \theta_{\rm t} = \theta$ when the closest legitimate receivers are selected in the presence of ENIS and LNIS for $b = 2$, $P_{\rm so}^* = 0.1$, $\lambda_\ell = 1$ [node/m^2], $R_{\rm s} = 4$ [cib/s/Hz], and $\lambda_{\rm e} = 0.1$ (continuous lines) or $\lambda_{\rm e} = 0.5$ [node/m^2] (dashed lines).

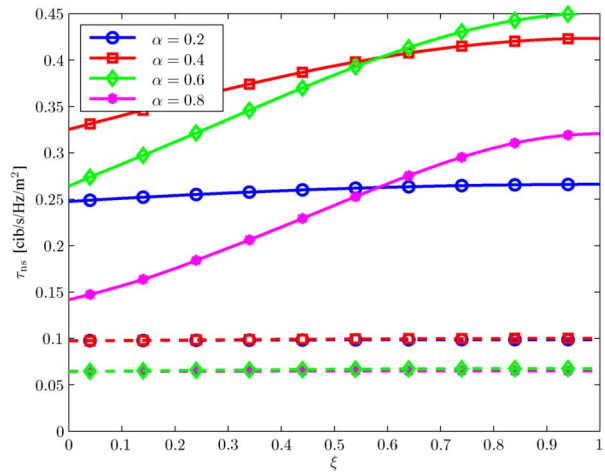

Fig. 11. Network secrecy throughput density as a function of ξ when the closest legitimate receivers are selected in the presence of ENIS with $\theta_{\rm e} = 2\pi(1-\xi)$ and ANIG for $b = 2$, $P_{\rm so}^* = 0.1$, $\lambda_\ell = 1$ [node/m^2], $R_{\rm s} = 4$ [cib/s/Hz], and $\lambda_{\rm e} = 0.1$ (continuous lines) or $\lambda_{\rm e} = 0.5$ [node/m^2] (dashed lines).

Fig. 11 shows the network secrecy throughput density $\tau_{\rm ns}$ as a function of ξ for different values of α when ENIS and ANIG strategies are employed by eavesdropping and legitimate networks, respectively. It can be observed that ANIG can increase the network secrecy by increasing ξ (note that $\xi = 0$ corresponds to the absence of ANIG). However, by comparing Fig. 10 to Fig. 11, one can observe that LNIS is more effective than ANIG in enhancing the network secrecy when ENIS is employed by the eavesdropping network.

VIII. Final Remark

A framework for design and analysis of wireless networks with intrinsic secrecy has been developed. In particular, the concept of network secrecy and new metrics for its evaluation have been introduced. To quantify these metrics, the received SIR in the legitimate network and in the eavesdropping network are characterized. This paper offers a new perspective on the role of node spatial distribution, wireless propagation medium, and aggregate network interference on network secrecy. Specifically, the analysis yields insights into the essence of network intrinsic secrecy and provides guidelines for devising competitive strategies that exploit properties inherent in wireless networks. Regarding the propagation medium, our results reveal that the effects of path loss dominate those of fading. It is shown that network interference can provide significant benefits to network secrecy. This work enables a deeper understanding of how intrinsic properties of wireless networks can be exploited to enhance the network secrecy, paving the way to more secure and safer communications in the information society.

Appendix A
Derivation of (20)

Since a generic homogeneous PPP $\mathbf{\Pi}$ is stationary, for any property Γ, $\mathbb{P}\{\mathbf{\Pi} + \boldsymbol{\nu} \in \Gamma\} = \mathbb{P}\{\mathbf{\Pi} \in \Gamma\}$ for all $\boldsymbol{\nu} \in \mathbb{R}^n$ [69]. To account for the confidential information generated from a bounded set $\mathcal{A}_t \subset \mathbb{R}^n$, the origin of the reference system can be shifted to the position of the jth node in $\mathcal{A}_t$. Let $\mathbf{\Pi} \triangleq \mathbf{\Pi}_{\rm tx} \cup \mathbf{\Pi}_{\rm rx} \cup \mathbf{\Pi}_{\rm e} \cup \mathbf{\Pi}_{\rm jx}$ and $f(\mathbf{\Pi}) \triangleq \sum_{j\in\mathcal{T}} \mathbb{1}_{\{\rm o\}}(\mathbf{X}_j) R_{j,\mathcal{R}_{j,\bar{k}},\mathcal{E}_{j,i}}$, (17) can be rewritten as

$$R_{\rm ns}\left(\Omega_{\mathcal{A}_t}\right) = \sum_{\mathbf{X}_j \in \mathcal{A}_t \bigcap \mathbf{\Pi}_{\rm tx}} f(\mathbf{\Pi} - \mathbf{X}_j). \tag{66}$$

If $\sup\{r : \mathcal{B}(r) \subseteq \mathcal{A}_t\} \to \infty$ as $t \to \infty$ for a convex averaging sequence $\{\mathcal{A}_t\}$ with $\mathcal{A}_1 \subset \mathcal{A}_2 \subset \cdots \subset \mathbb{R}^n$, then (19) can be written as

$$\begin{aligned}\rho_{\rm ns} &= \lim_{t\to\infty} \frac{1}{|\mathcal{A}_t|} \sum_{\mathbf{X}_j \in \mathcal{A}_t \bigcap \mathbf{\Pi}_{\rm tx}} f(\mathbf{\Pi} - \mathbf{X}_j) \\ &= \lim_{t\to\infty} \frac{\mathbf{\Pi}_{\rm tx}(A_t)}{|\mathcal{A}_t|} \frac{1}{\mathbf{\Pi}_{\rm tx}(\mathcal{A}_t)} \sum_{\mathbf{X}_j \in \mathcal{A}_t \bigcap \mathbf{\Pi}_{\rm tx}} f(\mathbf{\Pi} - \mathbf{X}_j)\end{aligned}$$

where $\mathbf{\Pi}_{\rm tx}(\mathcal{A}_t)$ is the number of points from $\mathbf{\Pi}_{\rm tx}$ contained in $\mathcal{A}_t$. From [69, Proposition 1.23] and recalling that, for bounded real functions, the limit of a product is the product of the limits, we obtain

$$\rho_{\rm ns} = \lambda_{\rm tx} \mathbb{E}_{\rm o}\left\{f(\mathbf{\Pi})\right\} \tag{67}$$

provided that $\mathbb{E}_{\rm o}\{f(\mathbf{\Pi})\} < \infty$. This results in (20).

Appendix B
Derivation of (41)

For each $x \in \mathbb{R}$, the CF of $G_{0,\mathcal{R}_{0,(k)}}$ can be written as

$$\begin{aligned}\psi_{G_{0,\mathcal{R}_{0,(k)}}}(\jmath\omega) &= \psi_{\left|H_{0,\mathcal{R}_{0,(k)}}\right|^2}(\jmath\omega) \\ &\quad \times \mathbb{E}_{D_{0,\mathcal{R}_{0,(k)}}}\left\{\psi_{I_{\mathcal{R}_{0,(k)}}}\left(-\jmath\omega D_{0,\mathcal{R}_{0,(k)}}^{2b} x\right)\right\}\end{aligned} \tag{68}$$

where $I_{\mathcal{R}_{0,(k)}}$ is a Stable distributed RV according to (8), with CF given by

$$\psi_{I_{\mathcal{R}_{0,(k)}}}(\jmath\omega) = \exp\left(-\lambda_{\rm ir}\gamma|\omega|^{\frac{1}{b}}\left[1 + \frac{\jmath\omega}{|\jmath\omega|}\tan\left(\frac{\pi}{2b}\right)\right]\right). \tag{69}$$

Since the squared distance $D^2_{0,\mathcal{R}_{0,(k)}}$ is an Erlang distributed RV [85]–[87] with CF given by

$$\psi^2_{\mathcal{D}_{0,\mathcal{R}_{0,(k)}}}(\jmath\omega) = \left(1 - \frac{\jmath\omega}{\pi\lambda_{\rm rx}}\right)^{-k} \tag{70}$$

we obtain $\psi_{G_0,\mathcal{R}_{0,(k)}}(\jmath\omega)$ as in (41).

Appendix C
Derivation of (42)

To characterize the maximum SIR among nodes with index in $\mathcal{R}_0$, consider $\mathcal{R}_0$ with cardinality $N_{\mathcal{R}_0} \triangleq |\mathcal{R}_0|$. The CDF of $\eta_{0,\mathcal{R}_0}$ conditioned on $N_{\mathcal{R}_0}$ is given by[28]

$$F_{\eta_{0,\mathcal{R}_0}|N_{\mathcal{R}_0}}(x) = \begin{cases} \left[F_{Z_{0,\mathcal{R}_{0,k}}}(x)\right]^{N_{\mathcal{R}_0}} & N_{\mathcal{R}_0} \geq 1 \\ 1 & N_{\mathcal{R}_0} = 0. \end{cases}$$

By taking the expectation of $F_{\eta_{0,\mathcal{R}_0}|N_{\mathcal{R}_0}}(x)$ over $N_{\mathcal{R}_0}$, we obtain (42).

Appendix D
Derivation of (48)

For Nakagami-m fading channels, the conditional CDF of $Z_{0,\mathcal{R}_{0,(k)}}$ is given by

$$\begin{aligned} &F_{Z_{0,\mathcal{R}_{0,(k)}}|D_{0,\mathcal{R}_{0,(k)}},I_{0,\mathcal{R}_{0,(k)}}}(x) \\ &\quad = 1 - \sum_{i=0}^{m-1} \frac{1}{i!}\left(mD^{2b}_{0,\mathcal{R}_{0,(k)}} I_{\mathcal{R}_{0,(k)}} x\right)^i e^{-mxD^{2b}_{0,\mathcal{R}_{0,(k)}} I_{\mathcal{R}_{0,(k)}}} \\ &\quad = 1 - \sum_{i=0}^{m-1} \frac{(-1)^i}{i!}\left[\frac{d^i}{ds^i} e^{-mxsD^{2b}_{0,\mathcal{R}_{0,(k)}} I_{\mathcal{R}_{0,(k)}}}\right]_{s=1}. \end{aligned} \tag{71}$$

By taking the expectation over $I_{\mathcal{R}_0,(k)}$, the CDF of $Z_{0,\mathcal{R}_{0,(k)}}$ conditioned on $D_{0,\mathcal{R}_{0,(k)}}$ results in

$$\begin{aligned} &F_{Z_{0,\mathcal{R}_{0,(k)}}|D_{0,\mathcal{R}_{0,(k)}}}(x) \\ &\quad = 1 - \sum_{i=0}^{m-1} \frac{(-1)^i}{i!}\left[\frac{d^i}{ds^i}\mathcal{L}_{I_{\mathcal{R}_{0,(k)}}}\left(D^{2b}_{0,\mathcal{R}_{0,(k)}} mxs\right)\right]_{s=1} \end{aligned} \tag{72}$$

where $\mathcal{L}_{I_{\mathcal{R}_{0,(k)}}}(s)$ is the Laplace transformation of $I_{\mathcal{R}_{0,(k)}}$, which is given by

$$\mathcal{L}_{I_{\mathcal{R}_{0,(k)}}}(s) = \exp\left(-\lambda_{\rm ir}\frac{\gamma}{\cos\left(\frac{\pi}{2b}\right)}|s|^{\frac{1}{b}}\right). \tag{73}$$

The expectation over $D^2_{0,\mathcal{R}_{0,(k)}}$ provides the CDF of $Z_{0,\mathcal{R}_{0,(k)}}$ as given in (48).

Acknowledgment

The authors gratefully acknowledge G. J. Foschini and L. A. Shepp for insightful discussions, and R. Cohen, W. Dai, W. Suwansantisuk, and T. Wang for careful reading of the manuscript.

References

[1] D. Kahn, *The Codebreakers, The Story of Secret Writing*. New York, NY, USA: Macmillan, 1967.
[2] W. Diffie and M. E. Hellman, "New directions in cryptography," *IEEE Trans. Inf. Theory*, vol. IT-22, no. 6, pp. 644–652, Nov. 1976.
[3] M. Hellman, "An extension of the Shannon theory approach to cryptography," *IEEE Trans. Inf. Theory*, vol. IT-23, no. 3, pp. 289–294, May 1977.
[4] C. E. Shannon, "Communication theory of secrecy systems," *Bell Syst. Tech. J.*, vol. 28, no. 4, pp. 656–715, Oct. 1949.
[5] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, Oct. 1975.
[6] S. K. 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.
[7] H. Mahdavifar and A. Vardy, "Achieving the secrecy capacity of wiretap channels using polar codes," *IEEE Trans. Inf. Theory*, vol. 57, no. 10, pp. 6428–6443, Oct. 2011.
[8] M. Andersson, V. Rathi, R. Thobaben, J. Kliewer, and M. Skoglund, "Nested polar codes for wiretap and relay channels," *IEEE Commun. Lett.*, vol. 14, no. 8, pp. 752–754, Aug. 2010.
[9] O. O. Koyluoglu and H. El Gamal, "Polar coding for secure transmission and key agreement," in *Proc. IEEE Int. Symp. Pers., Indoor Mobile Radio Commun.*, Instanbul, Turkey, Sep. 2010, pp. 2698–2703.
[10] E. Hof and S. Shamai, "Secrecy-achieving polar-coding," in *Proc. IEEE Inf. Theory Workshop*, Dublin, Ireland, Sep. 2010, pp. 1–5.
[11] 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.
[12] 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.
[13] X. Zhou, M. R. McKay, B. Maham, and A. Hjorungnes, "Rethinking the secrecy outage formulation: A secure transmission design perspective," *IEEE Commun. Lett.*, vol. 15, no. 3, pp. 302–304, Mar. 2011.
[14] Y. Liang and H. V. Poor, "Multiple-access channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 54, no. 3, pp. 976–1002, Mar. 2008.
[15] R. Bassily and S. Ulukus, "Ergodic secret alignment," *IEEE Trans. Inf. Theory*, vol. 58, no. 3, pp. 1594–1611, Mar. 2012.
[16] 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.
[17] E. Ekrem and S. Ulukus, "Secrecy in cooperative relay broadcast channels," *IEEE Trans. Inf. Theory*, vol. 57, no. 1, pp. 137–155, Jan. 2011.
[18] E. Ekrem and S. Ulukus, "The secrecy capacity region of the Gaussian MIMO multi-receiver wiretap channel," *IEEE Trans. Inf. Theory*, vol. 57, no. 4, pp. 2083–2114, Apr. 2011.
[19] X. He, A. Khisti, and A. Yener, "MIMO broadcast channel with an unknown eavesdropper: Secrecy degrees of freedom," *IEEE Trans. Commun.*, 2014, to be published.
[20] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE Trans. Wireless Commun.*, vol. 7, no. 6, pp. 2180–2189, Jun. 2008.
[21] S. Goel and R. Negi, "Secret communication in presence of colluding eavesdroppers," in *Proc. Military Commun. Conf.*, Atlantic City, NJ, USA, Oct. 2005, pp. 1501–1506.
[22] 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, pp. 139–147, Feb. 2012.
[23] O. O. Koyluoglu, C. E. Koksal, and H. El Gamal, "On secrecy capacity scaling in wireless networks," *IEEE Trans. Inf. Theory*, vol. 58, no. 5, pp. 3000–3015, May 2012.
[24] A. O. Hero, "Secure space-time communication," *IEEE Trans. Inf. Theory*, vol. 49, no. 12, pp. 3235–3249, Dec. 2003.
[25] F. Oggier and B. Hassibi, "The secrecy capacity of the MIMO wiretap channel," in *Proc. IEEE Int. Symp. Inf. Theory*, Toronto, ON, Canada, Jul. 2008, pp. 524–528.
[26] S. Shafiee, N. Liu, and S. Ulukus, "Towards the secrecy capacity of the Gaussian MIMO wire-tap channel: The 2-2-1 channel," *IEEE Trans. Inf. Theory*, vol. 55, no. 9, pp. 4033–4039, Sep. 2009.
[27] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas I: The MISOME wiretap channel," *IEEE Trans. Inf. Theory*, vol. 56, no. 7, pp. 3088–3104, Jul. 2010.
[28] R. Bassily, E. Ekrem, X. He, E. Tekin, J. Xie, M. R. Bloch, S. Ulukus, and A. Yener, "Cooperative security at the physical layer: A summary of recent advances," *IEEE Signal Process. Mag.*, vol. 30, no. 5, pp. 16–28, Sep. 2013.

[28] We consider the SIR equal to zero for the case of $N_{\mathcal{R}_0} = 0$.

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

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

[31] R. Wilson, D. Tse, and R. A. Scholtz, "Channel identification: Secret sharing using reciprocity in ultrawideband channels," *IEEE Trans. Inf. Forensics Security*, vol. 2, no. 3, pp. 364–375, Sep. 2007.

[32] L. Lai, Y. Liang, and H. V. Poor, "A unified framework for key agreement over wireless fading channels," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 2, pp. 480–490, Apr. 2012.

[33] Y. Shen and M. Z. Win, "Intrinsic information of wideband channels," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 9, pp. 1875–1888, Sep. 2013.

[34] S. Anand and R. Chandramouli, "On the secrecy capacity of fading cognitive wireless networks," in *Proc. IEEE Int. Conf. Cogn. Radio Oriented Wireless Netw. Commun.*, Singapore, May 2008, pp. 1–5.

[35] M. Haenggi, "The secrecy graph and some of its properties," in *Proc. IEEE Int. Symp. Inf. Theory*, Toronto, ON, Canada, Jul. 2008, pp. 539–543.

[36] A. Sarkar and M. Haenggi, "Secrecy coverage," in *Proc. Asilomar Conf. Signals, Syst., Comput.*, Pacific Grove, CA, USA, Nov. 2010, pp. 42–46.

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

[38] P. C. Pinto, J. O. Barros, and M. Z. Win, "Secure communication in stochastic wireless networks—Part I: Connectivity," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 1, pp. 125–138, Feb. 2012.

[39] J. Lee, A. Conti, A. Rabbachin, and M. Z. Win, "Distributed network secrecy," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 9, pp. 1889–1900, Sep. 2013.

[40] J. F. Kingman, *Poisson Processes*. Oxford, U.K.: Oxford Univ. Press, 1993.

[41] M. Z. Win, "A mathematical model for network interference," presented at the IEEE Commun. Theory Workshop, Sedona, AZ, USA, May 2007.

[42] M. Z. Win, P. C. Pinto, and L. A. Shepp, "A mathematical theory of network interference and its applications," *Proc. IEEE*, vol. 97, no. 2, pp. 205–230, Feb. 2009.

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

[44] J. Orriss and S. K. Barton, "Probability distributions for the number of radio transceivers which can communicate with one another," *IEEE Trans. Commun.*, vol. 51, no. 4, pp. 676–681, Apr. 2003.

[45] E. Salbaroli and A. Zanella, "Interference analysis in a Poisson field of nodes of finite area," *IEEE Trans. Veh. Technol.*, vol. 58, no. 4, pp. 1776–1783, May 2009.

[46] J. G. Andrews, S. Weber, M. Kountouris, and M. Haenggi, "Random access transport capacity," *IEEE Trans. Wireless Commun.*, vol. 9, no. 6, pp. 2101–2111, Jun. 2010.

[47] A. Rabbachin, T. Q. Quek, H. Shin, and M. Z. Win, "Cognitive network interference," *IEEE J. Sel. Areas Commun.*, vol. 29, no. 2, pp. 480–493, Feb. 2011.

[48] E. S. Sousa, "Performance of a spread spectrum packet radio network link in a Poisson field of interferers," *IEEE Trans. Inf. Theory*, vol. 38, no. 6, pp. 1743–1754, Nov. 1992.

[49] A. Ghasemi and E. S. Sousa, "Interference aggregation in spectrum-sensing cognitive wireless networks," *IEEE J. Sel. Topics Signal Process.*, vol. 2, no. 1, pp. 41–56, Feb. 2008.

[50] P. C. Pinto and M. Z. Win, "Communication in a Poisson field of interferers—Part I: Interference distribution and error probability," *IEEE Trans. Wireless Commun.*, vol. 9, no. 7, pp. 2176–2186, Jul. 2010.

[51] J. Ilow, D. Hatzinakos, and A. N. Venetsanopoulos, "Performance of FH SS radio networks with interference modeled as a mixture of Gaussian and alpha-stable noise," *IEEE Trans. Commun.*, vol. 46, no. 4, pp. 509–520, Apr. 1998.

[52] X. Yang and A. P. Petropulu, "Co-channel interference modeling and analysis in a Poisson field of interferers in wireless communications," *IEEE Trans. Signal Process.*, vol. 51, no. 1, pp. 64–76, Jan. 2003.

[53] S. Govindasamy, D. W. Bliss, and D. H. Staelin, "Spectral efficiency in single-hop ad-hoc wireless networks with interference using adaptive antenna arrays," *IEEE J. Sel. Areas Commun.*, vol. 25, no. 7, pp. 1358–1369, Sep. 2007.

[54] D. Dardari, A. Conti, C. Buratti, and R. Verdone, "Mathematical evaluation of environmental monitoring estimation error through energy-efficient wireless sensor networks," *IEEE Trans. Mobile Comput.*, vol. 6, no. 7, pp. 790–802, Jul. 2007.

[55] A. Rabbachin, T. Q. Quek, P. C. Pinto, I. Oppermann, and M. Z. Win, "Non-coherent UWB communication in the presence of multiple narrowband interferers," *IEEE Trans. Wireless Commun.*, vol. 9, no. 11, pp. 3365–3379, Nov. 2010.

[56] J. Lee, J. G. Andrews, and D. Hong, "Spectrum-sharing transmission capacity," *IEEE Trans. Wireless Commun.*, vol. 10, no. 9, pp. 3053–3063, Sep. 2011.

[57] J. Reich, V. Misra, D. Rubensteinand, and G. Zussman, "Connectivity maintenance in mobile wireless networks via constrained mobility," in *Proc. IEEE Conf. Comput. Commun.*, Shanghai, China, Apr. 2011, pp. 927–935.

[58] A. Conti, B. M. Masini, F. Zabini, and O. Andrisano, "On the downlink performance of multi-carrier CDMA systems with partial equalization," *IEEE Trans. Wireless Commun.*, vol. 6, no. 1, pp. 230–239, Jan. 2007.

[59] N. C. Beaulieu and D. J. Young, "Designing time-hopping ultrawide bandwidth receivers for multiuser interference environments," *Proc. IEEE*, vol. 97, no. 2, pp. 255–284, Feb. 2009.

[60] M. Chiani and A. Giorgetti, "Coexistence between UWB and narrowband wireless communication systems," *Proc. IEEE*, vol. 97, no. 2, pp. 231–254, Feb. 2009.

[61] A. Rabbachin, A. Conti, and M. Z. Win, "The role of aggregate interference on intrinsic network secrecy," in *Proc. IEEE Int. Conf. Commun.*, Ottawa, ON, Canada, Jun. 2012, pp. 3548–3553.

[62] J. Lee, H. Shin, and M. Z. Win, "Secure node packing of large-scale wireless networks," in *Proc. IEEE Int. Conf. Commun.*, Ottawa, ON, Canada, Jun. 2012, pp. 815–819.

[63] M. Z. Win, A. Rabbachin, J. Lee, and A. Conti, "Cognitive network secrecy with interference engineering," *IEEE Netw.*, 2014, to be published.

[64] G. J. Foschini, Private Conversation AT&T Labs-Research, May 2007.

[65] P. C. Pinto and M. Z. Win, "Communication in a Poisson field of interferers—Part II: Channel capacity and interference spectrum," *IEEE Trans. Wireless Commun.*, vol. 9, no. 7, pp. 2187–2195, Jul. 2010.

[66] A. Giorgetti and M. Chiani, "Influence of fading on the Gaussian approximation for BPSK and QPSK with asynchronous cochannel interference," *IEEE Trans. Wireless Commun.*, vol. 4, no. 2, pp. 384–389, 2005.

[67] M. Chiani, A. Conti, and O. Andrisano, "Outage evaluation for slow frequency-hopping mobile radio systems," *IEEE Trans. Commun.*, vol. 47, no. 12, pp. 1865–1874, Dec. 1999.

[68] G. Samoradnitsky and M. Taqqu, *Stable Non-Gaussian Random Processes*. London, U.K.: Chapman & Hall, 1994.

[69] F. Baccelli and B. Błaszczyszyn, *Stochastic Geometry and Wireless Networks*, ser. Foundations and Trends in Networking. Boston, MA, USA: NOW, 2009, vol. 1, Theory.

[70] A. Conti, M. Z. Win, M. Chiani, and J. H. Winters, "Bit error outage for diversity reception in shadowing environment," *IEEE Commun. Lett.*, vol. 7, no. 1, pp. 15–17, Jan. 2003.

[71] A. Conti, M. Z. Win, and M. Chiani, "On the inverse symbol error probability for diversity reception," *IEEE Trans. Commun.*, vol. 51, no. 5, pp. 753–756, May 2003.

[72] M. Z. Win, N. C. Beaulieu, L. A. Shepp, B. F. Logan, and J. H. Winters, "On the SNR penalty of MPSK with hybrid selection/maximal ratio combining over IID Rayleigh fading channels," *IEEE Trans. Commun.*, vol. 51, no. 6, pp. 1012–1023, Jun. 2003.

[73] P. Mary, M. Dohler, J.-M. Gorce, G. Villemaud, and M. Arndt, "BPSK bit error outage over Nakagami-m fading channels in lognormal shadowing environments," *IEEE Commun. Lett.*, vol. 11, no. 7, pp. 565–567, Jul. 2007.

[74] A. Conti, W. M. Gifford, M. Z. Win, and M. Chiani, "Optimized simple bounds for diversity systems," *IEEE Trans. Commun.*, vol. 57, no. 9, pp. 2674–2685, Sep. 2009.

[75] W. M. Gifford, A. Conti, M. Chiani, and M. Z. Win, "On the SNR penalties of ideal and non-ideal subset diversity systems," *IEEE Trans. Inf. Theory*, vol. 58, no. 6, pp. 3708–3724, Jun. 2012.

[76] J. Gil-Pelaez, "Note on the inversion theorem," *Biometrika*, vol. 38, no. 3/4, pp. 481–482, Dec. 1951.

[77] M. Z. Win, A. Conti, S. Mazuelas, Y. Shen, W. M. Gifford, D. Dardari, and M. Chiani, "Network localization and navigation via cooperation," *IEEE Commun. Mag.*, vol. 49, no. 5, pp. 56–62, May 2011.

[78] S. Gezici, Z. Tian, G. B. Giannakis, H. Kobayashi, A. F. Molisch, H. V. Poor, and Z. Sahinoglu, "Localization via ultra-wideband radios: A look at positioning aspects for future sensor networks," *IEEE Signal Process. Mag.*, vol. 22, no. 4, pp. 70–84, Jul. 2005.
[79] Y. Shen and M. Z. Win, "Fundamental limits of wideband localization—Part I: A general framework," *IEEE Trans. Inf. Theory*, vol. 56, no. 10, pp. 4956–4980, Oct. 2010.
[80] N. Patwari, J. N. Ash, S. Kyperountas, A. O. Hero, R. L. Moses, and N. S. Correal, "Locating the nodes: Cooperative localization in wireless sensor networks," *IEEE Signal Process. Mag.*, vol. 22, no. 4, pp. 54–69, Jul. 2005.
[81] D. Dardari, A. Conti, U. J. Ferner, A. Giorgetti, and M. Z. Win, "Ranging with ultrawide bandwidth signals in multipath environments," *Proc. IEEE*, vol. 97, no. 2, pp. 404–426, Feb. 2009.
[82] U. A. Khan, S. Kar, and J. M. F. Moura, "Distributed sensor localization in random environments using minimal number of anchor nodes," *IEEE Trans. Signal Process.*, vol. 57, no. 5, pp. 2000–2016, May 2009.
[83] U. A. Khan, S. Kar, and J. M. F. Moura, "DILAND: An algorithm for distributed sensor localization with noisy distance measurements," *IEEE Trans. Signal Process.*, vol. 58, no. 3, pp. 1940–1947, Mar. 2010.
[84] A. Conti, M. Guerra, D. Dardari, N. Decarli, and M. Z. Win, "Network experimentation for cooperative localization," *IEEE J. Sel. Areas Commun.*, vol. 30, no. 2, pp. 467–475, Feb. 2012.
[85] H. R. Thompson, "Distribution of distance to n-th neighbour in a population of randomly distributed individuals," *Ecology*, vol. 37, no. 2, pp. 391–394, Apr. 1956.
[86] S. Srinivasa and M. Haenggi, "Distance distributions in finite uniformly random networks: Theory and applications," *IEEE Trans. Veh. Technol.*, vol. 59, no. 2, pp. 940–949, Feb. 2010.
[87] D. P. Bertsekas and R. G. Gallager, *Data Networks*, 2nd ed. Englewood Cliffs, NJ, USA: Prentice-Hall, 1992.

Alberto Rabbachin (S'03–M'07) received the M.S. degree in telecommunications engineering from the University of Bologna, Bologna, Italy, in 2001, and the Ph.D. degree in electrical engineering from the University of Oulu, Oulu, Finland, in 2008.

He was a Postdoctoral Fellow with the Massachusetts Institute of Technology, Cambridge, MA, USA. He is now a Project Officer with the European Commission. His research interests involve communication theory and stochastic geometry applied to real problems in wireless networks including network secrecy, cognitive radio, ultrawideband transceiver design, network synchronization, ranging techniques, and interference exploitation.

Dr. Rabbachin serves as an Editor for the IEEE COMMUNICATIONS LETTERS and in the organization of numerous international conferences. He received the International Outgoing Marie Curie Fellowship, the Nokia Fellowship, the European Commission JRC Best Young Scientist Award, and the IEEE Communications Society's William R. Bennett Prize in the Field of Communications Networking.

Andrea Conti (S'99–M'01–SM'11) received the Laurea degree (*summa cum laude*) in telecommunications engineering and Ph.D. degree in electronic engineering and computer science from the University of Bologna, Bologna, Italy, in 1997 and 2001, respectively.

He is a Professore Aggregato with the University of Ferrara, Ferrara, Italy. He also holds Research Affiliate appointments with the IEIIT; Consiglio Nazionale delle Ricerche, Turin, Italy; and the LIDS, Massachusetts Institute of Technology, Cambridge, MA, USA. His research interests involve theory and experimentation of wireless systems and networks including network localization, adaptive diversity communications, cooperative relaying techniques, and network secrecy.

Dr. Conti is serving as an Editor for the IEEE WIRELESS COMMUNICATIONS LETTERS and served as an Associate Editor for the IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS and as an Editor for the IEEE COMMUNICATIONS LETTERS. He is elected Chair of the IEEE Communications Society's Radio Communications Technical Committee and is an IEEE Distinguished Lecturer. He is a recipient of the HTE Puskás Tivadar Medal and is co-recipient of the IEEE Communications Society's Fred W. Ellersick Prize and of the IEEE Communications Society's Stephen O. Rice Prize in the Field of Communications Theory.

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

He is a Professor with the Massachusetts Institute of Technology (MIT), Cambridge, MA, USA, and the founding Director of the Wireless Communication and Network Sciences Laboratory. Prior to joining MIT, he was with AT&T Research Laboratories, Middletown, NJ, USA, and with the Jet Propulsion Laboratory, Pasadena, CA, USA. His research encompasses developing fundamental theories, designing algorithms, and conducting experimentation for a broad range of real-world problems.

Dr. Win is a Fellow of the AAAS. He is an elected Member-at-Large on the IEEE Communications Society Board of Governors. He served as Editor for various IEEE journals and chaired a number of international conferences. He received the International Prize for Communications Cristoforo Colombo, the Copernicus Fellowship, the Fulbright Fellowship, and the Laurea Honoris Causa from the University of Ferrara, Ferrara, Italy. Together with students and colleagues, his papers have received several awards including the IEEE Communications Society's Stephen O. Rice Prize, the IEEE Aerospace and Electronic Systems Society's M. Barry Carlton Award, and the IEEE Antennas and Propagation Society's Sergei A. Schelkunoff Transactions Prize. He was honored with the IEEE Kiyo Tomiyasu Award and the IEEE Eric E. Sumner Award.