SIR Meta Distribution in Physical Layer Security with Interference Correlation

Qimei Cui*, Xueying Jiang*, Xinlei Yu*, Yuanjie Wang†, and Martin Haenggi‡
*National Engineering Lab for Mobile Network Technologies,
Beijing University of Posts and Telecommunications, Beijing, 100876, China
†State Key Laboratory of Railway Traffic Control and Safety, Beijing Jiaotong University, Beijing, 100044, China
‡Department of Electrical Engineering, University of Notre Dame, IN, 46556, USA
Email:{cuiqimei, jiangxy}@bupt.edu.cn; xinleiyu@hotmail.com;
wang.yuanjie@outlook.com; mhaenggi@nd.edu

***Abstract*—The meta distribution of the signal-to-interference ratio (SIR) provides more fine-grained information about the link performance than the standard success probability. This paper studies the reliability in cellular networks with physical layer security constraints using the meta distribution. We consider a cellular network where the BSs are distributed as Possion point process. We provide the distribution of the opportunistic secure spectrum access probability when connection success and secrecy success occurs simultaneously, taking into account the interference correlation. We gain insights on the links reliability in the network under different security levels and the effect on the link reliability of the distance between legitimate user and eavesdropper.**

I. Introduction

A. Motivation

Security has always been an important issue in wireless network transmission. Traditional security schemes operate at the medium access control (MAC) layer and the network layer using cryptographic technologies, which are effective in most cases. But they have limitations, such as their computational complexity, so it is difficult to implement secret key management in dynamic wireless networks. As a result, more and more attention is paid on physical layer security. Most of the previous papers focused on the secure transmission of links such as secure connection and secure transmission rate, but did not consider the overall security of the whole network. A key quantity of interest in wireless networks is the success probability $p_s(\theta) \triangleq \mathbb{P}(\text{SIR} > \theta)$ of the transmission over the typical link, which corresponds to the complementary cumulative distribution function (CCDF) of the signal-to-interference ratio (SIR). While this spatially averaged value is the certainly important, it does not reveal how concentrated the link success probabilities are. A more fine-grained performance metric—the meta distribution which is the CCDF of the conditional success probability—can solve problems such as "What fraction of users in a Poisson cellular network achieve 90% link reliability if the required SIR is 5 dB?".

B. Related Work

The meta distribution of the Poisson bipolar and cellular networks was introduced in [1], where the b-th moment of the conditional success probability in both bipolar networks and cellular networks were derived based on stochastic geometry. The moments were then used to obtain the meta distribution. The first and second moments were combined to obtain a simple beta distribution approximation, which provided an excellent approximation for the meta distribution. The meta distribution for device-to-device (D2D) underlay and the local delay were given in [2]. In [3], the meta distribution of the millimeter wave communication in the D2D scenario and the meta distribution of the transmission rate were analysed, and a general beta distribution as a modified approximation was given. [4] considered two types of users, namely the typical user and the cell-corner user, in the downlink coordinated multipoint transmission/reception (CoMP) including joint transmission (JT) and dynamic point blanking (DPB), and dynamic point selection/dynamic point blanking (DPS/DPB), and calculated the meta distribution of the SIR.

Information-theoretic security, widely accepted as the strictest notion of security, was combined with stochastic geometry for the first time in [5], where the secrecy graph was introduced, which models the network connectivity under secrecy constraints. The properties of the secrecy graph were further analyzed in [6]. Secure coverage in downlink Poisson cellular networks was introduced and studied in [7]. [8] defined a performance metric named the secrecy transmission capacity. The authors used tools and existing results from stochastic geometry to obtain the secrecy transmission capacity in Rayleigh fading channels. It is shown that the application of a secrecy guard zone with artificial noise is a simple technique that can be used to reduce the throughput cost of achieving secure networks. In [9], the authors quantified the effect of spatial interference correlation on opportunistic secure spectrum access (OSSA) in cellular-networks. [10] studied the meta distribution of the secrecy rate in physical layer security considering both colluding and non-colluding eavesdroppers, but ignoring interference.

C. Contributions

In this paper, we focus on the meta distribution of the SIR under physical layer security. The typical legitimate user and a nearby eavesdropper are considered. Through analytical

derivations and simulations, we give the opportunistic conditional secure spectrum access probability and its distribution considering interference correlation. We also obtain the reliability of the network when different levels of security are required and explore the effect of the distance between legitimate user and eavesdropper on the reliability.

II. System Model

A. SIR Model

We consider the problem of physical layer security in a single-tier downlink network. The base stations (BSs) are distributed according to a homogeneous Poisson point process (PPP) Φ_{BS} of intensity λ_{BS}. We focus on the downlink with the nearest-BS association. A cellular user is placed at the origin, i.e. legitimate user, who, under expectation over Φ_{BS}, becomes the typical user for any stationary model of users. We consider passive eavesdropping, where the eavesdropper (Eve) intercepts the signal without any attack. Eve is located at $\mathbf{v} = (v, 0)$. A realization of this network model is shown in Fig. 1. The BSs are always active, and the standard path loss law with path loss exponent α and Rayleigh fading are adopted, i.e., the channel gain between the transmitter $\mathbf{x}$ and the receiver $\mathbf{y}$ including large-scale fading and small-scale fading can be expressed as $h_{\mathbf{xy}}\|\mathbf{x}-\mathbf{y}\|^{-\alpha}$, where $h_{\mathbf{xy}}$ is i.i.d exponential with unit mean and α ($\alpha > 2$) is the path loss exponent. The effect of thermal noise is neglected.

The SIR of the typical user is given by

$$\begin{aligned}\mathrm{SIR_u} &= \frac{P_{\mathrm{BS}} h_{\mathbf{x}_0}\|\mathbf{x}_0\|^{-\alpha}}{\sum\limits_{\mathbf{x}\in\mathbf{\Phi}_{\mathrm{BS}}\setminus\{\mathbf{x}_0\}} P_{\mathrm{BS}} h_{\mathbf{x}}\|\mathbf{x}\|^{-\alpha}} \\ &= \frac{h_{\mathbf{x}_0}\|\mathbf{x}_0\|^{-\alpha}}{\sum\limits_{\mathbf{x}\in\mathbf{\Phi}_{\mathrm{BS}}\setminus\{\mathbf{x}_0\}} h_{\mathbf{x}}\|\mathbf{x}\|^{-\alpha}},\end{aligned} \tag{1}$$

where P_{BS} is the BS's transmission power, $h_{\mathbf{x_0}}$ is the Rayleigh fading between the typical user and its serving BS $\mathbf{x}_0$, and $\|\mathbf{x_0}\|^{-\alpha}$ is the path loss. $h_{\mathbf{x}}$ is the Rayleigh fading from interference BSs to the typical user, and $\|\mathbf{x}\|^{-\alpha}$ is the path loss between interference BS and the typical user.

Denoting the eavesdropper located at $\mathbf{v} = (v, 0)$ by $\mathbf{e}$, the received SIR is given by

$$\begin{aligned}\mathrm{SIR_e} &= \frac{P_{\mathrm{BS}} g_{\mathbf{x}_0}\|\mathbf{v}-\mathbf{x}_0\|^{-\alpha}}{\sum\limits_{\mathbf{x}\in\mathbf{\Phi}_{\mathrm{BS}}\setminus\{\mathbf{x}_0\}} P_{\mathrm{BS}} g_{\mathbf{x}}\|\mathbf{v}-\mathbf{x}\|^{-\alpha}} \\ &= \frac{g_{\mathbf{x}_0}\|\mathbf{v}-\mathbf{x}_0\|^{-\alpha}}{\sum\limits_{\mathbf{x}\in\mathbf{\Phi}_{\mathrm{BS}}\setminus\{\mathbf{x}_0\}} g_{\mathbf{x}}\|\mathbf{v}-\mathbf{x}\|^{-\alpha}},\end{aligned} \tag{2}$$

where $g_{\mathbf{x}_0}$ is the Rayleigh fading from the typical user's serving BS to the Eve, and $g_{\mathbf{x}}$ is the Rayleigh fading from the typical user's interfering BSs to Eve, $\|\mathbf{v}-\mathbf{x}_0\|^{-\alpha}$ is the path loss for the eavesdropping link, and $\|\mathbf{v}-\mathbf{x}\|^{-\alpha}$ is the path loss for Eve's interfering link.

We define the following three success probabilities for the confidential message transmission.

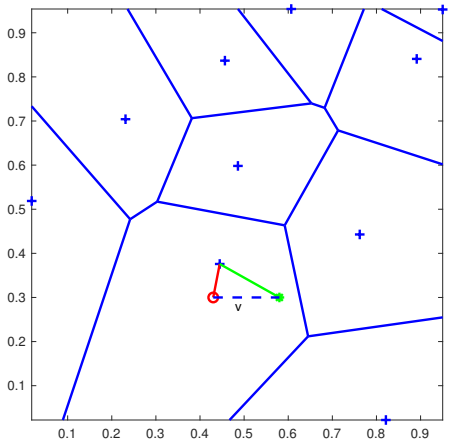

Fig. 1. A realization of the network model. The cross markers represent the BSs, the circle marker represents the typical legitimate user. The typical user is associated to the nearest BS. A line connecting circle marker and cross marker indicates the downlink legitimate link. The typical user and BSs form a cellular network. The star marker represents the eavesdropper, whose position is offset to the right by a distance of v from the typical legitimate user. The line connecting the star marker and the cross marker indicates the eavesdropping link.

- **Conditional connection success probability**: The probability that the SIR from the serving BS to the typical user is above the threshold θ_{u} given the point process Φ_{BS}, denoted by $P_{\mathrm{cs}}(\theta_{\mathrm{u}}) = \mathbb{P}(\mathrm{SIR_u} > \theta_{\mathrm{u}} \mid \Phi_{\mathrm{BS}})$.
- **Conditional secrecy success probability**: The probability that the SIR from the typical user's serving BS to Eve is below the threshold θ_{e} given the point process Φ_{BS}, denoted by $P_{\mathrm{ss}}(\theta_{\mathrm{e}}) = \mathbb{P}(\mathrm{SIR_e} < \theta_{\mathrm{e}} \mid \Phi_{\mathrm{BS}})$.
- **Conditional OSSA probability**: The probability of opportunistic secure spectrum access (OSSA), which has been proposed in [9], given the point process Φ_{BS}, denoted by P_{OSSA}. Due to the conditional independence given Φ_{BS}, $P_{\mathrm{OSSA}} = P_{\mathrm{cs}}(\theta_{\mathrm{u}})P_{\mathrm{ss}}(\theta_{\mathrm{e}})$

B. Meta Distribution

The meta distribution is defined as the CCDF of the random variable

$$P_{\mathrm{s}}(\theta) \triangleq \mathbb{P}\left(\mathrm{SIR} > \theta \mid \Phi_{\mathrm{BS}}\right), \tag{3}$$

which is the conditional SIR CCDF given the point process Φ_{BS}. Hence, the meta distribution is formally given by

$$\bar{F}(\theta, x) \triangleq \bar{F}_{P_{\mathrm{s}}}(\theta, x) = \mathbb{P}\left(P_{\mathrm{s}}(\theta) > x\right), \quad x \in [0, 1], \tag{4}$$

where $\mathbb{P}$ is the probability measure of the point process Φ_{BS}. It is quite likely impossible to calculate the meta distribution directly from the definition in (4), hence the moments of $P_{\mathrm{s}}(\theta)$ are considered. The b-th moment of $P_{\mathrm{s}}(\theta)$ is denoted by

$$\begin{aligned}M_b(\theta) &\triangleq \mathbb{E}\left(P_{\mathrm{s}}(\theta)^b\right) = \int_0^1 x^b dF_{P_{\mathrm{s}}}(x) \\ &= \int_0^1 b x^{b-1} \bar{F}_{P_{\mathrm{s}}}(x)\mathrm{d}x,\end{aligned} \tag{5}$$

and the standard success probability can be expressed as $p_{\rm s}(\theta) \equiv M_1(\theta)$, i.e., the first moment of the conditional success probability. The exact meta distribution can be obtained by the Gil-Pelaez theorem [11] from the purely imaginary moments $M_{jt} = \mathbb{E}(P_{\rm s}(\theta)^{jt}), j \triangleq \sqrt{-1}, t \in \mathbb{R}^+$. It is still difficult to calculate numerical results of meta distribution, so we approximate the meta distribution by matching its first and second moment to the beta distribution, which has been found to be an excellent match. The meta distribution can provide detailed information compared with the mean success probability. First, the success probability is the mean of the conditional probability random variable, while the meta distribution fully characterizes the random variable. It can answer questions such as "What fraction of users in a Poisson cellular network achieve 90% link reliability if the required SIR is 5 dB?". It's -1st moment provides the mean local delay, defined as the mean numbers of transmissions needed untill successful reception [12].

III. Analytical Results for Interference Correlated

A. Moments of the Conditional OSSA Probability

In this section, we first derive the b-th moment of the conditional OSSA probability, and then we use the first and second moments to obtain the beta distribution, which gives an excellent approximation for the meta distribution.

Due to the nearest-BS association, a BS serves all the users in its Voronoi cell, and the serving BS is the one who is the nearest to the typical user. The distance between the typical user located at origin and its serving BS is denoted by $\gamma_{\rm BS} = \|\mathbf{x}_0\|$. The PDF of $\gamma_{\rm BS}$ can be obtained according to the void probability of PPP as

$$f_{\gamma_{\rm BS}}(r) = 2\pi\lambda_{\rm BS} r \exp\left(-\pi\lambda_{\rm BS} r^2\right). \tag{6}$$

Theorem 1 (The b-th Moment of $P_{\rm OSSA}$) *The b-th moment M_b ($b \in \mathbb{C}$) of the conditional OSSA probability $P_{\rm OSSA}$ is*

$$M_b = \sum_{k=0}^{\infty} \binom{b}{k} (-1)^k \int_0^{2\pi}\int_0^{\infty} \frac{f_{\gamma_{\rm BS}}(r)}{2\pi} \cdot \exp\left(-\int_0^{2\pi}\int_r^{\infty} G_{b,k}\ \lambda_{\rm BS} x \mathrm{d}x\mathrm{d}\phi\right)\mathrm{d}r\mathrm{d}\theta, \tag{7}$$

where

$$G_{b,k} = 1 - \frac{\left(1+\theta_{\rm u} r^{\alpha} x^{-\alpha}\right)^{-b}}{\left(1+\theta_{\rm e}\left(\frac{r^2+v^2-2rv\cos\theta}{x^2+v^2-2xv\cos\phi}\right)^{\alpha/2}\right)^{k}}. \tag{8}$$

Proof: The conditional connection success probability for the typical user is given by

$$\begin{aligned}
P_{\rm cs}(\theta_{\rm u}) &= \mathbb{P}\left(\mathrm{SIR}_{\rm u} > \theta_{\rm u} \mid \Phi_{\rm BS}\right) \\
&= \mathbb{P}\Big(h_{\mathbf{x}_0} > \theta_{\rm u} \sum_{\mathbf{x}\in\mathbf{\Phi}_{\rm BS}\setminus\{\mathbf{x}_0\}} h_{\mathbf{x}} \frac{\|\mathbf{x}_0\|^{\alpha}}{\|\mathbf{x}\|^{\alpha}} \mid \Phi_{\rm BS}\Big) \\
&\overset{(a)}{=} \mathbb{E}_{h_{\mathbf{x}}}\left[\exp\Big(-\theta_{\rm u} \sum_{\mathbf{x}\in\mathbf{\Phi}_{\rm BS}\setminus\{\mathbf{x}_0\}} h_{\mathbf{x}} \frac{\|\mathbf{x}_0\|^{\alpha}}{\|\mathbf{x}\|^{\alpha}}\Big) \mid \Phi_{\rm BS}\right] \\
&= \mathbb{E}_{h_{\mathbf{x}}}\left[\prod_{\mathbf{x}\in\mathbf{\Phi}_{\rm BS}\setminus\{\mathbf{x}_0\}} \exp\left(-\frac{\theta_{\rm u}\|\mathbf{x}_0\|^{\alpha}}{\|\mathbf{x}\|^{\alpha}} h_{\mathbf{x}}\right)\right] \\
&\overset{(b)}{=} \prod_{\mathbf{x}\in\mathbf{\Phi}_{\rm BS}\setminus\{\mathbf{x}_0\}} \frac{1}{1+\frac{\theta_{\rm u}\|\mathbf{x}_0\|^{\alpha}}{\|\mathbf{x}\|^{\alpha}}},
\end{aligned} \tag{9}$$

where (a) is according to the moment generating function of $h_{\mathbf{x}_0} \sim \exp(1)$ and (b) follows since $h_{\mathbf{x}}$ are i.i.d. exponential with unit mean.

In the same way, the conditional secure success probability for Eve is given by

$$\begin{aligned}
P_{\rm ss}(\theta_{\rm e}) &= \mathbb{P}\left(\mathrm{SIR}_{\rm e} < \theta_{\rm e} \mid \Phi_{\rm BS}\right) \\
&= 1 - \mathbb{P}\left(\mathrm{SIR}_{\rm e} > \theta_{\rm e} \mid \Phi_{\rm BS}\right) \\
&= 1 - \mathbb{P}\Big(g_{\mathbf{x}_0} > \theta_{\rm e} \sum_{\mathbf{x}\in\Phi_{\rm BS}\setminus\{\mathbf{x}_0\}} g_{\mathbf{x}} \frac{\|\mathbf{v}-\mathbf{x}_0\|^{\alpha}}{\|\mathbf{v}-\mathbf{x}\|^{\alpha}} \mid \Phi_{\rm BS}\Big) \\
&= 1 - \mathbb{E}_{g_{\mathbf{x}}}\left[\exp\Big(-\theta_{\rm e} \sum_{\mathbf{x}\in\Phi_{\rm BS}\setminus\{\mathbf{x}_0\}} g_{\mathbf{x}} \frac{\|\mathbf{v}-\mathbf{x}_0\|^{\alpha}}{\|\mathbf{v}-\mathbf{x}\|^{\alpha}}\Big) \mid \Phi_{\rm BS}\right] \\
&= 1 - \prod_{\mathbf{x}\in\mathbf{\Phi}_{\rm BS}\setminus\{\mathbf{x}_0\}} \frac{1}{1+\frac{\theta_{\rm e}\|\mathbf{v}-\mathbf{x}_0\|^{\alpha}}{\|\mathbf{v}-\mathbf{x}\|^{\alpha}}}.
\end{aligned} \tag{10}$$

Using a similar proof as in [1], the b-th moment for the conditional OSSA probability of the typical user can be obtained by

$$\begin{aligned}
M_b = \mathbb{E}[P_{\rm OSSA}^b] &= \mathbb{E}\left[P_{\rm cs}^b(\theta_{\rm u}) P_{\rm ss}^b(\theta_{\rm e})\right] \\
&= \mathbb{E}\left[P_{\rm cs}^b(\theta_{\rm u})(1-\bar{P}_{\rm ss}(\theta_{\rm e}))^b\right] \\
&= \sum_{k=0}^{\infty} \binom{b}{k} (-1)^k \underbrace{\mathbb{E}\left[P_{\rm cs}^b(\theta_{\rm u}) \bar{P}_{\rm ss}^k(\theta_{\rm e})\right]}_{M_{b,k}},
\end{aligned} \tag{11}$$

where

$$\begin{aligned}
M_{b,k} &= \mathbb{E}\left[\prod_{\mathbf{x}\in\mathbf{\Phi}_{\rm BS}\setminus\{\mathbf{x}_0\}} \Big(\frac{1}{1+\frac{\theta_{\rm u}\|\mathbf{x}_0\|^{\alpha}}{\|\mathbf{x}\|^{\alpha}}}\Big)^b \Big(\frac{1}{1+\frac{\theta_{\rm e}\|\mathbf{v}-\mathbf{x}_0\|^{\alpha}}{\|\mathbf{v}-\mathbf{x}\|^{\alpha}}}\Big)^k\right] \\
&\overset{(a)}{=} \mathbb{E}_{\gamma_{\rm BS}}\left[\exp\left(-\int_0^{2\pi}\int_r^{\infty} G_{b,k}\ \lambda_{\rm BS} x \mathrm{d}x\mathrm{d}\phi\right)\right] \\
&\overset{(b)}{=} \int_0^{2\pi}\int_0^{\infty} \exp\left(-\int_0^{2\pi}\int_r^{\infty} G_{b,k}\lambda_{\rm BS} x \mathrm{d}x\mathrm{d}\phi\right)\frac{f_{\gamma_{\rm BS}}(r)}{2\pi}\mathrm{d}r\mathrm{d}\theta,
\end{aligned} \tag{12}$$

and (a) employs the probability generating functional (PGFL) of the PPP [13], and (b) uses the PDF of $\gamma_{\rm BS}$. Substituting the result of (11), Theorem 1 can be obtained. ■

Remark 1: It is easy to obtain M_1 (the OSSA probability) and M_2 from Theorem 1. The first moment M_1 of the conditional OSSA probability P_{OSSA} is

$$M_1 = \frac{1}{{}_2F_1\left(1,-\delta;1-\delta;-\theta_{\text{u}}\right)} - \int_0^{2\pi}\int_0^{\infty} \exp\left(-\lambda_{\text{BS}}\int_0^{2\pi}\int_r^{\infty} G_{1,1} x\mathrm{d}x\mathrm{d}\phi\right)\frac{f_{\gamma_{\text{BS}}}(r)}{2\pi}\mathrm{d}r\mathrm{d}\theta, \tag{13}$$

and the second moment M_2 of the conditional OSSA probability P_{OSSA} is

$$M_2 = \frac{1}{{}_2F_1\left(2,-\delta;1-\delta;-\theta_{\text{u}}\right)} - 2\int_0^{2\pi}\int_0^{\infty} \exp\left(-\lambda_{\text{BS}}\int_0^{2\pi}\int_r^{\infty} G_{2,1} x\mathrm{d}x\mathrm{d}\phi\right)\frac{f_{\gamma_{\text{BS}}}(r)}{2\pi}\mathrm{d}r\mathrm{d}\theta + \int_0^{2\pi}\int_0^{\infty} \exp\left(-\lambda_{\text{BS}}\int_0^{2\pi}\int_r^{\infty} G_{2,2} x\mathrm{d}x\mathrm{d}\phi\right)\frac{f_{\gamma_{\text{BS}}}(r)}{2\pi}\mathrm{d}r\mathrm{d}\theta. \tag{14}$$

Generally, if b is a positive integer, the infinite sum in (7) reduces to a finite sum from 0 to b.

Remark 2 (Asymptotic property of θ_{e}): When $\theta_{\text{e}} \to \infty$, we have $\mathbb{P}\left(\text{SIR}_{\text{e}} < \theta_{\text{e}} \mid \Phi_{\text{BS}}\right) \to 1$, hence

$$M_b = \mathbb{E}[\mathbb{P}\left(\text{SIR}_{\text{u}} > \theta_{\text{u}} \mid \Phi_{\text{BS}}\right)^b \mathbb{P}\left(\text{SIR}_{\text{e}} < \theta_{\text{e}} \mid \Phi_{\text{BS}}\right)^b] = \frac{1}{{}_2F_1\left(b,-\delta;1-\delta;-\theta_{\text{u}}\right)}, \tag{15}$$

i.e., M_b will approach to the standard b-th moment without secrecy constraint, as shown as Fig. 6.

Remark 3 (The b-th moment for independent interference): When the interferences are independent for typical user and its eavesdropper, the b-th moment is given by

$$M_b = \mathbb{E}[\mathbb{P}\left(\text{SIR}_{\text{u}} > \theta_{\text{u}} \mid \Phi_{\text{BS}}\right)^b]\mathbb{E}[\mathbb{P}\left(\text{SIR}_{\text{e}} < \theta_{\text{e}} \mid \Phi_{\text{BS}}\right)^b] = \frac{1}{{}_2F_1\left(b,-\delta;1-\delta;-\theta_{\text{u}}\right)} M_{b\text{e}}, \tag{16}$$

where

$$M_{b\text{e}} = \sum_{k=0}^{\infty}\binom{b}{k}(-1)^k \int_0^{2\pi}\int_0^{\infty} \frac{f_{\gamma_{\text{BS}}}(r)}{2\pi} \cdot \exp\left(-\int_0^{2\pi}\int_r^{\infty} G_{k\text{e}}\lambda_{\text{BS}} x\mathrm{d}x\mathrm{d}\phi\right)\mathrm{d}r\mathrm{d}\theta \tag{17}$$

and

$$G_{k\text{e}} = 1 - \left(1 + \theta_{\text{e}}\left(\frac{r^2+v^2-2rv\cos\theta}{x^2+v^2-2xv\cos\phi}\right)^{\frac{\alpha}{2}}\right)^{-k} \tag{18}$$

is the b-th moment for Eve.

B. Beta Approximation

The beta distribution provides an excellent approximation of the meta distribution [1], [4], [14]. The PDF of a beta distributed random variable X is

$$f_X(x) = \frac{x^{\frac{\mu(\beta+1)-1}{1-\mu}}(1-x)^{\beta-1}}{\text{B}(\mu\beta/(1-\mu),\beta)}, \tag{19}$$

where $\text{B}(:,:)$ is the beta function. The mean is μ, and the variance is

$$\sigma^2 = \text{var } X = \frac{\mu(1-\mu)^2}{\beta+1-\mu}. \tag{20}$$

Matching mean $\mu = M_1$, variance $\sigma^2 = M_2 - M_1^2$, we find

$$\beta = \frac{\mu(1-\mu)^2}{\sigma^2} - (1-\mu) = \frac{(\mu-M_2)(1-\mu)}{M_2-\mu^2}. \tag{21}$$

With M_1 and M_2 given in (13) and (14), respectively, this beta distribution approximates the distribution of P_{OSSA}.

IV. Numerical Results

The intensity of the BSs used in this section is $\lambda = 10/\text{km}^2$. And we use the relationship $v = \frac{1}{2\sqrt{\lambda}}$ in most figures of this paper, since the Eve can be placed in a half of the average distance of two BSs due to this relationship. It is also used in [9]. We set $\theta_{\text{u}} = \theta_{\text{e}} + 0.1$ (all in dB) for the OSSA probability, variance and the meta distribution, and use various values of α, θ_{e} and v into account for comparison. According to Wyner's encoding scheme [15], here we require $\theta_{\text{u}} > \theta_{\text{e}}$ in order to communicate securely.

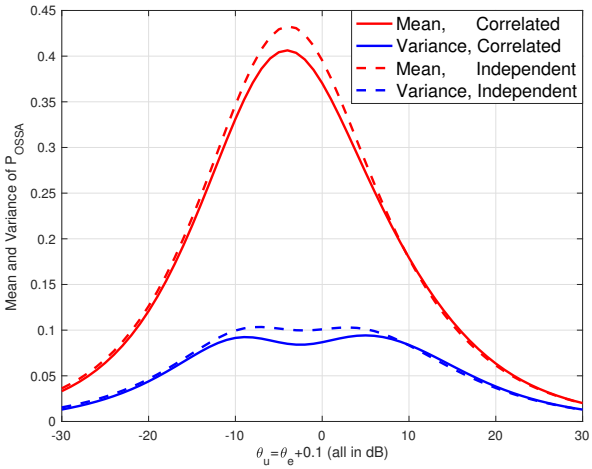

Fig. 2. The mean M_1 and the variance $M_2 - M_1^2$ of P_{OSSA} at $v = \frac{1}{2\sqrt{\lambda}}$ and $\alpha = 4$ for the network. The solid lines show the OSSA probability and variance when interferences are correlated. The dashed lines show the OSSA probability and variance when interferences are independent.

Fig. 2 is the plot of the OSSA probability and variance against θ_{u} (and θ_{e}) when the interferences are correlated or not. It shows that the interference correlation leads to a decrease in the OSSA probability and variance for thresholds around 0 dB. Fig. 3 shows the meta distribution of the network. For the chosen parameters, with the increase of the required reliability, the number of links is gradually decreasing, and it has a tendency to decrease slowly after a quick decrease. Fig. 4 shows that with the increase of α, OSSA probability and variance increase, and the peak of the OSSA probability will shift to the right, while the variance stays basically the same. Fig. 5 indicates that as α decreases,

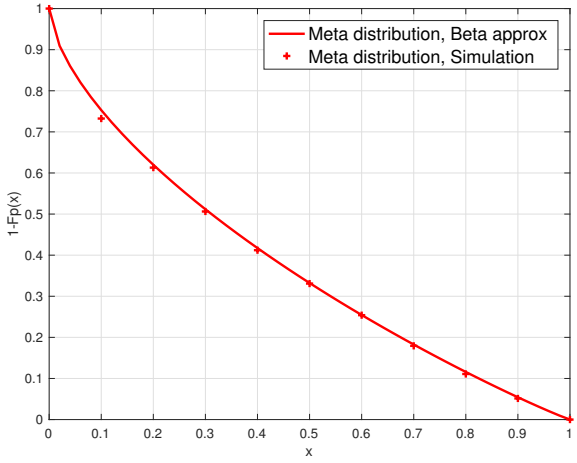

Fig. 3. The meta distribution at $\theta_{\rm u} = 0$ dB, $\theta_{\rm e} = -0.1$ dB, $v = \frac{1}{2\sqrt{\lambda}}$ and $\alpha = 4$. The solid line shows the meta distribution approximated by the beta distribution. Markers show the Monte Carlo simulations.

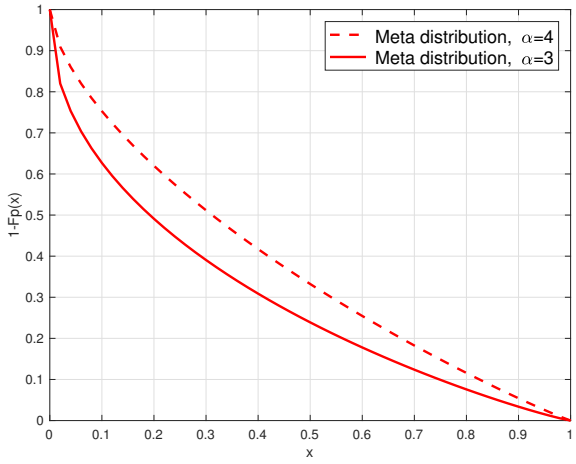

Fig. 5. The meta distribution at $\theta_{\rm u} = 0$ dB, $\theta_{\rm e} = -0.1$ dB, $v = \frac{1}{2\sqrt{\lambda}}$. The solid line and the dashed line show the meta distribution with $\alpha = 3, 4$ respectively.

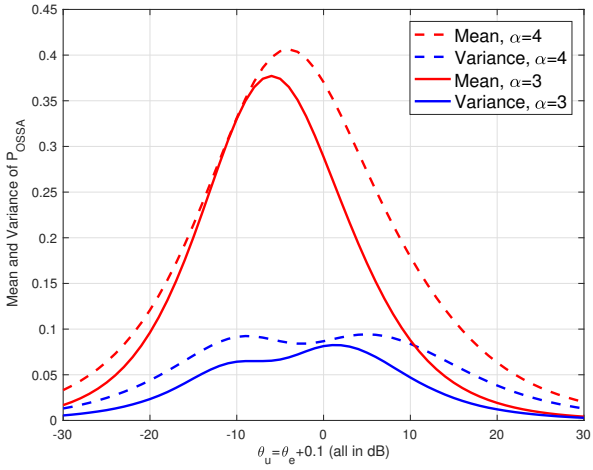

Fig. 4. The mean M_1 and the variance $M_2 - M_1^2$ of $P_{\rm OSSA}$ at $v = \frac{1}{2\sqrt{\lambda}}$ for the network. The solid lines and the dashed lines show the mean and variance with $\alpha = 3, 4$ respectively.

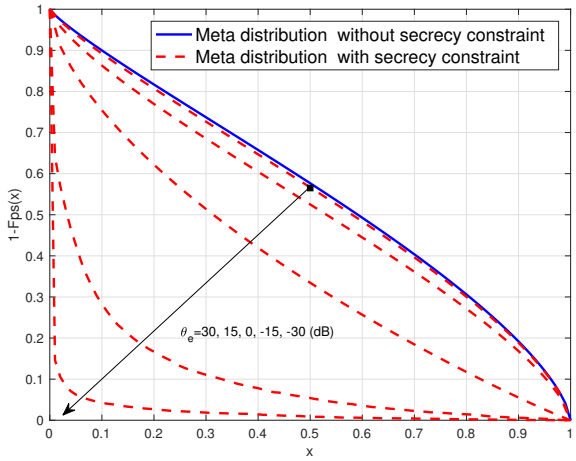

Fig. 6. The meta distribution at $\theta_{\rm u} = 0$ dB, $\alpha = 4$ and $v = \frac{1}{2\sqrt{\lambda}}$. The solid line shows the meta distribution without secrecy constraint, and the dashed lines show the meta distribution with secrecy constraint when $\theta_{\rm e} = 30, 15, 0, -15, -30$ dB.

the meta distribution overall decreases, and it decreases faster when x is smaller. Fig. 6 shows when $\theta_{\rm u} = 0$ dB, and $\theta_{\rm e}$ changes, where a smaller $\theta_{\rm e}$ means a higher security level, the link reliability of the network will decrease. And as the secrecy constraint decreases, the curves will approach the standard meta distribution quickly. Fig. 7 shows that when the eavesdropper is far away from the typical user relative to the distance from the user to its serving BS, the link reliability of the network will also increase and approach to the meta distribution without secrecy constraint gradually.

V. CONCLUSIONS

In this paper, a framework for network reliability of secrecy transmission based on the meta distribution is proposed. We first derive the moments on the conditional success probability $P_{\rm cs}$ for the legitimate user and $P_{\rm ss}$ for the eavesdropper and the conditional OSSA probability for the network, taking into account the interference correlation. Then an exact expression as well as a simple yet accurate approximation for the meta distribution of the SIR is provided. Finally we derive the distribution for perfect secrecy transmission which was used to study the impact of physical layer security in the whole network.

Using this framework, we explore the effect of the differences in the thresholds $\theta_{\rm u} - \theta_{\rm e}$ on the performance of the network. The effect of the distance between eavesdropper and the typical user on the percentage of users that are covered securely with a certain reliability is also studied.

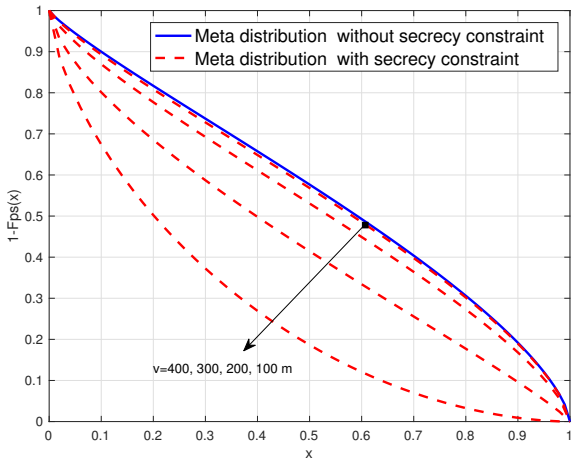

Fig. 7. The meta distribution at $\theta_{\rm u} = 0$ dB, $\theta_{\rm e} = -0.1$ dB and $\alpha = 4$. The solid line shows the standard meta distribution, and the dashed lines show the meta distribution with secrecy constraint when $v = 400, 300, 200, 100$m. When $v = \frac{1}{2\sqrt{\lambda}}$ i.e. $v = 158$m, the meta distribution is shown in Fig. 3

REFERENCES

[1] M. Haenggi, "The meta distribution of the SIR in Poisson bipolar and cellular networks," *IEEE Trans. Wireless Commun.*, vol. 15, pp. 2577–2589, Apr. 2016.

[2] M. Salehi, A. Mohammadi, M. Haenggi, 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.

[3] N. Deng and M. Haenggi, "A fine-grained analysis of millimeter-wave device-to-device networks," *IEEE Trans. Commun.*, vol. 65, pp. 4940–4954, Nov. 2017.

[4] Q. Cui, X. Yu, Y. Wang, and M. Haenggi, "The SIR meta distribution in Poisson cellular networks with base station cooperation," *IEEE Trans. Commun.*, vol. 66, pp. 1234–1249, Mar. 2018.

[5] M. Haenggi, "The secrecy graph and some of its properties," in *2008 IEEE International Symposium on Information Theory (ISIT'08)*, Toronto, Canada, Jul. 2008, pp. 539–543.

[6] A. Sarkar and M. Haenggi, "Percolation in the secrecy graph," *Discrete Appl. Math.*, vol. 161, pp. 2120–2132, Sep. 2013.

[7] A. Sarkar and M. Haenggi, "Secrecy coverage," *Internet Mathematics*, vol. 9, pp. 199–216, Jun. 2013.

[8] X. Zhou, R. K. Ganti, J. G. Andrews, and A. Hjorungnes, "On the throughput cost of physical layer security in decentralized wireless networks," *IEEE Trans. Wireless Commun.*, vol. 10, pp. 2764–2775, Aug. 2011.

[9] K. S. Ali, H. ElSawy, M. Haenggi, and M.-S. Alouini, "The effect of spatial interference correlation and jamming on secrecy in cellular networks," *IEEE Wireless Commun. Lett.*, vol. 6, pp. 530–533, Aug. 2017.

[10] J. Tang, G. Chen, and J. P. Coon, "The meta distribution of the secrecy rate in the presence of randomly located eavesdroppers," *IEEE Wireless Commun. Lett.*, 2018, to appear.

[11] J. Gil-Pelaez, "Note on the inversion theorem," *Biometrika*, vol. 38, pp. 481–482, 1951.

[12] M. Haenggi, "The local delay in Poisson networks," *IEEE Trans. Inf. Theory*, vol. 59, pp. 1788–1802, Mar. 2013.

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

[14] Y. Wang, M. Haenggi, and Z. Tan, "The meta distribution of the SIR for cellular networks with power control," *IEEE Trans. Commun.*, vol. 66, pp. 1745–1757, Apr. 2018.

[15] A. D. Wyner, "Wire tap channel," *Bell Syst Tech J*, vol. 54, pp. 1355–1387, Oct. 1975.