View metadata, citation and similar papers at core.ac.uk
brought to you by CORE
provided by Open Repository and Bibliography - Luxembourg

2017 IEEE Inter. Symp. on Personal, Indoor and Mobile Radio Communications (PIMRC), Montreal, Canada

Secrecy Analysis of Random Wireless Networks with Multiple Eavesdroppers

Satyanarayana Vuppala, Symeon Chatzinotas and Björn Ottersten
[satyanarayana.vuppala; symeon.chatzinotas; bjorn.ottersten]@uni.lu
Interdisciplinary Centre for Security, Reliability and Trust, University of Luxembourgh,
29, Avenue J.F Kennedy, L-1855 Luxembourg

***Abstract*—In this paper, we investigate the secrecy outage probability of random wireless networks from the perspective of the k-th best source, which has still not been well characterized. We consider the artificial noise (AN) transmission strategy at source nodes to confuse the eavesdropper. Furthermore, we use a 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 in bounding the number of sources that can cooperate 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 results are presented under various assumptions of densities, antenna gains, AN transmission factors and path loss exponents.**

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

I. Introduction

The key goals of future generation wireless communication systems include billions of connected devices, data rates in the range of Gbps, lower latencies, increased reliability, improved coverage and environment-friendly, low-cost, and energy efficient operation. Therefore, wireless security is becoming increasingly crucial in such communication systems, leading researchers to investigate information theoretic approaches to achieve secrecy in the wireless channel. Considerable efforts have been made by authors in [1]–[4] to develop information-theoretic security, which enhances the chance of a secure communication in the presence of eavesdroppers.

It is worth mentioning that the contribution [1] of Wyner lies in the introduction of the notion of *wiretap channel* for the discrete memoryless channel. Later on, the concept of wiretap channel has been extended to generalized channels, such as additive white Gaussian noise (AWGN) channels by Cheong and Hellman [2], and broadcast wireless channel by Csiszár and Körner [3].

In recent past, a considerable amount of reasearch has been done on intrinsic secrecy in random wireless networks [5]–[8]. In this direction, artificial noise (AN) transmission is shown to be one of key approaches to guarantee security provided that the instantaneous channel state information (CSI) of each eavesdropper is not available [5]. The transmitter uses multiple antenna to allocate some of the available power to transmit artificially generated noise, in addition to the information bearing signal, in the null-space of the channel of the legitimate user. The objective of AN transmission is to degrade the eavesdroppers channel so that the secrecy capacity of the legitimate channel is achieved. Recently, AN-aided secure transmission has gained immense research interest. To mention some, in [6], the authors adopted AN-aided secure communication to design the maximal throughput scheme under secrecy constraint where the CSI is updated adaptively through feedback. Whereas [7], [9] analysed an achievable secrecy rate and used this to optimise the transmitted power allocation between AN and information signal. In this paper, we also adopt a AN-aided secure communication where the source nodes allocate some power to radiate AN to mask the information signal from eavesdroppers.

On the other hand, considering user association criteria in cellular networks, authors in [10] characterized the secrecy outage probability of the k-th nearest receiver (i.e., the index is based on the distance between the source and the destination). Moving in this direction, Vuppala *et al.* have proposed a novel concept of "security region" [11], defined as the region in which the set of ordered nodes can safely communicate with typical destination for a given secrecy outage constraint. However, *the results unveiled in [11] are limited to the noise limited case. Moreover, the works [8], [10], [11] do not exploit the Coordinated Multi-point transmission (CoMP) from the perspective of security region.*

In this paper, we address the mentioned challenges by deriving the received k-th best signal to noise interference ratio (SINR) distributions from the sources to the destination and eavesdroppers and expressions for the secrecy outage probability of random networks. We construct the CoMP network using the concept of security-region which is based on the K^* best sources. Selecting such best sources to coordinate among each other can further *improve the security* of the network. At this point we would like to state that this model is applicable to

978-1-5386-3531-5/17/$31.00 © 2017 IEEE

any fading scenarios and also for models which include colluding eavesdroppers. The contributions of this work are multi-fold and are given as:

- For a given secrecy outage constraint, a novel *security-region* concept is studied.
- We obtain closed-form expression for the limiting number of ordered sources that can participate in the CoMP.
- Finally, we derive the secrecy outage probability of CoMP sources that include only the sources which are within the security-region.

II. System Model

We consider a network in Euclidean space of dimension d, modeled by a homogeneous Poisson Point Process (PPP) [12] 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 $\lambda_{\rm e}$. All 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 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.

We assume that source nodes use some portion of the transmit power P_k, *i.e.* $(1-\phi)P_k$, to radiate AN in the null-space the channel of the transmitter, leaving the other portion of transmit power, ϕP_k, to transmit information bearing signal, provided that $0 \leq \phi \leq 1$. For tractable analysis, we adopt a sectoring model with AN from [13]. Therefore, each source node has a main lobe of gain G_l with probability of angle of spread ϵ. Whereas, during AN transmission, source node possesses a main lobe of gain G_a with probability of angle of spread $1-\epsilon$. It is also assumed that the sectors of the information signals and AN are non-overlapping.

With a slight abuse of notation, let's consider Φ_s as the sets of interfering source locations. Using stochastic geometry tools, the interfering source nodes can be divided into two independent PPPs: (1) source nodes, Φ_s^l, that send information signals to the nearest receiver with intensity $\epsilon\lambda_s$; (2) source nodes, Φ_s^a, transmitting AN to the receiver with intensity $(1-\epsilon)\lambda_s$ for $0 \leq \epsilon \leq 1$. As a result, the SINR at destination from a given k-th source can be rewritten as

$$\tilde{\zeta}_k \triangleq \frac{P_k G_k |\mathbf{h}_k|^2 {r_k}^{-\alpha}}{\sigma_k^2 + \sum\limits_{i\in\Phi_s^l} \phi P_k G_l |\mathbf{h}_i|^2 r_i^{-\alpha} + \sum\limits_{i\in\Phi_s^a} (1-\phi) P_k G_a |\mathbf{h}_i|^2 r_i^{-\alpha}}, \tag{1}$$

where G_k is the received gain at destination, $\mathbf{h}_k$ denotes the fading gain between a given source and destination; r_k is the distance between source and destination; σ_k^2 stands for AWGN power; and the path loss exponent is denoted by α; $\mathbf{h}_i$ denotes the fading gain between interfering source and destination; and r_i is the distance between interfering source and destination.

In current model, multiple eavesdroppers are considered to coexist within the cellular network in the presence of interfering source nodes. Through cooperation, the eavesdroppers jointly process the received signal and thus can nullify the interference arising due to the information signal among source nodes [14]. Therefore, the aggregate interference at eavesdropper is only affected by the AN transmission and AWGN. Readers are advised to read [14, Section III-B] to get detailed insight on this specific eavesdropping strategy. The resulting SINR at eavesdropper $\tilde{\zeta}_{\rm e}$ is

$$\tilde{\zeta}_{\rm e} \triangleq \frac{P_k G_{\rm e} |\mathbf{h}_{{\rm e},k}|^2 {r_{\rm e}}^{-\alpha}}{\sigma_{\rm e}^2 + \sum\limits_{i\in\Phi_s^a} (1-\phi) P_k G_a |\mathbf{h}_{{\rm e},i}|^2 r_i^{-\alpha}}, \tag{2}$$

where $G_{\rm e}$ is the received gain at eavesdropper, $\mathbf{h}_{{\rm e},k}$ denotes the fading gain between a given source and eavesdropper; $r_{\rm e}$ is the distance between source and eavesdropper; $\sigma_{\rm e}^2$ stands for AWGN power; $\mathbf{h}_{{\rm e},i}$ denotes the fading gain between interfering source and eavesdropper; and $r_{\rm e}$ is the distance between interfering source and eavesdropper.

Moreover, we focus on the worst-case eavesdropping strategy where the secrecy performance of the system based on solely on the most malicious eavesdropper with the largest SINR of the received signal. Therefore, the resulting SINR at the eavesdropper can be derived from equation (2) as

$$\hat{\zeta}_{\rm e} = \max_{{\rm e}\in\Phi_{\rm e}} \left\{ \frac{P_k G_{\rm e} |\mathbf{h}_{{\rm e},k}|^2 {r_{\rm e}}^{-\alpha}}{\sigma_{\rm e}^2 + \mathcal{I}_{\rm e}^a} \right\}, \tag{3}$$

where $\mathcal{I}_{\rm e}^a = \sum\limits_{i\in\Phi_s^a} (1-\phi) P_k G_a |\mathbf{h}_{{\rm e},i}|^2 r_i^{-\alpha}$.

Thus, the secrecy capacity between any k-th source and a typical destination is given as [15]

$$\mathcal{C}_s = \max\{0, \log_2\left(1+\tilde{\zeta}_k\right) - \log_2\left(1+\hat{\zeta}_{\rm e}\right)\} \text{bit/s/Hz}, \tag{4}$$

The *secrecy outage probability* is defined as [15]

$$\mathcal{P}_{\rm out} \triangleq \Pr\{\mathcal{C}_s < R_s\} = \Pr\left\{\log_2\!\left(\tfrac{1+\tilde{\zeta}_k}{1+\hat{\zeta}_e}\right) < R_s\right\}, \tag{5}$$

where R_s denotes the required target secrecy rate.

The secrecy outage probability between the source and destination node (in the presence of randomly located multiple eavesdroppers) can be derived from (5) as [8], [11], [15]

$$\mathcal{P}_{\rm out} = \int_0^\infty (1 - F_{\hat{\zeta}_{\rm e}}(\beta(y))) f_{\tilde{\zeta}_k}(y) {\rm d}y, \tag{6}$$

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.

Let us consider the case where the typical destination is able to identify which of its candidate sources has the maximum SINR, subsequently associating to that best source. In such system, we now define a 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 [16]. 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. To analyze such scenario with coordinated multi-point sources, we assume that all the sources exchange required ideal information amongst themselves through a backhaul connection.

$$\mathcal{S} \triangleq \{(K^*, \epsilon), \forall K^* \in \{1, \cdots, k^*\}, \mathcal{P}_{\text{out}} \leq \epsilon\}, \quad (7)$$

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 Outage and Maximal Limit

In this section, first we characterize the SINR distributions for the k-th best source and best eavesdropper. Afterwards, with possession of these SINR distributions of channels from sources to the destination node and the best eavesdropper, the secrecy outage probability is characterized. Finally, we devise a limit on the k-th best source to construct the security region using the secrecy outage constraint.

A. Received SINR Distributions

In this section, we intend to characterize the secrecy outage probability of a communication link between k-th best source and typical destination. Hence, the distributions of interest concerning the legitimate network are those corresponding to the SINR of each legitimate source ζ_k. In contrast, for a given legitimate SINR ζ_k what determines the secrecy capacity of a channel subjected to fading is not a specific eavesdropper, but rather the eavesdropper with the *maximum* SINR amongst them.

Lemma 1. *The received SINR distribution of best eavesdropper can be given as [17]*

$$F_{\hat{\zeta}_{\text{e}}}(z) = \exp\left(-\pi\lambda_{\text{e}} z^{\frac{-2}{\alpha}} \mathbb{E}_{\xi_{\text{e}}}\left(\xi_{\text{e}}^{\frac{2}{\alpha}}\right)\right), \quad (8)$$

and, an integral-form expression for $\mathbb{E}_{\xi_{\text{e}}}\left(\xi_{\text{e}}^{\frac{2}{\alpha}}\right)$ *under Rayleigh fading channel follows from Appendix B, is given as*

$$\mathbb{E}_{\xi_{\text{e}}}\left(\xi_{\text{e}}^{\frac{2}{\alpha}}\right) = \frac{2}{\alpha}\int_0^{\infty} x^{\frac{2}{\alpha}-1} e^{\frac{-z\,\sigma_{\text{e}}^2}{P_k G_{\text{e}}}} \mathbb{E}_{\mathcal{I}_{\text{e}}^a}\left[e^{\frac{-z\mathcal{I}_{\text{e}}^a}{P_k G_{\text{e}}}}\right], \quad (9)$$

where

$$\mathbb{E}_{\mathcal{I}_{\text{e}}^s}\left[\exp\left(\frac{-z\mathcal{I}_{\text{e}}^a}{P_k G_{\text{e}}}\right)\right] = e^{-\frac{\pi(1-\epsilon)\lambda_i z^{\frac{2}{\alpha}}\left((1-\phi)\frac{G_a}{G_{\text{e}}}\right)^{\frac{2}{\alpha}}}{\text{sinc}(\frac{2}{\alpha})}}. \quad (10)$$

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

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* SINR amongst the sources. One can find the SINR distribution of best source using the similar approach from Lemma 1.

Lemma 2. *The SINR distribution of the best source to the destination ($\hat{\zeta}_k$) can be given as*

$$F_{\hat{\zeta}_k}(z) = \exp\left(-\pi\lambda_{\text{s}} z^{\frac{-2}{\alpha}} \mathbb{E}_{\xi_k}\left(\xi_k^{\frac{2}{\alpha}}\right)\right), \quad (11)$$

where

$$\mathbb{E}_{\xi_k}\left(\xi_k^{\frac{2}{\alpha}}\right) = \frac{2}{\alpha}\int_0^{\infty} x^{\frac{2}{\alpha}-1} e^{\frac{-z\,\sigma_k^2}{P_k G_k}} \prod_{j\in s,a} \mathbb{E}_{\mathcal{I}_k^j}\left[e^{\frac{-z\mathcal{I}_k^j}{P_k G_k}}\right]. \quad (12)$$

where $\mathbb{E}_{\mathcal{I}_k^j}[.]$ *follows from the proof of Lemma 1.*

Proof. The proof follows from Lemma 1. □

Subsequently, we consider the case where the user connect to the node with the k-th best SINR, i.e., the k-th source provides the destination with the k-th maximum SINR.

Lemma 3. *The SINR distribution of the k-th best source ($\grave{\zeta}_k$) can be given as*

$$F_{\grave{\zeta}_k}(z) = \frac{\Gamma\left((2^{R_s}z)^{\frac{-2}{\alpha}}\Xi_k, k\right)}{(k-1)!}, \quad (13)$$

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

Proof. This proof follows from [11, Proposition 3]. □

B. Secrecy Outage Probability

Now, considering Lemma 3, the secrecy outage probability with respect to the k-th best source can be given in following proposition.

Proposition 1. *The secrecy outage probability for the link between the destination and the k-th best source in presence of the n-th best eavesdropper can be given as*

$$\mathcal{P}_{\text{out}} = \sum_{j=0}^{k-1} \frac{\Gamma(j+n)2^{\frac{-2jR_s}{\alpha}}}{j!\,\Gamma(n)\Xi_k^{-j}\Xi_{\text{e}}^{-n}}\left(\frac{1}{2^{\frac{-2R_s}{\alpha}}\Xi_k + \Xi_{\text{e}}}\right)^{j+n}, \quad (14)$$

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

Proof. The derivation of this proof follows straightforwardly by substituting the received SINR distributions of the typical destination and an eavesdropper in equation (6), and hence intermediate steps are omitted here due to space constraints. □

C. Maximal Limit

Now, in the following proposition we characterize the security-region of our system. From Proposition 1, one can obtain the maximum possible k-th index for a given secrecy outage constraint ω.

Proposition 2. *The limiting number of ordered sources that can securely communicate with the destination in presence of the best eavesdropper can be given as*

$$k^* = \log_{\frac{\Upsilon}{\Upsilon+1}}(1-\omega). \tag{15}$$

Proof: By defining $\Upsilon = \frac{2^{\frac{-2R_s}{\alpha}}\Xi_k}{\Xi_{\mathrm{e}}}$, $\mathcal{P}_{\mathrm{out}}$ in Eq. (14) can be re-written for the best eavesdropper case *i.e* $n = 1$ as

$$\mathcal{P}_{\mathrm{out}} = \sum_{j=0}^{k-1} \frac{\Upsilon^j}{(\Upsilon+1)^{j+1}}. \tag{16}$$

The Eq. (16) can be expressed as a geometric series as

$$\mathcal{P}_{\mathrm{out}} = \left(\frac{1}{\Upsilon+1}\right)\frac{1-(\frac{\Upsilon}{\Upsilon+1})^k}{1-\frac{\Upsilon}{\Upsilon+1}}. \tag{17}$$

Finally, the limiting value of K, *i.e* k^*, sources for a given secrecy outage constraint ω can be given from above equation (17) as

$$k^* = \log_{\frac{\Upsilon}{\Upsilon+1}}(1-\omega). \tag{18}$$

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

$$n^* = \log_{\frac{1}{\Upsilon+1}}(\omega). \tag{19}$$

Proof. This proof is obtained from Proposition 2 by keeping $k = 1$. □

IV. Secrecy Analysis of CoMP

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 Φ_{s}. To this end, the Matern hardcore point process models are more suitable. Unfortunately, the probability generating functionals does not exist in most of cases [18], [19]. But, it has been said in [18], [20] that the nodes further away from the hard core distance, d can still be modelled as a PPP with a approximated density. 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 $\bar{\Phi}_c$ with a density of $\bar{\lambda}_c$. 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

$$\bar{\zeta}_k = \sum_{x\in\bar{\Phi}_c} |h_x|^2 ||r_x||^{-\alpha}. \tag{20}$$

Now, the set of interfering source node locations[1], i.e., non-cooperating source nodes can be denoted as $\bar{\Phi}_s$ with density $\bar{\lambda}_s$. Hence, the SINR distribution in CoMP scenario is given as [21]

$$\bar{\zeta}_k = \frac{\sum\limits_{x\in\bar{\Phi}_c} P_k G_k |\mathbf{h}_x|^2 {r_x}^{-\alpha}}{\sigma_k^2 + \bar{\mathcal{I}}_k}, \tag{21}$$

where $\bar{\mathcal{I}}_k = \sum\limits_{i\in\bar{\Phi}_s^l} \phi P_k G_l |\mathbf{h}_i|^2 r_i^{-\alpha} + \sum\limits_{i\in\bar{\Phi}_s^a} (1-\phi) P_k G_a |\mathbf{h}_i|^2 r_i^{-\alpha}$.

In general case, the CoMP aggregates the power of all information signals to improve the communication rate. However, the aggregation of all the signals from the nodes which do not have sufficient power may not be a good practise. Thus, it is important to select the best nodes for the aggression process which can leads to minimum secrecy outage. In the following Lemma, we will provide a closed-form expressions for such aggregation by leveraging the analysis from [21].

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

Lemma 4. *The CDF of the aggregate SINR in CoMP scenario with interference can be given as*

$$F_{\bar{\zeta}_k}(z) = 1 - \int\limits_{0<\xi_1<\cdots\xi_K<\infty} \mathcal{L}_{\sigma_k^2}\left(\frac{z}{\sum\limits_{c\in\bar{\Phi}_c} x_c^{-1}}\right)\prod_{j\in s,a}\mathcal{L}_{\bar{\mathcal{I}}_k^j}\left(\frac{z}{\sum\limits_{c\in\bar{\Phi}_c} x_c^{-1}}\right) f_{\xi}(x_c)\mathrm{d}x_c, \tag{22}$$

where

$$\mathcal{L}_{\sigma^2}(t) = e^{-\frac{t\,\sigma_k^2}{P_k G_k}} \tag{23}$$

$$f_{\xi}(x) = \prod_{s\in\bar{\Phi}_c} \frac{2}{\alpha}\pi\bar{\lambda}_c\, x^{\frac{2}{\alpha}-1} e^{-\pi\bar{\lambda}_c x^{\frac{2}{\alpha}}}, \tag{24}$$

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

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

Using equation (4), the secrecy outage probability ($R_s = 0$) is given by

$$\mathcal{P}_{\text{out}} = \int_0^{\infty} F_{\bar{\zeta}_k}(z) f_{\hat{\zeta}_e}(z)\mathrm{d}z, \tag{25}$$

where $f_{\hat{\zeta}_e}(z)$ can be obtained by taking derivative of $\bar{F}_{\zeta_e}(z)$ in (8) and $F_{\bar{\zeta}_k}(z)$ follows from Lemma 4. Unfortunately the above integral does not admit closed-form. However, one can evaluate the integral numerically.

V. Numerical Results

Unless stated otherwise, we consider the following simulation parameters: $\lambda_s = 0.00001$, $\lambda_e = 0.00005$, $P_t = 0$ dB, $\epsilon = 0.1$, $\phi = 0.1$, $G_k = G_e = G_l = 5$ dB, $G_a = -5$ dB and $\alpha = 2.5$. Also the target rate is kept constant at $R_s = 0.1$ bit/s/Hz. Fig. 1 shows the secrecy outage probability as a function of the k-th best source index for various target secrecy rates. 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 path gain or fading gain from the source. Here, we also stress on the fact that the increase in the path loss exponent degrades the eavesdropper channel worse which leads to decrease in the secrecy outage probability. It is also intuitively clear from the figure that the increasing target secrecy rate leads to an increase in the secrecy outage probability.

Following the footprints of Fig. 1, we now plot the secrecy outage probability as function of k-th best source index in Fig. 2 for different values of λ_e and ϕ. Similar settings are considered in Fig. 2 except for the path loss exponent and target secrecy rate. We can conclude that when the typical destination is receiving from the k-th source node, the secrecy outage probability increases in

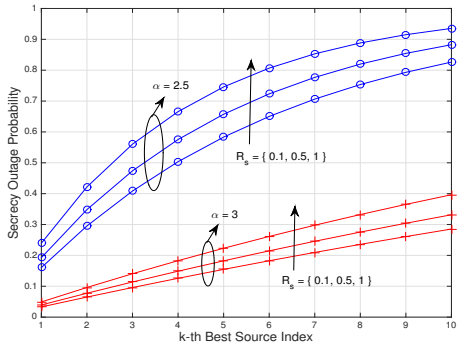

Fig. 1: Secrecy outage probability as a function of k-th best source index for different R_s.

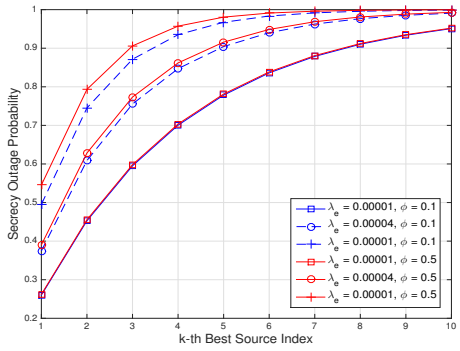

Fig. 2: Secrecy outage probability as a function of k-th best source index for different λ_e.

an ascending order. It is also clear from the figure that the increasing density of eavesdroppers leads to an increase in the secrecy outage probability, and this phenomena is well proved in recent literature on secrecy. But the important point to consider is that with decreasing the fraction of total transmitted power, ϕ, the secrecy capacity improves slightly. This is because the low values of ϕ implies allocating higher share of power to convey AN rather than information bearing signal. In turn, it increases the density source nodes which will ultimately degrade the eavesdropper's channel and thus, yields an improved secrecy capacity. Therefore, we can conclude from Fig.1 and Fig. 2 that the eavesdropper density, the path loss exponent, the transmit power fraction ϕ and the k-th source index play a major role in determining the secrecy capacity.

Leveraging from Fig. 1 and Fig. 2, we now depict the mentioned results from the point of view of the security-region in Fig. 3. This figure plots the results derived in Proposition 2. We show the limiting value of K sources located inside the security-region that can be accommodated for a given secrecy outage constraint ω. These sources inside the security-region can participate to form the CoMP sources. Some important results that can be seen from the figure are: 1) the total number of sources taking part in the communication increases

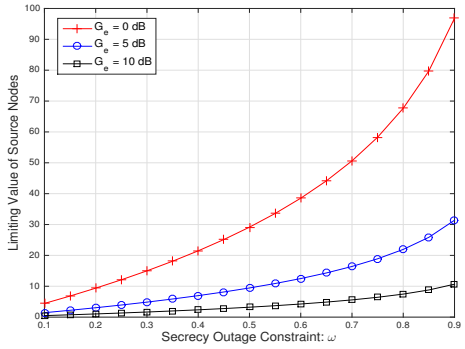

Fig. 3: Illustration of the limiting value of sources.

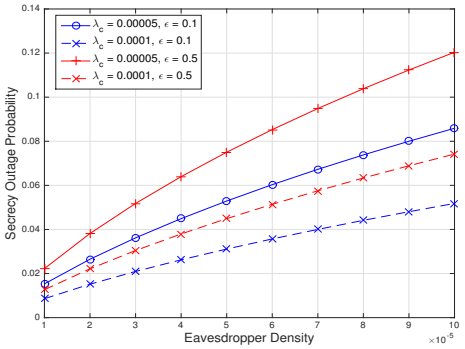

Fig. 4: Secrecy outage probability as a function of target rate for different best source indices.

with the increase in secrecy outage probability constraint and 2) the total number of sources that can affect the communication decreases with the increase in received gain at eavesdropper. The first result can be explained as - relaxing the outage constraint allows the system to accommodate more number of users at the cost of security. The second result can be explained fact that the increase in gain allows the eavesdropper to intercept the secure communication.

Finally in Fig. 4 we compare the secrecy outage probability as a function of eavesdropper density for different values of the probability of angle spread ϵ and cooperating source node densities. It can be concluded from the figure that as the probability of angle of spread ϵ increases, the outage probability of system increases. This phenomena can be explained the fact that higher ϵ values imply that an increased main lobe gain for source nodes to transmit information signal. Hence, less power will be allocated for AN transmission irrespective of available total transmit power. As a result, the eavesdropper channel will suffer a little as a result of AN transmission. We can conclude from the figure that the more the gain is allocated to transmit AN, the worse the eavesdropper channel becomes; consequently, the higher the probability of non-zero secrecy capacity is achieved. Furthermore, increasing the density of cooperating sources, reduces the probability of secrecy outage. It is also evident from all figures that the secrecy capacity of CoMP sources outperforms the best source, which is quite intuitive.

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, AN transmission factor such as ϕ and ϵ, antenna gains and the eavesdropper density also play a crucial role in determining the security-region.

VI. Concluding Remarks

In this paper, the secrecy outage probability $\mathcal{P}_{\text{out}}$ is derived with respect to the received SINR from the k-th best source. Based on this result, security-region is defined and a bound on the number of sources that can cooperate among each other to form the CoMP network is given. Specifically, it is show that CoMP sources within the security-region enhances the achievable secrecy capacity of the network. Furthermore, the benefit of AN-aided secure communication is illustrated in conjunction with CoMP networks. Moreover, the analysis presented in this paper can be helpful in determining the number of eavesdroppers which impact the performance of the collusion pool.

Appendix A
Proof of Lemma 1

Let $\Phi_{\text{e}} = \left\{ x_i \triangleq r^{-\alpha} \right\}$ be a path gain process. By using Mapping theorem [22], the density function of this point process can be given as

$$\lambda(x) = \frac{2\pi\lambda_{\text{e}}}{\alpha} x^{\frac{-2}{\alpha}-1}. \tag{26}$$

Let $\xi_{\text{e}} = P_k G_{\text{e}} |\mathbf{h}_{\text{e},k}|^2 / (\mathcal{I}_{\text{e}}^a + \sigma_{\text{e}}^2)$. 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 [22] can be written as

$$\hat{\lambda}(y) = \int_0^\infty \lambda(x)\rho(x,y)\, \mathrm{d}x, \tag{27}$$

where

$$\rho(x,y) = \frac{\mathrm{d}}{\mathrm{d}y}(1 - F_{\xi_{\text{e}}}(y/x)) = -\tfrac{y}{x^2} f_{\xi_{\text{e}}}(y/x). \tag{28}$$

Thus (27) becomes

$$\begin{aligned}
\hat{\lambda}(y) &= \frac{1}{\alpha_i} \int_0^\infty 2\pi\lambda_{\text{e}} x^{\frac{-2}{\alpha}-1} \rho(x,y)\, \mathrm{d}x, \\
&\overset{(z=\frac{y}{x})}{=} \frac{1}{\alpha} 2\pi\lambda_{\text{e}}\, y^{\frac{-2}{\alpha}-1} \int_0^\infty z^{\frac{2}{\alpha}} f_{\xi_{\text{e}}}(z)\, \mathrm{d}z, \\
&= \frac{1}{\alpha} 2\pi\lambda_{\text{e}}\, y^{\frac{-2}{\alpha}-1} \mathbb{E}_{\xi_{\text{e}}} \left(\xi_{\text{e}}^{\frac{2}{\alpha}} \right).
\end{aligned} \tag{29}$$

where the characterisation of $\mathbb{E}_{\xi_\mathrm{e}}\left(\xi_\mathrm{e}^{\frac{2}{\alpha}}\right)$ is given in Appendix B under Rayleigh fading. The proof concludes by evaluating the path gain distribution for best source using void probability of a PPP.

Appendix B
Proof of $\mathbb{E}_{\xi_\mathrm{e}}(.)$

Let

$$\xi_\mathrm{e} = \frac{P_k G_\mathrm{e} |\mathbf{h}_{\mathrm{e},k}|^2}{\mathcal{I}_\mathrm{e}^a + \sigma_\mathrm{e}^2}. \tag{30}$$

Under the assumption of Rayleigh fading channel, the CCDF of conditional SINR distribution, $\bar{F}_{\xi_\mathrm{e}}(z)$ is given as

$$\bar{F}_{\xi_\mathrm{e}}(z) = \exp\left(\frac{-z\,\sigma_\mathrm{e}^2}{P_k G_\mathrm{e}}\right) \mathbb{E}_{\mathcal{I}_\mathrm{e}^a}\left[\exp\left(\frac{-z\mathcal{I}_\mathrm{e}^a}{P_k G_\mathrm{e}}\right)\right]. \tag{31}$$

Following the footprints of the proof of [8, Lemma 1], the expectation (Laplace function) of I_e^a thus becomes

$$\mathbb{E}_{\mathcal{I}_d^s}\left[e^{\frac{-z\mathcal{I}_\mathrm{e}^a}{P_k G_\mathrm{e}}}\right] = e^{-\frac{\pi(1-\epsilon)\lambda_i z^{\frac{2}{\alpha}}\left((1-\phi)\frac{G_a}{G_\mathrm{e}}\right)^{\frac{2}{\alpha}}}{\mathrm{sinc}(\frac{2}{\alpha})}}. \tag{32}$$

The proof concludes after calculating the partial moment of ξ_e using (31) as below

$$\mathbb{E}_{\xi_\mathrm{e}}\left(\xi_\mathrm{e}^{\frac{2}{\alpha}}\right) = \frac{2}{\alpha}\int_0^\infty x^{\frac{2}{\alpha}} \bar{F}_{\xi_\mathrm{e}}(x)\mathrm{d}x. \tag{33}$$

Appendix C
Proof of Lemma 4

Let $\xi^{-1} = {r_s}^{-\alpha}$. The CCDF of the SINR distribution, $\bar{F}_{\bar{\zeta}_k}(z)$, is

$$\bar{F}_{\bar{\zeta}_k}(z) = \Pr\{\bar{\zeta}_k > z\} = \Pr\left[\bar{\zeta}_k > z\bar{\mathcal{I}}_k\right], \tag{34}$$

$$\overset{(a)}{=} \mathbb{E}_{\bar{\mathcal{I}}_k,\sigma_k^2}\left[\exp\left(\frac{z\,(\bar{\mathcal{I}}_k + \sigma_k^2)}{\sum \xi_s^{-1}}\right)\right],$$

$$\overset{(b)}{=} \int_{0<\xi_1<\cdots\xi_K<\infty} \mathcal{L}_{\sigma_k^2}\left(\frac{z}{\sum\limits_{c\in\Phi_c} x_c^{-1}}\right)\mathcal{L}_{\bar{\mathcal{I}}_k}\left(\frac{z}{\sum\limits_{c\in\Phi_c} x_c^{-1}}\right) f_\xi(x_c)\mathrm{d}x_c,$$

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

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

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

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

[6] X. Zhang, X. Zhou, and M. R. McKay, "On the Design of Artificial-Noise-Aided Secure Multi-Antenna Transmission in Slow Fading Channels," *IEEE Transactions on Vehicular Technology*, vol. 62, no. 5, pp. 2170–2181, Jun 2013.

[7] 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 Transactions on Communications*, vol. 63, no. 11, pp. 4347–4362, Nov 2015.

[8] Y. J. Tolossa, S. Vuppala, G. Kaddoum, and G. Abreu, "On the uplink secrecy capacity analysis in D2D-enabled cellular network," *IEEE Systems Journal*, vol. pp, no. pp, May 2017.

[9] X. Zhou and M. R. McKay, "Secure Transmission With Artificial Noise Over Fading Channels: Achievable Rate and Optimal Power Allocation," *IEEE Transactions on Vehicular Technology*, vol. 59, no. 8, pp. 3831–3842, Oct 2010.

[10] J. Bai, X. Tao, J. Xu, and Q. Cui, "The secrecy outage probability for the *i*th closest legitimate user in stochastic networks," *IEEE Commun. Lett.*, vol. 18, no. 7, pp. 1230–1233, Jul. 2014.

[11] 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.

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

[13] C. Wang and H. M. Wang, "Physical Layer Security in Millimeter Wave Cellular Networks," *IEEE Trans. Wireless Commun. (in press)*, vol. xx, no. xx, pp. xx–xx, May. 2016.

[14] X. Zhang, X. Zhou, and M. R. McKay, "Enhancing Secrecy With Multi-Antenna Transmission in Wireless Ad-Hoc Networks," *IEEE Trans. Inf. Forens. Security*, 2013.

[15] 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.

[16] 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.

[17] 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.

[18] 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.

[19] M. Haenggi, "Mean interference in hard-core wireless networks," *IEEE Commun. Lett.*, vol. 15, no. 8, pp. 792–794, Aug. 2011.

[20] 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.

[21] 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.

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