MAXIMUM SECRECY RATE IN INHOMOGENEOUS POISSON NETWORKS

*Giovanni Chisci** *Andrea Conti** *Lorenzo Mucchi*† *Moe Z. Win*‡

*ENDIF, University of Ferrara, Ferrara, Italy, e-mail: giovanni.chisci@unife.it, a.conti@ieee.org
†DINFO, University of Florence, Florence, Italy, e-mail: lorenzo.mucchi@unifi.it
‡LIDS, Massachusetts Institute of Technology, Cambridge, Massachusetts, e-mail: moewin@mit.edu

ABSTRACT

The impressive growth of secrecy-sensitive wireless applications calls for methods to complement traditional cryptography. In particular, physical-layer security is attractive to enhance communication confidentiality by exploiting the characteristics of the wireless environment. Recent works on information-theoretic wireless network secrecy have shown how to exploit interference to enhance the level of information confidentiality for node spatial distribution according to a homogeneous Poisson point process. We propose a framework for design and analysis of inhomogeneous Poisson networks with maximum secrecy rate. We determine the effects of the inhomogeneous node spatial distribution on the secrecy metrics, which provide guidelines for network design.

***Index Terms*—** Wireless networks, maximum secrecy rate, inhomogeneous Poisson point process, fading channels.

1. INTRODUCTION

Wireless network secrecy is essential for numerous emerging applications [1]. Due to the broadcast nature of the wireless channel, it is easy for an eavesdropper to intercept the confidential information.

The works of Shannon [2] and Wyner [3] establish the foundation of information-theoretic secrecy. Such works disclose the possibility of transmitting secret information with perfect confidentiality if the transmission rate is below the secrecy capacity of the channel.

Previous works addressing information-theoretic secrecy use stochastic geometry and, in particular, homogeneous Poisson point processes (HPPPs) to model the stochastic network and devise interference engineering strategies (IESs) for enhanced secrecy [4–13]. The IESs enables legitimate users to exploit the network interference to undermine the reception of unwanted listeners.

This research was supported, in part, by the "5×1000" contribution assigned to the University of Ferrara, the Convenzioni ICAD-UNIFE and DINFO-ENDIF, the Copernicus Fellowship, the National Science Foundation under Grant CCF-1525705, and the MIT Institute for Soldier Nanotechnologies.

In scenarios of practical interest, the homogeneous assumption can be unrealistic [14–17]. Other stationary point processes have been used to consider attraction and repulsion between terminals [18–21]. Such point processes enable the analysis at the typical point of the network, but don't reveal the effect of high spatial variability of the node distribution on the local performance.

To analyze the performance of secure networks under more generic setups, we introduce inhomogeneous Poisson networks and analyze the spatial variability of the maximum secrecy rate (MSR), i.e., the maximum information rate that can be sent over a channel without the occurrence of an information leakage. The proposed analysis is based on the interference and signal-to-interference ratio (SIR) characterizations and shows the density of the MSR as a surface on the Euclidean plane rather than evaluating a single value at the typical point. We also define the *network secrecy rate* (NSR) to describe the overall network secrecy.

This paper develops a framework for design of wireless networks with secrecy accounting for 1) inhomogeneous node spatial distribution, 2) the wireless medium, and 3) the aggregate interference. The analysis is corroborated by simulations in different network scenarios.

2. NETWORK MODEL

Consider a finite heterogeneous network composed of the legitimate transmitters (LTs), legitimate receivers (LRs), intentional interferers (IIs), and eavesdropping receivers (ERs). We denote locations on a bounded region $\mathcal{A}$ of the Euclidean plane by $\boldsymbol{x} \in \mathcal{A} \subset \mathbb{R}^2$.

The LTs and the LRs exchange confidential information through the wireless medium and are spatially distributed according to the inhomogeneous Poisson point processes (IPPPs) Π_{tx} and Π_{rx} with intensity functions $\lambda_{\text{tx}}(\boldsymbol{x})$ and $\lambda_{\text{rx}}(\boldsymbol{x})$, respectively. The ERs are malicious nodes that attempt to intercept the confidential information; they are described by the IPPP Π_{ex} with intensity function $\lambda_{\text{ex}}(\boldsymbol{x})$. The IIs introduce additional interference in the network to reduce the listening capability of the ERs and are modeled by the IPPP Π_{jx} with intensity function $\lambda_{\text{jx}}(\boldsymbol{x})$.

For the sake of simpicity, the interferers affecting the LRs and the ERs are described by Π_{ir} and Π_{ie} with intensity functions $\lambda_{\text{ir}}(\boldsymbol{x}) = \lambda_{\text{tx}}(\boldsymbol{x})$ and $\lambda_{\text{ie}}(\boldsymbol{x}) = \lambda_{\text{tx}}(\boldsymbol{x}) + \lambda_{\text{jx}}(\boldsymbol{x})$, respectively. Further explanations on techniques to impair eavesdropping channels without damaging legitimate ones are given in [4, 8, 12].

In the following, we characterize statistically the aggregate interference and the received SIR, in order to analyze the spatial behavior of the MSR of an inhomogeneous network.

3. INTERFERENCE CHARACTERIZATION IN INHOMOGENEOUS POISSON NETWORKS

The stochastic behavior of the aggregate interference in a homogeneous Poisson infinite network is analyzed in [22], where the interference distribution is the same at each location of the network. This section presents the distribution of the aggregate interference in an inhomogeneous Poisson finite network. We conduct an analysis conditional to the legitimate transmitter location $\boldsymbol{x}_j$.

Consider the aggregate interference power at the receiver in $\mathsf{x}_k \in \Pi_{\text{rx}}$ while the LT is located at $\boldsymbol{x}_j \in \mathcal{A}$, i.e.,

$$\mathsf{i}_{j,k} = \sum_{\mathsf{x}_q \in \Pi_{\text{ir}}} \mathsf{h}_{q,k} \mathsf{r}_{j,k}^{-2b} \tag{1}$$

where $\mathsf{h}_{q,k}$ are the Gamma distributed fading power coefficients with mean 1 and shape parameter m, $\mathsf{r}_{q,k} = ||\mathsf{x}_q - \mathsf{x}_k||$ is the Euclidean distance between the nodes at x_q and x_k, the large-scale path loss model is assumed to be r^{-2b} over distance r where b is the amplitude path loss exponent, the reference power is 1 for every transmitting node.

The distribution of the aggregate interference $\mathsf{i}_{j,k}$ is specified by the probability generating functional of a Poisson point process (PPP) [23], which allows to evaluate the Laplace transform of the interference at a given location as

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

where $\mathcal{L}_{\mathsf{h}}(\cdot)$ is the well-known Laplace transform of the channel coefficients. Note that the distribution of the interference is here translation-variant unlike the homogeneous case [22]. In the next section we characterize the received SIR at the selected receiver.

4. STATISTICAL CHARACTERIZATION OF SIR

Consider a system in an interference-limited condition. The performance is driven by the SIR

$$\mathsf{z}_{j,k} = \frac{|\mathsf{h}_{j,k}|^2 \mathsf{r}_{j,k}^{-2b}}{\mathsf{i}_{j,k}} \,. \tag{3}$$

Hereafter we extend the analysis carried out in [13] to inhomogeneous networks.

4.1. Randomly Selected Receiver

In the Nakagami-m fading case, the channel power gain is Gamma distributed. Hence the Laplace transform of the interference can be exploited to evaluate the cumulative distribution function (CDF) of the SIR $\mathsf{z}_{j,k}$. Following steps similar to those of Section V-A and Appendix D in [13], we obtain

$$F_{\mathsf{z}_{j,k}}(z) = 1 - \sum_{l=0}^{m-1} \frac{(-1)^l}{l!} \left[\frac{d^{(l)}}{ds^l} \mathbb{E}_{\mathsf{x}_k}\left\{\mathcal{L}_{\mathsf{i}_{j,k}|\mathsf{x}_k}\left(s\, m\, \mathsf{r}_{j,k}^{2b} z\right)\right\}\right]_{s=1} \tag{4}$$

where $s \in \mathbb{C}$, $\mathcal{L}_{\mathsf{i}_{j,k}|\mathsf{x}_k}(\cdot)$ is computed by (2), the expectation is obtained with respect to (w.r.t.) $f_{\mathsf{x}_k}(\boldsymbol{x}_k) = \lambda_{\text{rx}}(\boldsymbol{x}_k)/\Lambda_{\text{rx}}(\mathcal{A})$ and $\Lambda_{\text{rx}}(\mathcal{A}) = \int_{\mathcal{A}} \lambda_{\text{rx}}(\boldsymbol{x}) d\boldsymbol{x}$ is the intensity measure of Π_{rx} over $\mathcal{A}$. Note that, in general, the integral in (2) cannot be computed in closed form. Hence $F_{\mathsf{z}_{j,k}}(z)$ in (4) must be computed by numerically.

4.2. Maximum SIR Legitimate Receiver

This section analyzes the distribution of the received SIR when the transmitter selects the receiver with the maximum SIR. We account for two network scenarios: the full inhomogeneous network (FIN) and the partial inhomogeneous network (PIN). A case study is also presented.

Consider an LT in $\boldsymbol{x}_j$ that selects the LR with the highest SIR among those in a bounded set $\mathcal{A}_{\mathcal{R}_j} \subset \mathbb{R}^2$. Define $\mathsf{x}_{\breve{k}}$ as the random location of the maximum SIR receiver where $\breve{k} \triangleq \arg \max_{k\,:\,\mathsf{x}_k \in \Pi_{\text{rx}}} \{\mathsf{z}_{j,k}\}$.

4.2.1. Maximum SIR Receiver CDF for the FIN

Let Π_{tx} and Π_{rx} be two IPPPs described by $\lambda_{\text{tx}}(\boldsymbol{x})$ and $\lambda_{\text{rx}}(\boldsymbol{x})$, respectively. Let $\mathsf{n}_{\mathcal{A}_{\mathcal{R}_j}}$ be the number of LRs selectable by $\boldsymbol{x}_j$. If $\mathsf{n}_{\mathcal{A}_{\mathcal{R}_j}} = 0$, the conditional CDF of $\mathsf{z}_{j,\breve{k}}$, i.e., the SIR at the receiver with maximum SIR, is assumed to be $F_{\mathsf{z}_{j,\breve{k}}|\mathsf{n}_{\mathcal{A}_{\mathcal{R}_j}}}(z) = 1$; if $\mathsf{n}_{\mathcal{A}_{\mathcal{R}_j}} > 0$, then such a CDF is

$$F_{\mathsf{z}_{j,\breve{k}}|\mathsf{n}_{\mathcal{A}_{\mathcal{R}_j}}}(z) = \prod_{k=1}^{\mathsf{n}_{\mathcal{A}_{\mathcal{R}_j}}} F_{\mathsf{z}_{j,k}}(z) = \left[F_{\mathsf{z}_{j,k}}(z)\right]^{\mathsf{n}_{\mathcal{A}_{\mathcal{R}_j}}} \,. \tag{5}$$

The unconditional CDF is then obtained by marginalizing (5) w.r.t. the Poisson random variable $\mathsf{n}_{\mathcal{A}_{\mathcal{R}_j}}$ with mean $\Lambda_{\text{rx}}(\mathcal{A}_{\mathcal{R}_j})$ as

$$F_{\mathsf{z}_{j,\breve{k}}}(z) = e^{\left[F_{\mathsf{z}_{j,k}}(z) - 1\right] \Lambda_{\text{rx}}(\mathcal{A}_{\mathcal{R}_j})} . \tag{6}$$

4.2.2. Maximum SIR Receiver CDF for the PIN

Let Π_{tx} and Π_{rx} be an IPPP and an HPPP described by $\lambda_{\text{tx}}(\boldsymbol{x})$ and λ_{rx}, respectively. Consider that the LT selects a receiver in $\mathcal{A}_{\mathcal{R}_j} = \mathcal{B}_{\boldsymbol{x}_j}(r_{\text{M}})$, i.e., a ball in $\mathbb{R}^2$ centered in $\boldsymbol{x}_j$ with maximum radius r_{M}. Hence, the polar coordinates of a generic

$$\mathcal{L}_{\mathsf{i}_{j,k}|\mathsf{r}_{j,k},\boldsymbol{\theta}_{j,k}}(s)=\exp\left\{-\int_{\mathcal{A}}\left(1-\frac{(((u-u_j-r_{j,k}\cos\theta_{j,k})^2+(v-v_j-r_{j,k}\sin\theta_{j,k})^2))^{2b}}{s+(((u-u_j-r_{j,k}\cos\theta_{j,k})^2+(v-v_j-r_{j,k}\sin\theta_{j,k})^2))^{2b}}\right)\frac{\Lambda_{\text{tx}}(\mathcal{A})}{2\pi\sigma^2}e^{-\frac{u^2+v^2}{2\sigma^2}}dudv\right\} \tag{8}$$

receiver w.r.t. the transmitter are independent random variables (RVs) with uniform distribution, i.e., $\mathsf{r}_{j,k}^2 \sim \mathcal{U}(0, r_{\text{M}}^2]$, $\boldsymbol{\theta}_{j,k} \sim \mathcal{U}[0, 2\pi)$. $F_{\mathsf{z}_{j,\breve{k}}}(z)$ is obtained by (6) with $\Lambda_{\text{rx}}(\mathcal{A}_{\mathcal{R}_j}) = \lambda_{\text{rx}}\pi r_{\text{M}}^2$, where $F_{\mathsf{z}_{j,k}}(z)$ is computed following the steps of Section 4.1 and by specializing (4) with $\mathbb{E}_{\mathbf{x}_k}\{\mathcal{L}_{\mathsf{i}_{j,k}|\mathbf{x}_k}(\cdot)\} = \mathbb{E}_{\mathsf{r}_{j,k}}\{\mathbb{E}_{\boldsymbol{\theta}_{j,k}}\{\mathcal{L}_{\mathsf{i}_{j,k}|\mathsf{r}_{j,k},\boldsymbol{\theta}_{j,k}}(\cdot)\}\}$.

4.2.3. Case Study (Gaussian PIN in Rayleigh Fading)

Consider the scenario described in Section 4.2.2 with Rayleigh fading ($m = 1$) and Gaussian intensity function with variance σ^2 on each direction for the IPPP describing the LTs' locations, i.e., $\lambda_{\text{tx}}(\boldsymbol{x}) = \frac{\Lambda_{\text{tx}}(\mathcal{A})}{2\pi\sigma^2}e^{-\frac{u^2+v^2}{2\sigma^2}}$ where u, v are the Cartesian coordinates of $\boldsymbol{x}$. The CDF of $\mathsf{z}_{j,\breve{k}}$ is given by (6) with $\Lambda_{\text{rx}}(\mathcal{A}_{\mathcal{R}_j}) = \lambda_{\text{rx}}\pi r_{\text{M}}^2$ where

$$F_{\mathsf{z}_{j,k}}(z) = 1 - \mathbb{E}_{\mathsf{r}_{j,k}}\left\{\mathbb{E}_{\boldsymbol{\theta}_{j,k}}\left\{\mathcal{L}_{\mathsf{i}_{j,k}|\mathsf{r}_{j,k},\boldsymbol{\theta}_{j,k}}\left(s\, m\mathsf{r}_{j,k}^{2b}z\right)\right\}\right\} \tag{7}$$

where $\mathcal{L}_{\mathsf{i}_{j,k}|\mathsf{r}_{j,k},\boldsymbol{\theta}_{j,k}}(\cdot)$ is given by (8), $\mathsf{r}_{j,k}^2 \sim \mathcal{U}(0, r_{\text{M}}^2]$, and $\boldsymbol{\theta}_{j,k} \sim \mathcal{U}[0, 2\pi)$.

The analysis of the eavesdropping link is analogous to the one of the legitimate link. It is sufficient to substitute Π_{ex}, λ_{ex}, Π_{ie}, and λ_{ie}, for Π_{rx}, λ_{rx}, Π_{ir}, and λ_{ir}, respectively.

5. SECRECY METRICS

This section defines local and global secrecy metrics for inhomogeneous networks in an interference-limited condition.

Recall the definition of the MSR[1] of a link with the LT in $\boldsymbol{x}_j$, conditional on the node locations and the channel realizations [13], and for maximum SIR destination selection as

$$R_{j,\breve{k},\breve{l}} = \left[c(z_{j,\breve{k}}) - c(z_{j,\breve{l}})\right]^+ \tag{9}$$

where $c(z) \triangleq \log_2(1+z)$ [bit/s/Hz] is the conditional capacity with Gaussian signaling and $[\,\cdot\,]^+ \triangleq \max\{\cdot\,, 0\}$.

We define the *local network secrecy rate density* (LNSRD) at $\boldsymbol{x}_j \in \mathcal{A}$ as

$$\rho_j(\boldsymbol{x}_j) \triangleq \lambda_{\text{tx}}(\boldsymbol{x}_j)R_j \tag{10}$$

where $R_j \triangleq \mathbb{E}_j\{R_{j,\breve{k},\breve{l}}\}$ is the average MSR w.r.t. all the channels and point configurations of a link having the LT at $\boldsymbol{x}_j$. The LNSRD is measured in [cib/s/Hz/m^2] and represents the secrecy rate per unit area in $\boldsymbol{x}_j$. The definition makes sense; in fact, the per-link average MSR R_j is weighted by the density of link in $\boldsymbol{x}_j$.

[1]The MSR is measured in measured in [cib/s/Hz] and represent the maximum confidential information rate that can be employed by an LT while satisfying the condition of perfect secrecy [2, 3].

Note that Eq. (10) shows that local variations of LNSRD are due to the direct dependency on $\lambda_{\text{tx}}(\boldsymbol{x}_j)$ and the implicit dependency on intensity functions $\lambda_{\text{tx}}(\boldsymbol{x})$, $\lambda_{\text{rx}}(\boldsymbol{x})$, $\lambda_{\text{jx}}(\boldsymbol{x})$, and $\lambda_{\text{ex}}(\boldsymbol{x})$ through $\mathbb{E}_j\{\cdot\}$.

The expectation $\mathbb{E}_j\{\cdot\}$ is computed over $\mathsf{z}_{j,\breve{k}}$ and $\mathsf{z}_{j,\breve{l}}$, which are assumed as stochastically independent, as

$$R_j = \int_0^\infty c(z_2)F_{\mathsf{z}_{j,\breve{l}}}(z_2)f_{\mathsf{z}_{j,\breve{k}}}(z_2)dz_2 - \int_0^\infty\int_0^{z_2} c(z_1)f_{\mathsf{z}_{j,\breve{l}}}(z_1)f_{\mathsf{z}_{j,\breve{k}}}(z_2)dz_1dz_2\,. \tag{11}$$

Now, let us consider the spatial average of R_j, i.e.,

$$\overline{R} \triangleq \int_{\mathcal{A}} R_j(\boldsymbol{x})f_{\mathbf{x}_j}(\boldsymbol{x})d\boldsymbol{x} = \frac{1}{\Lambda_{\text{tx}}(\mathcal{A})}R_{\text{ns}}\,. \tag{12}$$

The global metric associated with the LNSRD is the NSR

$$R_{\text{ns}} \triangleq \int_{\mathcal{A}} \rho_j(\boldsymbol{x})d\boldsymbol{x} \tag{13}$$

which represents the total secrecy rate over $\mathcal{A}$, is measured in [cib/s/Hz], and is evaluated by its pointwise density $\rho_j(\boldsymbol{x})$.

6. NUMERICAL RESULTS

This section presents numerical results from different network scenarios to reveal the influence of the inhomogeneous spatial distributions on the secrecy metrics as well as to highlight its spatial variations and their driving features.

Consider a circular region $\mathcal{A}$ with maximum radius R_{max}. The four PPPs Π_{tx}, Π_{rx}, Π_{jx}, and Π_{ex} (in this given order) can be homogeneous (H) or inhomogeneous (I) in the following scenarios: IIHH, IIII, IIHI, IHIH, HHIH, HHHH, and HHII. For simplicity, we consider Gaussian intensity functions with variance σ^2 centered in the origin of $\mathcal{A}$ (isotropic problem). For each network, the mean number of points over $\mathcal{A}$ is taken such that satisfies $\Lambda_{\square}(\mathcal{A}) = \alpha_{\square}\lambda_{\text{h}}|\mathcal{A}|$ where $\square = \{\text{tx}, \text{rx}, \text{jx}, \text{ex}\}$, λ_{h} is the intensity of a reference HPPP, and $\alpha_{\square}$ is a scaling factor.

Fig. 1 shows $\rho_j(\boldsymbol{x}_j)$ as a function of the distance $||\boldsymbol{x}_j||$ of the transmitter from the origin. From a comparative analysis of the different scenarios we obtain the following insights.

The intensity function of LTs shapes the performance's curve. Even if the average MSR per link is low, in the *high density* (HD) region around the origin, there are several LTs per unit area that carry a non-zero secrecy rate. Conversely, the scarcity of transmitters in the *low density* (LD) region at the Gaussian tail forces a performance decay.

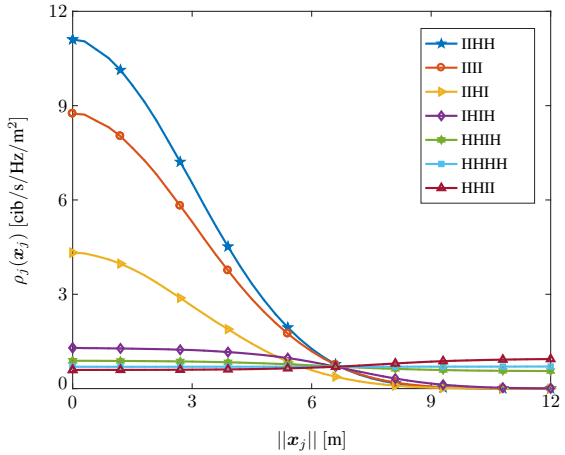

Fig. 1: LNSRD against the distance $||\boldsymbol{x}_j||$ in different scenarios with $R_{\text{max}} = 15$ [m], $\lambda_{\text{h}} = 1$ [node/m^2], $m = 1$, $b = 2$, $\alpha_{\text{tx}} = \alpha_{\text{rx}} = \alpha_{\text{jx}} = \alpha_{\text{ex}} = 0.5$, and $\sigma = 3$ [m].

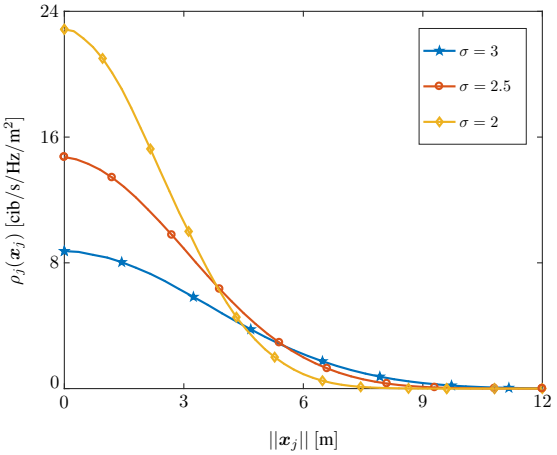

Fig. 2: LNSRD against the distance $||\boldsymbol{x}_j||$ for different variances σ^2, $R_{\text{max}} = 15$ [m], $\lambda_{\text{h}} = 1$ [node/m^2], $m = 1$, $b = 2$, $\alpha_{\text{tx}} = \alpha_{\text{rx}} = 0.5$, $\alpha_{\text{jx}} = 0$, and $\alpha_{\text{ex}} = 0.1$.

Table 1: NSR [cib/s/Hz] values for scenarios of Fig. 1.

IIHH	IIII	IIHI	IHIH	HHIH	HHHH	HHII
3775.5	3080.1	1662.8	813.2	824.6	787.1	816.3

Table 2: NSR [cib/s/Hz] values for scenarios of Fig. 2.

$\sigma=3$	$\sigma=2.5$	$\sigma=2$
3595.1	4306.5	5385.1

The scenarios in which LTs and LRs are both inhomogeneous show the best performance. The decay in the LD region does not heavily penalize the NSR (see Table 1). In the HD region, the high availability of LRs decreases the average internode distance of legitimate links, i.e., $\mathsf{r}_{j,\check{k}}$. Hence the capacity of the legitimate link, which drives the achievable MSR, rises. Note that the NSR in the HHHH scenario is outperformed by the one in the IIHH, IIII, and IIHI scenarios by 480%, 390%, and 210%, respectively.

The effect of inhomogeneous IIs in the HD region is stronger in scenarios where LTs and LRs are both inhomogeneous. In fact, when the capacity of the legitimate link is high, it is worth investing resources in impairing the eavesdropping link capacity with additional interference (see IIHI and IIII in Fig. 1).

In regions where ERs are dense, they have a good channel capacity on average. Hence, the achievable capacity gap in (9) is small. In those regions the effect of additional interference is very little (see HHII in Fig. 1).

Dense IIs cannot drive a significative increase in the achievable performance by themselves because they affect just eavesdropping link capacities. Hence the performance of the HHIH setting just slightly fluctuates around the one of the HHHH setting.

Fig. 2 shows $\rho_j(\boldsymbol{x}_j)$ as a function of $\boldsymbol{x}_j$ for different variances σ^2 in the IIII scenario for inactive IIs. Table 2 shows that smaller variances improve the overall performance besides the performance loss in the sparse region (a reduction of 67% of the variance the NSR increase by 150%).

Note that the presented cases studies are designed to highlight the diverse behavior of secrecy metrics in correspondence of high density or sparsity of any of the four networks; hence the case studies are simple and insightful but also, to some extent, artificial. In practical applications, variables like different antennas' gain, number of antennas in MIMO receivers (and possibility to perform beamforming), and more severe assumptions about the eavesdroppers' capabilities should be taken into account. Nevertheless, the take-out messages about the baseline features of inhomogeneous networks still hold.

7. CONCLUSION

This paper develops a framework for the analysis of wireless networks with intrinsic secrecy to inhomogeneous Poisson networks. Such a framework accounts for the node spatial distribution, wireless environment, and aggregate interference. We characterized the distribution of the aggregate interference and of the received SIR. Furthermore, we defined the LNSRD, a new metric to reveal the effects of the variability of node distributions, and the NSR to describe the overall secrecy performance of a network. By the analysis of several network scenarios, we found that the availability of receivers along with the integration of several low-rate confidential communications are the key enabler for confidential communications. We point out for a future research smart routing techniques, which we envision to be a method to obtain secrecy in multi hop ad-hoc networks.

8. REFERENCES

[1] Moe Z. Win, Liangzhong Ruan, Alberto Rabbachin, Yuan Shen, and Andrea Conti, "Multi-tier network secrecy in the ether," *IEEE Commun. Mag.*, vol. 53, no. 6, pp. 28–32, Jun. 2015.

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

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

[4] Satashu Goel and Rohit Negi, "Guaranteeing secrecy using artificial noise," *IEEE Trans. Wireless Commun.*, vol. 7, no. 6, pp. 2180–2189, June 2008.

[5] S. Ali. A. Fakoorian, Hamid Jafarkhani, and A. Lee Swindlehurst, "Secure space-time block coding via artificial noise alignment," in *Proc. Asilomar Conf. on Signals, Systems, and Computers*, Monterey, CA, USA, Nov. 2011, pp. 651 – 655.

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

[7] Ender Tekin and Aylin Yener, "The general Gaussian multiple-access and two-way wiretap channels: Achievable rates and cooperative jamming," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2735–2751, June 2008.

[8] Lun Dong, Zhu Han, Athina P. Petropulu, and H. Vincent Poor, "Improving wireless physical layer security via cooperating relays," *IEEE Trans. Signal Process.*, vol. 58, no. 3, pp. 1875–1888, Mar. 2010.

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

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

[11] Jemin Lee, Andrea Conti, Alberto Rabbachin, and Moe Z. Win, "Distributed network secrecy," *IEEE J. Sel. Areas Comm.*, vol. 31, no. 9, pp. 1889–1990, Sept. 2013.

[12] Liangzhong Ruan, Vincent K. Lau, and Moe Z. Win, "Generalized interference alignment – Part II: Application to wireless secrecy," *IEEE Trans. Signal Process.*, vol. 64, no. 10, pp. 2688–2701, May 2016.

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

[14] Christian Bettstetter, Giovanni Resta, and Paolo 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, Sept. 2003.

[15] Zhenhua Gong and Martin 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.

[16] Erik Steinmetz, Matthias Wildemeersch, Tony Q. S. Quek, and Henk Wymeersch, "A stochastic geometry model for vehicular communication near intersections," in *Proc. IEEE Global Telecomm. Conf. Workshops*, Dec. 2015, pp. 1–6.

[17] Flavio Zabini and Andrea 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, Sept. 2016.

[18] Hesham ElSawy, Ekram Hossain, and Martin 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, Aug. 2013.

[19] Hesham ElSawy and Ekram Hossain, "A modified hard core point process for analysis of random CSMA wireless networks in general fading environments," *IEEE Trans. Commun.*, vol. 61, no. 4, pp. 1520–1534, Apr. 2013.

[20] Young J. Chun, Mazen Hasna, and Ali Ghrayeb, "Modeling heterogeneous cellular networks interference using Poisson cluster processes," *IEEE J. Sel. Areas Commun.*, accepted 2015.

[21] Mehrnaz Afshang, Harpreet S. Dhillon, and Peter H. J. Chong, "Fundamentals of cluster-centric content placement in cache-enabled device-to-device networks," *IEEE Trans. Commun.*, vol. 12, no. 4, pp. 2511–2526, June 2016.

[22] Moe Z. Win, Pedro C. Pinto, and Lawrence A. Shepp, "A mathematical theory of network interference and its applications," *Proc. IEEE*, vol. 97, no. 2, pp. 205–230, Feb. 2009, special issue on *Ultra-Wide Bandwidth (UWB) Technology & Emerging Applications*.

[23] Martin Haenggi, *Stochastic Geometry for Wireless Networks*, Cambridge University Press, Cambridge, UK, 2013.