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.

I. INTRODUCTION

I NFORMATION 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]. 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. 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: rabbachin@ieee.org).

A. Conti was 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: mowie@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

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 \( \Pi_t \) with spatial density \( \lambda_t \). \( \Pi_t \) is composed of point processes \( \Pi_{tx} \) and \( \Pi_{rx} \) with spatial densities \( \lambda_{tx} \) and \( \lambda_{rx} \) corresponding to the legitimate transmitters and the legitimate receivers, respectively. Thus, 

\[
\lambda_t = \lambda_{tx} + \lambda_{rx} \tag{1}
\]

is defined such that \( \lambda_{tx} = \alpha \lambda_t \) and \( \lambda_{rx} = (1 - \alpha) \lambda_t \) with \( \alpha \in (0, 1) \).

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 \( \Pi_e \) with spatial density \( \lambda_e \).

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. \( \lambda_{ix} = \lambda_{tx} + \lambda_{ir} \) represents the total spatial density of nodes interfering the legitimate network and the eavesdropping network, respectively. The network of intentional interferers is described by the point process \( \Pi_{ix} \) with spatial density \( \lambda_{ix} \).

The quantities \( \lambda_{ir} = \lambda_{rx} \) and \( \lambda_{ir} = \lambda_{tx} + \lambda_{ir} \) 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 \( \Pi_{tx}, \Pi_{rx}, \Pi_{ix}, \) and \( \Pi_{ix} \), respectively. Let \( \mathcal{F} \) and \( \mathcal{I} \) denote the index sets of legitimate transmitters and of intentional interferers, respectively. Consider a bounded set \( \mathcal{A} \subset \mathbb{R}^n \). For the \( j \)-th legitimate transmitter in \( \mathcal{A} \),

\( \mathcal{R}_j \) denotes the index set of potential legitimate receivers for the \( j \)-th transmitter, and

\( \mathcal{I}_j \) hereafter, the \( j \)-th 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 $j$th transmitter.

Note, the probability that there are no transmitters in $\mathcal{A}$ is $e^{-\lambda_{\text{vol}} |\mathcal{A}|}$ 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 $R_{j,k} \in \mathcal{R}_j$ (i.e., the $k$th potential legitimate receiver among those of the $j$th transmitter), and an eavesdropper with index $\mathcal{E}_{j,i} \in \mathcal{E}_j$ (i.e., the $i$th eavesdropper among those of the $j$th 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 $j$th transmitter is given by

$$ Y_{u,v}^{(C)} = \sqrt{P_T} \frac{H_{u,v}}{D_{u,v}^\rho} S_u + W_v $$

where, for the $j$th legitimate transmitter

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

with $\ell$ or $v$ denoting the legitimate link or eavesdropping link, respectively. In (2), $P_T$ is the signal power at the reference distance $d_0$ from the transmitter; $H_{u,v} \in \mathcal{C}$ is the quasi-static channel gain; $D_{u,v} = \|X_u - X_v\|/d_0$ is the normalized Euclidian distance between the transmitter and the receiver at the random positions $X_u$ and $X_v$, respectively; $S_u$ is a transmitted symbol; $\rho$ is the amplitude path-loss exponent; and $W_v$ is the disturbance composed of the network interference and the receiver noise. Specifically

$$ W_v = \sqrt{P_T} \sum_{q \in \mathcal{I}_v} \frac{H_{q,v}}{D_{q,v}^\rho} S_q + W_v $$

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

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

with the resulting disturbance conditioned on the PPP $\Phi_{ij}$ is complex Gaussian

$$ W_v \overset{\mathcal{D}}{\sim} N_c(0, \mathsf{V}(S) P_L + \sigma_v^2) $$

where $\mathsf{V}(S)$ is the variance of a transmitted complex symbol $S$ and $P_L$ is the normalized network interference power given by

$$ P_L = \sum_{q \in \mathcal{I}_v} \frac{|H_{q,v}|^2}{D_{q,v}^{2\rho}} $$

Note that since $P_L$, in (7) depends on $\Phi_{ij}$, it can be seen as a random variable taking different values for each realization of the $\Phi_{ij}$. In particular, for nodes in $\mathcal{R}^2$, the random variable (RV) $P_L$ follows a Stable distribution [41], [42], [48].

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.

1) Absence of Network Interference: Conditioned on $\frac{\psi_{u,v}^{(a)}}{\psi_{u,v}^{(c)}}$ and $\frac{\psi_{u,v}^{(a)}}{\psi_{u,v}^{(c)}}$, with $\psi_{u,v}^{(c)} \in \mathbb{C}$, $\mathcal{D}_{u,v} = \{H_{u,v}, D_{u,v}\}$, the wireless-tap channel reduces to the Gaussian wire-tap channel. Specifically, the conditional MSR in the absence of interference is given by

$$ R_{u,v} = \langle C \left( \frac{\psi_{u,v}^{(a)}}{\psi_{u,v}^{(c)}} \right) - C \left( \frac{\psi_{u,v}^{(a)}}{\psi_{u,v}^{(c)}} \right) \rangle $$

The term

$$ C \left( \frac{\psi_{u,v}^{(a)}}{\psi_{u,v}^{(c)}} \right) = c(\mathcal{Z}_{u,v}) $$

is the conditional capacity of the legitimate link $\square = j$ or eavesdropping link $\square = e$ in the absence of network interference with

$$ \mathcal{Z}_{u,v} = \frac{|H_{u,v}|^2 P_L}{D_{u,v}^{2\rho} + \sigma_v^2} $$

8In a space with more than two dimensions, the RV still follows a skewed stable distribution with different parameters [68].

9Hereafter, consider a network scenario composed of multiple legitimate and eavesdropping links with receivers that treat interference as noise.

10For notational convenience, define $c(x) = \log_2 (1 + x)$ bits/s/Hz.
2) Presence of Network Interference: Conditioned on $\Psi_u^{(e)}$, and $\Psi_u^{(c)}$, with $\Psi_u^{(c)} = \{H_{u,v}, D_{u,v}, l_c\}$, the MSR in the presence of interference is given by

$$R_{u,v^c,c} = C\left(\Psi_u^{(e)}\right) - C\left(\Psi_u^{(c)}\right) + .$$  

(13)

The term

$$C\left(\Psi_u^{(c)}\right) = c(Z_{u,v})$$

is the conditional capacity of the legitimate link or eavesdropping link in the presence of network interference, where

$$Z_{u,v} = \frac{H_{u,v}}{D_{u,v} (P_T l_k + \sigma^2)}.$$

(15)

The MSR of the legitimate link from the $i$th transmitter to the $k$th receiver, conditioned on $\Psi_i^{(e)}$, is determined by the minimum MSR over all possible eavesdroppers in the network attempting to intercept the confidential information as

$$R_{i,j,k}^{(e)}, R_{i,j,k}^{(c)} = [c(Z_{j,i,k}) - c(\eta_{j,i,k})].$$

(16)

where $\eta_{j,i,k} = Z_{j,i,k}$, and $i = \arg\max_{j \in \mathcal{E}_{i}} Z_{j,i,k}$.

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

$$R_{\text{sec}}(\Omega_A) = \sum_{i \in \mathcal{T}} I_A(X_i) \{ R_{i,j,k} \}.$$

(17)

where $\Omega_A = \Omega_i^{(e)} \cup \Omega_i^{(c)}$ with

$$\Omega_i^{(e)} = \{ \Psi_i^{(e)} : X_j \in \mathcal{A}, \mathcal{R}_{j,k} \in \mathcal{R}_i \}$$

(18a)

$$\Omega_i^{(c)} = \{ \Psi_i^{(c)} : X_j \in \mathcal{A}, \mathcal{E}_{j,k} \in \mathcal{E}_i \}.$$

(18b)

In (17), $I_A(X_j)$ accounts for the legitimate transmitters in $\mathcal{A}$ according to

$$I_A(X_j) = \begin{cases} 1 & \text{if } X_j \in \mathcal{A} \\ 0 & \text{otherwise} \end{cases}$$

and $\mathcal{R}_{j,k} = \{ \mathcal{R}_{j} \}$ is the index of the selected receiver for the $j$th transmitter. The network secrecy rate density is defined as the limit over $\Omega_A$ and can be expressed as

$$\rho_{\text{sec}} = \lim_{t \to \infty} R_{\text{sec}}(\Omega_A).$$

(19)

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

$$\rho_{\text{sec}} = \lambda_{\text{sec}} R.$$

(20)

where $R = \mathbb{E}_0\{R_{0,\mathcal{R}_i^{(e)}, \mathcal{E}_{i,k}}\}$ is the average MSR of a typical link in the network [69] and over the channel gains. When $l_{R_{i,k}}$ and $l_{E_{i,k}}$ are statistically independent, the average MSR can be written as

$$R = \mathbb{E}_{\mathcal{R}_{i,k}} \mathbb{E}_{\mathcal{E}_{i,k}} \left\{ \mathbb{E}_{\eta_{0,i,k}} \left[ \left[ c(Z_{0,i,k}), c(\eta_{0,i,k}) \right] \right] \right\}$$

$$- \int_0^\infty c(y) f_{\eta_{0,i,k}}(y) f_{Z_{0,i,k}, \mathcal{R}_{i,k}}(y) dy$$

$$- \int_0^\infty \int_0^\infty c(z) f_{\eta_{0,i,k}}(z) f_{Z_{0,i,k}, \mathcal{R}_{i,k}}(y) dy dz.$$

(21)

Remark: The PDF of $Z_{0,i,k}$, 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 $R^*$ and for transmitters in $\mathcal{A}$, the number of legitimate links in outage is

$$K_{\text{out}}(\Omega_A, R^*) = \sum_{j \in \mathcal{T}} I_A(X_j) I_{[0,R^*]} \left( R_{j,k} \right).$$

(22)

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

$$\kappa_{\text{out}}(R^*) = \lim_{t \to \infty} K_{\text{out}}(\Omega_A, R^*)$$

(23)

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

$$\kappa_{\text{out}}(R^*) = \lambda_{\text{sec}} P_{\text{out}}(R^*)$$

(24)

where $P_{\text{out}}(R^*)$ is the probability that a legitimate link is in outage given by

$$P_{\text{out}}(R^*) = \left[ \mathbb{P}_{\mathcal{R}_{i,k}} \left( \mathbb{P}_{\mathcal{E}_{i,k}} \left( \int_{y=0}^{1+R^*} f_{\eta_{0,i,k}}(y) \mathbb{I}_{\left[ R^*, t \right]}(y) dy \right) \right) \right].$$

(25)

Remark: To achieve the MSR, the transmitter has to know the signal-to-interference-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

$13$Conditioned on $\Psi_u^{(e)}$, the instantaneous amplitude of the aggregate interference is Gaussian distributed [64]–[67], and the capacity of the legitimate and eavesdropping links is expressed using $c(.)$.

$14$The expectation $\mathbb{E}_r$ 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 $j = r$.}
secrecy throughput is introduced to characterize the confidential information flowing through the legitimate network.

D. Probability to Transmit Information With Secrecy

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

$$P_{se} = P\{c(\eta_j, \varepsilon) > R_j^{(\ell)} - R_s|\mathcal{M}_2\}$$

where $R_j^{(\ell)}$ is the transmission rate of a legitimate link associated with the $j$th transmitter, $R_s$ is the desired rate of confidential information, and $\mathcal{M}_2$ indicates the event that a confidential information message is transmitted. 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 $j$th legitimate transmitter sends a no-information message when $\mathcal{Z}_{j,\mathcal{R}}$ for a selected receiver is below a minimum required value $\mu$; otherwise, a confidential information message is transmitted. Therefore, the probability of confidential message transmission is

$$P_{t}(\mu) = P\{\mathcal{M}_2\} = P\{\mathcal{Z}_{j,\mathcal{R}} > \mu\}.$$  

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

$$P_{so}(\mu) = P\{c(\eta_j, \varepsilon) > c(\mathcal{Z}_{j,\mathcal{R}}) - R_s\mathcal{Z}_{j,\mathcal{R}} > \mu\}$$

$$= \frac{1}{1 - F_{\mathcal{Z}_{j,\mathcal{R}}}^{(\mathcal{Z}_{j,\mathcal{R}})}(\mu)} \int \left[ F_{\mathcal{Z}_{j,\mathcal{R}}}^{(\mathcal{Z}_{j,\mathcal{R}})}(\mu + \frac{1}{2R_s} - 1) - F_{\mathcal{Z}_{j,\mathcal{R}}}^{(\mathcal{Z}_{j,\mathcal{R}})}(\mu) \right] dy.$$  

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

$$\mu^* = \arg\max_{\mu \in \mathcal{M}} P_{t}(\mu)$$

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

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.

11The transmission of a confidential message can be based on the SINR at the intended receiver.

E. Network Secrecy Throughput Density

For a given $R_s$ and $P_{so}^{*}$, the secrecy throughput of the legitimate link associated with the $j$th transmitter, conditioned on $\mathcal{Z}_{j,\mathcal{R}}$, is given by

$$T_j,\mathcal{R}_{j,\mathcal{R}} = R_s1_{\mu^*,\infty\mathcal{Z}_{j,\mathcal{R}}}.$$  

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

$$T_{us}^{(\mathcal{A})} = \sum_{j \in \mathcal{A}} 1_{A}(\mathcal{X}_j)T_j,\mathcal{R}_{j,\mathcal{R}}.$$  

Then, the network secrecy throughput density is given by

$$\tau_{us} = \lim_{\alpha \to +\infty} \frac{T_{us}^{(\mathcal{A})}}{|\mathcal{A}|} = \lambda \mathcal{A}T.$$  

For a given $R_s$ and $P_{so}^{*}$, the secrecy throughput of the legitimate link associated with the $j$th transmitter, conditioned on $\mathcal{Z}_{j,\mathcal{R}}$, is given by

$$T_j,\mathcal{R}_{j,\mathcal{R}} = R_s1_{\mu^*,\infty\mathcal{Z}_{j,\mathcal{R}}}.$$  

Then, the network secrecy throughput density is given by

$$\tau_{us} = \lim_{\alpha \to +\infty} \frac{T_{us}^{(\mathcal{A})}}{|\mathcal{A}|} = \lambda \mathcal{A}T.$$  

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 $k$th closest receiver, or 2) the receiver with the maximum SIR. We consider interference limited conditions and characterize the SIRs at the $j$th legitimate receiver and at the $k$th eavesdropper, which are respectively given by

$$Z_{0,\mathcal{R}_{0,k}} \sim \frac{|H_{0,\mathcal{R}_{0,k}}|^2}{D_{0,\mathcal{R}_{0,k}}^2 |R_{0,k}|}$$

and

$$Z_{0,\mathcal{R}_{0,k}} \sim \frac{|H_{0,\mathcal{R}_{0,k}}|^2}{D_{0,\mathcal{R}_{0,k}}^2 |\mathcal{R}_{0,k}|}.$$  

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) $k$th 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 $k$th closest receiver.

18Note that the network secrecy throughput density in (33) has a double dependency on both $\lambda_{\mathcal{A}}$ and $\mathcal{R}$, since $P_{t}(\mu)$ also depends on the density of transmitters and the secrecy rate.
transmitter, consider the ordered index set of legitimate receivers \( \{R_{o}(k)\} \) where the ordering is based on distances, i.e., \( D_{0,R_{o}(k)} \leq D_{0,R_{o}(k+1)} \) \( \forall k \). The CDF \( F_{z_{o},R_{o}(k)}(x) \) is given by

\[
F_{z_{o},R_{o}(k)}(x) = F \left\{ \frac{H_{0,R_{o}(k)}}{D_{0,R_{o}(k)}^{2}} \leq x \right\}
\]

(37)

where \( G_{0,R_{o}(k)} = \frac{H_{0,R_{o}(k)}}{D_{0,R_{o}(k)}^{2}} - x D_{0,R_{o}(k)} h_{R_{o}(k)} \). Using the inversion theorem [76]

\[
F_{z_{o},R_{o}(k)}(x) = g_{G_{0,R_{o}(k)}}(x) \]

(39)

where

\[
g_{G}(x) = \frac{1}{\pi} \int_{0}^{\infty} \Re \left\{ \frac{\psi_{G}(j\omega)}{j\omega} \right\} d\omega
\]

(40)

and \( \psi_{G}(\cdot) \) is the characteristic function CF of the RV \( G \). In Appendix B, the CF \( \psi_{G_{0},R_{o}(k)}(j\omega) \) is derived as

\[
\psi_{G_{0},R_{o}(k)}(j\omega) = \psi_{M}(j\omega) \left( 1 + \frac{\lambda_{ir}}{\lambda_{tx}} \right) \left( 1 + \frac{j\omega}{\lambda_{tx}} \tan \left( \frac{\pi}{2}\right) \right)^{-k}
\]

(41)

Equation (39), together with (40) and (41), gives the CDF of \( Z_{0,R_{o}(k)} \).

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

2) Maximum SIR Legitimate Receiver: Consider all legitimate receivers, with index set \( R_{o} \), in a bounded set \( A_{R} \). The CDF of \( \eta_{o,R_{o}} \) can be obtained following similar derivation as in Section IV-A.2 as

\[
F_{\eta_{o},R_{o}}(x) = e \left\{ F_{z_{o},R_{o}(k)}(x) - x \right\}
\]

(46)

where

\[
F_{z_{o},R_{o}(k)}(x) = g_{G_{0},R_{o}(k)}(x)
\]

(43)

with \( g_{G}(\cdot) \) defined in (40). The CF \( \psi_{G_{0},R_{o}(k)}(j\omega) \) is given by (68) and (69), except that \( D_{0,R_{o}(k)} \) is replaced by \( D_{0,R_{o}(k)}^{2} \).

For a two-dimensional circular region \( A_{R} \) centered at the legitimate transmitter with radius \( d_{A_{R}} \), the squared distances \( D_{0,R_{o}}^{2} \) for various \( k \)'s are independent and identically distributed (i.i.d.) with uniform distribution in \( [0,d_{A_{R}}^{2}] \). Therefore, the CF of \( G_{0,R_{o}(k)} \) becomes

\[
\psi_{G_{0},R_{o}(k)}(j\omega) = \psi_{H_{0},R_{o}(k)}(j\omega) e^{-\lambda_{ir}x + \frac{\lambda_{tx}}{j\omega} \tan \left( \frac{\pi}{2}\right)} D_{0,R_{o}}^{2} - 1
\]

(44)

B. SIR in the Eavesdropping Network

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

\[
F_{\eta_{e},E_{e}}(x) = e \left\{ F_{z_{e},E_{e}(k)}(x) - x \right\}
\]

(45)

Using the fact that \( F_{z_{e},E_{e}(k)}(x) \) is a Stable RV according to (8), we obtain the CF \( \psi_{G_{e},E_{e}(k)}(j\omega) \) 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 \( A_{E} \) centered at the legitimate transmitter with radius \( d_{A_{E}} \), the CDF \( F_{z_{e},E_{e}(k)}(x) \) is given by (43)–(45), except: \( R_{o,k} \) is replaced by \( E_{e,k} \) in (43), and \( R_{0,k} \), \( \lambda_{ir} \), and \( d_{M} \) are replaced by \( \lambda_{e,k} \), \( \lambda_{tx} \), and \( d_{M} \) 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.

A. SIRS in the Legitimate Network

1) \( k \)th 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

\[
F_{z_{o},R_{o}(k)}(x) = E_{\eta_{o},R_{o}(k)} \left\{ F_{z_{o},R_{o}(k)}(x) \right\}
\]

(46)

where

\[
F_{z_{o},R_{o}(k)}(x) = g_{G_{0},R_{o}(k)}(x)
\]

(43)

with \( g_{G}(\cdot) \) defined in (40). The CF \( \psi_{G_{0},R_{o}(k)}(j\omega) \) is given by (68) and (69), except that \( D_{0,R_{o}(k)} \) is replaced by \( D_{0,R_{o}(k)}^{2} \).

For a two-dimensional circular region \( A_{R} \) centered at the legitimate transmitter with radius \( d_{A_{R}} \), the CDF of \( \eta_{o,R_{o}(k)} \) can be expressed as (see derivation in Appendix C)

\[
F_{\eta_{o},R_{o}(k)}(x) = e \left\{ F_{z_{o},R_{o}(k)}(x) - x \right\}
\]

(46)

where

\[
F_{z_{o},R_{o}(k)}(x) = g_{G_{0},R_{o}(k)}(x)
\]

(43)

with \( g_{G}(\cdot) \) defined in (40). The CF \( \psi_{G_{0},R_{o}(k)}(j\omega) \) is given by (68) and (69), except that \( D_{0,R_{o}(k)} \) is replaced by \( D_{0,R_{o}(k)}^{2} \).

For a two-dimensional circular region \( A_{R} \) centered at the legitimate transmitter with radius \( d_{A_{R}} \), the SIR becomes

\[
\psi_{G_{0},R_{o}(k)}(j\omega) = \psi_{H_{0},R_{o}(k)}(j\omega) e^{-\lambda_{ir}x + \frac{\lambda_{tx}}{j\omega} \tan \left( \frac{\pi}{2}\right)} D_{0,R_{o}}^{2} - 1
\]

(44)

Note that the right side of (39) is written explicitly as a function of \( x \) to emphasize the dependence of \( G_{0,R_{o}(k)} \) on \( x \).

Note that the notation \( \Re \{ \cdot \} \) indicates the real part of its argument, \( j = \sqrt{-1} \), and \( \psi_{G}(\cdot) \Delta \{ \Re \{ \cdot \} \} \).

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.

22Integer values for fading severity \( m \) are considered.
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 \( F_{Z_{\theta,\tau_{y},k}}(x) \). The CDF of \( Z_{0,\tau_{y},k} \) can be written as

\[
F_{Z_{0,\tau_{y},k}}(x) = \mathbb{E}_{Z_{0,\tau_{y},k}} \left\{ F_{Z_{0,\tau_{y},k}}(x) \right\}
\]

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

\[
F_{Z_{0,\tau_{y},k}}(x) = 1 - \sum_{i=0}^{m-1} \frac{(-1)^i x^i}{i!} \int_{\gamma}^{\infty} d\gamma \left( \frac{\gamma}{\pi} \right)^{\frac{m}{2}} \left( d_{\text{Mr}}^2 - d_{\text{Mr}}^2 \right) \]

for \( x > 0 \), and 0 otherwise, where

\[
\Xi(\gamma, x, s, d_{\text{Mr}}, d_{\text{Me}}) \Delta \frac{\lambda_{\text{Mr}} e^{-\frac{\gamma}{\gamma}} \lambda_{\text{Mr}}^2}{\lambda_{\text{Me}}^2} e^{-\frac{\gamma}{\gamma}} \lambda_{\text{Me}}^2.
\]

Substituting (51) into (42), the CDF for the maximum SIR \( F_{\eta_{0,\tau_{y},k}}(x) \) is obtained. To complete the derivation, we take the limit as \( d_{\text{Mr}} \to \infty \), resulting in

\[
F_{\eta_{0,\tau_{y},k}}(x) = \exp \left( - \sum_{i=0}^{m-1} \frac{(-1)^i x^i}{i!} \right) \left( \frac{\pi}{\gamma} \right)^{\frac{m}{2}} \left( d_{\text{Mr}}^2 - d_{\text{Mr}}^2 \right) \]

for \( x > 0 \) and 0 otherwise. Letting \( d_{\text{Me}} \to \infty \), the CDF of the maximum SIR becomes

\[
F_{\eta_{0,\tau_{y},k}}(x) = \exp \left( - \sum_{i=0}^{m-1} \frac{(-1)^i x^i}{i!} \right) \left( \frac{\pi}{\gamma} \right)^{\frac{m}{2}} \left( d_{\text{Mr}}^2 - d_{\text{Mr}}^2 \right) \]

Differentiating (56) 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 \( \lambda_{\text{Mr}} / \lambda_{\text{Me}} \).

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 \( \eta_{0,\tau_{y},k} \) can be expressed as in (45) where, for Nakagami-\( m \) fading, \( F_{Z_{\theta,\tau_{y},k}}(x) \) is given by

\[
F_{Z_{\theta,\tau_{y},k}}(x) = 1 - \sum_{i=0}^{m-1} \frac{(-1)^i x^i}{i!} \int_{\gamma}^{\infty} d\gamma \left( \frac{\gamma}{\pi} \right)^{\frac{m}{2}} \left( d_{\text{Mr}}^2 - d_{\text{Mr}}^2 \right) \]

for \( x > 0 \) and 0 otherwise. Letting \( d_{\text{Me}} \to \infty \), we obtain the CDF of \( \eta_{0,\tau_{y},k} \) given by (53) except \( \eta_{0,\tau_{y},k} \), \( \lambda_{\text{Mr}} \), and \( \lambda_{\text{Me}} \) are replaced by \( \eta_{0,\tau_{y},k} \), \( \lambda_{\text{Mr}} \), and \( \lambda_{\text{Me}} \), respectively. Note that the distribution of the maximum SIR depends on the ratio \( \lambda_{\text{Mr}} / \lambda_{\text{Me}} \).

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 \( d_{\text{Me}} \) from the transmitter are neutralized.24 In this case, the squared distances \( d_{\text{Me}}^2 \) of the remaining eavesdroppers are i.i.d. and follow a uniform distribution in \([d_{\text{Mr}}^2, d_{\text{Me}}^2]\). Therefore, the CDF of \( Z_{0,\tau_{y},k} \) becomes

\[
F_{\eta_{0,\tau_{y},k}}(x) = 1 - \sum_{i=0}^{m-1} \frac{(-1)^i x^i}{i!} \int_{\gamma}^{\infty} d\gamma \left( \frac{\gamma}{\pi} \right)^{\frac{m}{2}} \left( d_{\text{Mr}}^2 - d_{\text{Mr}}^2 \right) \]

Letting \( d_{\text{Me}} \to \infty \), the CDF of the maximum SIR becomes

\[
F_{\eta_{0,\tau_{y},k}}(x) = \exp \left( - \sum_{i=0}^{m-1} \frac{(-1)^i x^i}{i!} \right) \left( \frac{\pi}{\gamma} \right)^{\frac{m}{2}} \left( d_{\text{Mr}}^2 - d_{\text{Mr}}^2 \right) \]

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 \( \theta_{\text{a}} \) radians, in which case the effective density of interferers \( \lambda_{\text{Me}} \) affecting the eavesdroppers is

\[
\lambda_{\text{Me}} = \frac{\theta_{\text{a}}}{2\pi} (\lambda_{\text{Mr}} + \lambda_{\text{Mr}}) \]

23For 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.

24Consider that eavesdroppers within the neutralization region of transmitter \( j \) are still capable of eavesdropping other transmitters.
Such strategy also affects the density of the eavesdroppers capable of intercepting the confidential information, whose effective density $\lambda_e$ is given by

$$\lambda_e = \lambda_v \quad (58a)$$

or

$$\lambda_e = \frac{\theta_v}{2\pi} \lambda_v \quad (58b)$$

depending on whether the eavesdroppers have or do not have the knowledge of legitimate transmitter positions.\textsuperscript{25}

Replacing $\lambda_v$ and $\lambda_v$ with $\lambda_e$ and $\lambda_v$, 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.

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 $\theta_e$ radians, in which case the effective density of interferers $\lambda_{ir}$ affecting the legitimate receivers is

$$\lambda_{ir} = \frac{\theta_e}{2\pi} \lambda_{tx} \quad (59)$$

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

$$\lambda_{rx} = \lambda_{rx} \quad (60a)$$

or

$$\lambda_{rx} = \frac{\theta_e}{2\pi} \lambda_{rx} \quad (60b)$$

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 $\theta_t$ radians, in which case the effective density $\lambda_e$ of the eavesdroppers capable of intercepting the confidential information is

$$\lambda_e = \frac{\theta_t}{2\pi} \lambda_v \quad (61)$$

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

$$\lambda_{ir} = \frac{\theta_t}{2\pi} \lambda_{tx} \quad (62)$$

$$\lambda_{ie} = \frac{\theta_t}{2\pi} \lambda_{tx} + \lambda_{tx} \quad (63)$$

Now, consider the LNIS strategy where both the legitimate transmitters and receivers employ antennas with aperture angles $\theta_t$ and $\theta_r$, respectively, in which case the effective density $\lambda_{ir}$ of interferers affecting the legitimate receivers is

$$\lambda_{ir} = \frac{\theta_t \theta_r}{4\pi^2} \lambda_{tx} \quad (64)$$

Replacing $\lambda_{rx}$, $\lambda_{rx}$, and $\lambda_{rx}$ with $\lambda_{tx}$, $\lambda_{rx}$, $\lambda_{rx}$, and $\lambda_{tx}$, 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 $\lambda_{ir}$ affecting the legitimate receivers is

$$\lambda_{ir} = (1 - \xi) \lambda_{tx} \quad (65)$$

Replacing $\lambda_{ir}$ with $\lambda_{ir}$, 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.\textsuperscript{26}

A. Destinations Selection

Fig. 3 shows the network secrecy rate density $\mu_{sec}$ in cib/s/Hz/m$^2$ as a function of $\alpha$ when the $k$th closest receivers are selected in the legitimate network for different values of $k$. It can be observed that $\mu_{sec}$ 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 $\alpha$ maximizing $\mu_{sec}$ exists. This is due to the fact that the network interference affects both legitimate and eavesdropping networks, therefore it can be either beneficial or

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

\textsuperscript{26}In the following, consider a two-dimensional network and (unless otherwise stated) Rayleigh fading, infinite $d_{ve}$, and $d_{ve} = 1$ m. Although the analysis of the network secrecy metrics accounts for the presence of intentional interfering nodes, consider (unless otherwise stated) $\lambda_{ve} = 0$ as a worst case for network secrecy.
RABBACHIN et al.: WIRELESS NETWORK INTRINSIC SECRECY

Fig. 3. Network secrecy rate density as a function of $\alpha$ when the kth closest legitimate receivers are selected for $k = 2$, $\lambda_T = 1$ [node/m$^2$], and $\lambda_s/\lambda_T = 0.1$. 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 $\alpha$ when the closest legitimate receivers (k = 1) are selected (diamonds) and when the receivers with highest SIR ($\eta_m, \eta_e$) are selected (circles) for $b = 2$, $P_s^* = 0.1$, $R_s = 4$ [cib/s/Hz], and $\lambda_s = 0.1$ [node/m$^2$].

Fig. 5. Network secrecy throughput density as a function of $\alpha$ when the closest legitimate receivers are selected for $P_s^* = 0.1$, $R_s = 4$ [cib/s/Hz], $\lambda_T = 1$ [node/m$^2$], $\lambda_s = 0.1$ [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 $\tau_{ns}$ as a function of $\alpha$ and $\lambda_s$, when the closest legitimate receivers are selected, for $m = 0.5$ node/m and $0.5$ node/m. It can be observed that $\tau_{ns}$ scales with $\alpha$. It can also be seen that the maximum throughput density region shifts toward lower $\lambda_s$ and higher $\lambda_T$ for low values of $\lambda_s$.

Fig. 7 shows the network secrecy throughput density $\tau_{ns}$ as a function of $\alpha$ for different values of $\lambda_s$ when the closest legitimate receivers are selected. As expected, $\tau_{ns}$ decreases as the density of eavesdroppers increases. It can also be observed that the optimal $\alpha$ shifts toward higher values as $\lambda_s$ increases.

This behavior can be attributed to the fact that, for a higher $\lambda_s$, a larger amount of network interference is needed to mitigate the eavesdropper capabilities.

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 $\lambda_T$, while for small $\lambda_T$, 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 $\tau_{ns}$ as a function of $\alpha$, 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 $\tau_{ns}$ 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 $\alpha$ shifts toward higher values as $b$ increases.

Fig. 6(a) and (b), respectively, shows the contours of network secrecy throughput density $\tau_{ns}$ as a function of $\alpha$ and $\lambda_s$, when the closest legitimate receivers are selected, for $m = 2$ and 0.5 node/m$^2$. It can be observed that $\tau_{ns}$ scales with $\lambda_s$. It can also be seen that the maximum throughput density region shifts toward lower $R_s$ and higher $\alpha$ for a lower value of $\lambda_T$. 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 $\tau_{ns}$ as a function of $\alpha$ for different values of $\lambda_s$ when the closest legitimate receivers are selected. As expected, $\tau_{ns}$ decreases as the density of eavesdroppers increases. It can also be observed that the optimal $\alpha$ shifts toward higher values as $\lambda_s$ increases. This behavior can be attributed to the fact that, for a higher $\lambda_s$, a larger amount of network interference is needed to mitigate the eavesdropper capabilities.

Note that, for a fixed $\alpha$, a higher density of legitimate receivers corresponds to a lower average link distance.
intentional interferers and legitimate nodes) for different values of \( \alpha \) when the closest legitimate receivers are selected. It can be observed that \( \tau_{\alpha} \) increases as \( \lambda_{I}/\lambda_t \) 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 \( \tau_{\alpha} \) approaches the asymptotic values, corresponding to the absence of eavesdroppers. Note that the asymptotic value of \( \tau_{\alpha} \) depends on \( \alpha \), which is related to the number of legitimate links and the amount of network interference. Note also that the asymptotic values are reached by lower values of \( \lambda_{I}/\lambda_t \) for lower \( \alpha \).

C. Competitive Strategies for Network Secrecy

Fig. 9 shows the network secrecy throughput density \( \tau_{\alpha} \) as a function of \( d_{\text{ave}} \) for different values of \( \alpha \) when NERN is employed (note that \( d_{\text{ave}} = 0 \) corresponds to the absence of NERN). It can be observed that \( \tau_{\alpha} \) increases with \( d_{\text{ave}} \) and approaches the asymptotic values corresponding to the absence of eavesdroppers. This behavior can be attributed to the fact that a higher \( d_{\text{ave}} \) 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 \( \tau_{\alpha} \) as a function of antenna aperture angles for different values of \( \alpha \) and \( \lambda_{I} \) 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 (\( \theta_{\alpha} = \theta_t = \theta_e = \theta \)), the \( \tau_{\alpha} \) increases as \( \theta \) decreases.

Fig. 11 shows the network secrecy throughput density \( \tau_{\alpha} \) as a function of \( \xi \) for different values of \( \alpha \) 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 \( \xi \) (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.
Fig. 9. Network secrecy throughput density as a function of $d_{\text{min}}$ when the closest legitimate receivers are selected in the presence of NERN for $b = 2$, $P_v^R = 0.1$, $R_s = 4$ [cib/s/Hz], $\lambda_s = 1$ [node/m$^2$], and $\lambda_x = 0.5$ [node/m$^2$].

Fig. 10. Network secrecy throughput density as a function of $\theta$ when the closest legitimate receivers are selected in the presence of ENIS and LNIS for $b = 2$, $P_v^R = 0.1$, $\lambda_s = 1$ [node/m$^2$], $R_s = 4$ [cib/s/Hz], and $\lambda_x = 0.1$ (continuous lines) or $\lambda_x = 0.5$ [node/m$^2$] (dashed lines).

Fig. 11. Network secrecy throughput density as a function of $\xi$ when the closest legitimate receivers are selected in the presence of ENIS with $\theta_x = 2\pi(1 - \xi)$ and ANIG for $b = 2$, $P_v^R = 0.1$, $\lambda_s = 1$ [node/m$^2$], $R_s = 4$ [cib/s/Hz], and $\lambda_x = 0.3$ (continuous lines) or $\lambda_x = 0.5$ [node/m$^2$] (dashed lines).

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 $\Pi$ is stationary, for any property $\mathcal{P}$, $\mathbb{P}\{\mathcal{P} + \omega \in \mathcal{P}\} = \mathbb{P}\{\mathcal{P} \in \mathcal{P}\}$ for all $\omega \in \mathbb{R}^n$ [69]. To account for the confidential information generated from a bounded set $A_t \subset \mathbb{R}^n$, the origin of the reference system can be shifted to the position of the $j$th node in $A_t$. Let $\Pi_t \triangleq \Pi_t \cup \Pi_{tx} \cup \Pi_{tx}$ and $f(\Pi) \triangleq \sum_{j \in A_t} 1_{(\xi_j) \in (X_j)_{R_j}(\pi_j, z, \xi)}$, (17) can be rewritten as

$$R_{tx}(\Omega_{A_t}) = \sum_{X_j \in A_t \cap \Omega_{A_t}} f(\Pi - X_j)$$  \hspace{1cm} (66)

If $\sup_{\tau : B(\tau) \subset A_t} t \to \infty$ as $t \to \infty$ for a convex averaging sequence $\{A_t\}$ with $A_1 \subset A_2 \subset \cdots \subset \mathbb{R}^n$, then (19) can be written as

$$\rho_{tx} = \lim_{t \to \infty} \frac{1}{|A_t|} \sum_{X_j \in A_t \cap \Omega_{A_t}} f(\Pi - X_j)$$

$$= \lim_{t \to \infty} \frac{\Pi_{tx}(A_t)}{|A_t|} \frac{1}{\Pi_{tx}(A_t)} \sum_{X_j \in A_t \cap \Omega_{A_t}} f(\Pi - X_j)$$

where $\Pi_{tx}(A_t)$ is the number of points from $\Pi_{tx}$ contained in $A_t$. 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

$$\rho_{tx} = \lambda_{tx} \mathcal{F}_{\omega} \{f(\Pi)\}$$  \hspace{1cm} (67)

provided that $\mathcal{F}_{\omega} \{f(\Pi)\} < \infty$. This results in (20).

APPENDIX B

DERIVATION OF (41)

For each $x \in \mathcal{H}$, the CF of $G_0 \mathcal{R}(\cdot, x)$ can be written as

$$\psi(G_0 \mathcal{R}(\cdot, x)) \{j\omega\} = \psi_{G_0 \mathcal{R}(\cdot, x)}(\cdot \in (j\omega))$$

$$\times \mathcal{E}(\mathcal{U}, \mathcal{U}, x, k) \{\psi_{G_0 \mathcal{R}(\cdot, x)}(\cdot \in (j\omega)) - j\omega D_{\mathcal{R}}^G(\cdot, \mathcal{R}(\cdot, x), x)\}$$  \hspace{1cm} (68)
where \( \rho_{0;k,i} \) is a Stable distributed RV according to (8), with CF given by

\[
\psi_{\rho_{0;k,i}}(j\omega) = \exp \left( -\lambda_{s} \gamma |j\omega|^{\gamma} \left[ 1 + \frac{j\omega}{\pi \lambda_{r}s} \tan \left( \frac{\pi}{2k} \right) \right] \right).
\]

(69)

Since the squared distance \( D_{0,k,R_{0};(k)}^{2} \) is an Erlang distributed RV [85]–[87] with CF given by

\[
\psi_{D_{0,k,R_{0};(k)}}^2(j\omega) = \left( 1 - \frac{j\omega}{\pi \lambda_{r}s} \right)^{-k}
\]

(70)

we obtain \( \psi_{\rho_{0,R_{0};k}}(j\omega) \) as in (41).

APPENDIX C

DERIVATION OF (42)

To characterize the maximum SIR among nodes with index in \( R_{0} \), consider \( R_{k} \) with cardinality \( N_{R_{k}} \triangleq R_{k} \). The CDF of \( \eta_{0,R_{k}} \) conditioned on \( N_{R_{k}} \) is given by\(^{28}\)

\[
F_{\eta_{0,R_{k}};N_{R_{k}}}(x) = \left\{ \begin{array}{ll}
F_{Z\cdot\rho_{0,R_{k}};N_{R_{k}}}(x) & N_{R_{k}} \geq 1 \\
1 & N_{R_{c}} = 0.
\end{array} \right.
\]

(71)

By taking the expectation of \( F_{\eta_{0,R_{k}};N_{R_{k}}}(x) \) over \( N_{R_{0}} \), we obtain (42).

APPENDIX D

DERIVATION OF (48)

For Nakagami-m fading channels, the conditional CDF of \( Z_{0,N_{c}}(k) \) is given by

\[
F_{Z_{0},N_{c},k}(Z_{0,N_{c},k}) = \left[ \frac{d}{dz} \mathcal{L}_{f_{N_{c},k}}(z) \right]_{z=1}
\]

(72)

By taking the expectation over \( I_{R_{0},(k)} \), the CDF of \( Z_{0,R_{0}(k)} \) conditioned on \( D_{0,N_{c},k} \), results in

\[
F_{Z,N_{c},k}(Z_{N_{c},k}) = \left[ \frac{d}{dz} \mathcal{L}_{f_{N_{c},k}}(z) \right]_{z=1}
\]

(73)

where \( \mathcal{L}_{f_{N_{c},k}}(s) \) is the Laplace transformation of \( f_{N_{c},k} \), which is given by

\[
\mathcal{L}_{f_{N_{c},k}}(s) = \exp \left( -\lambda_{s} \frac{\gamma}{\cos \left( \frac{\pi}{2k} \right)} |s|^{\frac{1}{\gamma}} \right).
\]

The expectation over \( D_{0,R_{0}(k)}^2 \) provides the CDF of \( Z_{0,R_{0}(k)} \) as given in (48).

\(^{28}\)We consider the SIR equal to zero for the case of \( N_{R_{c}} = 0 \).

ACKNOWLEDGMENT

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

REFERENCES


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 Professor 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 Cristofero 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.