Intrinsic Secrecy in Inhomogeneous Stochastic Networks

Giovanni Chisci, *Member, IEEE*, Andrea Conti, *Senior Member, IEEE*, Lorenzo Mucchi, *Senior Member, IEEE*, and Moe Z. Win, *Fellow, IEEE*

***Abstract*— Network secrecy is vital for a variety of wireless applications and can be accomplished by exploiting network interference. Recently, interference engineering strategies (IESs) have been developed to harness network interference, depending on the wireless environment (node distribution, transmission policy, and channel conditions). Typically, the node spatial distribution has been modeled according to a homogeneous Poisson point process for mathematical tractability. However, such a model can be inadequate for inhomogeneous (e.g., sensor and vehicular) networks. This paper develops a framework for the design and analysis of inhomogeneous wireless networks with intrinsic secrecy. Based on the characterization of the network interference and received signal-to-interference ratio for different receiver selection strategies. Local and global secrecy metrics are introduced for characterizing the level of intrinsic secrecy in inhomogeneous wireless networks from a link and a network perspective. The benefits of IESs are quantified by simulations in various scenarios, thus corroborating the analysis. Results show that IESs can elevate the network secrecy significantly.**

***Index Terms*— Wireless network secrecy, inhomogeneous Poisson point process, interference engineering, fading channels.**

I. Introduction

NETWORK INTRINSIC SECRECY is the capacity of a network to hide a portion of the transmitted information from unwanted listeners by solely relying on the physical properties of the wireless channel. Its exploitation is a key enabler for several emerging wireless applications including operation and control of cyber-physical systems [1]–[3], Internet of things (IoT) [4]–[6], and vehicular networks [7]–[9].

Manuscript received December 27, 2016; revised December 27, 2017 and August 31, 2018; accepted February 3, 2019; approved by IEEE/ACM TRANSACTIONS ON NETWORKING Editor K. Jamieson. Date of publication June 21, 2019; date of current version August 16, 2019. This research was supported in part by FAR and the "5×1000" Young Researcher Mobility Project, University of Ferrara, in part by the Copernicus Fellowship, in part by the National Science Foundation under Grant CCF-1525705, and in part by the MIT Institute for Soldier Nanotechnologies. The material in this paper was presented, in part, at the 2017 IEEE International Conference on Acoustics, Speech, and Signal Processing. *(Corresponding author: Giovanni Chisci.)*

G. Chisci and A. Conti are with the Department of Engineering, University of Ferrara, 44122 Ferrara, Italy (e-mail: giovanni.chisci@unife.it; a.conti@ieee.org).

L. Mucchi is with the Department of Information Engineering, University of Florence, 50139 Florence, Italy (e-mail: lorenzo.mucchi@unifi.it).

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

Digital Object Identifier 10.1109/TNET.2019.2911126

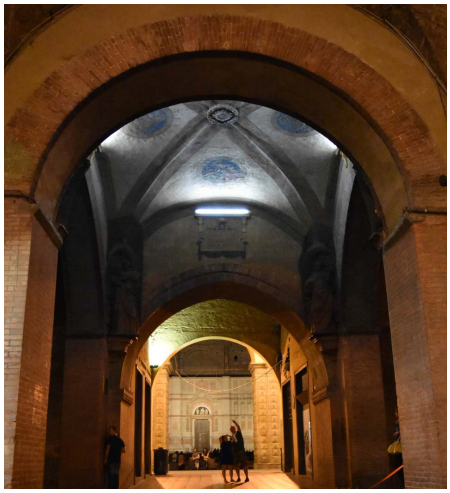


Fig. 1. *Voltone del Podestà* in Piazza Maggiore, Bologna, Italy: an example of intrinsic communication confidentiality.

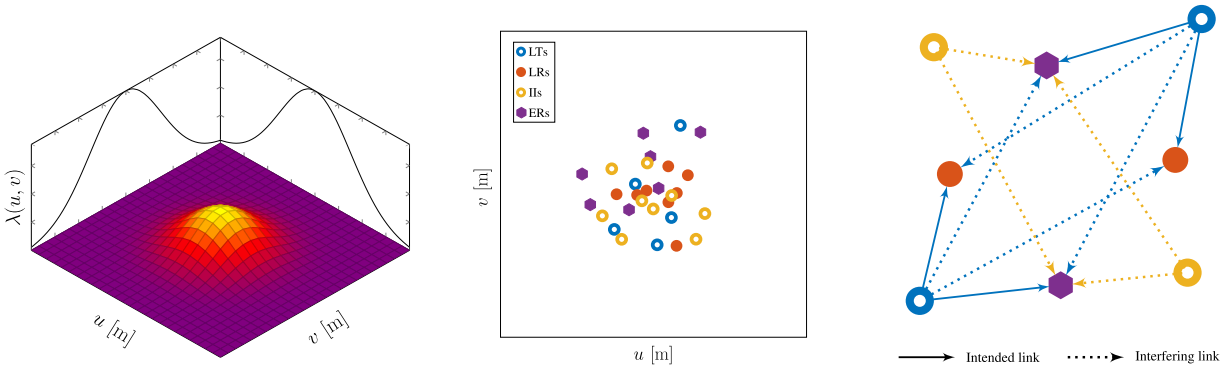
A. Big Picture

The need for communication confidentiality has existed since antiquity. A simple and famous example is the Caesar cipher, used by Julius Caesar according to Suetonius for protecting missives of military significance [10]. Nowadays, the confidentiality of wireless communications has become crucial for new emerging secrecy-sensitive applications. In fact, the broadcast wireless channel facilitates the information eavesdropping; on the other hand, it offers the possibility to exploit aggregate interference for enhancing the secrecy level.

Intrinsic secrecy has emerged in the broader area of physical-layer security [11] as a possible way to complement the traditional cryptographic techniques [12]–[14]. Recent studies based on [15], [16] highlight that aggregate interference can be beneficial for network secrecy if exploited properly [17], [18]. In particular, the network geometry affects the intrinsic secrecy due to two main factors:

- wireless signals attenuate with distances, hence active node locations have a prominent effect on the level of aggregate interference; and
- interference engineering strategies, (IESs) can be devised to imbalance the signal-to-interference-plus-noise ratio s (SINRs) at legitimate and eavesdropping receivers.

An example of environment preserving communication confidentiality is shown in Fig. 1. In particular, only persons at



(a) Intensity function. (b) Realization. (c) System model.

Fig. 2. Fig. 2(a) shows a Gaussian intensity function. Fig. 2(b) displays a realization of the network with Gaussian intensity function. Fig. 2(c) presents the system model composed by four overlaid subnetworks.

two diagonal corners can hear each other due to the peculiar shape of the structure, thereby forming a confidential channel.

B. Related Works and Motivation

The secrecy capacity of a wire-tap channel was introduced in [16]. After the characterization of the discrete memoryless channel, secrecy capacity is studied in Gaussian wire-tap channels [19], in fading channels [20], in the presence of interference [21], with multi-antenna links [22], for multilevel network scenarios [23], and with eavesdropper collusion [24].

Recently, several IESs have been proposed to enhance the secrecy of small networks consisting of source, destination, helping nodes and eavesdroppers. Techniques like artificial noise [25]–[27], artificial noise alignment [28]–[30], friendly jamming [31]–[33], and cooperative jamming [34]–[36] have been developed to impair the eavesdropping channel and, hence, achieve a non-zero secrecy rate at the legitimate receiver. Generalized interference alignment techniques that maximize network secrecy for large-scale stochastic networks have been proposed in [37] and [38].

Other recent works explore intrinsic secrecy in ad-hoc [17], [39], [40], cellular [41]–[44], D2D enabled [45], [46], full-duplex enabled [47], and multi-tier [48] networks with stochastic topology. Such papers consider the homogeneous Poisson point process (HPPP) for modeling node spatial distributions, which has been extensively adopted to characterize the aggregate interference in large wireless networks [49]–[54] because of its tractability. However, the HPPP cannot capture practical scenarios that may involve spatial clustering, location-dependent access control, and non-uniform mobility.

Several types of stationary point processes have been introduced to study wireless networks with spatial correlation, e.g., Cox, cluster, hardcore, Gibbs, and determinantal point processes [55]–[57]. Such point processes account for properties like attraction, repulsion, and regularity in node patterns, to study the spatial distribution both of clustered and cellular networks [58], [59]. Such stationary models have the advantage of being able to describe the average performance of a network in a tractable way. Nevertheless, such translation invariant models have the main limitation of not being capable of describing the location-dependent performance within a network. For this reason we consider inhomogeneous point processes to tackle the spatial variability of the network performance. This has found application in different scenarios such as mobile, vehicular, and sensor networks [60]–[64].

Consider a clustered network, when classical homogeneous Poisson cluster model is used, only the average performance at the typical point can be determined [65]. We aim to provide a spatial description of secrecy metrics that consider the inhomogeneous distribution of the nodes. Furthermore, secrecy needs to be guaranteed over the whole network, and the analysis at a typical point is inadequate. Therefore, it is important to study the *inhomogeneous network* where nodes are spatially distributed according to an inhomogeneous Poisson point process (IPPP) (see Fig. 2(a)-2(b)). The considered setting represents a challenging generalization with respect to (w.r.t.) the homogeneous one, especially for what concerns the characterizations of the interference and SINR when a receiver selection strategy is employed.

C. Contribution

This paper provides foundations for inhomogeneous wireless networks with intrinsic secrecy. Our approach relies on the characterization of the signal-to-interference ratio (SIR) accounting for (i) the spatial distributions of legitimate transmitter s (LTs), legitimate receiver, s (LRs), eavesdropping receiver s (ERs), and intentional interferer, s (IIs); (ii) the wireless propagation medium; and (iii) the aggregate interference at each receiver. We consider three scenarios: full inhomogeneous network, (FIN), full homogeneous network, (FHN), and partial inhomogeneous network, (PIN). The key contributions of the paper can be summarized as follows:

- a framework for the design and analysis of wireless networks with intrinsic secrecy accounting for inhomogeneous distribution of legitimate nodes, intentional interferers, and eavesdroppers;
- the statistical characterization of the aggregate interference and received SIR in legitimate and eavesdropping

networks for FIN, FHN, and PIN with different receiver selection strategies;
- the introduction of local and global secrecy metrics for characterizing the level of intrinsic secrecy in inhomogeneous networks from a link and a network perspective; and
- the quantification of the benefits enabled by IESs in different wireless scenarios and description of the associated physical interpretations.

Our approach combines information theory, communication theory, probability theory, and stochastic geometry to develop a theoretical analysis, which is corroborated by simulations in different network settings. The novelty of the work is in the analysis of the location-dependent performance of the network, which allows to characterize accurately the different local secrecy levels arising from the diverse local node densities. The main difficulty is to hold tractability while considering the intricate relations between the distributions of LTs, LRs, ERs, and IIs. This makes difficult to characterize the aggregate interference and the SIR. Nevertheless, we devise a systematic procedure to characterize and compute key performance indicators for any receiver selection strategy by means of numerical integrations.

The rest of the paper is organized as in the following: Section II presents the network model. Section III analyzes the aggregate interference distribution in inhomogeneous networks. Section IV develops the statistical characterization of the received SIR in generic and Nakagami-m fading channels for different receiver selection strategies. Section V defines local and global secrecy metrics for inhomogeneous networks. Section VI presents case studies with different node inhomogeneous deployments. Section VII provides numerical results and section VIII gives our final remarks. The notations used in this paper is summarized in Table I.

TABLE I
NOTATION USED THROUGHOUT THE PAPER

Symbol	Usage
$\mathcal{A} \subseteq \mathbb{R}^d$	Bounded Borel set in $\mathbb{R}^d$
$\mathsf{i},\ i$	Random variable and its realization
$\mathbf{x},\ \boldsymbol{x}$	Random vector and its realization
$\Pi,\ \mathit{\Pi}$	Point process and its realization
$\mathbb{1}_Y(\cdot)$	Indicator function for the property Y
$\mathsf{n}(\mathcal{A})$	Number of points in $\mathcal{A}$
$\lambda(\cdot)$	Intensity function [nodes/m^d]
$\Lambda(\cdot)$	Intensity measure over $\mathcal{A}$ [nodes]
$\mathbb{S}\{\cdot\}$	receiver selection operator
$\mathbb{E}\{\cdot\}$	Expectation operator
$\mathbb{P}\{\cdot\}$	Probability operator
$\mathbb{E}^{!j}\{\cdot\}$	Reduced Palm expectation given $\boldsymbol{x}_j$
$\mathcal{T},\ \mathcal{J}$	Index sets of LTs and IIs
$\mathcal{R}_j$	Index set of receivers of $\boldsymbol{x}_j$
$\mathcal{E}_j$	Index set of eavesdroppers of $\boldsymbol{x}_j$
$k \in \mathcal{R}_j$	index of the generic receiver of $\boldsymbol{x}_j$
$\bar{k} = \mathbb{S}\{\mathcal{R}_j\}$	Index of the receiver selected by $\boldsymbol{x}_j$
(k)	Index of the k^{th} closest LR to $\boldsymbol{x}_j$
$\breve{k}$	Index of the maximum SIR LR of $\boldsymbol{x}_j$
$\mathsf{i}_{j,k}$	Interference at $\mathbf{x}_k$ given $\boldsymbol{x}_j$
$\mathsf{i}_{j,k}\|\mathbf{x}_k$	Interference at $\boldsymbol{x}_k$ given $\mathbf{x}_j = \boldsymbol{x}_j$
$f_{\mathsf{z}}(\cdot)$	PDF of the RV z
$F_{\mathsf{z}}(\cdot)$	CDF of the RV z
$\psi_{\mathsf{i}}(\cdot)$	CF of the RV i
$\mathcal{L}_{\mathsf{i}}(\cdot)$	Laplace transform of the RV i
$\mathsf{r}_{j,(k)}$	Distance between $\boldsymbol{x}_j$ and its k^{th} closest LR
$\varphi_{j,\bar{k},\breve{k}}$	MSR of at the selected LR of $\boldsymbol{x}_j$
$\mathcal{U}(a,b]$	Uniform distribution on the interval $(a,b]$
$\mathcal{P}(a)$	Poisson' distribution with parameter a
$\|\cdot\|,\ \|\cdot\|$	Euclidean norm, Lebesgue measure
$\Re\{\cdot\}$	Real part of the complex argument

II. NETWORK MODEL

Consider four overlaid networks as in Fig. 2(b): the legitimate transmitter network, (LTN); legitimate receiver network, (LRN); eavesdropping receiver network, (ERN); and intentional interferer network, (IIN). These networks are modeled via independent IPPPs defined over a d-dimensional Euclidean space. Recall that a point process Π is defined over a bounded Borel set[1] $\mathcal{A} \subseteq \mathbb{R}^d$ and has the twofold nature of being a random measure, i.e., the number of points in $\mathcal{A}$, $\Pi(\mathcal{A}) \triangleq \mathsf{n}(\mathcal{A})$, and a random sequence of points, i.e., $\Pi = \{\mathbf{x}_1, \mathbf{x}_2, \dots\} = \{\mathbf{x}_{\mathsf{n}(\mathcal{A})}\}$. Furthermore, Π is characterized by the intensity function $\lambda(\boldsymbol{x})$ for all $\boldsymbol{x} \in \mathcal{A}$ or, equivalently, by the intensity measure $\Lambda(\mathcal{A})$, where[2]

$$\Lambda(\mathcal{A}) = \int_{\mathcal{A}} \lambda(\boldsymbol{x}) d\boldsymbol{x}. \tag{1}$$

The considered networks are described in the following points.

- The LTN and the LRN form the legitimate network, which consists of nodes exchanging confidential information. The LTN and the LRN are denoted by the point processes Π_{tx} and Π_{rx} with intensity functions $\lambda_{\text{tx}}(\boldsymbol{x})$ and $\lambda_{\text{rx}}(\boldsymbol{x})$, respectively.
- The ERN is composed of malicious nodes trying to intercept the confidential information exchanged through the legitimate network. It is described by the point process Π_{ex} with intensity function $\lambda_{\text{ex}}(\boldsymbol{x})$.
- The IIN is composed of nodes that introduce dummy messages to jam the radio channel and impair the ERs' channels. The IIN is described by the point process Π_{jx} with intensity function $\lambda_{\text{jx}}(\boldsymbol{x})$.

The aforementioned point processes enable to account for the capabilities of LRs and ERs of controlling or mitigating the received interference. In particular, the point processes of

[1]A Borel set is the smallest σ-algebra on $\mathbb{R}^d$ that contains all the open subsets of $\mathbb{R}^d$ [66].

[2]The intensity function of point processes represents the density of nodes per unit area and is measured in [nodes/m^d]. The intensity measure is the mean number of points of Π on $\mathcal{A}$.

interferers affecting the LRs and ERs are modeled by IPPPs with intesity functions given, respectively, by

$$\lambda_{\mathrm{ir}}(\boldsymbol{x}) = \beta_{\mathrm{tr}}\lambda_{\mathrm{tx}}(\boldsymbol{x}) + \beta_{\mathrm{jr}}\lambda_{\mathrm{jx}}(\boldsymbol{x}) \tag{2a}$$

$$\lambda_{\mathrm{ie}}(\boldsymbol{x}) = \beta_{\mathrm{te}}\lambda_{\mathrm{tx}}(\boldsymbol{x}) + \beta_{\mathrm{je}}\lambda_{\mathrm{jx}}(\boldsymbol{x}) \tag{2b}$$

where the parameters $\beta_{\mathrm{tr}}, \beta_{\mathrm{te}}, \beta_{\mathrm{jr}}, \beta_{\mathrm{je}} \in [0,1]$ capture the capability of each subnetwork to control the interference, based on the employed IES. Such capabilities are accounted for at the level of point processes by thinning the network contributions to the interference for both the LTN and IIN. For example, at the receiver side interference cancellation can be employed if the sequence of transmitted symbols is known, while at the transmitter side interference alignment can be exploited to null the interference at some specific locations via beamforming [38].[3]

Let $\mathcal{T}$ and $\mathcal{J}$ denote the index sets of LTs and IIs, respectively. For the j^{th} LT in $\mathcal{T}$, $\mathcal{R}_j$ denotes the index set of potential LRs and $\mathcal{E}_j$ the index set of ERs. For a legitimate link, $k \in \mathcal{R}_j$ indicates the receiver index. Similarly, for an eavesdropping link, $i \in \mathcal{E}_j$ indicates the ER index.

III. Interference Panorama in Inhomogeneous Wireless Networks

In wireless networks, noise and interference affect the performance. In interference-limited conditions the additive noise is considered negligible w.r.t. the aggregate interference. In the following, we neglect the effect of the noise and assume an interference-limited regime. It is well known that the interference distribution at a given point of a network can be described by the characteristic function (CF) or equivalently by the Laplace transform [66]. When the network is modeled by HPPPs the interference distribution is location-independent [49] while for IPPPs is location-dependent.

Consider a random link composed of a transmitter at $\boldsymbol{x}_j$ and a receiver at $\mathsf{x}_k \in \Pi_{\mathrm{rx}}$ in $\mathcal{A} \subseteq \mathbb{R}^d$. The signal power received at x_k is

$$\mathsf{p}_{j,k} = p_{\mathrm{T}}|\mathsf{s}_j|^2 \frac{\mathsf{h}_{j,k}}{\mathsf{r}_{j,k}^{2b}} \tag{3}$$

where p_{T} is the transmitted power, $|\mathsf{s}_j|^2$ is the power of the complex transmitted symbol, b is the amplitude path-loss exponent, $\mathsf{h}_{j,k} \in \mathbb{C}$ is the quasi-static channel power gain, and $\mathsf{r}_{j,k} = \|\boldsymbol{x}_j - \mathsf{x}_k\|$ is the Euclidean distance between the locations $\boldsymbol{x}_j$ and x_k. The aggregate interference power level at x_k is given by

$$\mathsf{i}_{j,k} = \sum_{\mathsf{x}_q \in \Pi_{\mathrm{ir}}} p_{\mathrm{T}}|\mathsf{s}_q|^2 \frac{\mathsf{h}_{q,k}}{\mathsf{r}_{q,k}^{2b}}. \tag{4}$$

In the following, we consider $p_{\mathrm{T}} = 1$, $|\mathsf{s}|^2 = 1$, and independent and identically distributed (i.i.d.) channel power gains.[4] Note that $\mathsf{i}_{j,k}$ is a random variable (RV) taking different values for each realization of point processes and channels.

[3]For specific treatises of IESs see, e.g., [24]–[38].

[4]Consider that every LT and IIs transmit symbols s_j and s_q, respectively, with symbol $|\mathsf{s}_j|^2 = |\mathsf{s}_q|^2 = |\mathsf{s}|^2 = 1$ for all $j \in \mathcal{T}$ and $q \in \mathcal{J}$. For all pairs of locations $\boldsymbol{x}_j, \boldsymbol{x}_k \in \mathcal{A}$, the same channel gain distribution is assumed (i.e., $\psi_{\mathsf{h}_{j,k}}(\cdot) = \psi_{\mathsf{h}}(\cdot)$).

The conditional CF of the interference at a given location can be expressed by means of the probability generating functional (PGFL) of the Poisson point process (PPP) [66] as

$$\psi_{\mathsf{i}_{j,k}|\mathsf{x}_k}(\jmath\omega) = \exp\left\{-\int_{\mathcal{A}}\left(1 - \psi_{\mathsf{h}}\left(\frac{\jmath\omega}{\|\boldsymbol{x} - \mathsf{x}_k\|^{2b}}\right)\right)\lambda_{\mathrm{ir}}(\boldsymbol{x})d\boldsymbol{x}\right\} \tag{5}$$

where $\psi_{\mathsf{h}}(\cdot)$ is the CF of the channel gain and $\jmath$ is the imaginary unit.

It is worth noting that the statistical distribution of the aggregate interference depends on the location x_k of the receiver. This is because from each given location $\mathsf{x}_k = \boldsymbol{x}_k$ we see a different *panorama of interferers*, which is the distribution of the interferers seen from $\boldsymbol{x}_k$. Note that IESs, when applied, modify the intensity of the interferers $\lambda_{\mathrm{ir}}(\boldsymbol{x})$ according to (2a) by the parameters β_{tr} and β_{jr}, which can range from 0 (perfect interference cancellation) to 1 (no interference mitigation applied).

We now introduce the unconditional CF of the interference, which is useful when an SIR analysis is carried out considering a receiver selection strategy, as will be shown in Section IV. The unconditional CF is obtained by marginalizing $\psi_{\mathsf{i}_{j,k}|\mathsf{x}_k}(\jmath\omega)$ over the spatial probability density function (PDF) $f^{\mathrm{rx}}_{\mathsf{x}_k}(\boldsymbol{x})$ of the receiver's location x_k as

$$\psi_{\mathsf{i}_{j,k}}(\jmath\omega) = \mathbb{E}_{\mathsf{x}_k}\left\{\psi_{\mathsf{i}_{j,k}|\mathsf{x}_k}(\jmath\omega)\right\} \tag{6}$$

where

$$f^{\mathrm{rx}}_{\mathsf{x}_k}(\boldsymbol{x}) = \frac{\lambda_{\mathrm{rx}}(\boldsymbol{x})}{\Lambda_{\mathrm{rx}}(\mathcal{A})} \tag{7}$$

for all $\boldsymbol{x} \in \mathcal{A}$ and zero otherwise. For a receiver selected randomly, according to the spatial distribution in (7), $\psi_{\mathsf{i}_{j,k}}(\jmath\omega)$ is location-independent, i.e., $\psi_{\mathsf{i}_{j,k}}(\jmath\omega) = \psi_{\mathsf{i}}(\jmath\omega)$.

To consider other receiver selection strategies than the random one, we express both the marginalization and the spatial distribution of (6) and (7) w.r.t. the polar coordinates of $\boldsymbol{x}_k$. For networks in $\mathcal{A} \subseteq \mathbb{R}^2$, the position $\boldsymbol{x}_k$ can be conveniently expressed by means of its polar coordinates w.r.t. the position $\boldsymbol{x}_j$, i.e.,

$$\boldsymbol{x}_k = \begin{bmatrix} u_k \\ v_k \end{bmatrix} = \begin{bmatrix} u_j + r_{j,k}\cos\theta_{j,k} \\ v_j + r_{j,k}\sin\theta_{j,k} \end{bmatrix}. \tag{8}$$

Then (6) takes the form of

$$\psi_{\mathsf{i}_{j,k}}(\jmath\omega) = \mathbb{E}_{\mathsf{r}_{j,k},\boldsymbol{\theta}_{j,k}}\left\{\psi_{\mathsf{i}_{j,k}|\mathsf{r}_{j,k},\boldsymbol{\theta}_{j,k}}(\jmath\omega)\right\} \tag{9}$$

where $\psi_{\mathsf{i}_{j,k}|\mathsf{r}_{j,k},\boldsymbol{\theta}_{j,k}}(\jmath\omega)$ is given in (10) at the bottom of the next page with $\lambda_{\mathrm{ir}}(\boldsymbol{x})$ given in (2a) and the expectation is performed w.r.t. the joint PDF of $\mathsf{r}_{j,k}$ and $\boldsymbol{\theta}_{j,k}$, i.e., $f_{\mathsf{r}_{j,k},\boldsymbol{\theta}_{j,k}}(r_{j,k},\theta_{j,k})$. As it will be shown in the following section, this model simplifies the statistical analysis of the received SIR for the considered receiver selection strategies.

Recall that if the interferers are uniformly distributed over $\mathcal{A} \subseteq \mathbb{R}^2$, where the external bound of $\mathcal{A}$ tends to infinity, the distribution of the aggregate interference is location-independent and its CF is given in closed form

$$\psi_{\mathsf{i}_{j,k}|\mathsf{r}_{j,k},\boldsymbol{\theta}_{j,k}}(\jmath\omega)=\exp\left\{-\int_{\mathcal{A}}\Big(1-\psi_{\mathsf{h}}\Big(\jmath\omega\big((u-u_j-r_{j,k}\cos\theta_{j,k})^2+(v-v_j-r_{j,k}\sin\theta_{j,k})^2\big)^{-b}\Big)\Big)\lambda_{\mathrm{ir}}(u,v)dudv\right\} \quad (10)$$

as [49]

$$\psi_{\mathsf{i}_{j,k}|\mathbf{x}_k}(\jmath\omega)=\psi_{\mathsf{i}_{j,k}}(\jmath\omega) \quad (11a)$$

$$=\exp\left\{-\lambda_{\mathrm{ir}}\gamma|\omega|^{\frac{1}{b}}\left[1+\frac{\jmath\omega}{|\jmath\omega|}\tan\left(\frac{\pi}{2b}\right)\right]\right\}. \quad (11b)$$

Then, $\mathsf{i}_{j,k}$ belongs to the class of *skewed stable* RVs

$$\mathsf{i}_{j,k}\sim\mathcal{S}\left(\frac{1}{b},1,\lambda_{\mathrm{ir}}\gamma\right) \quad (12)$$

where

$$\gamma=\pi B_{\frac{1}{b}}^{-1}\mathbb{E}\{\mathsf{h}^{\frac{1}{b}}\} \quad (13a)$$

$$B_a=\begin{cases}\dfrac{1-a}{\Gamma(2-a)\cos\left(\frac{\pi a}{2}\right)} & \text{for } a\neq 1\\ \dfrac{2}{\pi} & \text{for } a=1\end{cases} \quad (13b)$$

and where $\Gamma(\cdot)$ is the Gamma function.

IV. Statistical Characterization of SIR

We consider interference-limited systems, wherein the performance is driven by the SIR, which is defined by

$$\mathsf{z}_{j,k}\triangleq\frac{\mathsf{h}_{j,k}}{\mathsf{r}_{j,k}^{2b}\mathsf{i}_{j,k}}. \quad (14)$$

Different receiver selection strategies are taken into account for characterizing the SIR of a legitimate link. In particular, the confidential information can be sent to: 1) a randomly selected receiver; 2) the receiver with maximum SIR; or 3) the k^{th} closest receiver. The LR index for the j^{th} transmitter is selected according to the selection strategy $\mathbb{S}\{\cdot\}$ as $\bar{k}=\mathbb{S}\{\mathcal{R}_j\}$. Regarding the eavesdropping link, we consider only the ER with maximum instantaneous SIR, i.e., the most dangerous and limiting for secrecy performance.

A. SIR in the Legitimate Network

For a transmitter located at $\boldsymbol{x}_j$, we characterize the SIR received by the LR at $\mathbf{x}_{\bar{k}}$. Note that this characterization is local and is conditioned on the transmitter location. The analysis generalizes the results of [17] to inhomogeneous wireless networks. In particular, we extend in Lemmas 1 and 2 obtained in Sections IV and V of [17], respectively.

1) Randomly Selected Receiver: Hereafter we provide two lemmas to characterize the distribution of the SIR given a random selection strategy.

Lemma 1 (SIR Distribution in Generic Fading Channels): Let $\mathbf{x}_k\in\Pi_{\mathrm{rx}}$ be the location of the receiver randomly selected by the transmitter at $\boldsymbol{x}_j$ according to the spatial PDF in (7). The cumulative distribution function (CDF) of the SIR $\mathsf{z}_{j,k}$ is found to be

$$F_{\mathsf{z}_{j,k}}(z)=\frac{1}{2}+\frac{1}{\pi}\int_0^\infty\Re\Big\{\frac{\psi_{\mathsf{g}_{j,k}}(\jmath\omega)}{\jmath\omega}\Big\}d\omega \quad (15a)$$

$$\psi_{\mathsf{g}_{j,k}}(\jmath\omega)=\psi_{\mathsf{h}_{j,k}}(\jmath\omega)\mathbb{E}_{\mathbf{x}_k}\Big\{\psi_{\mathsf{i}_{j,k}|\mathbf{x}_k}\left(-\jmath\omega\mathsf{r}_{j,k}^{2b}z\right)\Big\} \quad (15b)$$

where $\mathsf{g}_{j,k}\triangleq\mathsf{h}_{j,k}-z\mathsf{r}_{j,k}^{2b}\mathsf{i}_{j,k}$ and $\psi_{\mathsf{i}_{j,k}|\mathbf{x}_k}(\cdot)$ is given by (5).

Proof: The proof follows directly from the Gil-Pelaez inversion theorem [67] and the independence between the channel gain and the interference. The steps of the proof are similar to those in Sections IV-A1, IV-A2, and Appendix B of [17], except for the generalization

$$\mathbb{E}_{\mathsf{r}_{j,k}}\left\{\psi_{\mathsf{i}_{j,k}}\left(-\jmath\omega\mathsf{r}_{j,k}^{2b}z\right)\right\}=\mathbb{E}_{\mathbf{x}_k}\left\{\psi_{\mathsf{i}_{j,k}|\mathbf{x}_k}\left(-\jmath\omega\|\boldsymbol{x}_j-\boldsymbol{x}_k\|^{2b}z\right)\right\}. \quad (16)$$

□

Lemma 2 (SIR Distribution in Nakagami-m Fading Channels): For the scenario of Lemma 1 with Nakagami-m fading channels, the CDF of $\mathsf{z}_{j,k}$ found to be

$$F_{\mathsf{z}_{j,k}}(z)=1-\sum_{i=0}^{m-1}\frac{(-1)^i}{i!}\left[\frac{d^{(i)}}{ds^i}\mathbb{E}_{\mathbf{x}_k}\Big\{\mathcal{L}_{\mathsf{i}_{j,k}|\mathbf{x}_k}\left(s\,m\,r_{j,k}^{2b}z\right)\Big\}\right]_{s=1} \quad (17)$$

where $s\in\mathbb{C}$, and $\mathcal{L}_{\mathsf{i}_{j,k}|\mathbf{x}_k}(\cdot)$ is the conditional Laplace transform of the interference obtained from (5) with[5]

$$\mathcal{L}_{\mathsf{i}}(s)=\psi_{\mathsf{i}}(\jmath\omega)\big|_{\jmath\omega=-s}. \quad (18)$$

Proof: The proof follows directly by considering the exponential distribution of the channel gain, which allows to use the Laplace transform of the interference. The steps of the proof are similar to those in Section V-A and Appendix D of [17]. □

Note from (15b) and (17) that the key step for the evaluation of the SIR distribution is the marginalization of the conditional CF (or Laplace transform) of the aggregate interference, i.e., $\psi_{\mathsf{i}_{j,k}|\mathbf{x}_k}(\cdot)$ (or $\mathcal{L}_{\mathsf{i}_{j,k}|\mathbf{x}_k}(\cdot)$), over the distribution of the receiver location $\mathbf{x}_k$.

2) Maximum SIR Legitimate Receiver: Based on the results shown in Section IV-A.1, the following three results (i.e., Theorem 1 and Corollaries 1 and 2) are provided to obtain the CDF of the SIR when the maximum SIR receiver selection strategy is adopted by transmitters. Three different network scenarios will be taken into account. In particular, Theorem 1 concerns the analysis of the FIN, Corollary 1 analyzes the FHN as a special case of the FIN and recalls results from [17], while Corollary 2 gives a formulation for PINs. Furthermore, Case Study 1 is presented to provide insights from our findings.

[5]Note that the Laplace transform and the CF of the aggregate interference are both defined from the probability generating functional [66].

Consider an LT at $\boldsymbol{x}_j$ and all the LRs with index set $\mathcal{R}_j$ in a bounded set $\mathcal{A}_{\mathcal{R}_j} \subset \mathbb{R}^d$. The location of the maximum SIR receiver is $\mathsf{x}_{\breve{k}} \in \Pi_{\text{rx}}$ where $\breve{k} \triangleq \arg\max_{k\in\mathcal{R}_j}\{\mathsf{z}_{j,k}\}$.

Theorem 1 (FIN: SIR Distribution for Maximum SIR Receiver): Let the LTN and the LRN be described by the IPPPs Π_{tx} and Π_{rx} in $\mathcal{A} \in \mathbb{R}^2$ with intensity functions $\lambda_{\text{tx}}(\boldsymbol{x})$ and $\lambda_{\text{rx}}(\boldsymbol{x})$, respectively. The CDF of the SIR at $\mathsf{x}_{\breve{k}}$ when $\boldsymbol{x}_j$ is the location of the considered transmitter, i.e., $\mathsf{z}_{j,\breve{k}} \triangleq \max_{k\in\mathcal{R}_j}\{\mathsf{z}_{j,k}\}$, is found to be

$$F_{\mathsf{z}_{j,\breve{k}}}(z) = \exp\left\{\left(F_{\mathsf{z}_{j,k}}(z) - 1\right)\Lambda_{\text{rx}}(\mathcal{A}_{\mathcal{R}_j})\right\} \tag{19}$$

where $F_{\mathsf{z}_{j,k}}(z)$ is the CDF of the SIR of a generic link obtained by Lemma 1 and 2 for generic and Nakagami-m fading, respectively.

Proof: The proof is given in Appendix I. □

Corollary 1 (FHN: SIR Distribution for Maximum SIR Receiver): Let the LTN and the LRN be described by the HPPPs Π_{tx} and Π_{rx} in $\mathcal{A} \subseteq \mathbb{R}^2$ with intensities λ_{tx} and λ_{rx}, respectively. Let $\mathcal{A}_{\mathcal{R}_j}$ be a circular region centered in $\boldsymbol{x}_j$ with radius r_{M} in which the LRs are located. The CDF of $\mathsf{z}_{j,\breve{k}}$ is found to be as in (19) with $\Lambda_{\text{rx}}(\mathcal{A}_{\mathcal{R}_j}) = \pi r_{\text{M}}^2\lambda_{\text{rx}}$, where $F_{\mathsf{z}_{j,k}}(z)$ is defined in (15), $\mathsf{i}_{j,k}$ is a skewed stable RV with a CF given by (11b), and $\mathsf{r}_{j,k}^2 \sim \mathcal{U}(0, r_{\text{M}}^2]$.

Proof: The proof is given in Appendix II. □

Corollary 2 (PIN: SIR Distribution for Maximum SIR Receiver): Let the LTN and the LRN be described by the IPPP Π_{tx} in $\mathcal{A} \subseteq \mathbb{R}^2$ with intensity function $\lambda_{\text{tx}}(\boldsymbol{x})$, and the HPPP Π_{rx} with intensity λ_{rx}, respectively. The CDF of $\mathsf{z}_{j,\breve{k}}$ is found to be as in (19) with $\Lambda_{\text{rx}}(\mathcal{A}_{\mathcal{R}_j}) = \pi r_{\text{M}}^2\lambda_{\text{rx}}$, where $F_{\mathsf{z}_{j,k}}(z)$ is defined in (15) and

$$\psi_{\mathsf{g}_{j,k}}(\jmath\omega) = \psi_{\mathsf{h}_{j,k}}(\jmath\omega) \times \mathbb{E}_{\mathsf{r}_{j,k}}\mathbb{E}_{\Theta_{j,k}}\left\{\psi_{\mathsf{i}_{j,k}|\mathsf{r}_{j,k},\Theta_{j,k}}\left(-\jmath\omega\mathsf{r}_{j,k}^{2b}z\right)\right\} \tag{20}$$

where $\psi_{\mathsf{i}_{j,k}|\mathsf{r}_{j,k},\Theta_{j,k}}(\jmath\omega)$ is given by (10), $\mathsf{r}_{j,k}^2 \sim \mathcal{U}(0, r_{\text{M}}^2]$, and $\Theta_{j,k} \sim \mathcal{U}(0, 2\pi]$.

Proof: The proof is given in Appendix III. □

Case Study 1: Consider the PIN setting of Corollary 2, in a Nakagami-m fading channel with mean power Ω. Consider also a LTN with a Gaussian[6] intensity function centered in the origin of a coordinate system (see Fig. 2(a)) with variance σ^2 on each axis, i.e.,

$$\lambda_{\text{tx}}(\boldsymbol{x}) = \frac{\Lambda_{\text{tx}}(\mathcal{A})}{2\pi\sigma^2}e^{-\frac{u^2+v^2}{2\sigma^2}}. \tag{21}$$

The CDF of $\mathsf{z}_{j,\breve{k}}$ is found to be as in (19) with $\Lambda_{\text{rx}}(\mathcal{A}_{\mathcal{R}_j}) = \pi r_{\text{M}}^2\lambda_{\text{rx}}$, and

$$F_{\mathsf{z}_{j,k}}(z) = 1 - \sum_{i=0}^{m-1}\frac{(-1)^i}{i!} \times \left[\frac{d^{(i)}}{ds^i}\mathbb{E}_{\mathsf{r}_{j,k}}\mathbb{E}_{\Theta_{j,k}}\left\{\mathcal{L}_{\mathsf{i}_{j,k}|\mathsf{r}_{j,k},\Theta_{j,k}}\left(s\,m\mathsf{r}_{j,k}^{2b}z\right)\right\}\right]_{s=1} \tag{22}$$

where $\mathcal{L}_{\mathsf{i}_{j,k}|\mathsf{r}_{j,k},\Theta_{j,k}}\left(s\,mr_{j,k}^{2b}z\right)$ is given by (23) at the bottom of this page, $\Lambda_{\text{ir}}(\mathcal{A})$ is obtained by (1) and (2a), $\mathsf{r}_{j,k}^2 \sim \mathcal{U}(0, r_{\text{M}}^2]$, and $\Theta_{j,k} \sim \mathcal{U}(0, 2\pi]$.

Proof: Case Study 1 is a special case of Corollary 2 with a Gaussian intensity function and Nakagami-m fading. The derivation of (22) is obtained from Lemma 2 instead of Lemma 1. Eq. (10) is rearranged taking into account (18), (21), and the Laplace transform of the channel gain in Nakagami-m fading, i.e., $\mathcal{L}_{\mathsf{h}}(s) = \left(\frac{m}{\Omega\, s+m}\right)^m$, thus resulting in (23). □

3) k^{th} Closest Receiver: Consider all the selectable LRs $k = 1, 2, \ldots, \mathsf{n}(\mathcal{A}_{\mathcal{R}_j})$ of the transmitter at $\boldsymbol{x}_j$ and the orderly index set of the LRs $\{(k)\}$ where the ordering is based on distances, i.e., $\mathsf{r}_{j,(k)} \leq \mathsf{r}_{j,(k+1)}$ for all k. When the k^{th} closest LR is selected, i.e., $\breve{k} = (k)$, the following result holds.

Theorem 2 (FIN: SIR Distribution for the k^{th} Closest Receiver): In the FIN setting of Theorem 1, the CDF of the SIR between $\boldsymbol{x}_j$ and its k^{th} closest receiver at $\mathsf{x}_{(k)}$, i.e., $\mathsf{z}_{j,(k)}$, is found to be (15) with $k = (k)$,[7] and

$$\psi_{\mathsf{g}_{j,(k)}}(\jmath\omega) = \psi_{\mathsf{h}_{j,(k)}}(\jmath\omega) \times\mathbb{E}_{\mathsf{r}_{j,(k)}}\left\{\mathbb{E}_{\Theta_{j,(k)}|\mathsf{r}_{j,(k)}}\left\{\psi_{\mathsf{i}_{j,(k)}|\mathsf{r}_{j,(k)},\Theta_{j,(k)}}\left(-\jmath\omega r_{j,(k)}^{2b}z\right)\right\}\right\} \tag{24}$$

where $\psi_{\mathsf{i}_{j,(k)}|\mathsf{r}_{j,(k)},\Theta_{j,(k)}}(\jmath\omega)$ is given by (10) with $k = (k)$. The distributions of $\mathsf{r}_{j,(k)}$ ad $\Theta_{j,(k)}$ are derived in (46), (47), and (48).

Proof: Consider Lemma 1 with $k = (k)$ in (15). Before carrying out the expectation as in (15b), let us emphasize that $\mathsf{r}_{j,(k)}$ and $\Theta_{j,(k)}$ are dependent RVs. In fact, if the LRs are inhomogeneous, for a certain value of the distance $\overline{r}_{j,(k)}$, there exists an angular direction $\overline{\theta}_{j,(k)}$ in which the probability of finding the k^{th} closest receiver is maximized, due to the higher intensity, i.e.,

$$\overline{\theta}_{j,(k)} = \arg\max_{\theta\in\mathcal{C}_{j,(k)}}\lambda_{\text{rx}}\left(\overline{r}_{j,(k)}, \theta\right) \tag{25}$$

where $\mathcal{C}_{j,(k)}$ is the the circumference with center $\boldsymbol{x}_j$ and radius $\overline{r}_{j,(k)}$. Considering $k = (k)$, (15b) can be rearranged by the chain rule of conditional expectation to obtain (24); then (10) is plugged in with (k) in place of k. □

Corollary 3 (FHN: SIR Distribution for the k^{th} Closest Receiver): In the FHN setting of Corollary 1, the CDF of $\mathsf{z}_{j,(k)}$ is found to be as in (15) where $k = (k)$, $\mathsf{i}_{j,(k)}$ is a skewed

[6]This intensity function can be interpreted as a bivariate Gaussian PDF with same variance on the two jointly Gaussian components (see [68]), weighted by $\Lambda_{\text{tx}}(\mathcal{A})$.

[7]In the rest of the subsection, whenever we refer to an equation involving the index k of a generic receiver, the reader should substitute it with (k) for the case of the k^{th} closest receiver.

$$\mathcal{L}_{\mathsf{i}_{j,k}|\mathsf{r}_{j,k},\Theta_{j,k}}(s\,m\,r_{j,k}^{2b}z) = \exp\left\{-\int_{\mathcal{A}}\left(1 - \left(\frac{\left((u-u_j-r_{j,k}\cos\theta_{j,k})^2+(v-v_j-r_{j,k}\sin\theta_{j,k})^2\right)^b}{\Omega\, s\, {r_{j,k}}^{2b}z+((u-u_j-r_{j,k}\cos\theta_{j,k})^2+(v-v_j-r_{j,k}\sin\theta_{j,k})^2)^b}\right)^m\right)\frac{\Lambda_{\text{ir}}(\mathcal{A})}{2\pi\sigma^2}e^{-\frac{u^2+v^2}{2\sigma^2}}dudv\right\} \tag{23}$$

stable RV with CF given by (11b) except for the replacement $k=(k)$, and $\mathsf{r}^2_{j,(k)}$ is an Erlang distributed RV [69]–[71] with CF given by

$$\psi_{\mathsf{r}^2_{j,(k)}}(\jmath\omega)=\left(1-\frac{\jmath\omega}{\pi\lambda_{\mathrm{rx}}}\right)^{-k}. \tag{26}$$

Proof: Consider (15b) with $k=(k)$. Since transmitter and receiver locations are modeled according to HPPPs over the set $\mathcal{A}$, the aggregate interference CF is given by (11b) where $k=(k)$. Furthermore, the squared distance $\mathsf{r}^2_{j,(k)}$ between $\boldsymbol{x}_j$ and its k^{th} closest receiver at $\mathbf{x}_{(k)}$ is an Erlang RV with CF defined in (26). □

Corollary 4 (PIN: SIR Distribution for the k^{th} Closest Receiver): Consider the PIN setting as in Corollary 2. The CDF of $\mathsf{z}_{j,(k)}$ is given by (10), (15a), and (20) with $k=(k)$; where $\mathsf{r}^2_{j,(k)}$ is Erlang distributed with CF given by (26); and $\theta_{j,(k)}\sim\mathcal{U}(0,2\pi]$.

Proof: The proof directly follows from that of Corollary 2 by substituting (k) for k and by considering the Erlang distribution for the square distance $\mathsf{r}^2_{j,(k)}$. □

Case Study 2: Consider the scenario in Case Study 1 but with the k^{th} closest receiver selection strategy. The CDF of $\mathsf{z}_{j,(k)}$ is found to be

$$F_{\mathsf{z}_{j,(k)}}(z)=1-\sum_{i=0}^{m-1}\frac{(-1)^i}{i!}\times\left[\frac{d^{(i)}}{ds^i}\mathbb{E}_{\mathsf{r}_{j,(k)}}\mathbb{E}_{\theta_{j,(k)}}\left\{\mathcal{L}_{\mathsf{i}_{j,(k)}|\mathsf{r}_{j,(k)},\theta_{j,(k)}}\left(s\,mr^{2b}_{j,(k)}z\right)\right\}\right]_{s=1} \tag{27}$$

where $\mathcal{L}_{\mathsf{i}_{j,(k)}|\mathsf{r}_{j,(k)},\theta_{j,(k)}}\left(s\,mr^{2b}_{j,(k)}z\right)$ is obtained in (23) with $k=(k)$, $\mathsf{r}^2_{j,(k)}$ is an Erlang distributed RV with CF defined in (26), and $\theta_{j,(k)}\sim\mathcal{U}(0,2\pi]$.

Proof: Case Study 2 is a special case of Corollary 4 with Gaussian intensity function and Nakagami-m fading. The derivation of (27) is obtained from Lemma 2. □

B. SIR in the Eavesdropping Network

The framework for the characterization of the SIR in the eavesdropping network follows that derived for the legitimate network. The main difference comes from the assumption of considering a population of IIs that help the legitimate network in enhancing the level of information confidentiality. In particular, IIs know the positions of LRs and have the capability of nulling the transmission power emitted in the directions of such receivers, effectively deteriorating only the reception of the ERN. Specifically, either IIs are equipped with multiple antennas and, hence, can perform null-steering beamforming or interference alignment [38] at the LRs' locations, or multiple IIs with a single antenna cooperate to mimic multiantenna jammers [25].

In Section VII, we also show scenarios in which IIs are inactive and, hence, the eavesdropping channels are as much impaired as the legitimate ones. Practical techniques to impair eavesdropping channels can be found in [25], [26], [28], [29], [31], [32], and [34]–[38]. All results of Section IV-A.2 hold also for the eavesdropping link, where the interferers of the ERN are modeled by the PPP Π_{ie} with intensity function $\lambda_{\mathsf{ie}}(\boldsymbol{x})$ obtained by (2b), which accounts for the capability of the ERs of mitigating the interference from the LTN and the IIN by the parameters β_{te} and β_{je}, respectively. The eavesdropping link consists of the transmitter at $\boldsymbol{x}_j$ and the receiver at $\mathbf{x}_i\in\Pi_{\mathsf{ex}}$. Recall that the secrecy performance is determined by the ER with maximum SIR. The results of Section IV-A.2 are used, specifically with ER index $\check{l}\in\mathcal{E}_j$ such that $\mathsf{z}_{j,\check{l}}\triangleq\max_{i\in\mathcal{E}_j}\{\mathsf{z}_{j,l}\}$ in place of the selected receiver with index $\bar{k}$.

V. Network Secrecy Metrics

This section defines the secrecy metrics for inhomogeneous networks based on the framework developed in Section IV for the received SIR characterization. The aggregate interference can dramatically change among different locations of the network, depending on the panorama of interferers at the considered point. Hence, we first introduce local secrecy metric, then we define global metrics to summarize the overall network performance.

A. Maximum Secrecy Rate

In Section III-A of [17], the maximum secrecy rate, (MSR) is defined for scenarios with interference generated by a homogeneous network, when receivers treat interference as noise. Recall the conditional MSR $\varphi_{j,\bar{k},\check{l}}$, which is the maximum transmission rate that a transmitter can employ remaining in the condition of perfect secrecy [15], [16]. The MSR of the link consisting of the LT, the selected LR and the ER at $\boldsymbol{x}_j$, $\boldsymbol{x}_{\bar{k}}$, and $\boldsymbol{x}_{\check{l}}$, respectively, is determined by the most capable ER (i.e., the one with highest SIR) with index $\check{l}\triangleq\arg\max_{i\in\mathcal{E}_j}\{\mathsf{z}_{j,l}\}$. The conditional MSR is given by

$$\varphi_{j,\bar{k},\check{l}}=\left[c(\mathsf{z}_{j,\bar{k}})-c(\mathsf{z}_{j,\check{l}})\right]^+ \tag{28}$$

and it is measured in confidential information bits per second per Hertz, i.e., [cib/s/Hz], where $c(z)\triangleq\log_2(1+z)$ [bit/s/Hz] is the capacity of the Gaussian wireless-tap channel, $\mathsf{z}_{j,\bar{k}}$ is the SIR at the selected receiver, $\mathsf{z}_{j,\check{l}}$ is the SIR at the ER with maximum SIR, and $[\cdot]^+$ provides the greater between its argument and zero. Hence, the local maximum secrecy rate, (LMSR) is defined as the average MSR of a link originated in $\boldsymbol{x}_j$ over channel gains and point configurations, i.e.,

$$R_j\triangleq\mathbb{E}^{!j}\{\varphi_{j,\bar{k},\check{l}}\}. \tag{29}$$

where $\mathbb{E}^{!j}\{\cdot\}$ denotes the reduced Palm expectation conditional on the intended transmitter at $\boldsymbol{x}_j$. Such expectation is taken over all point configurations having the intended transmitter at $\boldsymbol{x}_j$, removing it from the point sequence (c.f. [66]). Consider $\mathsf{z}_{j,\bar{k}}$ and $\mathsf{z}_{j,\check{l}}$ to be independent.[8] The expectation in (29) is computed over all possible values of the SIR as

$$R_j=\int_0^\infty c(z_2)F_{\mathsf{z}_{j,\check{l}}}(z_2)f_{\mathsf{z}_{j,\bar{k}}}(z_2)dz_2-\int_0^\infty\int_0^{z_2}c(z_1)f_{\mathsf{z}_{j,\check{l}}}(z_1)f_{\mathsf{z}_{j,\bar{k}}}(z_2)dz_1dz_2\,. \tag{30}$$

[8]The approximation that neglect the spatial correlation of the interference has been shown to be good in [17] (see Fig. 3)

Remark 1: R_j represents the average MSR of a link with the LT located in $\boldsymbol{x}_j$. Hence, it is a metric that describes secrecy performance from the single link perspective, which is particularly useful for link design.

It is also worth defining a metric to describe the secrecy performance from the network perspective. The local network secrecy rate density, (LNSRD) is defined as

$$\rho_j(\boldsymbol{x}_j) \triangleq \lambda_{\text{tx}}(\boldsymbol{x}_j) R_j \tag{31}$$

for all $\boldsymbol{x}_j \in \mathcal{A}$ and measured in [cib/s/Hz/m^2]. Note that such a metric is a density, as it is weighted for the intensity function of transmitters at $\boldsymbol{x}_j$, and describe the performance in terms of secrecy rate per unit area. The definition of $\rho_j(\boldsymbol{x}_j)$ highlights the amount of information confidentiality that can be achieved in a certain region. This can be high not only if every single link has a high MSR, but also if that region is densely populated by links with low MSR values.

To describe the overall network performance, we define a global secrecy metric that takes into account all the possible locations of the LT $\boldsymbol{x}_j$. For that purpose, consider the spatial average of R_j as

$$\overline{R} \triangleq \int_{\mathcal{A}} R_j(\boldsymbol{x}) f^{\text{tx}}_{\mathbf{x}_j}(\boldsymbol{x}) d\boldsymbol{x} \tag{32a}$$

$$= \frac{1}{\Lambda_{\text{tx}}(\mathcal{A})} \int_{\mathcal{A}} \rho_j(\boldsymbol{x}) d\boldsymbol{x} \tag{32b}$$

$$= \frac{1}{\Lambda_{\text{tx}}(\mathcal{A})} R_{\text{ns}} \tag{32c}$$

where $f^{\text{tx}}_{\mathbf{x}_j}(\boldsymbol{x}) = \lambda_{\text{tx}}(\boldsymbol{x})/\Lambda_{\text{tx}}(\mathcal{A})$ and (31) are used to obtain (32b). Then, (32b) is used together with (32c) to define the network secrecy rate, (NSR) as

$$R_{\text{ns}} \triangleq \int_{\mathcal{A}} \rho_j(\boldsymbol{x}) d\boldsymbol{x} \tag{33}$$

which is measured in [cib/s/Hz].

Remark 2: Differently from R_j, that is related to a single link, R_{ns} is related to all the links in the set $\mathcal{A}$ and represents the total secrecy rate over $\mathcal{A}$. Furthermore, $\rho_j(\boldsymbol{x}_j)$ represents the pointwise density associated with R_{ns}.

B. Secrecy Throughput Density

An LT cannot achieve the MSR unless it knows the SIRs at the selected receiver and at each ER. It is worth introducing a metric that characterizes the confidential information flowing through legitimate links, which is blind w.r.t. the instantaneous ERs' positions and channels (only stochastic information is assumed). In Sections III-D and III-E of [17], the network secrecy throughput density is defined. We now generalize such a metric to account for inhomogeneous distributions of nodes.

Consider a desired rate of confidential information R_{s} and a maximum tolerable secrecy outage probability, (SOP) $P^{\star}_{\text{so}}$. The LT at $\boldsymbol{x}_j$ transmits the confidential information only if the SIR at the selected receiver is greater than a threshold μ, namely the secrecy protection ratio. Such an event happens with probability $P_{\text{it},j}(\mu) \triangleq \mathbb{P}\left\{\mathsf{z}_{j,\bar{k}} > \mu\right\}$. The secrecy outage event is characterized by the SOP, which is given by

$$P_{\text{so},j}(R_{\text{s}}, \mu) \triangleq \mathbb{P}\left\{c(\mathsf{z}_{j,\check{l}}) > c(\mathsf{z}_{j,\bar{k}}) - R_{\text{s}} | \mathsf{z}_{j,\bar{k}} > \mu\right\} \tag{34a}$$

$$= \frac{1}{1 - F_{\mathsf{z}_{j,\bar{k}}}(\mu)} \times \Big[F_{\mathsf{z}_{j,\bar{k}}}(\mu) F_{\mathsf{z}_{j,\check{l}}}\big(\frac{\mu+1}{2^{R_{\text{s}}}} - 1\big) - F_{\mathsf{z}_{j,\bar{k}}}(\mu) + \int_{\frac{\mu+1}{2^{R_{\text{s}}}+1}}^{\infty} F_{\mathsf{z}_{j,\bar{k}}}(2^{R_{\text{s}}}(1+y) - 1) f_{\mathsf{z}_{j,\check{l}}}(y) dy\Big] \tag{34b}$$

which is obtained from the Bayes rule. Hence, the secrecy protection ratio of the network is set as the most conservative value over the transmitter location $\boldsymbol{x}_j$ that maximize $P_{\text{it},j}(\mu)$ such that $P_{\text{so},j}(R_{\text{s}}, \mu) \leq P^{\star}_{\text{so}}$, i.e.,

$$\mu^{\star} = \max_{\boldsymbol{x}_j \in \mathcal{A}} \Big\{ \arg \max_{\mu \in \mathcal{M}^j} P_{\text{it},j}(\mu) \Big\} \tag{35}$$

which is solved by exhaustive search where $\mathcal{M}^j = \{\mu : P_{\text{so},j}(R_{\text{s}}, \mu) \leq P^{\star}_{\text{so}}\}$. We then define the *local secrecy throughput* (LST) as

$$T_j \triangleq \mathbb{E}^{!j}\{\mathbb{1}_{[\mu^{\star},\infty)}(\mathsf{z}_{j,\bar{k}}) R_{\text{s}}\} \tag{36}$$

that is the average secrecy throughput for a link with the LT located at $\boldsymbol{x}_j$. Then, T_j is determined as

$$T_j = P_{\text{it},j}(\mu^{\star}) R_{\text{s}} \,. \tag{37}$$

To describe the secrecy throughput flowing in the network we define the local network secrecy throughput density, (LNSTD) as

$$\tau_j(\boldsymbol{x}_j) \triangleq \lambda_{\text{tx}}(\boldsymbol{x}_j) T_j \,. \tag{38}$$

Furthermore, in analogy to the NSR, we define the network secrecy throughput, (NST) to describe the overall network performance in terms of total secrecy throughput over a certain area $\mathcal{A}$ as

$$T_{\text{ns}} = \int_{\mathcal{A}} \tau_j(\boldsymbol{x}) d\boldsymbol{x} \,. \tag{39}$$

Remark 3: The local secrecy metrics R_j, T_j, $\rho_j(\boldsymbol{x}_j)$, and $\tau_j(\boldsymbol{x}_j)$ are defined pointwise and describe a surface for all $\boldsymbol{x}_j \in \mathcal{A}$. Global secrecy metrics like R_{ns} and T_{ns} condense the information provided by local metrics in single values that are proportional to the spatial means of R_j and T_j, respectively.

Remark 4: In (31) and (38), the spatial variability of LNSRD and LNSTD are mainly caused by two different effects: 1) direct dependency from $\lambda_{\text{tx}}(\boldsymbol{x}_j)$, and 2) implicit dependency from intensity functions $\lambda_{\text{tx}}(\boldsymbol{x})$, $\lambda_{\text{rx}}(\boldsymbol{x})$, $\lambda_{\text{jx}}(\boldsymbol{x})$, and $\lambda_{\text{ex}}(\boldsymbol{x})$ in R_j and T_j, respectively. Such an implicit dependency is due to the SIRs $\mathsf{z}_{j,\bar{k}}$ and $\mathsf{z}_{j,\check{l}}$, which themselves depend on the point process of the LRs, the point process of ERs, and that of the IIs.

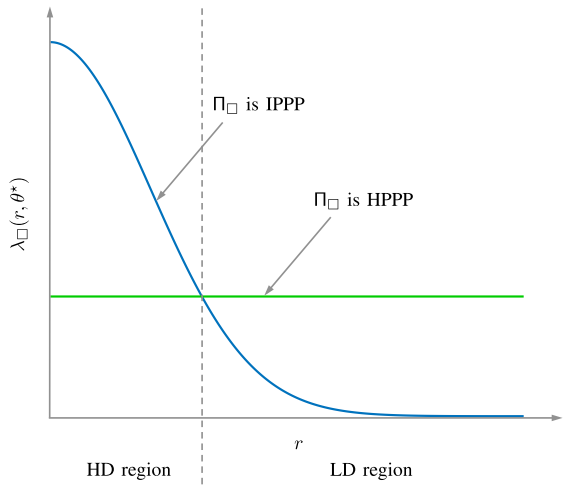


Fig. 3. Half of a section along one direction of the intensity function of $\Pi_\square$ when it is an IPPP and HPPP, respectively, with given measure $\Lambda_\square(\mathcal{A})$ and with $\square = \{\text{tx},\ \text{rx},\ \text{jx},\ \text{ex}\}$. It is divided in the HD and LD region.

VI. Case Studies

Sections III, IV, and V show the influence of intrinsic network properties such as node spatial distribution, wireless channel, and aggregate interference on network secrecy. Section II presents the network model as a superposition of four PPPs, where each of those is described by its intensity function. Inhomogeneities in such functions as well as local imbalances between values of different subnetworks heavily affect the local secrecy level. In this section we introduce and analyze some case studies to explore the inhomogeneous network secrecy performance. In particular, Section VI-A presents the *dense-sparse model* to capture the fundamental effect of a rise and a fall of the node intensity function compared to a constant level, while Section VI-B introduces several case studies where LTs, LRs, ERs, and IIs follow either the dense-sparse or the homogeneous models.

A. The Dense-Sparse Model

Consider a generic PPP in $\mathcal{A} \in \mathbb{R}^2$, i.e., $\Pi_\square$ with measure $\Lambda_\square(\mathcal{A})$ where $\square = \{\text{tx},\ \text{rx},\ \text{jx},\ \text{ex}\}$. The process $\Pi_\square$ can be either an HPPP or IPPP. For the IPPPs we have considered a Gaussian intensity functions centered in the origin with variance σ^2 on each axis (see Fig. 2(a)), hence

$$\lambda_\square(\boldsymbol{x}) = \begin{cases} \dfrac{\Lambda_\square(\mathcal{A})}{2\pi\sigma^2} e^{-\frac{u^2+v^2}{2\sigma^2}} & \text{if } \Pi_\square \text{ is an IPPP} \\ \lambda_\square & \text{if } \Pi_\square \text{ is an HPPP.} \end{cases} \tag{40}$$

For a fair comparison it is necessary that $\mathcal{A}$ and σ^2 are such that $\int_{\mathcal{A}} \frac{1}{2\pi\sigma^2} e^{-\frac{u^2+v^2}{2\sigma^2}} \simeq 1$.

We define the HD region by the surface in which the intensity function of the IPPP is greater than $\lambda_\square$ and the LD region by the surface in which such intensity function is smaller than $\lambda_\square$ (see Fig. 3). The former represents a peak of the node density while the latter represents a hole of the node density. Such a model is particularly adequate in scenarios where nodes are concentrated inside a specific area and tend to rarefy outside of it. Such a situation can occur in various scenarios including vehicular networks, e.g., at the intersection of two streets in an urban area or at the toll booth on a highway; in pedestrian networks, e.g., at a public event or at the traffic light in correspondence of a crosswalk; and in tactic scenario, e.g., a squadron of drones, and so on so forth. More realistic models can be considered to avoid the total rarefaction of the network. For example a superposition of a dense-sparse model with an homogeneous model can effectively represent a scenario with a high concentration of nodes in a specific area, that decrease to a standard uniform concentration. In such a case, the network can be considered as a superposition of point processes with intensity function composed by two parts, i.e., $\lambda_\square(\boldsymbol{x}) = \lambda_\square^{\text{inh.}}(\boldsymbol{x}) + \lambda_\square^{\text{hom.}}$. All the results of this paper directly apply to such a scenario.

B. Network Scenarios

While HPPPs are usually compared on a theoretically infinite surface by means of their intensity (nodes per square meter in a two dimension area), a fair comparison between IPPPs with different intensity functions can be carried out by considering their intensity measures over a bounded region $\mathcal{A}$. Hence we will consider different scenarios where each subnetwork follows the dense-sparse model. Then, we refer the intensity measures of the four subnetworks to that of an HPPP with intensity λ_{h} such that

$$\Lambda_{\text{tx}}(\mathcal{A}) = \alpha_1 \Lambda_{\text{h}}(\mathcal{A}) \tag{41a}$$
$$\Lambda_{\text{rx}}(\mathcal{A}) = (1-\alpha_1)\Lambda_{\text{h}}(\mathcal{A}) \tag{41b}$$
$$\Lambda_{\text{ex}}(\mathcal{A}) = \alpha_2 \Lambda_{\text{h}}(\mathcal{A}) \tag{41c}$$
$$\Lambda_{\text{jx}}(\mathcal{A}) = \alpha_3 \Lambda_{\text{h}}(\mathcal{A}) \tag{41d}$$

where $\alpha_1, \alpha_3, \alpha_2 \in [0,1]$ and $\Lambda_{\text{h}}(\mathcal{A}) = \lambda_{\text{h}}|\mathcal{A}|$. Then, we define six case studies describing network scenarios where imbalances between the spatial distributions of the LTN, LRN, ERN, and IIN are considered. We introduce some specific terminology to refer to the considered scenarios: the first specification (smart/non smart) refers to the LTN and LRN, whereas the second specification (informed/non-informed) to the ERN and IIN. In particular, the following case studies have been analyzed:

- smart informed, (SI): all PPPs are inhomogeneous;
- smart non-informed, (SNI): inhomogeneous LTN and LRN, homogeneous ERN and IIN;
- non-smart informed, (NSI): homogeneous LTN and LRN, inhomogeneous ERN and IIN;
- non-smart non-informed, (NSNI): all PPPs are homogeneous.

In addition, two hybrid scenarios have been considered; they will be referred to as follows:

- hybrid network scenario 1, (HNS1): inhomogeneous LTN and IIN, homogeneous LRN and ERN;
- hybrid network scenario 2, (HNS2): inhomogeneous IIN, homogeneous LTN, LRN, and ERN.

For each of the six settings above, the specification on the receiver selection strategy is also given (i.e., maximum SIR, (MS) or k^{th} closest, (KC)).

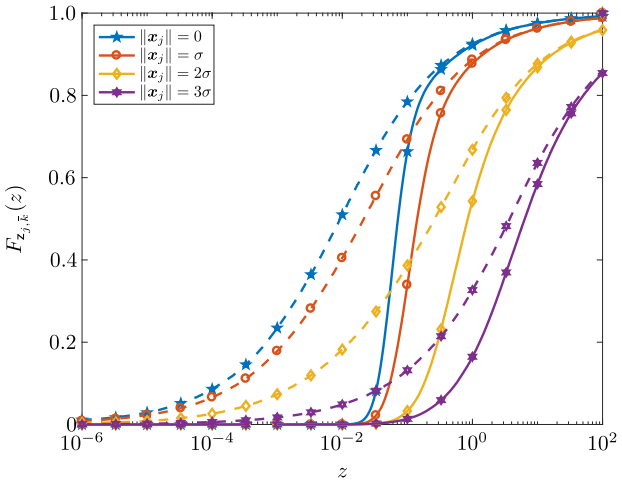


Fig. 4. $F_{\mathsf{z}_{j,\bar{k}}}(z)$ for various transmitter locations and receiver selection strategies with $\lambda_{\text{rx}} = 0.5$ [node/m^2]: maximum SIR (continuous lines) and closest (dashed lines). Theoretical results are displayed by lines and simulations by markers.

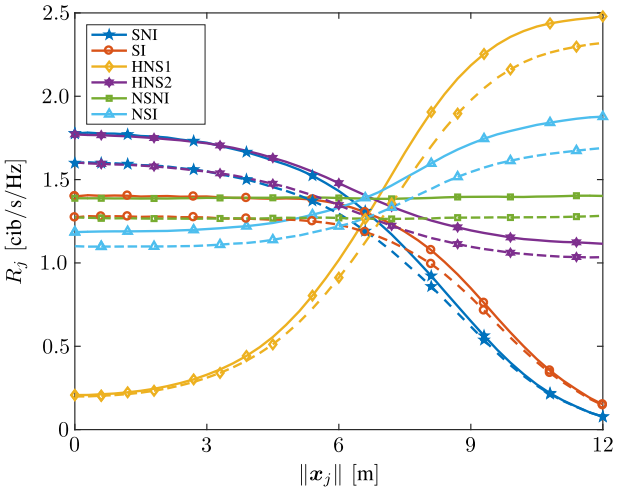


Fig. 5. LMSR as a function of the location of the LT (distance from the origin $\|\boldsymbol{x}_j\|$) with $\alpha_1 = \alpha_2 = \alpha_3 = 0.5$ and $\lambda_{\text{h}} = 1$ [node/m^2].

VII. Numerical Results

This section provides results based on the framework developed in Sections III, IV, and V. In the first part, we verify by simulations the analytical distribution of the SIR at the selected receiver. In the second part, we explore the spatial behavior of local secrecy metrics and we provide global secrecy metrics for different scenarios.[9]

For IPPPs we have considered Gaussian intensity functions centered at the origin with variance σ^2 on each axes (see Fig. 3). Nodes are randomly deployed in a disk with maximum radius $R_{\max} = 5\sigma = 15$ [m] with $\sigma = 3$ [m], $|\mathcal{A}| \simeq 706$ [m^2], $\Lambda_{\text{h}}(\mathcal{A}) = \lambda_{\text{h}}\pi R_{\max}^2$, and $\Lambda_{\square}(\mathcal{A})$ given by (41) for $\square = \{\text{tx}, \text{rx}, \text{jx}, \text{ex}\}$. The LTs operate with receiver selection according to two different modes: the MS and the KC with $k = 1$ in a Rayleigh ($m = 1$) fading channel with $b = 2$ and unit mean $\Omega = 1$.

A. CDF of the Received SIR

Fig. 4 shows the CDF $F_{\mathsf{z}_{j,\check{k}}}(z)$ of the received SIR at the MS receiver (continuous lines) and at the KC receiver (dashed lines) conditional to different locations of the considered transmitter (different markers correspond to different locations of the considered LT). A PIN has been considered. It can be observed that analytical results (lines) and simulations (markers) are in very good agreement.

B. Secrecy Metrics Analysis

1) Intrinsic Secrecy Performance: Fig. 5 shows the LMSR R_j as a function of the distance of the considered LT from the origin, i.e., $\|\boldsymbol{x}_j\|$, for different receiver selection strategies (solid and dashed lines for MS and KC selections, respectively), different network scenarios (different markers), and interferers intensities obtained by (2) with the IES defined by $\beta_{\text{tr}} = 1$, $\beta_{\text{jr}} = 0$, $\beta_{\text{te}} = 1$, $\beta_{\text{je}} = 1$. Let us remind the structure of the conditional MSR of a link with the LT at $\boldsymbol{x}_j$, i.e.,

$$\varphi_{j,\bar{k},\check{l}} = \left[\log\left\{1 + \mathsf{h}_{j,\bar{k}}\left[\sum_{\mathbf{x}_q \in \Pi_{\text{ir}}} \mathsf{h}_{q,\bar{k}}\left(\frac{\mathsf{r}_{j,\bar{k}}}{\mathsf{r}_{q,\bar{k}}}\right)^{2b}\right]^{-1}\right\} - \log\left\{1 + \mathsf{h}_{j,\check{l}}\left[\sum_{\mathbf{x}_w \in \Pi_{\text{ie}}} \mathsf{h}_{w,\check{l}}\left(\frac{\mathsf{r}_{j,\check{l}}}{\mathsf{r}_{l,\check{l}}}\right)^{2b}\right]^{-1}\right\}\right]^{+}. \quad (42)$$

Note the behavior of the HNS1 curve, which shows an imbalance between the distribution of LTs (inhomogeneous) and that of LRs (homogeneous). Intuitively, one can expect that the high density of LTs and IIs would lead to a high performance in the HD region. This is not verified due to the fact that both the path loss and the aggregate interference heavily impair the legitimate channels ($\mathsf{r}_{q,\bar{k}}$ for all $\mathbf{x}_q \in \Pi_{\text{ir}}$, i.e., the distances between interferers and the selected receiver by $\boldsymbol{x}_j$, are much lower than $\mathsf{r}_{j,\bar{k}}$ on average due to the massive interferers' density around the selected receiver compared to the limited receivers' availability around the transmitter) thus decreasing the performance in terms of achievable secrecy rate of the link. The performance improves for increasing $\|\boldsymbol{x}_j\|$ because the interference level decreases, i.e., $\mathsf{r}_{q,\bar{k}}$ for all $\mathbf{x}_q \in \Pi_{\text{ir}}$ increases on average with the increase of $\|\boldsymbol{x}_j\|$.

The performance of other scenarios is characterized by the balance between LTs' and LRs' densities. In the HD region, the NSI curve shows the high density of ERs (low $\mathsf{r}_{j,\check{l}}$ and, hence, low path loss), the SI overlaps with the NSNI, and the SNI overlaps with the HNS2, exhibiting the best performance. In the LD region, the NSI curve shows the low density of ERs (high $\mathsf{r}_{j,\check{l}}$ and, hence, high path loss), while the SI's and SNI's performance decays dramatically with the average of the internode distance between source and destination of the legitimate link, i.e., $\mathsf{r}_{j,\bar{k}}$ (inhomogeneous LRN), the NSNI's and HNS2's performance exhibit a floor (the LRN is homogeneous, hence $\mathsf{r}_{j,\bar{k}}$ does not increase arbitrarily, and the effect of path loss is limited).

[9]The results of this paper are complementary to those of [17], in which the effects of different node densities in the overlapping networks are considered for homogeneous settings.

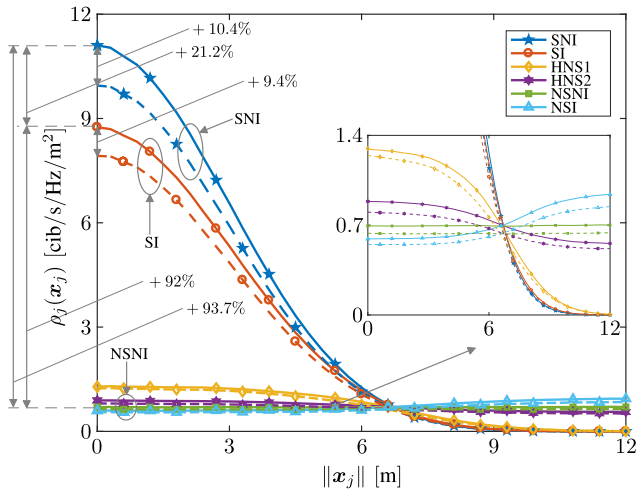


Fig. 6. LNSRD as a function of $\|\boldsymbol{x}_j\|$ with $\alpha_1 = \alpha_2 = \alpha_3 = 0.5$ and $\lambda_{\rm h} = 1$ [node/m^2].

It is worth noting the causes of the overlapping in the HD region of the SI and SNI curves with the NSNI and HNS2 curves, respectively. That is, in the HD region, LTs tends to select nearby LRs, and hence the panoramas of nodes seen from the intended LT and its selected LR are almost the same. Consider the legitimate link, we can think of approximating the aggregate interference with its maximum component, i.e.,

$$\sum_{\mathsf{x}_q \in \Pi_{\rm ir}} \frac{\mathsf{h}_{q,\bar{k}}}{\mathsf{r}_{q,\bar{k}}^{2b}} \simeq \frac{\mathsf{h}_{q^\star,\bar{k}}}{\mathsf{r}_{q^\star,\bar{k}}^{2b}} \tag{43}$$

where $\mathsf{x}_{q^\star} \in \Pi_{\rm ir}$ is the index of the interferer causing the highest received power. The SIR of the legitimate link depends on average by the ratio $\mathsf{r}_{j,\bar{k}}/\mathsf{r}_{q^\star,\bar{k}}$ that is related to the imbalances between the interferers' and receivers' panoramas seen from a transmitter at $\boldsymbol{x}_j$. A similar behavior can be expected for the eavesdropping link.

Remark 5: Consider a FIN and a FHN over a given area $\mathcal{A}$ with the same mean number of nodes $\Lambda_\square(\mathcal{A})$ for $\square = \{\text{tx, rx, jx, ex}\}$. If the subnetworks of the FIN have overlapped intensity profiles, the LMSR of the FIN in the HD region can be approximated by that of the FHN.

Fig. 6 shows the LNSRD $\rho_j(\boldsymbol{x}_j)$ as a function of the distance $\|\boldsymbol{x}_j\|$ of the considered LT from the origin for different receiver selection strategies, various network settings, and an IES capable of nulling the effect of IIs on the LRs, i.e., with interferer intensities obtained by (2) with $\beta_{\rm tr} = 1$, $\beta_{\rm jr} = 0$, $\beta_{\rm te} = 1$, $\beta_{\rm je} = 1$. It can be observed that the curves are obtained by weighting R_j through $\lambda_{\rm tx}(\boldsymbol{x}_j)$. Hence, in the HD region, a low performance of the single link (low LMSR from Fig. 5) can result in an acceptable performance from the network perspective (high LNSRD). This can be justified by the accumulative performance of a high density of links with non-zero secrecy rate, which leads a high LNSRD (see HNS1 curves in Fig. 5 and Fig. 6).

It can also be remarked that the best performance in terms of NSR (see Table II) is obtained when all the legitimate nodes are inhomogeneous (SNI and SI). In fact, in such scenarios the high density of legitimate links (inhomogeneous LTN) carries a multitude of contribution to the NSR; besides that, each contribution is high due to the high availability of receivers (inhomogeneous LRN), which allows each transmitter to select a receiver with a highly reliable channel. In particular a NSR values of 3775.5 and 3080.1 [cib/s/Hz] are obtained on the area $|\mathcal{A}| \simeq 706$ [m^2] in the SNI and SI scenarios, respectively.

TABLE II
NSR [CIB/S/HZ] VALUES IN FIG. 6

Scenario	MS selection	KC selection
SI	3080.1	2806.2
SNI	3775.5	3401.7
NSI	816.3	743.1
NSNI	787.1	718.1
HNS1	813.2	757.2
HNS2	824.6	750

From all the figures it can be observed that the selection of the receiver with maximum SIR instead of the $k^{\rm th}$ closest implies higher confidentiality, especially in more dense regions. For instance the MS selection allows to gain 373.8 [cib/s/Hz] of NSR compared to the KC selection in the SNI scenario (see Table II). Note also that in the SI and SNI settings the decay of performance in LD region is faster compared to the other settings (HNS1, HNS2, and NSNI). HNS2 and NSNI scenarios guarantee a performance floor, thanks to the homogeneity of the LRN.

Table II shows NSR values obtained by integrating numerically (33) for the considered settings. By comparing the NSR values of the smart scenarios (SI and SNI) with the others, and in particular with the one of the full homogeneous scenario (NSNI); a remarkable performance gap can be noticed.

Remark 6: Inhomogeneity together with interference engineering is especially beneficial for network secrecy when transmitters and the receivers of the legitimate network have intensity profiles with similar spatial variations

2) Variability of Spatial Distributions: Fig. 7 shows the LNSRD $\rho_j(\boldsymbol{x}_j)$ as a function of the distance $\|\boldsymbol{x}_j\|$ of the considered LT from the origin in the SI-MS scenario, for different values of the variance of intensity functions of the IPPPs, and with ERs resilient to jamming (e.g., performing interference cancellation on IIs), i.e., with interferer intensities obtained by (2) with the IES defined by $\beta_{\rm tr} = 1$, $\beta_{\rm jr} = 0$, $\beta_{\rm te} = 1$, $\beta_{\rm je} = 0$. It can be observed that node concentration highly influences the achievable secrecy performance in terms of secrecy rate per square meter.

Fig. 8 shows the LNSTD $\tau_j(\boldsymbol{x}_j)$ as a function of the distance $\|\boldsymbol{x}_j\|$ of the considered LT from the origin in the SI-MS scenario, for different values of the parameters α_3 and α_2 defined in (41d) and (41c), respectively. Three cases are compared: the first (blue stars) shows the performance for a small average number of ERs resilient to jamming from IIs ($\lambda_{\rm ie} = \lambda_{\rm tx}$ from (2b) with $\beta_{\rm je} = 0$); the second (red circles) highlights the performance loss as the average number of ER increases; and the third (yellow diamonds) shows the performance improvement obtained while restoring the effectiveness of IIs ($\lambda_{\rm ie} = \lambda_{\rm tx} + \lambda_{\rm jx}$ from (2b) with $\beta_{\rm je} = 1$).

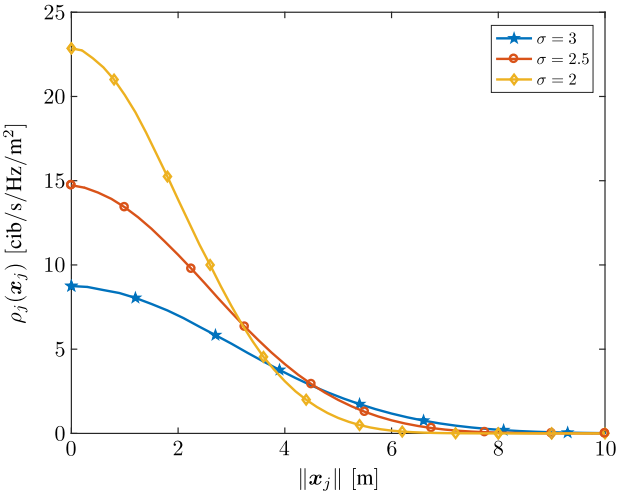


Fig. 7. LNSRD as a function of the location of $\|\boldsymbol{x}_j\|$ in the SI-MS scenario for different variances σ^2 of the intensities of IPPPs with $\beta_{\text{jr}} = \beta_{\text{je}} = 0$, with $\alpha_1 = 0.5$, $\alpha_3 = 0$, $\alpha_2 = 0.1$, and $\lambda_{\text{h}} = 1$ [node/m^2].

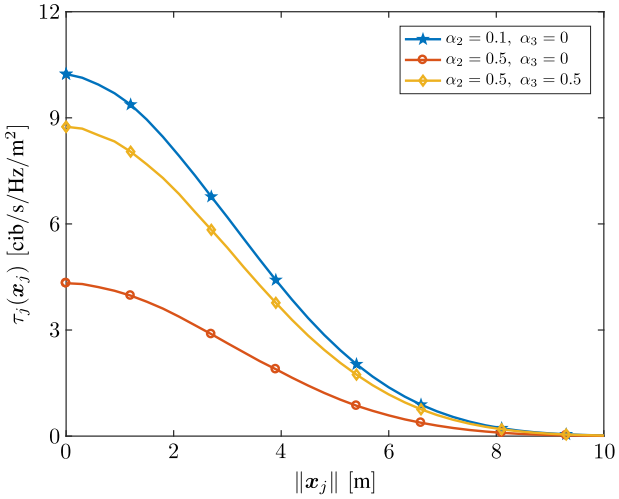


Fig. 8. LNSTD as a function of the location of $\|\boldsymbol{x}_j\|$ in the SI-MS scenario for different network settings in terms of ratios α_3 and α_2, with $\alpha_1 = 0.5$, $\lambda_{\text{h}} = 1$ [node/m^2], $R_{\text{s}} = 4$ [cib/s/Hz], and $P_{\text{so}}^{\star} = 0.1$.

VIII. Final Remark

This paper developed a framework for the design and analysis of inhomogeneous wireless networks with intrinsic secrecy. The aggregate interference and the received SIR have been characterized both in the legitimate and eavesdropping networks with different receiver selection strategies. Local and global secrecy metrics have been introduced for characterizing the level of intrinsic secrecy from a link and a network perspectives. Our findings show that IESs can significantly improve the network secrecy. In particular, for the same average number of nodes in a given area, inhomogeneous networks employing IESs can provide higher level of network secrecy compared to homogeneous ones. It has also been shown that inhomogeneity together with interference engineering is especially beneficial for network secrecy when the transmitters and the receivers of the legitimate network have intensity profiles with similar spatial variations. Finally, assessing the intrinsic secrecy of inhomogeneous networks by homogeneous models may lead to inaccurate conclusions.

Appendix I
Proof of Theorem 1

Let $\mathsf{n}(\mathcal{A}_{\mathcal{R}_j})$ be the number of LRs selectable by $\boldsymbol{x}_j$. The conditional CDF of $\mathsf{z}_{j,\check{k}}$ given $n(\mathcal{A}_{\mathcal{R}_j}) = 0$ is assumed to be $F_{\mathsf{z}_{j,\check{k}}|\mathsf{n}(\mathcal{A}_{\mathcal{R}_j})=0}(z) = 1$. Conversely, if $n(\mathcal{A}_{\mathcal{R}_j}) > 0$ we obtain

$$\begin{aligned} F_{\mathsf{z}_{j,\check{k}}|\mathsf{n}(\mathcal{A}_{\mathcal{R}_j})}(z) &= \mathbb{P}\left\{\mathsf{z}_{j,\check{k}} \le z | \mathsf{n}(\mathcal{A}_{\mathcal{R}_j}) = n(\mathcal{A}_{\mathcal{R}_j})\right\} \\ &= \mathbb{P}\left\{\mathsf{z}_{j,1} \le z, \mathsf{z}_{j,2} \le z, \ldots, \mathsf{z}_{j,n(\mathcal{A}_{\mathcal{R}_j})} \le z\right\} \\ &= \prod_{k=1}^{n(\mathcal{A}_{\mathcal{R}_j})} F_{\mathsf{z}_{j,k}}(z) = \left[F_{\mathsf{z}_{j,k}}(z)\right]^{n(\mathcal{A}_{\mathcal{R}_j})} \end{aligned} \tag{44}$$

where the $\mathsf{z}_{j,k}$ for $k = 1, 2, \ldots, n(\mathcal{A}_{\mathcal{R}_j})$ have been assumed i.i.d. The identical distribution is shown in (15b) and (17) for the generic receiver, while the assumption of independence of SIRs at different locations is verified [17]. Moreover, correlation is higher when the amount of common randomness is high, thus, for massively dense networks, networks with random access, multiple channels, and multiple codes,[10] suffer from low interference correlation [65], [72]. Since $\mathsf{n}(\mathcal{A}_{\mathcal{R}_j})$ is a Poisson RV with intensity measure $\Lambda_{\text{rx}}(\mathcal{A}_{\mathcal{R}_j})$, the CDF of $\mathsf{z}_{j,\check{k}}$ is obtained by the marginalization

$$\begin{aligned} F_{\mathsf{z}_{j,\check{k}}}(z) &= \mathbb{E}_{\mathsf{n}(\mathcal{A}_{\mathcal{R}_j})}\left\{F_{\mathsf{z}_{j,\check{k}}|\mathsf{n}(\mathcal{A}_{\mathcal{R}_j})}(z)\right\} \\ &= e^{-\Lambda_{\text{rx}}(\mathcal{A}_{\mathcal{R}_j})} + \sum_{n=1}^{\infty} e^{-\Lambda_{\text{rx}}(\mathcal{A}_{\mathcal{R}_j})} \frac{\left[\Lambda_{\text{rx}}(\mathcal{A}_{\mathcal{R}_j})\, F_{\mathsf{z}_{j,k}}(z)\right]^n}{n!}. \end{aligned} \tag{45}$$

The proof is then obtained by rearranging terms, also using the definition of the exponential function.

Appendix II
Proof of Corollary 1

The proof follows considering that (19), which holds in the FIN setting, holds also for the FHN where $\Lambda_{\text{rx}}(\mathcal{A}_{\mathcal{R}_j}) = |\mathcal{A}_{\mathcal{R}_j}|\lambda_{\text{rx}} = \pi r_{\text{M}}^2 \lambda_{\text{rx}}$. Since receiver locations are described by an HPPP in $\mathcal{A}_{\mathcal{R}_j}$, the squared distance $\mathsf{r}_{j,k}^2$ between $\boldsymbol{x}_j$ and a generic receiver at $\mathbf{x}_k$ is represented by a uniform RV $\mathcal{U}(0, r_{\text{M}}^2]$. Then recall that the distribution of the aggregate interference for an homogeneous panorama of interferers in $\mathbb{R}^2$ is the same in each point of the network (see (11b)-(12)) [49].

Appendix III
Proof of Corollary 2

Since Corollary 2 is a special case of Theorem 1, (19) directly applies to compute the CDF of $\mathsf{z}_{j,\check{k}}$. Then, when the receivers are characterized by an HPPP, $\mathsf{r}_{j,k}$ and $\theta_{j,k}$ are independent. Therefore (15b) assumes the form of (20). For the homogeneity of receivers $\mathsf{r}_{j,k}^2 \sim \mathcal{U}(0, r_{\text{M}}^2]$ and $\theta_{j,k} \sim \mathcal{U}(0, 2\pi]$.

[10] E.g., in cellular networks where base stations allocate different codes to separate the transmissions of different users during the uplink.

APPENDIX IV
STATISTICAL CHARACTERIZATION OF THE POLAR COORDINATES OF THE k^{th} CLOSEST RECEIVER

Hereafter, the distributions of RVs marginalized in the expectation of (24) are characterized.

1) The PDF of the distance between the LT at $\boldsymbol{x}_j$ and the k^{th} closest receiver is given by

$$f_{\mathsf{r}_{j,(k)}}(r) = \frac{d}{dr} F_{\mathsf{r}_{j,(k)}}(r) = \frac{d}{dr} \left\{ \mathbb{P}\left\{ \mathsf{r}_{j,(k)} \leq r \right\} \right\} \quad (46)$$

where

$$\begin{aligned} \mathbb{P}\left\{ \mathsf{r}_{j,(k)} \leq r \right\} &= 1 - \mathbb{P}\left\{ \mathsf{r}_{j,(k)} > r \right\} \\ &= 1 - \mathbb{P}\left\{ \mathsf{n}_{\text{rx}}(\mathcal{B}_j(r)) \leq k-1 \right\} \quad (47) \end{aligned}$$

and $\mathsf{n}_{\text{rx}}(\mathcal{B}_j(r))$ is a Poisson RV with intensity measure $\Lambda_{\text{rx}}(\mathcal{B}_j(r))$ representing the number of LRs in a ball with radius r and center $\boldsymbol{x}_j$, i.e., $\mathsf{n}_{\text{rx}}(\mathcal{B}_j(r))$ is a Poisson random variable with parameter $\Lambda_{\text{rx}}(\mathcal{B}_j(r))$.

2) The conditional PDF of the angle between the LT $\boldsymbol{x}_j$ and the k^{th} closest receiver given $\mathsf{r}_{j,(k)}$ is defined by

$$f_{\theta_{j,(k)}|\mathsf{r}_{j,(k)}}(\theta) = \frac{\lambda_{\text{rx}}(r_{j,(k)}, \theta)}{\Lambda_{\text{rx}}(\mathcal{C}_{j,(k)})} \quad (48)$$

where $\mathcal{C}_{j,(k)}$ is a circumference centered at $\boldsymbol{x}_j$ with radius $r_{j,(k)}$ and $\Lambda_{\text{rx}}(\mathcal{C}_{j,(k)})$ is the mean number of LRs on $\mathcal{C}_{j,(k)}$.

REFERENCES

[1] K.-D. Kim and P. R. Kumar, "Cyber–physical systems: A perspective at the centennial," *Proc. IEEE*, vol. 100, Special Centennial Issue, pp. 1287–1308, May 2012.

[2] Y. Zhang, G. Li, Q. Du, G. Lyu, and G. Zhang, "High-rate cooperative beamforming for physical-layer security in wireless cyber-physical systems," in *Proc. IEEE Int. Conf. Commun. Workshop*, Jun. 2015, pp. 2622–2626.

[3] K. Ly and Y. Jin, "Security challenges in CPS and IoT: From end-node to the system," in *Proc. IEEE Comput. Soc. Annu. Symp. VLSI*, Pittsburgh, PA, USA, Jul. 2016, pp. 63–68.

[4] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of things: A survey on enabling technologies, protocols, and applications," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 4, pp. 2347–2376, 4th Quart., 2015.

[5] M. R. Palattella *et al.*, "Internet of things in the 5G era: Enablers, architecture, and business models," *IEEE J. Sel. Areas Commun.*, vol. 34, no. 3, pp. 510–527, Mar. 2016.

[6] W. Trappe, R. Howard, and R. S. Moore, "Low-energy security: Limits and opportunities in the Internet of things," *IEEE Security Privacy*, vol. 13, no. 1, pp. 14–21, Jan. 2015.

[7] M. Azees, P. Vijayakumar, and L. J. Deborah, "Comprehensive survey on security services in vehicular ad-hoc networks," *IET Intell. Transp. Syst.*, vol. 10, no. 6, pp. 379–388, 2016.

[8] A. Bazzi, B. M. Masini, and A. Zanella, "Performance analysis of V2V beaconing using LTE in direct mode with full duplex radios," *IEEE Wireless Commun. Lett.*, vol. 4, no. 6, pp. 685–688, Dec. 2015.

[9] K. Zheng, Q. Zheng, P. Chatzimisios, W. Xiang, and Y. Zhou, "Heterogeneous vehicular networking: A survey on architecture, challenges, and solutions," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 4, pp. 2377–2396, 4th Quart., 2015.

[10] Svetonius, *The Lives of the Caesars*, vol. 1, (Translated by J. C. Rolfe), LOEB Classical Library, Ed. Cambridge, MA, USA: Harvard Univ. Press, 1998.

[11] P. A. Regalia, A. Khisti, Y. Liang, and S. Tomasin, "Secure communications via physical-layer and information-theoretic techniques," *Proc. IEEE*, vol. 103, no. 10, pp. 1698–1701, Oct. 2015.

[12] D. Kahn, *The Code-Breakers: The Story of Secret Writing*, Macmillan, Ed. New York, NY, USA: Scribner, 1967.

[13] W. Diffie and M. Hellman, "New directions in cryptography," *IEEE Trans. Inf. Theory*, vol. IT-22, no. 6, pp. 644–654, Nov. 1976.

[14] 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.

[15] C. E. Shannon, "Communication theory of secrecy systems," *Bell Labs Tech. J.*, vol. 28, no. 4, pp. 656–715, Oct. 1949.

[16] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, 1975.

[17] A. Rabbachin, A. Conti, and M. Z. Win, "Wireless network intrinsic secrecy," *IEEE/ACM Trans. Netw.*, vol. 23, no. 1, pp. 56–69, Feb. 2015.

[18] L. Ruan, A. Conti, and M. Z. Win, "Unified interference engineering for wireless information secrecy," *IEEE J. Sel. Areas Commun.*, vol. 36, no. 7, pp. 1579–1592, Jul. 2018.

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

[20] 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.

[21] X. Tang, R. Liu, P. Spasojevic, and H. V. Poor, "Interference assisted secret communication," *IEEE Trans. Inf. Theory*, vol. 57, no. 5, pp. 3153–3167, May 2011.

[22] F. Oggier and B. Hassibi, "The secrecy capacity of the MIMO wiretap channel," *IEEE Trans. Inf. Theory*, vol. 57, no. 8, pp. 4961–4972, Aug. 2011.

[23] 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.

[24] P. C. Pinto, J. 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.

[25] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE Trans. Wireless Commun.*, vol. 7, no. 6, pp. 2180–2189, Jun. 2008.

[26] D. Goeckel *et al.*, "Artificial noise generation from cooperative relays for everlasting secrecy in two-hop wireless networks," *IEEE J. Sel. Areas Commun.*, vol. 29, no. 10, pp. 2067–2076, Dec. 2011.

[27] S. H. Chae, W. Choi, J. H. Lee, and T. Q. S. Quek, "Enhanced secrecy in stochastic wireless networks: Artificial noise with secrecy protected zone," *IEEE Trans. Inf. Forensics Security*, vol. 9, no. 10, pp. 1617–1628, Oct. 2014.

[28] S. A. A. Fakoorian, H. Jafarkhani, and A. L. Swindlehurst, "Secure space-time block coding via artificial noise alignment," in *Proc. Asilomar Conf. Signals, Syst. Comput.*, Nov. 2011, pp. 651–655.

[29] A. Khisti and D. Zhang, "Artificial-noise alignment for secure multicast using multiple antennas," *IEEE Commun. Lett.*, vol. 17, no. 8, pp. 1568–1571, Aug. 2013.

[30] Z. Wang, M. Xiao, M. Skoglund, and H. V. Poor, "Secure degrees of freedom of wireless X networks using artificial noise alignment," *IEEE Trans. Commun.*, vol. 63, no. 7, pp. 2632–2646, Jul. 2015.

[31] J. P. Vilela, M. Bloch, J. Barros, and S. W. McLaughlin, "Wireless secrecy regions with friendly jamming," *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 2, pp. 256–266, Jun. 2011.

[32] R. Zhang, L. Song, Z. Han, B. Jiao, and M. Debbah, "Physical layer security for two way relay communications with friendly jammers," in *Proc. IEEE Global Telecommun. Conf.*, Dec. 2010, pp. 1–6.

[33] P. Siyari, M. Krunz, and D. N. Nguyen, "Friendly jamming in a MIMO wiretap interference network: A nonconvex game approach," *IEEE J. Sel. Areas Commun.*, vol. 35, no. 3, pp. 601–614, Mar. 2017.

[34] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor, "Improving wireless physical layer security via cooperating relays," *IEEE Trans. Signal Process.*, vol. 58, no. 3, pp. 1875–1888, Mar. 2010.

[35] J. Huang and A. L. Swindlehurst, "Cooperative jamming for secure communications in MIMO relay networks," *IEEE Trans. Signal Process.*, vol. 59, no. 10, pp. 4871–4884, Oct. 2011.

[36] J. Li, A. P. Petropulu, and S. Weber, "On cooperative relaying schemes for wireless physical layer security," *IEEE Trans. Signal Process.*, vol. 59, no. 10, pp. 4985–4997, Oct. 2011.

[37] L. Ruan, V. K. N. Lau, and M. Z. Win, "Generalized interference alignment—Part I: Theoretical framework," *IEEE Trans. Signal Process.*, vol. 64, no. 10, pp. 2675–2687, May 2016.

[38] L. Ruan, V. K. N. Lau, and M. Z. Win, "Generalized interference alignment—Part II: Application to wireless secrecy," *IEEE Trans. Signal Process.*, vol. 64, no. 10, pp. 2688–2701, May 2016.

[39] P. C. Pinto, J. 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.

[40] X. Zhou, R. K. Ganti, J. G. Andrews, and A. Hjorungnes, "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.

[41] H. Wang, X. Zhou, and M. C. Reed, "Physical layer security in cellular networks: A stochastic geometry approach," *IEEE Trans. Wireless Commun.*, vol. 12, no. 6, pp. 2776–2787, Jun. 2013.
[42] H.-M. Wang, T.-X. Zheng, J. Yuan, D. Towsley, and M. H. Lee, "Physical layer security in heterogeneous cellular networks," *IEEE Trans. Commun.*, vol. 64, no. 3, pp. 1204–1219, Mar. 2016.
[43] H.-M. Wang and T.-X. Zheng, *Physical Layer Security in Random Cellular Networks*. Singapore: Springer, 2016.
[44] H.-M. Wang, C. Wang, T.-X. Zheng, and T. Q. S. Quek, "Impact of artificial noise on cellular networks: A stochastic geometry approach," *IEEE Trans. Wireless Commun.*, vol. 15, no. 11, pp. 7390–7404, Nov. 2016.
[45] C. Ma *et al.*, "Interference exploitation in D2D-enabled cellular networks: A secrecy perspective," *IEEE Trans. Commun.*, vol. 63, no. 1, pp. 229–242, Jan. 2015.
[46] R. Zhang, X. Cheng, and L. Yang, "Cooperation via spectrum sharing for physical layer security in device-to-device communications underlaying cellular networks," *IEEE Trans. Wireless Commun.*, vol. 15, no. 8, pp. 5651–5663, Aug. 2016.
[47] T.-X. Zheng, H.-M. Wang, Q. Yang, and M. H. Lee, "Safeguarding decentralized wireless networks using full-duplex jamming receivers," *IEEE Trans. Wireless Commun.*, vol. 16, no. 1, pp. 278–292, Jan. 2017.
[48] M. Z. Win, L. Ruan, A. Rabbachin, Y. Shen, and A. Conti, "Multi-tier network secrecy in the ether," *IEEE Commun. Mag.*, vol. 53, no. 6, pp. 28–32, Jun. 2015.
[49] 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.
[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] 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.
[52] H. ElSawy and E. Hossain, "On stochastic geometry modeling of cellular uplink transmission with truncated channel inversion power control," *IEEE Trans. Wireless Commun.*, vol. 13, no. 8, pp. 4454–4469, Aug. 2014.
[53] H. ElSawy, E. Hossain, and M. Haenggi, "Stochastic geometry for modeling, analysis, and design of multi-tier and cognitive cellular wireless networks: A survey," *IEEE Commun. Surveys Tuts.*, vol. 15, no. 3, pp. 996–1019, 3rd Quart., 2013.
[54] H. ElSawy, A. Sultan-Salem, M.-S. Alouini, and M. Z. Win, "Modeling and analysis of cellular networks using stochastic geometry: A tutorial," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 1, pp. 167–203, 1st Quart., 2017.
[55] J. G. Andrews, R. K. Ganti, M. Haenggi, N. Jindal, and S. Weber, "A primer on spatial modeling and analysis in wireless networks," *IEEE Commun. Mag.*, vol. 48, no. 11, pp. 156–163, Nov. 2010.
[56] M. Haenggi, *Stochastic Geometry for Wireless Networks*. Cambridge, U.K.: Cambridge Univ. Press, 2013.
[57] N. Deng, W. Zhou, and M. Haenggi, "The Ginibre point process as a model for wireless networks with repulsion," *IEEE Trans. Wireless Commun.*, vol. 14, no. 1, pp. 107–121, Jan. 2015.
[58] R. K. Ganti and M. Haenggi, "Interference and outage in clustered wireless ad hoc networks," *IEEE Trans. Inf. Theory*, vol. 55, no. 9, pp. 4067–4086, Sep. 2009.
[59] N. Deng, W. Zhou, and M. Haenggi, "Heterogeneous cellular network models with dependence," *IEEE J. Sel. Areas Commun.*, vol. 33, no. 10, pp. 2167–2181, Oct. 2015.
[60] C. Bettstetter, G. Resta, and P. Santi, "The node distribution of the random waypoint mobility model for wireless ad hoc networks," *IEEE Trans. Mobile Comput.*, vol. 2, no. 3, pp. 257–269, Jul. 2003.
[61] Z. Gong and M. Haenggi, "Interference and outage in mobile random networks: Expectation, distribution, and correlation," *IEEE Trans. Mobile Comput.*, vol. 13, no. 2, pp. 337–349, Feb. 2014.
[62] N. Lu, T. H. Luan, M. Wang, X. Shen, and F. Bai, "Capacity and delay analysis for social-proximity urban vehicular networks," in *Proc. IEEE Global Telecommun. Conf. Workshops*, Mar. 2012, pp. 1476–1484.
[63] E. Steinmetz, M. Wildemeersch, T. Q. S. Quek, and H. Wymeersch, "A stochastic geometry model for vehicular communication near intersections," in *Proc. IEEE Globecom Workshops*, Dec. 2015, pp. 1–6.
[64] F. Zabini and A. Conti, "Inhomogeneous Poisson sampling of finite-energy signals with uncertainties in $\mathbb{R}^d$," *IEEE Trans. Signal Process.*, vol. 64, no. 18, pp. 4679–4694, Sep. 2016.
[65] M. Haenggi, "The meta distribution of the SIR in Poisson bipolar and cellular networks," *IEEE Trans. Wireless Commun.*, vol. 15, no. 4, pp. 2577–2589, Apr. 2016.
[66] S. N. Chiu, D. Stoyan, W. S. Kendall, and J. Mecke, *Stochastic Geometry and Its Applications* (Wiley Series in Probability and Statistics), 3rd ed. Hoboken, NJ, USA: Wiley, 2013.
[67] J. Gil-Pelaez, "Note on the inversion theorem," *Biometrika*, vol. 38, nos. 3–4, pp. 481–482, Dec. 1951.
[68] D. P. Bertsekas and J. N. Tsitsiklis, *Introduction to Probability*. Belmont, MA, USA: Athena Scientific, 2008.
[69] H. R. Thompson, "Distribution of distance to Nth neighbour in a population of randomly distributed individuals," *Ecology*, vol. 37, no. 2, pp. 391–394, Apr. 1956.
[70] 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.
[71] D. P. Bertsekas and R. G. Gallager, *Data Networks*, 2nd ed. Upper Saddle River, NJ, USA: Prentice-Hall, 1992.
[72] M. Gharbieh, H. ElSawy, A. Bader, and M.-S. Alouini, "Spatiotemporal stochastic modeling of IoT enabled cellular networks: Scalability and stability analysis," *IEEE Trans. Commun.*, vol. 65, no. 8, pp. 3585–3600, Aug. 2017.

Giovanni Chisci (S'15–M'18) received the Laurea degree in electrical engineering from the University of Florence in 2014, and the Ph.D. degree in information engineering from the University of Ferrara in 2018, where he is currently enrolled as a Postdoctoral Fellow. He was with the Wireless Information and Network Sciences Laboratory at MIT and with the Computer, Electrical and Mathematical Sciences and Engineering Division at KAUST in 2016 and 2018, respectively. His current research topics include theory and algorithm design for intrinsic network secrecy, low–latency networks, and cyber–physical systems.

Andrea Conti (S'99–M'01–SM'11) is a Professor at the University of Ferrara. In the summer of 2001, he was with AT&T Research Laboratories. He is a frequent visitor of LIDS at MIT, where he holds the Research Affiliate appointment. His research encompasses theory and experimentation of wireless systems and networks, including network localization and distributed sensing. He is a recipient of the HTE Puskás Tivadar Medal and of the IEEE Communications Society's Stephen O. Rice Prize. He is a cofounder and elected Secretary of the IEEE Quantum Communications and Information Technology Emerging Technical Subcommittee. He is an elected Fellow of the IET and served as an IEEE Distinguished Lecturer.

Lorenzo Mucchi (M'98–SM'12) is an Associate Professor at the University of Florence. His research interests involve theory and experimentation of wireless systems and networks including physical-layer security, visible light communications, ultra-wideband techniques, and body area networks. He is serving as an Associate Editor of the IEEE COMMUNICATIONS LETTERS and IEEE ACCESS, and he has been Editor-in-Chief for Elsevier Academic Press. He is a member of the European Telecommunications Standard Institute (ETSI) Smart Body Area Network (SmartBAN) group (2013) and team leader of the special task force 511 (2016) "SmartBAN Performance and Coexistence Verification."

Moe Z. Win (S'85–M'87–SM'97–F'04) is a Professor at MIT. Prior to joining MIT, he was with AT&T Research Laboratories and NASA Jet Propulsion Laboratory. His current research topics include network localization and navigation, network interference exploitation, and quantum information science. He received the IEEE Kiyo Tomiyasu Award, the IEEE Eric Sumner Award, the IEEE ComSoc Edwin Armstrong Achievement Award, the International Prize for Communications Cristoforo Colombo, the Copernicus Fellowship and the Laurea Honoris Causa from the Università degli Studi di Ferrara, and the U.S. Presidential Early Career Award for Scientists and Engineers. He is an ISI Highly Cited Researcher. He is serving on the SIAM Diversity Advisory Committee.