Secrecy Outage Analysis of k-th Best Link in Random Wireless Networks

Secrecy Outage Analysis of k-th Best Link in Random Wireless Networks

Satyanarayana Vuppala, *Member, IEEE*, Sudip Biswas, *Member, IEEE* and Tharmalingam Ratnarajah, *Senior Member, IEEE*

***Abstract*—In this paper, we analyze the secrecy characteristics of random wireless networks using stochastic geometric tools. The locations of the source and eavesdropper nodes are modeled as independent two-dimensional Poisson point processes. We investigate the secrecy outage probability of such networks from the perspective of the k-th best source, which has still not been well characterized. In particular, we derive the received path gain distributions of the typical destination and the eavesdropper from the k-th best source. Furthermore, we introduce a novel concept of security-region based on the k-th best source index. This is pragmatic in creating a protected communication zone for the typical destination and also to bound the number of sources that can coordinate in a Coordinated Multi-point transmission (CoMP) network. We further derive the secrecy outage probability for these CoMP sources based on the security-region. We also provide a closed-form expression for the maximum number of eavesdroppers for a given secrecy outage constraint, which can effect the secure communication. Tractable numerical and simulation results are presented under various assumptions of densities, path loss exponents and antenna figures.**

***Index Terms*—Secrecy outage, random wireless networks, stochastic geometry, fading, k-th best source index.**

I. Introduction

As the variety and the number of users of wireless networks grow, wireless security is becoming increasingly crucial in communication systems, leading researchers to investigate information theoretic approaches to achieve secrecy in the wireless channel. In recognition to these challenges, considerable efforts have been made by authors in [2]–[4] to develop information-theoretic security, which enhances the chance of a secure communication in the presence of eavesdroppers.

The theoretical foundations of information-theoretic security was led by Wyner, who introduced the concept of wiretap channel and analyzed the existence of reliable transmission conditions to achieve perfect secrecy in discrete memoryless channels [5]. Since then, the concept of information-theoretic security, i.e., physical layer security, has been extended to specific channels, such as additive white Gaussian noise (AWGN) channels by Cheong and Hellman [6], and broadcast wireless channel by Csiszár and Körner [7].

Obviously, previous works in the area such as those aforementioned are marked by significant abstraction from practical applicability, with various factors of relevance ignored for the sake of simplicity, to include: 1) the fact that wireless channels are often *subjected to fading* and 2) the fact that communicating devices compose *networks* often of *unknown topology* (randomly distributed nodes).

A few decades later, the increasing prospect of putting information theoretical secrecy concepts to actual use has motivated the community to deepen its understanding of the inherent secrecy capabilities of wireless systems by taking into account more realistic conditions of the wireless medium. Addressing point 1, for instance, the secrecy capacity of wireless fading channels was investigated in [2], [3] with expressions for the outage probability and average secrecy capacity of quasi-static fading channels also derived expressions in [4]. Considering point 2, and specifically when studying wireless secrecy in random networks using stochastic-geometric tools [8], the notion of *secrecy graphs* has emerged [9].

Following this trend, secrecy capacity scaling laws were studied in [10], and recently a new perspective on the role of node spatial distribution with wireless propagation mediums and aggregate network interference on network secrecy has been given in [11]. The secrecy capacity of unicast links in the presence of multiple eavesdroppers was investigated in [12], where the transmission to the k-th legitimate node was based on the order of the distance between the source and the destination.

Although, lately a considerable amount of reasearch has been done on intrinsic secrecy in random wireless networks [12]–[21], most current works focus on systems with single antenna and/or mainly study prorogation without fading or with Rayleigh fading [13], Nakagami fading [12], log-normal fading [16], and composite fading [17]. Hence, it is imperative to devise a more general model which can take into account any of the above mentioned fading scenarios. Furthermore, previous work on the impact of multiple antennas in random networks with secrecy constraint is not vast. However, the issue has not entirely escaped the attention of the community. For instance, while the authors in [22], [23] studied the secrecy multi-antenna transmission with artificial noise, [24] studied physical layer security in heterogeneous networks. Recently, [25] investigated the secure multi antenna transmission impaired by artificial noise and imperfect channel state information (CSI) in the presence of Poisson point process (PPP) based eavesdroppers.

Stochastic geometry approaches have recently gained significant attention to develop tractable models to analyze the performance of wireless networks [26]. In this approach, the wireless network is abstracted to a convenient point process that is used to capture the network properties. A homogeneous PPP is the most popular and tractable point process to model

This work was supported by the U.K. Engineering and Physical Sciences Research Council (EPSRC) under grant number EP/L025299/1.

S. Vuppala, S. Biswas, and T. Ratnarajah are with the Institute for Digital Communications, the University of Edinburgh, King's Building, Edinburgh, UK, EH9 3JL. E-mails: {s.vuppala, sudip.biswas, t.ratnarajah}@ed.ac.uk.

Correspondent author: Sudip Biswas.

Part of this paper has been presented at the IEEE International Conference on Communications (ICC 2016), Kuala Lumpur [1].

the locations of users and base stations in wireless networks. Similary, for inhomogeneous PPP based wireless networks, approximate signal to interference ratio analysis in general heterogeneous cellular networks is given in [27], while in [28] inhomogeneous Poisson sampling of finite-energy signals with uncertainties is given. Considering user association criteria in cellular networks, users are generally connected to the nearest source in terms of either considering the distance between users and source or received signal power at the users. Depending on these association criteria, users receive the message from either the nearest source or *best source* or the *k-th best source*. The best source can be considered to be the one that provides the user with the *maximum received path gain*. The k-th best source can be considered to be any potential source that provides the *k-th maximum path gain* to the user. The concept of k-th best source can be linked to Coordinated multi-point transmission (CoMP) networks, where more than one sources combine to provide the destination with higher gains. In such a scenario, it is of paramount importance to identify the K^* best sources out of K sources that can communicate securely with the destination. In this work, we identify a region comprising of such ordered K^* best nodes. We denote this region as the security-region of the network. Hence, it is intuitive to derive the k-th best path gain distribution between the typical user and the source. To the best of authors' knowledge, the secrecy capacity considering the k-th best path gain at the legitimate user or eavesdropper has not been evaluated. Furthermore, security-region can be considered as an important performance metric when designing such wireless networks.

In this paper, we address the mentioned challenges by deriving the received k-th best path gain distributions from the sources to the destination and eavesdroppers and expressions for the secrecy outage probability of random networks in the presence of eavesdroppers. We also introduce the concept of security-region for a given secrecy outage constraint based on the K^* best sources. At this point we would like to state that this model is applicable to any fading scenarios and also for models which include colluding eavesdroppers. The contributions of this work are multi-fold and are given as:

- We derive the received path gain distributions of the typical destination and the eavesdropper from the k-th best source under *general fading model*.
- Using the above results, we derive the secrecy outage probability $\mathcal{P}_{\rm out}$ for different scenarios with respect to the received path gain from any random source and the k-th best source under a general fading model.
- For a given secrecy outage constraint, a novel *security-region* concept is introduced. Henceforth, all the system parameters are looked upon based on this concept which gives a better insight into the secrecy capacity regions of random wireless networks.
- We obtain closed form expression for the limiting number of ordered sources that can participate in the CoMP.
- We also give a bound on maximum number of eavesdroppers which can effect the communication for a given secrecy outage constraint based on the received signal power.
- Finally, we give the aggregate path gain distribution for CoMP sources with respect to Rayleigh fading and a general fading scenario which is approximated with the gamma model. The CoMP sources include only the sources which are within the security-region.

Our findings indicate that the security-region can be considerably improved by an increase in the density of sources. Furthermore, we give a bound on the number of sources that can coordinate among each other to form the CoMP network. One can construct the CoMP sources by selecting all the best nodes instead of random sources from the security region in the network. Selecting the best sources to coordinate among each other can further improve the security of the network. Hence the CoMP sources within the security-region enhances the achievable secrecy capacity of the network. With both results in mind, the joint conclusion is that with the additional sources associated in the CoMP network, complex signal processing techniques are required to process the received signals and also maintain the required coordination among the sources. This may increase the complexity of the network and for systems with smaller dimensions and relaxed power constraints, it might be beneficial to use only the best source instead. An interesting outcome of the analysis is that providing insights on the uncertainty on the number of eavesdroppers.

The remainder of the paper is organized as follows. The system model is described in Section II, where the formulations of the secrecy outage probability and security-region are also briefly revised, while in Section III, we characterize the path gain distributions of the sources to the destination and the eavesdroppers. Moreover, in this section, we also derive expressions for the secrecy outage probabilities of random networks with multiple transmit antennas under generalized fading scenarios. In Section IV, we derive the aggregate path gain distribution from all the sources under a CoMP network followed by the derivation of the secrecy outage probability. Based on these derived expressions, numerical results are drawn and briefly discussed in Section V. Finally, concluding remarks are offered in Section VI.

II. System Model

We consider a network in Euclidean space of dimension d, modeled by a homogeneous PPP [29] with multiple source, destination and eavesdropper nodes. The sources and eavesdroppers location processes are denoted by $\Phi_{\rm s}$ and $\Phi_{\rm e}$ respectively with corresponding densities $\lambda_{\rm s}$ and $\lambda_{\rm e}$. The source and the eavesdropper PPPs are considered to be independent of each other. Without loss of generality, the source nodes can be interpreted as transmitters while the destination nodes and eavesdroppers as receivers. The sources transmit with the same power P_k for $k \in [1:K]$, where K is the total number of sources in the network. Without loss of generality, let the location of a given destination node define the origin of the space. Hereinafter, we consider the typical destination as the center of our analyses.

As shown in Fig. 1, consider that the sources wish to transmit information to a destination node, in the presence

TABLE I: Notations

Notation	Description
K	Total number of sources
Φ	Poisson Point Process (PPP)
λ	Density of the PPP
ζ_k	The received path gain from k-th source
$\hat{\zeta}_k$	The received path gain from best source
$\dot{\zeta}_k$	The received path gain from k-th best source
$\bar{\zeta}_k$	The aggregate path gain from all sources
R_s	Target rate
α	Path loss exponent
N_t	Number of antennas

of eavesdroppers, both subjected to generalized fading and path loss governed by the exponent α. We assume the sources to be equipped with N_t antennas. The antenna elements are deployed with a spacing of half the wavelength of the transmitted frequency to secure minimal correlation between the channels. All the destination nodes and eavesdroppers are each equipped with single antenna. The nifty thing about single antenna nodes is that they are inexpensive, simple and power efficient while still providing each node with high throughput. Moreover, the assumption that the nodes have single antennas can be considered as a special case of nodes having multiple antennas when we treat the extra antennas as if they were additional autonomous nodes.

Under the consideration of separate encoding scheme at each source, ith source sends an information symbol s_i through a linear beamforming vector $\mathbf{v}_i = [\nu_i^1, \cdots, \nu_i^{N_t}]^T$ with unit norm, i.e., $||\mathbf{v}_i||_2 = 1, i \in \Phi_s$. Therefore, the received signal at the typical destination can be given as

$$y = \underbrace{\sqrt{P_k}\mathbf{h}_{1,k}\mathbf{v}_k r_k^{-\alpha/2} s_k}_{\text{desired signal}} + \underbrace{\sum_{i\in\Phi_s} \mathbf{h}_{1,i}\mathbf{v}_i r_i^{-\alpha/2} s_i}_{\text{interference}} + \omega_1, \quad (1)$$

where $\mathbf{h}_{1,i} = [h_{1,i}^1, \cdots, h_{1,i}^{N_t}] \in \mathbb{C}^{1\times N_t}$ is the downlink channel between ith source to the typical destination[1] and each entry is independently identically distributed (IID) complex gaussian random variable with zero mean and unit variance. ω denotes the additive Gaussian noise and r_k is the distance between the k-th source and the typical destination.

The received SINR for the typical destination and any eavesdropper can now be given respectively as

$$\tilde{\zeta}_k \triangleq \frac{P_k|\mathbf{h}_{1,k}\mathbf{v}_k|^2 {r_k}^{-\alpha}}{\sigma^2 + \sum\limits_{i\in\Phi_s} P_k|\mathbf{h}_{1,i}\mathbf{v}_i|^2 r_i^{-\alpha}}, \quad (2)$$

$$\tilde{\zeta}_{\mathrm{e}} \triangleq \frac{P_k|\mathbf{h}_{\mathrm{e},k}\mathbf{v}_k|^2 {r_{\mathrm{e}}}^{-\alpha}}{\sigma^2 + \sum\limits_{i\in\Phi_s} P_k|\mathbf{h}_{e,i}\mathbf{v}_i|^2 r_i^{-\alpha}}. \quad (3)$$

Hereinafter, in conjunction to [13], for a given number of sources, we consider a interference-limited scenario. Thus,

[1]The subscript 1 in $\mathbf{h}_{1,l}$ corresponds to the typical destination.

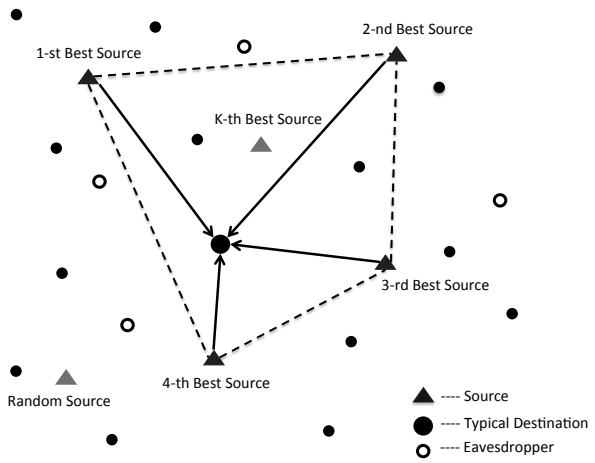


Fig. 1: An illustration of a network modeled by an overlay of sources, a typical destination and eavesdroppers and the security-region (dotted lines) with first 4 best sources.

the secrecy capacity between any k-th source and a typical destination is given as [30]

$$\mathcal{C}_s = \max\{0, \log_2(1+\zeta_k\rho) - \log_2(1+\zeta_{\mathrm{e}}\rho)\}\text{bit/s/Hz}, \quad (4)$$

where

$$\zeta_k = \frac{P_k|\mathbf{h}_{1,k}\mathbf{v}_k|^2 {r_k}^{-\alpha}}{\mathcal{I}_k}, \quad (5)$$

$$\zeta_{\mathrm{e}} = \frac{P_k|\mathbf{h}_{\mathrm{e},k}\mathbf{v}_k|^2 {r_{\mathrm{e}}}^{-\alpha}}{\mathcal{I}_{\mathrm{e}}}, \quad (6)$$

with $\mathcal{I}_k = \sum\limits_{i\in\Phi_s} P_k|\mathbf{h}_{1,i}\mathbf{v}_i|^2 r_i^{-\alpha}$,
and $\mathcal{I}_{\mathrm{e}} = \sum\limits_{i\in\Phi_s} P_k|\mathbf{h}_{e,i}\mathbf{v}_i|^2 r_i^{-\alpha}$ denoting the aggregate interference power[2] at the destination and eavesdropper, respectively. Hereinafter, for notational simplicity, we remove the subscript 1 from the channel vector.

Consequently, the probability that the secrecy capacity of such a channel is below a given threshold $R_s \geq 0$ – hereinafter referred to as *secrecy outage probability* – is defined as [30]

$$\mathcal{P}_{\text{out}} \triangleq \Pr\{\mathcal{C}_s < R_s\} = \Pr\left\{\log_2\left(\tfrac{1+\zeta_k}{1+\zeta_e}\right) < R_s\right\}, \quad (7)$$

The secrecy non-outage probability between the source and destination node (in the presence of randomly located multiple eavesdroppers) can be derived from (7) as

$$\begin{aligned}\mathcal{P}_{\text{out}} &= \int_0^\infty \int_{\beta(y)}^\infty f_{\zeta_{\mathrm{e}}}(x) f_{\zeta_k}(y)\mathrm{d}x\,\mathrm{d}y, \quad (8)\\ &= \int_0^\infty (1 - F_{\zeta_{\mathrm{e}}}(\beta(y))) f_{\zeta_k}(y)\mathrm{d}y,\end{aligned}$$

where $\beta(y) = [2^{R_s}(1+y) - 1]$, f_ζ and F_ζ denote the probability density function and the cumulative density fuction of ζ respectively.

[2]For tractable analysis, we assume that the received interferences at the destination and eavesdropper are independent.

We now rewrite the secrecy outage probability for the k-th best source in presence of the best eavesdropper as

$$\mathcal{P}_{\text{out}} = \Pr\left\{\log_2\left(\frac{1+\grave{\zeta}_k}{1+\hat{\zeta}_e}\right) < R_s\right\}, \tag{9}$$

where $\grave{\zeta}_k$ and $\hat{\zeta}_e$ are defined in Table I. Similarly, the secrecy outage probability expression follows for the case of CoMP network with $\bar{\zeta}_k$ and $\hat{\zeta}_e$. For such an interference limited scenario, we consider $R_s = 0$ in order to make the analyses tractable and obtain closed-form expressions.

We now introduce a new metric, security-region, from the perspective of the best source index. Note that, this concept of security-region is significantly different from the security region as described in the literature [30], [31]. It can be defined as the region in which the set of ordered K^* nodes can safely communicate with typical destination for a given secrecy outage constraint. These set of K^* nodes are the nodes that combine to form the CoMP network.

$$\mathcal{S} \triangleq \{(K^*, \epsilon), \forall K^* \in \{1, \cdots, k^*\}, \mathcal{P}_{\text{out}} \leq \epsilon\}, \tag{10}$$

where k^* is the limiting value of K for a given secrecy outage constraint. This limiting value, which defines the security-region will be computed in following section.

III. Secrecy Characterization: Selection of Source

In this section, we characterize the path gain distribution of the destination node from the source node or nodes considering three particular scenarios. In scenario 1, the destination node can receive signals from any source while in scenario 2, it can receive signals from the best source. In scenario 3, the destination node can receive the signal from the k-th best source.

A. Scenario 1: *Any Random Source*

To begin our analysis, in this section we consider a Rayleigh fading model. However, in the later sections, we generalize our analysis for any fading models and path loss exponent values.

1) Received Path Gain Distribution from a Source: We intend to characterize the secrecy outage probability of a communication link between any source and typical destination. Hence, the distributions of interest concerning the legitimate network are those corresponding to the path gain of each legitimate source ζ_k. Hence, $H_k = |\mathbf{h}_k \mathbf{v}_k|^2$ which follows a chi-square distribution [32] with $2N_t$ degrees of freedom. Recall that the probability density function of chi-square distribution can be given as

$$H_k \sim f(x) = \tfrac{N_t^{N_t}}{\Gamma(N_t)} x^{N_t - 1} e^{-N_t x}. \tag{11}$$

The cumulative density function for the path gain distribution from the source to the destination node is given in following Lemma.

Lemma 1. *The path gain distribution from a random source to the destination node can be given as*

$$\bar{F}_{\xi_k}(z) = \sum_{k=1}^{N_t} \binom{N_t}{k} (-1)^{k+1} \exp\left[-\frac{2\pi^2 \lambda_s r_k^2 z^{\frac{2}{\alpha}} k^{\frac{2}{\alpha}}}{\alpha \sin(\frac{2\pi}{\alpha})}\right] \tag{12}$$

Proof. A detailed proof is given in Appendix A. □

2) Path Gain Distribution of the Best Eavesdropper: In order to obtain an expression for the secrecy outage probability as in equation (7), the distribution of the path gain ζ_{e} needs to be derived. However, in contrast, for a given legitimate path gain ζ_k what determines the secrecy capacity of a channel subjected to fading is not any specific eavesdropper, but rather the eavesdropper with the *maximum*[3] (instantaneous) path gain amongst them.

Lemma 2. *The path gain distribution of the best eavesdropper can be given as [33]*

$$F_{\hat{\zeta}_{\text{e}}}(z) = \exp\left(-\pi \lambda_{\text{e}} z^{\frac{-2}{\alpha}} \mathbb{E}_{\xi_{\text{e}}}\left(\xi_{\text{e}}^{\frac{2}{\alpha}}\right)\right). \tag{13}$$

and, an integral-form expression for $\mathbb{E}_{\xi_{\text{e}}}\left(\xi_{\text{e}}^{\frac{2}{\alpha}}\right)$ *is given in Appendix C.*

Proof. A detailed proof is given in Appendix B. □

Under the assumption of interference cancellation at eavesdropper's side, the received best path gain can be given in following corollary.

***Corollary* 1.** *The path gain distribution of the best eavesdropper*[4] *can be given in interference-free network as*

$$F_{\hat{\zeta}_{\text{e}}}(z) = \exp\left(-\pi \lambda_{\text{e}} z^{\frac{-2}{\alpha}} \mathbb{E}_H\left(h_{\text{e}}^{\frac{2}{\alpha}}\right)\right). \tag{14}$$

Proof. The proof follows from Lemma 2. □

With possession of path gain distributions of channels from sources to the destination node and the best eavesdropper channels as derived in the preceding subsections, the secrecy outage probability can now be given as

$$\mathcal{P}_{\text{out}} = \frac{2}{\alpha} \sum_{k=0}^{N_t} \binom{N_t}{k} (-1)^{k+1} \beta \int_0^\infty e^{-\beta y^{\frac{2}{\alpha}}} y^{\frac{2}{\alpha}-1} \left(1 - e^{-\Xi_{\text{e}} y^{\frac{-2}{\alpha}}}\right) \mathrm{d}y, \tag{15}$$

where $\beta = \dfrac{2\pi^2 \lambda_s r_k^2 k^{\frac{2}{\alpha}}}{\alpha \sin(\frac{2\pi}{\alpha})}$ and $\Xi_{\text{e}} = \pi \lambda_{\text{e}} \mathbb{E}_{\xi_{\text{e}}}\left(\xi_{\text{e}}^{\frac{2}{\alpha}}\right)$.

Unfortunately, the above integral in (15) does not admit a closed-form solution. However, for a given $\alpha = 2$, the closed-form of the secrecy outage probability is given as

$$\mathcal{P}_{\text{out}} = 2 \sum_{k=1}^{N_t} \binom{N_t}{k} (-1)^{k+1} (\sqrt{\beta \Xi_{\text{e}}} \mathrm{K}_1[2\sqrt{\beta \Xi_{\text{e}}}]), \tag{16}$$

where $\mathrm{K}_{\text{a}}[\text{b}]$ is the modified Bessel function of the second kind.

[3]Here, it is implicitly assumed that eavesdroppers do *not* collude. The scenario with collusion will be discussed in future work.

[4]The best eavesdropper can be considered to be the one that receives the maximum path gain.

B. SCENARIO 2: *Best Source*

Let us consider the case where the typical destination is able to identify which of its candidate sources has the maximum path gain, subsequently associating to that source.

In the context of our analytical framework, this assumption implies that the secrecy capacity of the channel in question is governed by the statistics of the *maximum* path gain amongst the sources. One can find the path gain distribution of best source using the similar approach from lemma 2.

Lemma 3. *The path gain distribution of the best source to the destination ($\hat{\zeta}_k$) can be given as*

$$F_{\hat{\zeta}_k}(z) = \exp\left(-\pi\lambda_{\mathrm{s}} z^{\frac{-2}{\alpha}} \mathbb{E}_{\xi_k}\left(\xi_k^{\frac{2}{\alpha}}\right)\right). \tag{17}$$

Proof. The proof follows from Lemma 2. □

Now, using Proposition 1 and 2, we can derive the secrecy outage probability with respect to the best source and the best eavesdropper.

Proposition 1. *The secrecy outage probability of the best source channel to the destination in presence of the best eavesdropper can be given as*

$$\mathcal{P}_{\mathrm{out}} = \frac{\Xi_{\mathrm{e}}}{2^{\frac{-2R_s}{\alpha}}\Xi_k + \Xi_{\mathrm{e}}}, \tag{18}$$

where $\Xi_k = \pi\lambda_{\mathrm{s}}\mathbb{E}_{\xi_k}\left(\xi_k^{\frac{2}{\alpha}}\right)$.

Proof. A detailed proof is given in Appendix D. □

At this point, it is worthwhile to elucidate a few qualitative remarks on the secrecy outage probability expression as derived in (18).

***Corollary* 2.** *Considering similar fading and interference conditions at the destination and eavesdroppers, the secrecy outage probability can be given as*

$$\mathcal{P}_{\mathrm{out}} = \frac{\lambda_{\mathrm{e}}}{2^{-\frac{2R_s}{\alpha}}\lambda_{\mathrm{s}} + \lambda_{\mathrm{e}}}. \tag{19}$$

Proof. Proof follows directly from Proposition 1. □

Remark 1. *It can be noted that the above expression is precisely the same as the probability of achievable secrecy rate found in the AWGN channel [34]. The result that $\mathcal{P}_{\mathrm{out}}$ is* independent *of fading and interference is intuitively acceptable and the secrecy outage probability only depends on the path loss exponent and the density of the nodes.*

C. SCENARIO 3: *k-th Best Source*

This case relates to the scenario studied in [2], [4], in the sense that the selection of the device with the "best channel" can either occur in terms of the "best node" at a given time owing to the quasi-stationarity of the channel – as assumed in [4] – or in terms of the "best time" – as assumed in [2]. Subsequently, we consider for the sake of completion, the case where the k-th source provides the destination with the k-th maximum path gain.

Lemma 4. *The path gain distribution of the k-th best source ($\grave{\zeta}_k$) can be given as*

$$F_{\grave{\zeta}_k}(z) = \frac{\Gamma\left((2^{R_s}z)^{\frac{-2}{\alpha}}\Xi_k, k\right)}{(k-1)!}. \tag{20}$$

Proof. Denoting the distribution of path gain from the k-th best source node to typical destination by $F_{\hat{\zeta}_k}$, we have [35]

$$F_{\grave{\zeta}_k}(z) = \Pr(0\cdots k-1 \text{ points in } (\mathrm{z},\infty)), \tag{21}$$

$$= \sum_{j=1}^{k-1}\frac{\Lambda_{(z,\infty)}^{j}}{j!}e^{-\Lambda_{(z,\infty)}^{j}} = \frac{\Gamma\left((2^{R_s}z)^{\frac{-2}{\alpha}}\Xi_k, k\right)}{(k-1)!},$$

where the intensity measure $\Lambda_{(z,\infty)}$ (from the proof of Proposition 2) can be given as

$$\Lambda_{(z,\infty)} = \int_{z}^{\infty}\hat{\lambda}(y)\mathrm{d}y. \tag{22}$$

□

Now, considering Lemma 4, the secrecy outage probability with respect to the k-th best source can be given as below.

Proposition 2. *The secrecy outage probability for the link between the destination and the k-th best source in presence of the n-th eavesdropper can be given as*

$$\mathcal{P}_{\mathrm{out}} = \sum_{j=0}^{k-1}\frac{\Gamma(j+n)2^{\frac{-2jR_s}{\alpha}}(\Xi_k)^j(\Xi_{\mathrm{e}})^n}{j!\,\Gamma(n)}\left(\frac{1}{2^{\frac{-2R_s}{\alpha}}\Xi_k + \Xi_{\mathrm{e}}}\right)^{j+n}. \tag{23}$$

Proof. This derivation of this proof follows in a similar way as the proof of Proposition 1 and hence is omitted here. □

Remark 2. *For $k = 1$ and $n = 1$, Proposition 2 converges to Proposition 1 and the corollaries derived in the preceding subsections also hold for this scenario.*

Now, in the following proposition we characterize the security-region of our system. From Proposition 2, one can obtain the maximum possible k-th index for a given secrecy outage constraint ϵ.

Proposition 3. *The limiting number of ordered sources that can securely communicate with the destination in presence of the best eavesdropper can be given as*

$$k^* = \log_{\frac{\Upsilon}{\Upsilon+1}}(1-\epsilon). \tag{24}$$

Proof. By defining $\Upsilon = \frac{2^{\frac{-2R_s}{\alpha}}\Xi_k}{\Xi_{\mathrm{e}}}$, $\mathcal{P}_{\mathrm{out}}$ in Eq. (23) can be re-written for the best eavesdropper case *i.e* $n = 1$ as

$$\mathcal{P}_{\mathrm{out}} = \sum_{j=0}^{k-1}\frac{\Upsilon^j}{(\Upsilon+1)^{j+1}}. \tag{25}$$

The Eq. (25) can be expressed as a geometric series with common ratio as $\frac{\Upsilon}{\Upsilon+1}$ and the first term as $\frac{1}{\Upsilon+1}$. One can accordingly write the secrecy outage probability in (25) as

$$\mathcal{P}_{\mathrm{out}} = \left(\frac{1}{\Upsilon+1}\right)\frac{1-(\frac{\Upsilon}{\Upsilon+1})^k}{1-\frac{\Upsilon}{\Upsilon+1}}. \tag{26}$$

Finally, the limiting value of K, *i.e* k^*, sources for a given secrecy outage constraint ϵ can be given from above equation (26) as

$$k^* = \log_{\frac{\Upsilon}{\Upsilon+1}} (1-\epsilon). \tag{27}$$

□

***Corollary* 3.** *From the previous Proposition 3, using infinite geometric series, the secrecy outage probability $\mathcal{P}_{\rm out} \to 1$ when $k \to \infty$.*

This shows that in CoMP networks, it may not be useful to consider all the sources in the network. Instead, it is important to take into consideration only the limiting number of sources as stated in the previous proposition.

To draw another parallel with the literature on random networks, if cooperation is a part of the communication system used by legitimate nodes, it must be assumed that the same strategy will be exploited by eavesdroppers as well. The expressions derived in this paper may also be applicable to the scenario when the eavesdroppers are cooperating. This eavesdropper's cooperation can also be interpreted as collusion among the eavesdroppers. Therefore, we give a bound on maximum number of such eavesdroppers which can effect the communication for a given secrecy outage constraint in following proposition.

Proposition 4. *The maximum number of eavesdroppers that effects the secure communication for a given secrecy outage constraint ϵ can be computed as*

$$n^* = \log_{\frac{1}{\Upsilon+1}} (\epsilon). \tag{28}$$

Proof. This proof is obtained from Proposition 3 by keeping $k = 1$. □

IV. Secrecy Characterization: CoMP within the security-region

To analyze a scenario with coordinated multi-point sources, we assume that all the sources exchange required ideal information amongst themselves through a backhaul connection. This scenario provides maximum achievable secrecy capacity and tells the network designer the number of K best sources sufficient to achieve the ultimate secrecy performance of the network.

In this section we consider a CoMP network of sources based on the security-region. We assume that only the sources within the security-region are allowed to coordinate among each other to form the CoMP network. Since the security-region depends on the source node's secrecy outage probability, the set of sources that fall within the security-region may be considered as an inhomogeneous Poisson point process which can be obtained via location-dependent thinning of $\Phi_{\rm s}$. To be specific, such conditions are clearly distinct from the random and uniformly distributed network assumptions that lead to a Poison number of nodes per unit area *i.e.*, the PPP model – commonly adopted in recent stochastic geometry literature. To this end, the Matern hardcore models (Type I and Type II) of point processes are more suitable. However, the characterization of such models via the Laplace Functional and probability generating functionals is in reality a challenging problem. Therefore, the hard-core point processes are quite difficult to analyze due to the simple reason that their probability generating functionals do not exist [36]–[39]. But, it has been argued in [36], [37] that the nodes further away from the hard core distance, d can still be modelled as a PPP. Furthermore, it has been shown in [38] that MHCPP type II is better approximated with a PPP rather than Type I. Hence we assume that the total limiting number of sources to follow a Poisson distribution while they are still non-uniformly located within the coverage area of the cell due to thinning. Therefore, the set of transmitting best sources follow inhomogeneous PPP $\bar{\Phi}_{\rm s}$ with a density of $\bar{\lambda}_{\rm s}$. Now, the distribution of the equivalent aggregate source path gain $\bar{\zeta}_k$ is required in order to characterize the secrecy rate of random networks. Thus, we have

$$\bar{\zeta}_k = \sum_{x \in \bar{\Phi}_s} |h_x|^2 ||r_x||^{-\alpha}. \tag{29}$$

Further, we consider two cases, namely, 1) without interference and 2) with interference to characterize the secrecy rate of the network. Case 1 may be applicable for scenarios, such as when the density of non co-operating source nodes are very less, when perfect interference mitigation techniques under the assumption of perfect channel state information is considered, etc. Case 2 on the other hand is the more general case, where interference is one of the major bottlenecks affecting the performance of the CoMP network.

A. Without interference

Under the consideration of this model and the use of Campbell's theorem, the characteristic function of $\bar{\zeta}_k$ can be computed by [40] as

$$\phi_{\bar{\zeta}_k}(w) = \exp\left(-2\pi\bar{\lambda}_{\rm s} \int_H \int_{\mathbb{R}} \cdot [1 - e^{jwxr^{-\alpha}}] \cdot f_H(x)\, {\rm d}r {\rm d}x\right), \tag{30}$$

where j is the imaginary unit.

***Corollary* 4.** *For the case of $N_t = 1$, one can obtain the distribution of aggregate path gain with $\alpha = 4$ as*

$$F_{\bar{\zeta}_k}(z) = {\rm erfc}\left[\frac{\pi^2 \bar{\lambda}_{\rm s}}{4\sqrt{z}}\right]. \tag{31}$$

Proof. A detailed proof is given in Appendix E. □

Proposition 5. *The secrecy outage probability in presence of the best eavesdropper for CoMP sources with $\alpha = 4$ and $N_t = 1$ can be given as*

$$\mathcal{P}_{\rm out} = 1 - e^{\frac{\Xi_{\rm e}^2 2^{R_s+2}}{\pi^4 \bar{\lambda}_{\rm s}^2}} {\rm erfc}\left(\frac{2\Xi_{\rm e}\sqrt{2^{R_s}}}{\pi^2\bar{\lambda}_{\rm s}}\right). \tag{32}$$

Proof. With possession of corollary 4, the secrecy outage probability using equation (9) can be given as

$$\begin{aligned}\mathcal{P}_{\rm out} &= \int_0^\infty x^{-\frac{2}{\alpha}-1} e^{-\Xi_{\rm e} x^{-2/\alpha}} {\rm erfc}\left(\frac{\pi^2\bar{\lambda}_{\rm s}}{4\sqrt{2^{R_s}x}}\right) {\rm d}x, \\ &= 1 - e^{\frac{\Xi_{\rm e}^2 2^{R_s+2}}{\pi^4\bar{\lambda}_{\rm s}^2}} {\rm erfc}\left(\frac{2\Xi_{\rm e}\sqrt{2^{R_s}}}{\pi^2\bar{\lambda}_{\rm s}}\right),\end{aligned} \tag{33}$$

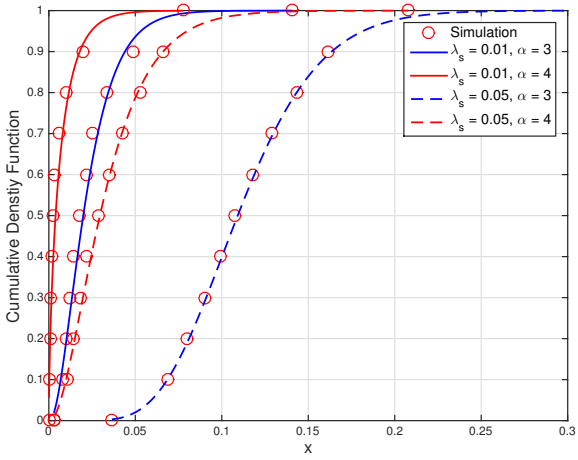


Fig. 2: Gamma model Vs Empirical for different values of density and α.

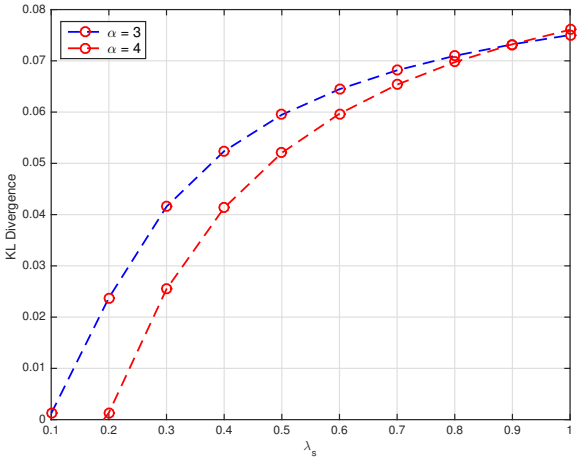


Fig. 3: Kullback-Leibler Divergence between Gamma Distribution and Empirical Distribution for various α.

where the above integral is a particular case of [41, pp. 31, Eq. 1.5.2.1]. □

Unfortunately neither equation (30) nor its inverse Laplace transform admits a closed form expression except for the specific case of fading [13]. However, the aggregate path gain can be characterized using their cumulants. Hence, we employ equation (30) to obtain the corresponding closed forms of the cumulants. Specifically, the i-th cumulant of $\phi(w)$ can be given by

$$\kappa(i) = \frac{1}{j^i} \frac{\mathrm{d}^n \log \phi(w)}{\mathrm{d}w^i}\Big|_{w=0} \tag{34}$$

After a series of integral calculations (refer to [40] for detailed derivations),

$$\kappa_{\bar{\zeta}_k}(i) = \frac{2\pi\bar{\lambda}_\mathrm{s}}{i\alpha - 2}\mathbb{E}_H\left(h_k^{\frac{2}{\alpha}}\right). \tag{35}$$

The closed form expressions of $\kappa_{\bar{\zeta}_k}(i)$ under Nakagami-m and Log-Normal distributions are also provided in [40].

Based on this exact cumulant expression as given in (35), various models for the distribution of the equivalent aggregate eavesdropper gain can be built. In this paper we discuss the gamma distribution model. The interested reader is referred to [42], to obtain more insights on the use of gamma variables.

Modeling $\bar{\zeta}_k$ as a Gamma Variate:

In order to obtain a more tractable and accurate model for the distribution of $\bar{\zeta}_k$, we consider a gamma model given as

$$f_{\bar{\zeta}_k}(x;\nu,\theta) = \frac{x^{\nu-1}e^{-\frac{x}{\theta}}}{\theta^\nu\Gamma(\nu)}, \tag{36}$$

where the parameters ν and θ are given by

$$\nu = \frac{\kappa^2_{\bar{\zeta}_k}(1)}{\kappa_{\bar{\zeta}_k}(2)} \quad \text{and} \quad \theta = \frac{\kappa_{\bar{\zeta}_k}(2)}{\kappa_{\bar{\zeta}_k}(1)}. \tag{37}$$

with the cumulants $\kappa^2_{\bar{\zeta}_k}(1)$ and $\kappa^2_{\bar{\zeta}_k}(2)$ being characterized using equation (35). For the simulation of approximation model, we have considered a Rayleigh fading channel with N_t antennas. Therefore, the i-th cumulant can be given as

$$\kappa_{\bar{\zeta}_k}(i) = \frac{2\pi\bar{\lambda}_\mathrm{s}}{(i\alpha - 2)} \cdot \frac{\Gamma(N_t + i)}{N_t^i\Gamma(N_t)}. \tag{38}$$

The accuracy of the Gamma model is illustrated in Fig. 3, where the empirical cumulative density function (CDF) of $\bar{\zeta}_k$ is compared against the Gamma distribution given in equation (36) for various α and $\bar{\lambda}_\mathrm{s}$. The results indicate that the Gamma approximation is in fact quite tight. Further the accuracy of gamma distribution can also be verified with Kull-back divergence between Monte-Carlo simulations and analytical approximation in Fig. 3. Note that interested readers can refer to [12] for more insights on Kull-back divergence. Likewise, this gamma approximation is also justified in recent literature [16], [42].

Proposition 6. *The secrecy outage probability in CoMP considering the gamma model to characterize the aggregate path gain in the presence of the best eavesdropper can be given as*

$$\mathcal{P}_\mathrm{out} = \frac{2\Xi_\mathrm{e}}{\alpha}\int_0^\infty \left(1 - e^{\frac{x}{\theta}}\sum_{j=0}^{\nu-1}\frac{x^j}{j!\theta^j}\right) e^{-\Xi_\mathrm{e}x^{-\frac{2}{\alpha}}} x^{-\frac{2}{\alpha}-1}\,\mathrm{d}x. \tag{39}$$

Proof. Proof is given in Appendix F. □

Corollary 5. *Consider severe signal attenuation (e.g., densely built urban area), the path loss exponent $\alpha = 4$. Accordingly, the secrecy outage probability considering CoMP sources can be given as*

$$\begin{aligned}\mathcal{P}_\mathrm{out} = 1 + \frac{2\Xi_\mathrm{e}}{\alpha}\Bigg(&\Xi_\mathrm{e}\theta^{j-1}\Gamma(j-1)\,{}_0F_2\left(;\frac{3}{2},2-j;-\frac{\Xi_\mathrm{e}^2}{4\theta}\right) \\ &-\theta^{j-\frac{1}{2}}\Gamma\left(j-\frac{1}{2}\right){}_0F_2\left(;\frac{1}{2},\frac{3}{2}-j;-\frac{\Xi_\mathrm{e}^2}{4\theta}\right) \\ &-2\Xi_\mathrm{e}^{2j-1}\Gamma(1-2j)\,{}_0F_2\left(;j,j+\frac{1}{2};-\frac{\Xi_\mathrm{e}^2}{4\theta}\right)\Bigg).\end{aligned} \tag{40}$$

Proof. Proof follows directly from the Proposition 6. □

B. With Interference

By taking interference into account, the path gain distribution for the CoMP can be re-written as

$$\tilde{\zeta}_k = \frac{\sum\limits_{x\in\bar{\Phi}_s} |h_x|^2 ||r_x||^{-\alpha}}{\bar{\mathcal{I}}_k}, \tag{41}$$

where $\bar{\mathcal{I}}_k$ is the interference from the sources that do not cooperate among each other[5]. The density of such non-cooperating source nodes denoted as λ_i. The optimum outcome of CoMP is to aggregate the power of all information signals which can leads to minimum secrecy outage. However, the aggregation of all the signals from the nodes which does not have sufficient power may not be a good practise. Thus, it is important to select the best nodes for the aggression process. In the following Lemma, we will provide a closed-form expressions for such aggregation by leveraging the analysis from [43].

Lemma 5. *The CDF of the aggregate path gain in CoMP scenario with interference can be given as*

$$F_{\tilde{\zeta}_k}(z) = 1 - \int\limits_{0<\xi_1<\cdots\xi_K<\infty} \mathcal{L}_{\bar{\mathcal{I}}_k}\left(\frac{z}{\sum\limits_{\mathrm{e}\in\Phi_{\mathrm{e}}} x_{\mathrm{e}}^{-1}}\right) f_{\xi}(x)\mathrm{d}x, \tag{42}$$

where

$$f_{\xi}(x) = \prod_{s\in\bar{\Phi}_s} \tfrac{2}{\alpha}\pi\bar{\lambda}_s\, x^{\frac{2}{\alpha}-1} e^{-\pi\bar{\lambda}_s x^{\frac{2}{\alpha}}}, \tag{43}$$

and, $\mathcal{L}_{\bar{\mathcal{I}}_k}(.)$ follows from the proof of Lemma 1.

Proof. A sketch of proof is given in Appendix G. □

Using equation (7), the probability of non-zero secrecy capacity is given by

$$\mathcal{P}_{\mathrm{out}} = \int_0^{\infty} F_{\tilde{\zeta}_k}(z) f_{\hat{\zeta}_{\mathrm{e}}}(z)\mathrm{dz}, \tag{44}$$

where $f_{\zeta_\ell}(z)$ can be obtained by taking derivative of $\bar{F}_{\zeta_\ell}(z)$ in (42) and $F_{\zeta_{\mathrm{e}}}(z)$ follows from Lemma 2. Unfortunately the above integral does not admit closed-form. However, one can evaluate the integral numerically.

Remark 3. *As stated before, the noise-limited case is a special case for scenarios, such as when non co-operating source nodes are very less in the network or when perfect interference mitigation techniques under the assumption of perfect CSI is considered. Hence, Lemma 5 can be simplified to Corollary 4 under the assumption of the above mentioned cases. Accordingly, the secrecy outage probability defined in equation* (44) *simplifies to equation* (33)*.*

V. Numerical Results

In this section, we validate the system model and also verify the results mentioned in the propositions. In general, the computations are done through Monte Carlo simulations which are then used to validate the analytical results. Unless stated otherwise, most of the values of the parameters used are inspired from the literature mentioned in the references. For the system guidelines, we mention these parameters and their corresponding values in Table II.

[5]Note that, the nodes that do not cooperate among each other are the ones that do not participate to form the security region.

TABLE II: Simulation Parameters

Notation	Parameter	Values
λ_{s}	Density	0.001 m^{-2}
λ_{e}	Density	0.001 m^{-2}
R_s	Target rate	0.1 bits
α	Path loss exponent	2, 4
N_t	Number of antennas	5
P	Node transmit power	1 Watt

With the expressions derived in the previous section, we can study the availability of secrecy in random wireless networks in the presence of randomly distributed eavesdroppers. Let us consider any random source transmitting a message to the typical destination. Hence, the secrecy outage probability is given according to (16) whose plot is shown in Fig. 4. In this figure, we consider the impact of number of antennas and eavesdropper's density on the secrecy outage probability.

As the value of N_t increases, the secrecy outage probability is relatively improved. Thus Fig. 4 suggests also that as the relative distance between source and destination increases, the secrecy outage increases. This figure basically helps in validating our results with the already established results in literature related to the number of antennas, eavesdropper density and the secrecy capacity.

Now, consider the case where the typical destination is associated to the best source rather random source. Fig. 5a shows the secrecy outage probability as a function of the k-th best source for different number of source densities. For this simulation the values of the parameters considered are : $\lambda_{\mathrm{e}} = 0.001,\ N_t = 5$ and $\alpha = 2$. Also the target rate is kept constant at $R_s = 0.1$. It is evident from the figure that as we increase the best source index, the secrecy outage probability also increases. The best source index can be interpreted either in terms of the fading gain or distance from the source. Similar settings are considered in Fig. 5b except for the source density which is now kept fixed at $\lambda_{\mathrm{s}} = 0.001$. This figure complements the results of the previous figure for different values of λ_e. Hence, we can conclude that when the typical destination is receiving from the k-th farthest node, the secrecy outage probability increases in an ascending order.

Under the assumption that the typical destination and the eavesdroppers experience the same fading at any particular time for a given k-th best source and the best eavesdropper pair, the secrecy outage probability may not depend on the fading conditions. Hence, the eavesdropper density, the path loss exponent and the k-th source index play a major role in determining the secrecy probability in such a scenario.

Following the footprints of Fig. 5, we now plot the secrecy outage probability in Fig. 6 with a special case of eavesdropper strategy, where eavesdroppers perform perfect interference

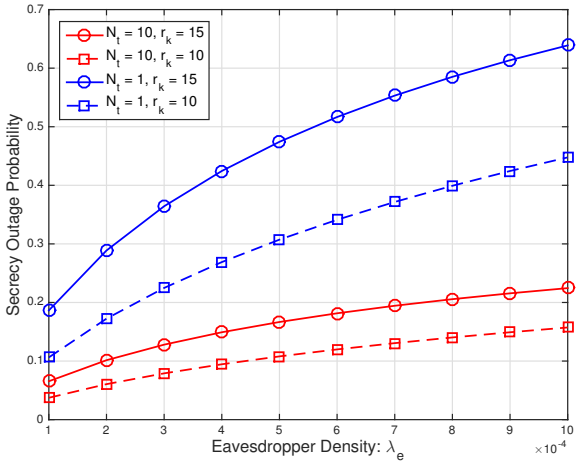
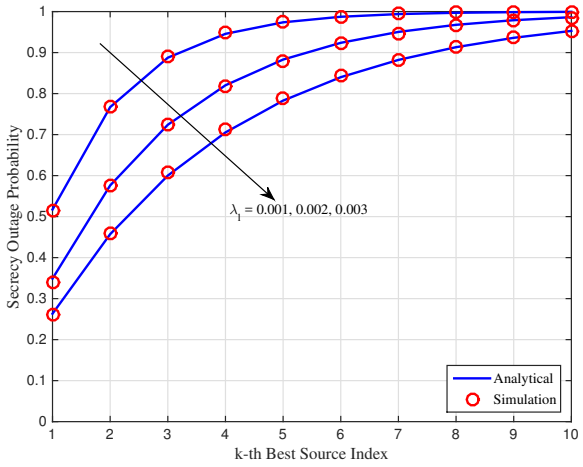
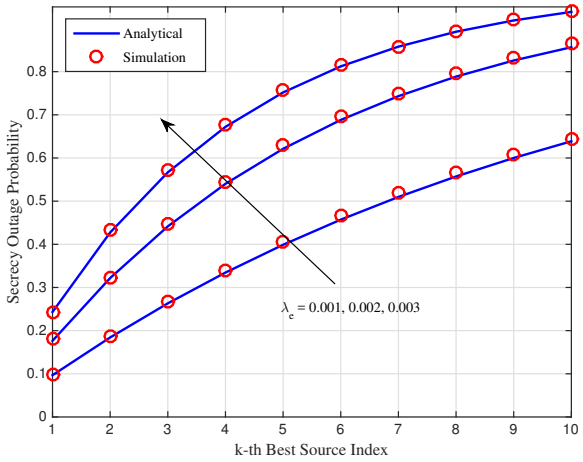


Fig. 4: Secrecy outage probability as a function of λ_e for various figure N_t.



(a) As a function of k-th best source index for different λ_s



(b) As a function of k-th best source index for different λ_e

Fig. 5: Secrecy outage probability as a function of k-th best

cancellation. Henceforth, only the source nodes are considered to be subjected to interference from the interferers. It is intuitively clear from the figure that the increasing density of sources leads to an increase in the secrecy outage probability which is in-contrast to Fig. 5a results. However it can be explained from fact that the interference impacts the legitimate communication severely and leads to secrecy outage. Therefore, cooperation among source nodes need to be considered in-order to improve the security of the system.

Leveraging from Fig. 5 and Fig. 6, we now depict the mentioned results from the point of view of the security-region in Fig. 7. This figure plots the results derived in proposition 3 and 4. We show both the limiting value of K sources located inside the security-region and the maximum number of eavesdroppers that can be accommodated for a given secrecy outage constraint. These sources inside the security-region can participate to form the CoMP sources. Two important results that can be seen from the figure are: 1) the total number of sources taking part in the communication increases with the increase in secrecy outage probability constraint and 2) the total number of eavesdroppers that can affect the communication decreases with the increase in secrecy outage probability constraint. The first result can be explained as - relaxing the outage constraint allows the system to accommodate more number of users. The second result can be explained as - when the outage probability is less, more number of eavesdroppers are required to affect the secure communication and vice versa.

In Fig. 8, the secrecy outage probability is shown with respect to a target rate for a given eavesdropper density. This figure complements the previous figures where the first best source outperforms the second. Here, we also stress on the fact that when $k = 1$, Proposition 2 matches with Proposition 1. Furthermore, with the increase in the path loss exponent, the secrecy outage probability decreases, as is evident from the figure. This phenomenon can be explained by the fact that

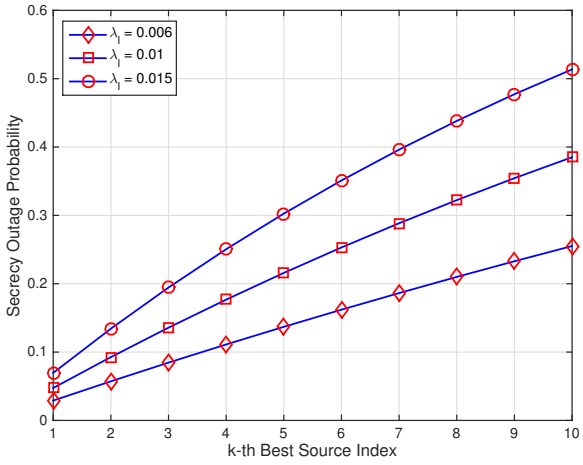


Fig. 6: Secrecy outage probability as a function of k-th best source index for different λ_s without considering interference at eavesdropper.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TCOMM.2017.2713385, IEEE Transactions on Communications

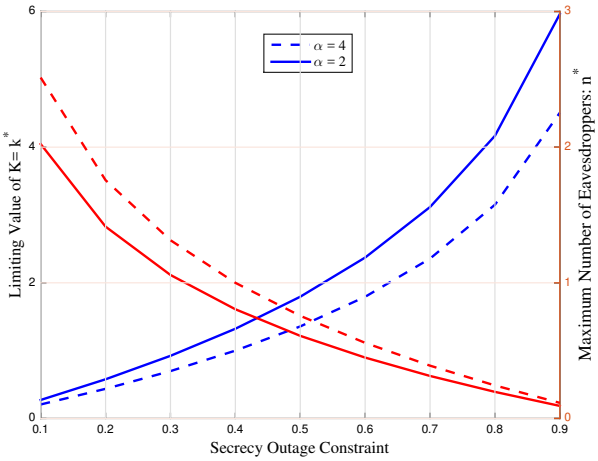


Fig. 7: Illustration of the limiting value of sources and the maximum number of eavesdroppers w.r.t ϵ for α.

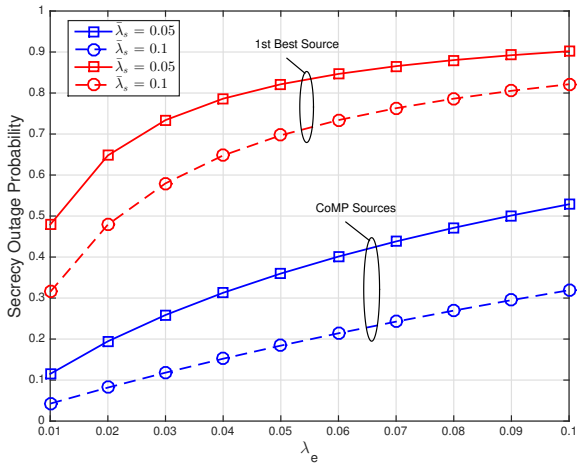


Fig. 9: Comparison of secrecy outage probability for the cases described in section III and IV as a function of eavesdropper density.

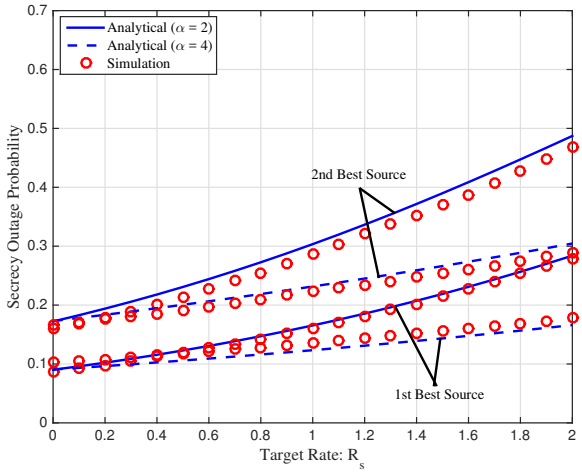


Fig. 8: Secrecy outage probability as a function of target rate for various path loss exponent α and for different best source indices.

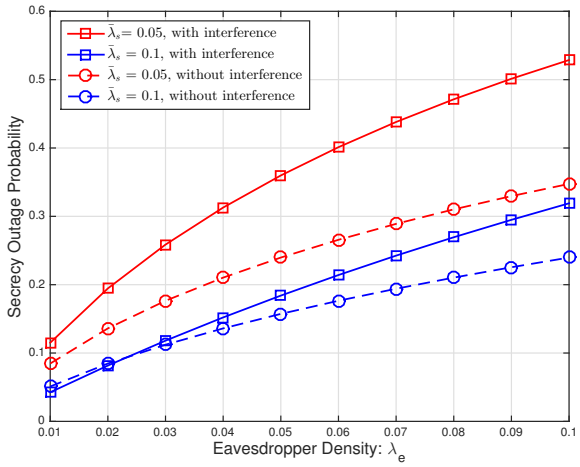


Fig. 10: Comparison of secrecy outage probability for CoMP scenario as a function of eavesdropper density.

the increase in path loss exponent causes higher distortion in signal at the eavesdropper for a given best source index.

Fig. 9 shows the comparison between the first best source and the CoMP sources. It is evident from the figure that the CoMP sources outperforms the first best source, which is quite intuitive. However, with the additional sources associated in the CoMP network, complex signal processing techniques are required to process the received signals and also maintain the required coordination among the sources. This may increase the complexity of the network and for systems with smaller dimensions with power constraints, it might be beneficial to use the best source.

An interesting outcome of the analysis is that the uncertainty of the number of sources communicating safely with the typical destination does not play a role any more with the introduction of the security-region. Furthermore, the path loss exponents and the eavesdropper density also play a major role in determining the security-region.

Finally in Fig. 10 we compare the secrecy outage probability as a function of eavesdropper density for the two cases of CoMP as mentioned in Section IV. The impact of interference can be clearly seen from the figure, where for a particular density, the network has more probability of outage when the interfering nodes are more. Furthermore, increasing the density of co-operating sources, reduces the probability of secrecy outage.

VI. Concluding Remarks

In this paper, the secrecy characteristics of random wireless networks with k-th best source indices was studied. The received path gain distributions of the typical destination and that of the best eavesdropper from the k-th best source are derived. Using these results, the secrecy outage probability $\mathcal{P}_{\text{out}}$ is also derived for different scenarios with respect to

the received path gain from any random source and the k-th best source. Based on the derived secrecy outage probability, security-region was defined which describes the number of sources that can safely communicate with a typical destination.

Specifically, it was shown that the security-region plays a crucial role in determining the secrecy capacity of CoMP networks. A bound on the number of sources that can cooperate among each other to form the CoMP network can be given with the help of the security-region. This may be useful in military applications where communication needs to be protected (or militarized) within a specific set of transmitters to guarantee high lever security of data. Moreover, the analysis presented in this paper can be helpful in determining the number of eavesdroppers which impact the performance of the collusion pool. An interesting outcome of the analysis is that the uncertainty of the number of eavesdroppers does not play a major role with the introduction of the security-region.

Further, the proposed cooperative scheme requires the instantaneous CSI of all sources, which may not be practical. However, co-operation can also work with partial CSI with specific CSI errors that can be implemented in the calculation of SINR in the paper. Co-operation among the sources with imperfect CSI will be considered in future extension of this work.

APPENDIX A
PROOF OF LEMMA 1

The CCDF of conditional SINR distribution, $F_{\zeta_k}(z)$, is

$$\bar{F}_{\xi_k}(z) = \Pr\{\xi_k > z\} = \Pr\left[\frac{P_k|\mathbf{h}_k\mathbf{v}_k|^2 {r_k}^{-\alpha}}{\mathcal{I}_k} > z\right] = \Pr\left[|\mathbf{h}_k\mathbf{v}_k|^2 > \frac{z\, r_k^{\alpha}}{P_k}\left(\mathcal{I}_k\right)\right]. \quad (45)$$

Under the assumption of Rayleigh fading, $H_k = |\mathbf{h}_k\mathbf{v}_k|^2$ follows a chi-square distribution [32] with $2N_t$ degrees of freedom and by employing the upper bound of gamma distribution with parameter N_t such that: $\mathbb{P}[H_k < \gamma] < (1-e^{-A\,\gamma})^{N_t}$ with $A = N_t(N_t!)^{\frac{-1}{N_t}}$, therefore, the equation (68) becomes

$$\bar{F}_{\xi_k}(z) = \sum_{k=1}^{N_t}\binom{N_t}{k}(-1)^k \mathrm{E}_{\mathcal{I}}\left[\exp\left(-\frac{\mathrm{z\,k\,r_k^{\alpha}}}{\mathrm{P_k}}\mathcal{I}\right)\right]. \quad (46)$$

The expectation of interference, *i.e* Laplace function for the $\mathcal{I}_k$ case is given as

$$\begin{aligned}
&\mathbb{E}_{\mathcal{I}}\left[\exp\left(-\frac{z\,k\,r_k^{\alpha}}{P_k}\mathcal{I}\right)\right] \\
&\overset{(a)}{=} \mathbb{E}_{\Phi_s}\left\{\prod_{i\in\Phi_s}\mathbb{E}_{H_i}\left[\exp\left(-zkr_k^{\alpha}\,H_i {x_i}^{-\alpha}\right)\right]\right\}, \\
&\overset{(b)}{=} \mathbb{E}_{\Phi_s}\left\{\prod_{i\in\Phi_s}\left(\frac{1}{1+zr_k^{\alpha}k\,{x_i}^{-\alpha}}\right)\right\}, \\
&\overset{(c)}{=} \exp\left[-2\pi\lambda_s\int_R^{\infty} r\left(1-\left(\frac{1}{1+zr_k^{\alpha}kx^{-\alpha}}\right)\right)\mathrm{d}x\right], \\
&= \exp\left[-\frac{2\pi^2\lambda_s r_k^2 z^{\frac{2}{\alpha}}k^{\frac{2}{\alpha}}}{\alpha\sin(\frac{2\pi}{\alpha})}\right]. \quad (47)
\end{aligned}$$

where (a) follows from the assumption of independent small scale fading, (b) follows from the use of exponential distributed random variables and (c) follows from the use of probability generating functionals of PPPs and $R \sim 0$. Finally, this proof concluded by providing the closed-form expression for the above integral.

APPENDIX B
PROOF OF LEMMA 2

Let $\Phi_{\mathrm{e}} = \left\{x_i \triangleq r^{-\alpha}\right\}$ be a path gain process. By using Mapping theorem [35], the density function of this point process can be given as

$$\lambda(x) = \frac{2\pi\lambda_{\mathrm{e}}}{\alpha}x^{\frac{-2}{\alpha}-1}. \quad (48)$$

Let $\xi = |\mathbf{h}_{\mathrm{e},k}\mathbf{v}_k|^2/\mathcal{I}_{\mathrm{e}}$. Since our propagation process Φ_{s} is also affected by fading and interference, *i.e* $\Phi = \{y_i \triangleq \xi_i x_i\}$, the density of this marked point process using the displacement theorem [35] can be written as

$$\hat{\lambda}(y) = \int_0^{\infty}\lambda(x)\rho(x,y)\,\mathrm{d}x, \quad (49)$$

where

$$\rho(x,y) = \frac{\mathrm{d}}{\mathrm{dy}}(1-F_{\xi_{\mathrm{e}}}(y/x)) = -\tfrac{y}{x^2}f_{\xi_{\mathrm{e}}}(y/x). \quad (50)$$

Thus (52) becomes

$$\begin{aligned}
\hat{\lambda}(y) &= \frac{1}{\alpha_i}\int_0^{\infty}2\pi\lambda_{\mathrm{e}}x^{\frac{-2}{\alpha}-1}\rho(x,y)\,\mathrm{d}x, \\
&= \frac{1}{\alpha}\int_0^{\infty}2\pi\lambda_{\mathrm{e}}\,x^{\frac{-2}{\alpha}-1}f_{\xi_{\mathrm{e}}}(y/x)\tfrac{1}{x}\,\mathrm{d}x, \\
&\overset{(z=\frac{y}{x})}{=} \frac{1}{\alpha}2\pi\lambda_{\mathrm{e}}\,y^{\frac{-2}{\alpha}-1}\int_0^{\infty}z^{\frac{2}{\alpha}}f_{\xi_{\mathrm{e}}}(z)\,\mathrm{d}z, \\
&= \frac{1}{\alpha}2\pi\lambda_{\mathrm{e}}\,y^{\frac{-2}{\alpha}-1}\mathbb{E}_{\xi_{\mathrm{e}}}\left(\xi_{\mathrm{e}}^{\frac{2}{\alpha}}\right). \quad (51)
\end{aligned}$$

where the characterisation of $\mathbb{E}_{\xi_{\mathrm{e}}}\left(\xi_{\mathrm{e}}^{\frac{2}{\alpha}}\right)$ is given in Appendix C under Rayleigh fading.

Using the void probability of a PPP, the path gain distribution for best source in the interval (z,∞) can thus be given as

$$\begin{aligned}
F_{\hat{\zeta}_{\mathrm{e}}}(z) &= \exp\left(-\int_z^{\infty}\hat{\lambda}(y)\mathrm{dy}\right), \quad (52)\\
&= \exp\left(-\frac{2\pi\lambda_{\mathrm{e}}}{\alpha}\,\mathbb{E}_{\xi_{\mathrm{e}}}\left(\xi_{\mathrm{e}}^{\frac{2}{\alpha}}\right)\int_z^{\infty}y^{\frac{-2}{\alpha}-1}\mathrm{dy}\right).
\end{aligned}$$

The proof concludes by evaluating the above integral in equation (52).

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TCOMM.2017.2713385, IEEE Transactions on Communications

APPENDIX C
PROOF OF $\mathbb{E}_{\xi_e}(.)$

Let

$$\xi_{\mathrm{e}} = \frac{|\mathbf{h}_{\mathrm{e},k}\mathbf{v}_k|^2}{\mathcal{I}_{\mathrm{e}}}. \tag{53}$$

Following the footprints of the proof of Lemma 1, the CCDF of conditional SINR distribution, $F_{\xi_k}(z)$ is given as

$$\bar{F}_{\xi_{\mathrm{e}}}(z) = \sum_{k=1}^{N_t} \binom{N_t}{k} (-1)^k \mathrm{E}_{\mathcal{I}} \left[\exp\left(-\mathrm{z\,k}\mathcal{I}_{\mathrm{e}}\right)\right], \tag{54}$$

where the expectation of interference, *i.e* Laplace function for the $\mathcal{I}_{\mathrm{e}}$ follows from the proof of Lemma 1, is given as

$$\mathbb{E}_{\mathcal{I}_{\mathrm{e}}}\left[\exp\left(-zk\mathcal{I}_{\mathrm{e}}\right)\right] = \exp\left[-\frac{2\pi^2\lambda_s z^{\frac{2}{\alpha}} k^{\frac{2}{\alpha}}}{\alpha \sin(\frac{2\pi}{\alpha})}\right]. \tag{55}$$

The proof concludes after calculating the partial moment of ξ_{e} using (54) as below

$$\mathbb{E}_{\xi_{\mathrm{e}}}\left(\xi_{\mathrm{e}}^{\frac{2}{\alpha}}\right) = \frac{2}{\alpha}\int_0^{\infty} x^{\frac{2}{\alpha}} \bar{F}_{\xi_{\mathrm{e}}}(x)\mathrm{d}x. \tag{56}$$

APPENDIX D
PROOF OF PROPOSITION 1

In order to evaluate the secrecy outage probability under scenario 2 as mentioned in Section III, we require the received path gain distributions at the typical destination and an eavesdropper which can be obtained using proposition 3. Using (9), the secrecy outage probability of the best source link can be given as

$$\mathcal{P}_{\mathrm{out}} = \int_0^{\infty}\int_0^{\beta(x)} f_{\hat{\zeta}_k}(y) f_{\hat{\zeta}_{\mathrm{e}}}(x)\,\mathrm{d}y\mathrm{d}x = \int_0^{\infty} \mathrm{F}_{\hat{\zeta}_{\mathrm{k}}}(\beta(\mathrm{x}))\mathrm{f}_{\hat{\zeta}_{\mathrm{e}}}(\mathrm{x})\mathrm{d}x. \tag{57}$$

Now, considering the high SNR regime, the secrecy outage probability can be given as

$$\mathcal{P}_{\mathrm{out}} = \frac{2\pi\lambda_{\mathrm{e}}}{\alpha}\int_0^{\infty} e^{-\pi\lambda_{\mathrm{s}} 2^{\frac{-2R_s}{\alpha}} x^{-\frac{2}{\alpha}} \mathbb{E}_{\xi_k}\left(\xi_k^{\frac{2}{\alpha}}\right)} \times x^{-\frac{2}{\alpha}-1} e^{-\pi\lambda_{\mathrm{e}} x^{-\frac{2}{\alpha}} \mathbb{E}_{\xi_{\mathrm{e}}}\left(\xi_{\mathrm{e}}^{\frac{2}{\alpha}}\right)} \mathrm{d}x, \tag{58}$$

Let us define the following two equalities

$$\Xi_k = \pi\lambda_{\mathrm{s}}\mathbb{E}_{\xi_k}\left(\xi_k^{\frac{2}{\alpha}}\right), \tag{59}$$

$$\Xi_{\mathrm{e}} = \pi\lambda_{\mathrm{e}}\mathbb{E}_{\xi_{\mathrm{e}}}\left(\xi_{\mathrm{e}}^{\frac{2}{\alpha}}\right). \tag{60}$$

Now, the above integral in (58) can be written as

$$\mathcal{P}_{\mathrm{out}} = \frac{2\Xi_{\mathrm{e}}}{\alpha}\int_0^{\infty} e^{-\left(2^{\frac{-2R_s}{\alpha}}\Xi_k + \Xi_{\mathrm{e}}\right)x^{-\frac{2}{\alpha}}} x^{-\frac{2}{\alpha}-1}\mathrm{d}x. \tag{61}$$

APPENDIX E
PROOF OF COROLLARY 4

The Laplace transform of the aggregate path gain can be given as

$$\begin{aligned}\mathcal{L}_{\bar{\zeta}_k}(w) &= \mathbb{E}\left[\exp\left(-w\sum_{x\in\Phi_{\mathrm{s}}}|h_x|^2||r||^{-\alpha}\right]\right), \\ &\overset{(a)}{=} \exp\left(-2\pi\lambda_{\mathrm{s}}\int_{\mathbb{R}^2}\mathbb{E}_h[1-e^{w\,|h_x|^2 x^{-\alpha}}]\cdot r\,\mathrm{d}r\right), \\ &\overset{(b)}{=} \exp\left(-\pi\lambda_{\mathrm{s}}\,\Gamma\left(1+\tfrac{2}{\alpha}\right)\Gamma\left(1-\tfrac{2}{\alpha}\right)w^{\frac{2}{\alpha}}\right),\end{aligned} \tag{62}$$

where (a) obtained from the property of PPP (Φ); (b) holds under Rayleigh fading assumption.

The closed form expression for above Laplace transform can be given from [44] as

$$f(y) = \frac{\pi^{\frac{3}{2}}\lambda_{\mathrm{s}} y^{-\frac{3}{2}}}{4}\exp\left(-\frac{\pi^4\lambda_{\mathrm{s}}^2}{16y}\right). \tag{63}$$

The proof concludes by taking the integration of the above equation.

APPENDIX F
PROOF OF PROPOSITION 6

Using the Gamma model for the aggregate path gain variate, the secrecy outage probability in presence of best the eavesdropper from (7) can be given as

$$\begin{aligned}\mathcal{P}_{\mathrm{out}} &= \int_0^{\infty} F_{\bar{\zeta}}(\beta(x)) f_{\hat{\zeta}_{\mathrm{e}}}(x)\mathrm{d}x, \\ &= \frac{2\Xi_{\mathrm{e}}}{\alpha}\int_0^{\infty}\left(1-e^{\frac{x}{\theta}}\sum_{j=0}^{\nu-1}\frac{x^j}{j!\theta^j}\right)e^{-\Xi_{\mathrm{e}}x^{-\frac{2}{\alpha}}}x^{-\frac{2}{\alpha}-1}\,\mathrm{d}x,\end{aligned} \tag{64}$$

where

$$F_{\bar{\zeta}}(x) = \frac{\gamma\left(\nu,\frac{x}{\theta}\right)}{\Gamma(\nu)} = 1-\sum_{i=0}^{\nu-1}\frac{1}{i!}\left(\frac{x}{\theta}\right)^i e^{-\frac{x}{\theta}}. \tag{65}$$

However, it is worthwhile to note that the above integral expression doesn't admit a closed form solution except for the specific case when $\alpha = 4$.

After evaluating the above integral, the closed form expression for secrecy outage probability for the specific case $\alpha = 4$ is given as

$$\begin{aligned}\mathcal{P}_{\mathrm{out}} = 1 &+ \frac{2\Xi_{\mathrm{e}}}{\alpha}\left(\Xi_{\mathrm{e}}\theta^{j-1}\Gamma(j-1){}_0F_2\left(;\frac{3}{2},2-j;-\frac{\Xi_{\mathrm{e}}^2}{4\theta}\right)\right. \\ &-\theta^{j-\frac{1}{2}}\Gamma\left(j-\frac{1}{2}\right){}_0F_2\left(;\frac{1}{2},\frac{3}{2}-j;-\frac{\Xi_{\mathrm{e}}^2}{4\theta}\right) \\ &\left.-2\Xi_{\mathrm{e}}^{2j-1}\Gamma(1-2j)\,{}_0F_2\left(;j,j+\frac{1}{2};-\frac{\Xi_{\mathrm{e}}^2}{4\theta}\right)\right).\end{aligned} \tag{66}$$

APPENDIX G
PROOF OF LEMMA 5

Let

$$\bar{\zeta_k} = \sum_{s\in\bar{\Phi}_s} |h_s|^2 {r_s}^{-\alpha} = \sum_{s\in\bar{\Phi}_s} |h_s|^2 \xi_s^{-1}, \tag{67}$$

where $\xi^{-1} = {r_s}^{-\alpha}$.

The CCDF of the SINR distribution, $\bar{F}_{\tilde{\zeta}_s}(z)$, is

$$\begin{aligned}\bar{F}_{\tilde{\zeta}_s}(z) &= \Pr\{\tilde{\zeta}_s > z\} = \Pr\left[\bar{\zeta}_s > z\bar{\mathcal{I}}_k\right], \\ &= \mathbb{E}_{\xi,\bar{\mathcal{I}}_k}\left[\Pr\left[\left|\sum_{s\in\Phi_s} h_s \xi_s^{-1/2}\right|^2 > z\ \bar{\mathcal{I}}_k\right]\right], \\ &\overset{(a)}{=} \mathbb{E}_{\bar{\mathcal{I}}_k}\left[\exp\left(\frac{z\ \bar{\mathcal{I}}_k}{\sum \xi_s^{-1}}\right)\right], \\ &\overset{(b)}{=} \int_{0<\xi_1<\cdots\xi_K<\infty} \mathcal{L}_{\bar{\mathcal{I}}_k}\left(\frac{z}{\sum_{s\in\Phi_s} x_s^{-1}}\right) f_\xi(x)\mathrm{d}x,\end{aligned} \tag{68}$$

where (a) follows from the cumulative density function of the exponentially distributed random variable $\tilde{\zeta}_s$ with mean $\sum \xi^{-1}$ and (b) is due to the expectation with respect to ξ. The characterization of $f_\xi(x)$ is omitted here due to space constraints. The Laplace transforms, i.e $\mathcal{L}_{\bar{\mathcal{I}}_k}$ follows from the proof of Lemma 1. The proof concludes after substituting this Laplace transforms into the integral in the above expression.

REFERENCES

[1] S. Vuppala, S. Biswas, T. Ratnarajah, and M. Sellathurai, "On the security region of best source indices in random wireless networks," in *Proc. IEEE International Conference on Communications*, Kuala Lumpur, Malaysia, May. 2016.

[2] P. K. Gopala, L. Lai, and H. El-Gamal, "On the secrecy capacity of fading channels," *IEEE Trans. Inform. Theory*, vol. 54, no. 10, pp. 4687 – 4698, Oct. 2008.

[3] Y. Liang, V. Poor, and S. Shamai, "Secure communication over fading channels," *IEEE Trans. Inform. Theory*, vol. 54, no. 6, pp. 2470 – 2492, Jun. 2008.

[4] M. Bloch, J. Barros, M. R. D. Rodrigues, and S. W. McLaughlin, "Wireless information-theoretic security," *IEEE Trans. Inform. Theory*, vol. 54, no. 6, pp. 2515 – 2534, Jun. 2008.

[5] A. D. Wyner, "The wire-tap channel," *Bell System Technical Journal*, vol. 54, no. 8, pp. 1355 –1367, Oct. 1975.

[6] L. Y. Cheong and M. Hellman, "The Gaussian wire-tap channel," *IEEE Trans. Inform. Theory*, vol. 24, no. 4, pp. 451 – 456, Jul. 1978.

[7] I. Csiszár and J. Körner, "Broadcast channels with confidential messages," *IEEE Trans. Inform. Theory*, vol. 24, no. 3, pp. 339 – 348, May 1978.

[8] M. Haenggi, "A geometric interpretation of fading in wireless networks: Theory and applications," *IEEE Trans. Inform. Theory*, vol. 54, no. 12, pp. 5500 – 5510, Dec. 2008.

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

[10] O. O. Koyluoglu, C. E. Koksal, and H. E. Gamal, "On secrecy capacity scaling in wireless networks," *IEEE Trans. Inform. Theory.*, vol. 58, no. 5, pp. 3000 – 3015, May. 2012.

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

[12] S. Vuppala and G. Abreu, "Unicasting on the secrecy graph," *IEEE Trans. Information Forensics and Security*, vol. 8, no. 9, pp. 1469 – 1481, Sep. 2013.

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

[14] Z. Gao, H. Zhu, S. Li, S. Du, and X. Li, "Security and privacy of collaborative spectrum sensing in cognitive radio networks," *IEEE Wireless Communications*, vol. 19, no. 6, pp. 106–112, Dec. 2012.

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

[16] S. Vuppala, W. Liu, T. Ratnarajah, and G. Abreu, "Secrecy outage analysis of cognitive wireless sensor networks," in *Proc. IEEE* 48th *Asilomar Conference on Signals, Systems and Computers*, Nov. 2-5 2014.

[17] H. Alves, C. H. M. de Lima, P. H. J. Nardelli, R. D. Souza, and M. Latva-aho, "On the secrecy of interference-limited networks under composite fading channels," *IEEE Signal Process. Letters*, vol. 22, no. 9, pp. 1306–1310, Jan. 2015.

[18] 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.

[19] N. Yang, L. Wang, M. Elkashlan, J. Yuan, and M. D. Renzo, "Safeguarding 5G wireless communication networks using physical layer security," *IEEE Commun. Mag.*, pp. 20–27, Apr. 2015.

[20] Y. Dang, L. Wang, M. Elkashlan, A. Nallanathan, and R. K. Mallik, "Physical layer security in three-tier wireless sensor networks: A stochastic geometry approach," *IEEE Trans. Inf. Forens. Security*, vol. 11, no. 6, pp. 1128–1138, Jun. 2016.

[21] H.-M. Wang and T. X. Zheng, *Physical Layer Security in Random Cellular Networks*. Springer, 2016.

[22] T.-X. Zheng, H.-M. Wang, J. Yuan, D. Towsley, and M. H. Lee, "Multi-antenna transmission with artificial noise against randomly distributed eavesdroppers," *IEEE Trans. Commun.*, vol. 63, no. 11, pp. 4347 – 4362, Nov. 2015.

[23] 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. pp, no. pp, Nov. 2016.

[24] 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.

[25] T. X. Zheng and H.-M. Wang, "Optimal power allocation for artificial noise under imperfect CSI against spatially random eavesdroppers," *IEEE Trans. Veh. Technol.*, vol. 65, no. 10, pp. 8812–8817, Oct. 2016.

[26] H. ElSawy, E. Hossain, and M. Haenggi, "Stochastic geometry for modeling, analysis, and design of multi-tier and congnitive cellular wireless networks:a survey," *IEEE Communications Surveys and Tutorials*, vol. 15, no. 3, pp. 996 – 1019, July 2013.

[27] H. Wei, N. Deng, W. Zhou, and M. Haenggi, "Approximate sir analysis in general heterogeneous cellular networks," *IEEE Trans. Commun.*, vol. 64, no. 3, pp. 1259–1273, Mar. 2016.

[28] F. Zabini and A. Conti, "Inhomogeneous poisson sampling of finite-energy signals with uncertainties in Rd," *IEEE Trans. Signal Process.*, vol. 64, no. 18, pp. 4679–4694, Sept. 2016.

[29] D. Daley and D. V. Jones, *An introduction to the theory of point processes.* NewYork: Springer, 1988.

[30] T.-X. Zheng, H.-M. Wang, and Q. Yin, "On transmission secrecy outage of a multi-antenna system with randomly located eavesdroppers," *IEEE Trans. Commun. Letters*, vol. 18, no. 8, pp. 1299–1302, Aug. 2014.

[31] W. Li, M. Ghogho, B. Chen, and C. Xiong, "Secure communication via sending artificical noise by the receiver: Outage secrecy capacity/region analysis," *IEEE Commun. Lett.*, vol. 16, no. 10, pp. 1628–1631, Oct. 2012.

[32] N. Lee, D. Morales-Jimenez, A. Lozano, and R. W. Heath, "Spectral efficiency of dynamic coordinated beamforming: A stochastic geometry approach," *IEEE Trans. Wireless Commun.*, vol. 14, no. 1, pp. 230–241, Jan. 2015.

[33] S. Vuppala, S. Biswas, and T. Ratnarajah, "An analysis on secure communication in millimeter/micro-wave hybrid networks," *IEEE Trans. Communications.*, vol. 64, no. 8, pp. 3507–3519, Aug. 2016.

[34] 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.

[35] M. Haenggi, *Stochastic Geometry for Wireless Networks*. Cambridge University Press, 2012.

[36] A. Hasan and J. G. Andrews, "The guard zone in wireless ad hoc networks," *IEEE Trans. Wireless Comm.*, vol. 4, no. 3, pp. 897–906, March 2007.

[37] H. Q. Nguyen, F. Baccelli, and D. Kofman, "A stochastic geometry analysis of dense IEEE 802.11 networks," in *IEEE International International Conference on Computer Communications*, 2007, p. 11991207.
[38] M. Haenggi, "Mean interference in hard-core wireless networks," *IEEE Commun. Lett.*, vol. 15, no. 8, pp. 792–794, Aug. 2011.
[39] S. Biswas, S. Vuppala, J. Xue, and T. Ratnarajah, "On the performance of relay aided millimeter wave networks," *IEEE J. Sel. Topics Signal Process.*, vol. 10, no. 3, pp. 576–588, Apr. 2016.
[40] A. Ghasemi and E. S. Sousa, "Interference aggregation in spectrum-sensing cognitive wireless networks," *IEEE Journal on Selected topics in Signal Processing.*, vol. 2, no. 1, pp. 41 – 56, Feb. 2008.
[41] A. P. Prudnikov, Y. A. Brychkov, and O. I. Marichev, *Integrals and Series - Elementary Functions*, ser. (in Russian). Moscow Fizmatlit, 2003, vol. 1.
[42] R. W. Heath, M. Kountouris, and T. Bai, "Modeling heterogeneous network interference using poisson point processes," *IEEE Transactions on Signal Processing*, vol. 61, no. 16, pp. 4114 – 4126, Aug. 2013.
[43] D. Maamari, N. Devroye, and D. Tuninetti, "Coverage in mmwave cellular networks with base station co-operation," *IEEE Trans. Wireless Commun.*, vol. 15, no. 4, pp. 2981–2994, Apr. 2016.
[44] J. Venkataraman, M. Haenggi, and O. Collins, "Shot noise models for outage and throughput analyses in wireless ad hoc networks outage and throughput analyses in wireless ad hoc networks," in *Proc. IEEE Military Communications Conference (MILCOM)*, Washington, DC, 2006.

Satyanarayana Vuppala (S'12-M'17) received the B.Tech. degree with distinction in Computer Science and Engineering from JNTU Kakinada, India, in 2009, and the M.Tech. degree in Information Technology from the National Institute of Technology, Durgapur, India, in 2011. He received the Ph.D. degree in Electrical Engineering from Jacobs University Bremen in 2014. He is currently a post-doctoral researcher at IDCOM in University of Edinburgh. His main research interests are physical, access, and network layer aspects of wireless security. He also works on performance evaluation of mmWave systems. He is a recipient of MHRD, India scholarship during the period of 2009-2011.

Sudip Biswas (S'15-M'17) received the B.Tech. degree in electronics and communication engineering from the Sikkim Manipal Institute of Technology, Sikkim, India, in 2010, the M.Sc. degree in signal processing and communications from the University of Edinburgh, Edinburgh, U.K. in 2013 and the Ph.D. degree in digital communications at the University of Edinburgh's Institute for Digital Communications (IDCOM) in 2017. He is currently working as a research associate at IDCOM in the University of Edinburgh. His research interests include various topics in wireless communications and network information theory with particular focus on stochastic geometry and possible 5G technologies such as massive MIMO, mmWave, LSA, NOMA and full-duplex.

Tharmalingam Ratnarajah (A'96-M'05-SM'05) is currently with the Institute for Digital Communications (IDCOM), University of Edinburgh, Edinburgh, UK, as a head of IDCOM and Professor in Digital Communications and Signal Processing. His research interests include signal processing and information theoretic aspects of 5G wireless networks, full-duplex radio, mmWave communications, random matrices theory, interference alignment, statistical and array signal processing and quantum information theory. He has published over 300 publications in these areas and holds four U.S. patents. He is currently the coordinator of the FP7 projects HARP (3.2M€) in the area of highly distributed MIMO and ADEL (3.7M€) in the area of licensed shared access. Previously, he was the coordinator of FP7 Future and Emerging Technologies project CROWN (2.3M€) in the area of cognitive radio networks and HIATUS (2.7M€) in the area of interference alignment. Dr Ratnarajah is a Fellow of Higher Education Academy (FHEA), U.K., and an associate editor of the IEEE Transactions on Signal Processing.