The Meta Distribution of the Secrecy Rate in the Presence of Randomly Located Eavesdroppers

Jinchuan Tang, *Student Member, IEEE,* Gaojie Chen, *Member, IEEE,* and Justin P. Coon, *Senior Member, IEEE*

Abstract—This letter studies the meta distribution of the secrecy rate for a legitimate link in the presence of eavesdroppers (EDs) with locations modeled as a Poisson point process (PPP). Both colluding and non-colluding EDs are considered. The meta distribution of the secrecy rate can provide the fraction of the realizations of EDs fulfilling a target secrecy rate. It can either be formulated using the Gil-Pelaez theorem with the imaginary moments of the conditional secrecy success probability (CSSP) given the realization of eavesdroppers or approximated by the beta distribution with the first two moments only. Hence, we first derive the bth moment of the CSSP for the colluding scenario. Then, we formulate the exact first moment and the approximated second moment of the CSSP for the non-colluding scenario using the Fortuin-Kasteleyn-Ginibre inequality. Finally, simulations are used to validate the analytic results.

Index Terms—Meta distribution, conditional secrecy success probability, Poisson point process, colluding and non-colluding eavesdroppers, and beta approximation.

I. INTRODUCTION

Physical layer security (PLS) is the idea that channel coding and signal processing techniques can be used to secure data confidentiality between connected devices [1]. Compared with the computationally secure encryption schemes, PLS promises theoretically perfect secrecy in a wireless channel [2]. A common performance metric used to analyze secrecy in fading channels is the secrecy success probability. This metric characterizes the probability that the instantaneous secrecy capacity of a legitimate connection is above the target secrecy rate when the system operates in the presence of randomly distributed colluding and non-colluding eavesdroppers (EDs) [3], [4]. In the colluding scenario, the EDs share their received signals with each other [4], while in the non-colluding scenario, each ED processes its received signal independently. To enhance the secrecy success probability in cellular networks, techniques such as antenna selection, user ordering, and artificial noise injection have been used [5], [6].

In networks with randomly distributed EDs, the secrecy success probability is typically defined to capture the *average* performance of a link. This definition loses the fine-grained detail about the fraction of the realizations of EDs fulfilling a target secrecy rate. To overcome this issue, the meta distribution of the signal-to-interference ratio (SIR) was

proposed in [7]. For a stationary and ergodic point process, this distribution yields the fraction of links fulfilling the target SIR in each realization of the point process. This basic theory was extended in [8] to study networks that exploit interference cancellation. In [9], the meta distribution of the SIR in the cellular network uplink and downlink with fractional power control was studied. The meta distribution in downlink D2D underlaid cellular networks has been analyzed in [10]. To the best of our knowledge, however, no progress has been made to characterize the meta distribution of the secrecy rate in networks with randomly located EDs. In this letter, we address exactly this task. The contributions of our work can be summarized as follows:

1) We characterize the bth moment of the conditional secrecy success probability (CSSP) in a closed-form expression for the colluding scenario so that the meta distribution can be formulated as an exact expression using the Gil-Pelaez inversion formula or as a beta approximation in the usual way.
2) For the non-colluding scenario, we calculate the exact first moment and an approximated second moment of the CSSP by using the Fortuin-Kasteleyn-Ginibre inequality so that a suitable beta approximation to the meta distribution can be obtained.

II. SYSTEM MODEL

A. Network layout

We consider the scenario depicted in Fig. 1, where the transmitter s located at the origin sends messages to a receiver d located at a deterministic distance from the origin [4], [11], [12][1]. The EDs are assumed to be Poisson point process (PPP) distributed in the plane $\mathbb{R}^2$ with density λ, which either collude or work independently to decode the message received on their Gaussian wire-tap links. Comparing with the Poisson bipolar model in [7], the distribution of EDs in our system model is similar to the distribution of interferers in the Poisson bipolar model. In spite of this, our model studies the meta distribution of the secrecy rate under an eavesdropping assumption rather than SIR as is the case in the Poisson bipolar model. The distance between s and d is $l_{s,d}$. The path loss model is $c^2(4\pi\nu)^{-2}l_{s,y}^{-\alpha}$, where c is the speed of light and ν is the carrier frequency, $l_{s,y}$ is the distance between s and a terminal (i.e. d or EDs) y, and α is the path loss exponent. The

[1]This letter considers the scenario where a carefully planned frequency reuse pattern is assumed, and the transmitter can occupy some resource blocks exclusively in a relatively large region. The co-channel interference for cellular networks will be studied in the future work.
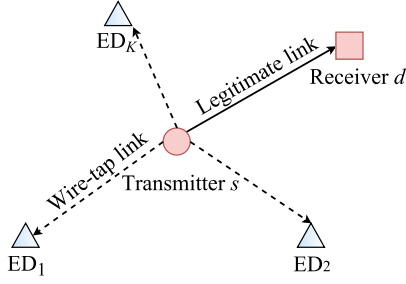
Fig. 1: Communication in the presence of eavesdroppers, where the dashed line and solid line denote wire-tap link and legitimate link, respectively.

fading of the channel is assumed to be Rayleigh, and the transmitting power is P_d. Hence, the received signal power at terminal y is denoted as $P_{s,y} = c^2(4\pi\nu)^{-2}l_{s,y}^{-\alpha}|h_{s,y}|^2 P_d$, and the receiving signal to noise ratio (SNR) at terminal y is given by $\text{SNR}_{s,y} = P_{s,y}/N_0$, where N_0 is the the additive white Gaussian noise (AWGN) power.

B. Secrecy capacity

The secrecy capacity of a link is the difference between the capacity of the legitimate link and the capacity achieved via a collection of wiretap links, which can be written as [4]

$$C_s = [\log_2(1 + \text{SNR}_{s,d}) - \log_2(1 + \mathscr{F}(\text{SNR}_{s,e}))]^+$$
$$\simeq \left[\log_2\left(\frac{|h_{s,d}|^2 l_{s,d}^{-\alpha}}{\mathscr{F}(|h_{s,e}|^2 l_{s,e}^{-\alpha})}\right)\right]^+, \quad (1)$$

where $[x]^+$ denotes $\max(0, x)$, operator $\mathscr{F}(\cdot)$ is either $\sum_{e\in\Phi}(\cdot)$ for the *colluding* scenario or $\max_{e\in\Phi}(\cdot)$ for the *non-colluding* scenario, Φ denotes the PPP of the EDs, and the symbol '$\simeq$' indicates that C_s asymptotically equals to the term on the right side of the symbol in the high SNR range.

C. The meta distribution of the secrecy rate

The CSSP of the typical user achieving a target secrecy rate R_t conditioning on the realization of Φ is given by

$$p(R_t) = \mathbb{P}(C_s > R_t \mid \Phi). \quad (2)$$

With the link reliability threshold p_t, the meta distribution is defined as

$$\overline{F}(R_t, p_t) = \mathbb{P}(p(R_t) > p_t), \quad (3)$$

which gives detailed information about the user experience by providing the proportion of users achieving R_t with a probability of p_t or above. Since it is difficult to calculate this meta distribution directly, the moments $M_b = \mathbb{E}(p(R_t)^b)$ are investigated instead [7]. Let $i^2 = -1$, $M_{it} = \mathbb{E}(p(R_t)^{it}) = \mathbb{E}(e^{it\log p(R_t)})$, the last term is denoted as the characteristic function $\varphi_X(t)$ and $X = \log p(R_t)$. The relationship between the complementary cumulative distribution function (CCDF) of a random variable X and its characteristic function is given by the Gil-Pelaez theorem [13]: $\overline{F}_X(x) = \frac{1}{2} +$

$\frac{1}{\pi}\int_0^\infty \frac{\Im[e^{-itx}\varphi_X(t)]}{t}\, \mathrm{d}t$, where $\Im[z]$ is the imaginary part of a complex number z. Thus, the meta distribution is given by

$$\overline{F}(R_t, p_t) = \frac{1}{2} + \frac{1}{\pi}\int_0^\infty \frac{\Im(e^{-it\log p_t} M_{it})}{t}\, \mathrm{d}t. \quad (4)$$

D. Beta approximation of the meta distribution

Since $p(R_t)$ is within $[0,1]$, a simplistic function named beta distribution can be used to approximate the meta distribution [7]. The probability density function of a beta distributed random variable Y is given by

$$f_Y(y \mid a, b) = \frac{y^{a-1}(1-y)^{b-1}}{\text{Beta}(a,b)}, \quad (5)$$

where $\text{Beta}(a,b) = \frac{\Gamma(a)\Gamma(b)}{\Gamma(a+b)}$, shape parameter $a, b > 0$, and its first and second moments are given by

$$\mathrm{E}[Y] = \frac{a}{a+b} \text{ and } \mathrm{Var}[Y] = \frac{ab}{(a+b)^2(a+b+1)}. \quad (6)$$

Let $M_1 = \mathrm{E}[Y]$ and $M_2 - M_1^2 = \mathrm{Var}[Y]$, the approximation of the meta distribution of the secrecy rate is written as

$$\overline{F}(R_t, p_t) \approx 1 - I_{p_t}\left(\frac{M_1 M_2 - M_1^2}{M_1^2 - M_2}, \frac{(1-M_1)(M_2 - M_1)}{M_1^2 - M_2}\right), \quad (7)$$

where $I_{p_t}(a, b)$ is the regularized incomplete beta function.

III. THE MOMENTS OF THE CSSP

A. Colluding EDs

Theorem 1. Letting $\theta = 2^{R_t}$, the bth moment of the CSSP for the colluding scenario is given by

$$M_b = \exp\left(-\lambda\pi l_{s,d}^2\Gamma(1 - 2/\alpha)\theta^{2/\alpha}\frac{\Gamma(b+2/\alpha)}{\Gamma(b)}\right). \quad (8)$$

Proof: The proof is similar to the derivation of Theorem 1 in [7] with transmit probability 1. □

B. Non-colluding EDs

1) General formula for M_b: The bth moment of the CSSP for the non-colluding scenario is given by

$$M_b = \mathbb{E}_\Phi\left[\mathbb{P}(C_s > R_t \mid \Phi)^b\right]$$
$$= \mathbb{E}_\Phi\left[\mathbb{P}\left(\max_{e\in\Phi}|h_{s,e}|^2 l_{s,e}^{-\alpha} < |h_{s,d}|^2 l_{s,d}^{-\alpha}/\theta\right)^b\right]$$
$$= \mathbb{E}_\Phi\left[\mathbb{E}_{h_{s,d}}\left[\prod_{e\in\Phi}\left(1 - \exp\left(-\frac{|h_{s,d}|^2 l_{s,d}^{-\alpha}}{\theta l_{s,e}^{-\alpha}}\right)\right) \mid h_{s,d}\right]^b\right]$$
$$= \mathbb{E}_\Phi\left[\left(\int_0^\infty \prod_{e\in\Phi}\left(1 - \exp\left(-\frac{x l_{s,d}^{-\alpha}}{\theta l_{s,e}^{-\alpha}}\right)\right)e^{-x}\, \mathrm{d}x\right)^b\right]. \quad (9)$$

This expression cannot be reduced to a simple analytic form for all the moments. To make progress, we investigate the case that can offer closed-form expressions for analysis based on beta approximation below.

2) Derivation of M_1 and M_2:

Theorem 2. The first moment of the CSSP for the non-colluding scenario is given by

$$M_1 = \frac{2\pi\sqrt{2pq}}{(2\pi)^{\frac{p}{2}+q}} G_{0,0}^{p+2q,0}\left(0, \frac{1}{p}, \ldots, \frac{p-1}{p}, \frac{1}{2q}, \frac{1}{q}, \ldots, 1 \left| \frac{p^{-p}A_1^p}{(2q)^{2q}} \right.\right),$$

$$(10)$$

where $G_{0,0}^{p+2q,0}$ is the Meijer G-function, which is defined as

$$
G_{p,q}^{m,n}\left(\begin{array}{c} a_1, \ldots, a_p \\ b_1, \ldots, b_q \end{array} \middle| x\right)
$$
$$
= \frac{1}{2\pi i}\int_L \frac{\prod_{j=1}^m \Gamma(b_j - s)\prod_{j=1}^n \Gamma(1-a_j+s)}{\prod_{j=m+1}^q \Gamma(1-b_j+s)\prod_{j=n+1}^p \Gamma(a_j-s)} x^s \, \mathrm{d}s,
$$

$$(11)$$

$A_1 = \lambda 2\pi\Gamma\left(\frac{2}{\alpha}\right)\frac{1}{\alpha}\left(\frac{l_{s,d}^2}{\theta^{-2/\alpha}}\right)$, the path loss exponent $\alpha = p/q$, with $p, q \in \mathbb{Z}^+$ so that α must be a rational number[2], and the second moment can be approximated as

$$M_2 \approx \frac{M_1^2}{2} + \frac{\pi\sqrt{2pq}}{(2\pi)^{\frac{p}{2}+q}}$$
$$\times G_{0,0}^{p+2q,0}\left(0, \frac{1}{p}, \ldots, \frac{p-1}{p}, \frac{1}{2q}, \frac{1}{q}, \ldots, 1 \left| \frac{p^{-p}A_2^p}{(2q)^{2q}} \right.\right),$$

$$(12)$$

where $A_2 = (2 - 2^{-2/\alpha})A_1$.

Proof: The first moment is derived as follows:

$$M_1 = \mathbb{E}_{h_{s,d}}\left[\mathbb{E}_\Phi\left[\prod_{e\in\Phi}\left(1 - \exp\left(-\frac{|h_{s,d}|^2 l_{s,d}^{-\alpha}}{\theta l_{s,e}^{-\alpha}}\right)\right)\right] \mid h_{s,d}\right]$$

$$\overset{(a)}{=} \int_0^\infty e^{-A_1 x^{-2/\alpha}} x e^{-x} \frac{\mathrm{d}x}{x}$$

$$\overset{(b)}{=} \frac{1}{2\pi i}\int_{\delta-i\infty}^{\delta+i\infty} \frac{A_1^{-\frac{w}{2/\alpha}}\Gamma\left(\frac{w}{2/\alpha}\right)}{2/\alpha}\Gamma(w+1)\,\mathrm{d}w$$

$$\overset{(c)}{=} \frac{1}{2\pi i}\int_{\frac{\delta}{2q}-i\infty}^{\frac{\delta}{2q}+i\infty} \frac{A_1^{-ps}\Gamma(ps)}{2q/p}\Gamma(2qs+1)2q\,\mathrm{d}s$$

$$\overset{(d)}{=} \frac{\sqrt{2pq}}{i(2\pi)^{\frac{p+2q}{2}}}\int_{\frac{\delta}{2q}-i\infty}^{\frac{\delta}{2q}+i\infty}\prod_{k=0}^{p-1}\Gamma\left(s+\frac{k}{p}\right)\prod_{k=0}^{2q-1}\Gamma\left(s+\frac{1+k}{2q}\right)$$

$$\times \left(A_1^p p^{-p}(2q)^{-2q}\right)^{-s}\,\mathrm{d}s$$

$$= \frac{2\pi\sqrt{2pq}}{(2\pi)^{\frac{p}{2}+q}} G_{0,0}^{p+2q,0}\left(0, \frac{1}{p}, \ldots, \frac{p-1}{p}, \frac{1}{2q}, \frac{1}{q}, \ldots, 1 \left| \frac{p^{-p}A_1^p}{(2q)^{2q}} \right.\right),$$

$$(13)$$

where (a) is the result of the probability generating functional of the PPP [14]; (b) is the Mellin convolution given by [15]

$$(f * g)(z) = \int_0^\infty f\left(\frac{z}{u}\right)g(u)\frac{\mathrm{d}u}{u} = \int_{\delta-i\infty}^{\delta+i\infty}\frac{\tilde{f}(w)\tilde{g}(w)\,\mathrm{d}w^z}{2\pi i z},$$

$$(14)$$

where $\tilde{f}(w)$ denotes the Mellin transform of a function $f(x)$, which is written as

$$\tilde{f}(w) = \int_0^\infty x^{w-1}f(x)\,\mathrm{d}x;$$

$$(15)$$

[2]A non-rational α can be approximated by a suitable rational value.

(c) is the result of a change of variables, i.e. $w = 2qs$, and δ is within the overlapped strip of analyticity of both $\tilde{f}(w)$ and $\tilde{g}(w)$; and (d) is obtained by the multiplication theorem

$$\Gamma(pz) = \frac{1}{(2\pi)^{\frac{p-1}{2}}\,p^{\frac{1}{2}-pz}}\prod_{k=0}^{p-1}\Gamma\left(z+\frac{k}{p}\right).$$

$$(16)$$

The second moment is defined as

$$M_2 = \mathbb{E}_\Phi\left[\mathbb{E}_{h_{s,d}}[f(\Phi, h_{s,d})]^2\right],$$

$$(17)$$

where $f(\Phi, h_{s,d}) = \prod_{e\in\Phi}\left(1 - \exp\left(-\frac{|h_{s,d}|^2 l_{s,d}^{-\alpha}}{\theta l_{s,e}^{-\alpha}}\right)\right)$. By using the Fortuin-Kasteleyn-Ginibre inequality, namely, $\mathbb{E}_\Phi\left[\mathbb{E}_{h_{s,d}}[f(\Phi, h_{s,d})]\right]^2 \leq M_2 \leq \mathbb{E}_\Phi\left[\mathbb{E}_{h_{s,d}}[f(\Phi, h_{s,d})^2]\right]$ [16], an approximation of M_2 can be given by

$$M_2 \approx \frac{M_1^2 + \mathbb{E}_\Phi\left[\mathbb{E}_{h_{s,d}}[f(\Phi, h_{s,d})^2]\right]}{2},$$

$$(18)$$

where

$$\mathbb{E}_\Phi\left[\mathbb{E}_{h_{s,d}}[f(\Phi, h_{s,d})^2]\right]$$
$$= \mathbb{E}_{h_{s,d}}\left[\mathbb{E}_\Phi\left[\prod_{e\in\Phi}\left(1 - \exp\left(-\frac{|h_{s,d}|^2 l_{s,d}^{-\alpha}}{\theta l_{s,e}^{-\alpha}}\right)\right)^2 \mid h_{s,d}\right]\right]$$
$$= \mathbb{E}_{h_{s,d}}\left[\exp(-F_2) \mid h_{s,d}\right],$$

and

$$F_2 = \lambda 2\pi\int_0^\infty\left[1 - \left(1 - \exp\left(-\frac{|h_{s,d}|^2 l_{s,d}^{-\alpha}}{\theta x^{-\alpha}}\right)\right)^2\right] x\,\mathrm{d}x$$

$$= \lambda 2\pi\int_0^\infty\sum_{k=1}^2\binom{2}{k}(-1)^{k+1}\exp\left(-\frac{k|h_{s,d}|^2 l_{s,d}^{-\alpha}}{\theta x^{-\alpha}}\right) x\,\mathrm{d}x$$

$$= A_2|h_{s,d}|^{-4/\alpha}.$$

$$(19)$$

Following this, the derivation of M_2 can be achieved by going through similar steps that used to obtain M_1. $\qquad\square$

IV. SIMULATIONS AND DISCUSSION

In this section, we provide simulation results to validate the analysis detailed above. During each Monte Carlo trial in the simulation, one realization of the PPP distributed EDs with density λ is considered in a 12×12 km^2 plane. A transmitter is located in the origin, while the intended receiver d is $l_{s,d} = 80$ m away from it. Meanwhile, $N_0 = -92$ dBm, $P_d = 0$ dBm, $R_t = 0$ and $\theta = 1$. The simulation results are obtained by averaging over 10^4 independent trials.

Fig. 2 gives the meta distribution of the secrecy rate vs. p_t for the colluding scenario with different values of α and λ. The simulation matches well with the numerical results, while the beta approximation shows slightly less accuracy when $\alpha = 4, \lambda = 80$ km^{-2}. The figure illustrates how the meta distribution varies with α and λ. The fundamental trends observed here, such as the benefits inherent in high path loss environments (i.e., increasing α), but it is interesting to note the severe penalty that λ induces through the sharp decay of $\bar{F}$ in the $\lambda = 100$ km^{-2} curves.
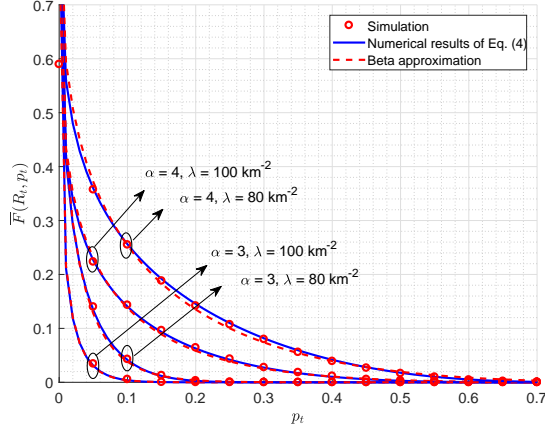
Fig. 2: The meta distribution of the secrecy rate vs. p_t for the colluding scenario.
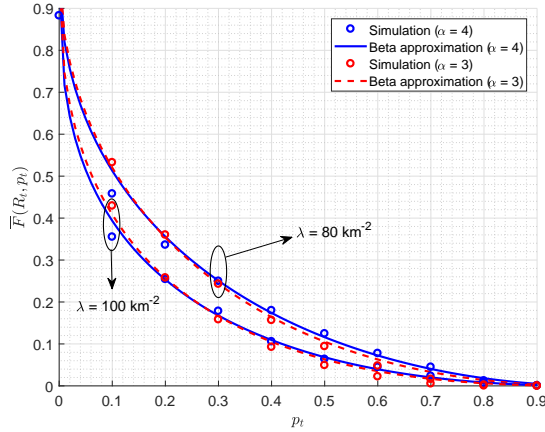

Fig. 3: The meta distribution of the secrecy rate vs. p_t for the non-colluding scenario.

Fig. 3 presents the meta distribution of the secrecy rate vs. p_t for the non-colluding scenario. It shows that the beta approximations from Theorem 2 work well in characterizing the meta distribution. It also shows that as α increases, $\overline{F}$ does not necessarily increase at all threshold p_t, which is different from the trend in Fig. 2. Meanwhile, compared with the colluding scenario, the increasing of α from 3 to 4 has less of an effect on $\overline{F}$ for the non-colluding scenario. Besides, for a given link reliability threshold $p_t = 0.6$, there are 4% satisfied spatial configurations of EDs for $\alpha = 4$ and $\lambda = 100$ km^{-2}, while 8% of configurations yield acceptable performance for $\alpha = 4$ and $\lambda = 80$ km^{-2}. Compared with the results of the colluding scenario in Fig. 2, the non-colluding scenario shows that a higher meta distribution has been achieved. It once again [17] shows that colluding among the EDs will decrease the probability of achieving a target secrecy rate of the legitimate link. In addition, $\overline{F}$ of the non-colluding scenario is lower bounded by the colluding scenario with the same parameters since the legitimate link of the non-colluding scenario will achieve a similar or even higher probability than its colluding

counterpart for the same realization.

V. CONCLUSION

In this letter, we studied the meta distribution of the secrecy rate for both colluding and non-colluding EDs scenarios. For the colluding scenario, the corresponding bth moments of the CSSP have been formulated in closed-form expressions. For the non-colluding scenario, the first two moments of the CSSP have been formulated. Simulation studies showed a good match between analytic and approximate results for both EDs scenarios. The results also showed that, unlike the colluding scenario, a larger path loss exponent does not necessarily yield more favorable performance at all the p_t for the non-colluding scenario. Meanwhile, the meta distribution for the non-colluding scenario is lower bounded by its colluding counterpart. The methods and analysis detailed in this letter can offer insight and design guidelines in PLS systems.

REFERENCES

[1] W. K. Harrison, J. Almeida, M. R. Bloch, S. W. McLaughlin, and J. Barros, "Coding for secrecy: An overview of error-control coding techniques for physical-layer security," *IEEE Signal Process. Mag.*, vol. 30, no. 5, pp. 41–50, Sep. 2013.

[2] H.-M. Wang and T.-X. Zheng, *Physical Layer Security in Random Cellular Networks*, 1st ed. Singapore: Springer, 2016.

[3] G. Geraci, S. Singh, J. G. Andrews, J. Yuan, and I. B. Collings, "Secrecy rates in broadcast channels with confidential messages and external eavesdroppers," *IEEE Trans. Wireless Commun.*, vol. 13, no. 5, pp. 2931–2943, May 2014.

[4] G. Chen, J. P. Coon, and M. Di Renzo, "Secrecy outage analysis for downlink transmissions in the presence of randomly located eavesdroppers," *IEEE Trans. Inf. Forensics Security*, vol. 12, no. 5, pp. 1195–1206, 2017.

[5] G. Chen, Y. Gong, P. Xiao, and J. A. Chambers, "Physical layer network security in the full-duplex relay system," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 3, pp. 574–583, Mar. 2015.

[6] G. Chen and J. P. Coon, "Secrecy outage analysis in random wireless networks with antenna selection and user ordering," *IEEE Wireless Commun. Lett.*, vol. 6, no. 3, pp. 334–337, Jun. 2017.

[7] M. Haenggi, "The meta distribution of the SIR in Poisson bipolar and cellular networks," *IEEE Trans. Wireless Commun.*, vol. 15, no. 4, pp. 2577–2589, Apr. 2016.

[8] Y. Wang, Q. Cui, M. Haenggi, and Z. Tan, "On the SIR meta distribution for Poisson networks with interference cancellation," *IEEE Wireless Commun. Lett.*, vol. PP, no. 99, Sep. 2017.

[9] Y. Wang, M. Haenggi, and Z. Tan, "The meta distribution of the SIR for cellular networks with power control," *Accepted in IEEE Trans. Commun.*, 2017.

[10] M. Salehi, A. Mohammadi, and M. Haenggi, "Analysis of D2D underlaid cellular networks: SIR meta distribution and mean local delay," *IEEE Trans. Commun.*, vol. 65, pp. 2904–2916, Jul. 2017.

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

[12] P. C. Pinto, J. Barros, and M. Z. Win, "Secure communication in stochastic wireless networks-part II: Maximum rate and collusion," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 1, pp. 139–147, Feb. 2012.

[13] J. Gil-Pelaez, "Note on the inversion theorem," *Biometrika*, vol. 38, no. 3-4, pp. 481–482, Dec. 1951.

[14] M. Haenggi, *Stochastic Geometry for Wireless Networks*. New York, NY, USA: Cambridge University Press, Oct. 2012.

[15] S. Yakubovich, "New inversion, convolution and Titchmarsh's theorems for the half-Hilbert transform," *Integral Transforms and Special Functions*, vol. 25, no. 12, pp. 955–968, Dec. 2014.

[16] R. Graham, "Applications of the FKG inequality and its relatives," in *Mathematical Programming: The State of the Art*. Springer, 1983, pp. 115–131.

[17] G. Chen, Y. Gong, P. Xiao, and J. A. Chambers, "Dual antenna selection in secure cognitive radio networks," *IEEE Trans. Veh. Technol.*, vol. 65, no. 10, pp. 7993–8002, Oct. 2016.