Hindawi
Security and Communication Networks
Volume 2019, Article ID 7869317, 9 pages
https://doi.org/10.1155/2019/7869317

Research Article

Physical Layer Security in Nonorthogonal Multiple Access Wireless Network with Jammer Selection

Langtao Hu, Xin Zheng, and Chunsheng Chen

Anqing Normal University, AnQing 246133, China

Correspondence should be addressed to Langtao Hu; 122634998@qq.com

Received 1 April 2019; Accepted 22 October 2019; Published 16 November 2019

Academic Editor: Salvatore Sorce

The physical layer security of downlink nonorthogonal multiple access (NOMA) network is analyzed. In order to improve the secrecy probability, friendly jammers are jointed in the NOMA network. Two jammer schemes are proposed in the NOMA network. All the jammers transmit jamming signal without jammer selection in the first scheme (NO JS scheme). Jammers are selected to transmit jamming signal if their interfering power on scheduled users is below a threshold in the second scheme (JS scheme). A stochastic geometry approach is applied to analyze the outage probability and the secrecy probability. Compared with the NO JS scheme and traditional scheme (without jointing jammers), the jammer selection scheme provides a good balance between the user outage probability and secrecy probability. Numerical results demonstrate that the security performance of the two proposed schemes can be improved by jointing the jammers in the NOMA wireless network.

1. Introduction

The development of mobile internet and Internet of Things brings lots of challenging requirements to fifth-generation (5G) networks, such as increasing high data rate and low latency [1–3]. The nonorthogonal multiple access has been considered as key promising multiple access candidates for 5G cellular networks. NOMA allows serving multiple users simultaneously using the same frequency/time resources at the cost of increased intracell interference. At the base station side, messages for multiple users are superposed by superposition coding. The successive interference cancellation (SIC) technique is applied to extract the intended message in the receiver side. Security is always an important issue for wireless networks, since the broadcast nature of wireless radio propagation makes it easily be overheard by eavesdroppers.

1.1. Related Works. Recently, NOMA has received remarkable attention both in the world of academia and industry [4–6]. Power-domain NOMA has been proposed for the 3GPP long-term evolution initiative in [4]. The authors in [5] investigated the performance of NOMA in a cellular downlink scenario with randomly deployed users. It was shown that NOMA can achieve superior ergodic sum rate performance than traditional orthogonal multiple access (OMA) counter parts. Challenges, opportunities, and future research trends for NOMA design are highlighted to provide some insight into the potential future work of researchers in [6]. The security performance of the NOMA networks can be improved by invoking the protected zone and by generating noise at the BS as shown by Liu et al. [7]. The physical layer security of uplink nonorthogonal multiple access is analyzed by Gerardo Gomez et al. [8]. Tao et al. [9] proposed a new reliable physical layer network coding and cascade-computation decoding scheme. The authors in [10] proposed an opportunistic multiple-jammer selection scheme for enhancing the physical layer security. The authors in [11] studied the security-reliability tradeoff analysis for conventional single-hop networks under a single passive eavesdropper attack. The authors in [12] enhanced physical layer security for downlink heterogeneous networks by using friendly jammers and full-duplex users. Recently, stochastic geometry has been used to model some network, such as large-scale HET wireless networks [10], massive MIMO-enabled HetNets [14], cognitive cellular wireless networks [15], multitier millimeter wave cellular networks [16], and NOMA network [17]. It has been succeeded to develop tractable models to characterize and better understand the performance of these networks, and these models have been shown to provide tractable yet accurate performance bounds for these networks.

1.2. Motivations and Contributions. In this paper, we investigate the physical layer security of NOMA with friendly jammers and multiple noncolluding eavesdroppers (EVEs) in large-scale networks with stochastic geometry. For the sake of easy deployment, all nodes in NOMA wireless network are equipped with single antenna, and eavesdroppers are randomly distributed along the whole plane. The jammers are assumed to transmit friendly artificial noise. To enhance the physical layer security, two schemes are proposed with jointing jammers in NOMA network. In order to alleviate the interference from jammers to scheduled users, a jammer selection policy is discussed based on the received jamming power at the user. When the jammer power is below a threshold, the jammer around the scheduled user is active; otherwise, the jammer is idle. Unlike the scheme in [7, 8], the security performance of the NOMA networks can be improved by generating noise at the BS in [7], and physical layer security in uplink NOMA is discussed in [8]. In this paper, friendly jammers will be jointed, which can enhance the physical layer security in downlink NOMA wireless network. The main contributions of this paper are summarized as follows:

(1) Two physical layer security schemes are proposed, where friendly jammers are jointed in NOMA wireless network. Jammers transmit friendly artificial noise. A jammer selection policy is discussed based on the received jamming power at user.

(2) Using stochastic geometry tools, the downlink NOMA performance is analyzed in terms of outage probability and secrecy probability. In particular, the BSs and user positions are model Poisson point process (PPP) on a 2-D plane. The active jammer positions are model Poisson hole process.

(3) All the analytical results are validated by system-level simulations. Our proposed schemes provide a better security performance compared with the traditional scheme.

The rest of the paper is organized as follows. In Section 2, we introduce the system model. In Section 3, the outage probability performance of proposed schemes is investigated. In Section 4, the user secrecy probability performance of proposed schemes is investigated. In Section 5, numerical simulation and analysis are discussed to verify these results. A conclusion is drawn in Section 6.

Notation: the expectation of function $f(x)$ with respect to x is denoted as $E[f(x)]$. Cumulative distribution function of $f(x)$ is denoted as $F_f(\,)$. The Laplace transform of $f(x)$ is denoted by $L_f(s)$. An exponential distributed random variable with mean 1 is denoted by $x \sim \exp(1)$. Let I_1 be a set and I_2 be a subset of I_1; then, $I_1 \backslash I_2$ denotes the set of elements of I_1 that do not belong to I_2.

2. System Model

In this paper, we consider a dense multicell NOMA downlink wireless network in presence of eavesdroppers (EVEs) as shown in Figure 1. All BSs users and EVEs are equipped with one antenna. The BS locations are distributed as an independent homogeneous PPP Φ_B with density λ_B in two-dimensional plane. Without loss of generality, the analysis is performed in a typical cell denoted as BS_0. Based on Slivnyak's Theorem, due to stationarity of Φ_B, the typical cell can reflect the averaged performance of the entire system. The system assumes a frequency reuse factor 1; hence, the same frequency resources are used in all cells. The radio resources are partitioned into a number of subbands. We assume the bandwidth of each subband is normalized to 1. The UE and EVE locations are distributed as an independent homogeneous PPP Φ_U and Φ_E with densities λ_U and λ_E, respectively. In this paper, the NOMA group includes two users. Existing results have shown that the NOMA group with more than two UEs may provide a better performance gain [18]. In order to process the SIC easily, two user NOMA networks are more practical in the reality system. UE_1 and UE_2 consist of a NOMA group. We assume $\lambda_U \gg \lambda_B$ so that a sufficient number of UEs can always be found to form the NOMA group in each cell. To enhance the security performance, friendly jammers are jointed in NOMA network. In the selective jammer scheme, a jammer is selected to be active if its interference power to the scheduler user is below a threshold. Actually, the threshold is the jammer exclusion zone around the scheduler user, i.e., $\Phi_{JS} = \left\{ j \mid j \in \Phi_J, P_J R_{j,U_i}^{-a} < P_J D^{-a}, \forall U_i \in \Phi_{U_s} \right\}$. Φ_{JS} is the Poisson hole process of active jammer. Φ_{U_s} denotes the point process of scheduled users. Φ_{U_s} is an inhomogeneous PPP, for which the density is λ_{U_s}. R_{j,U_i}^{-a} is the distance between the jammer and scheduled users. D is the exclusion zone radius. P_J is denoted as the transmit power of the jammer. a is the pathloss exponent. P_b is the total power of BS on a subband in downlink NOMA. The allocated powers of UE_1 and UE_2 can be denoted as $P_1 = \varepsilon P_b$ and $P_2 = (1 - \varepsilon) P_b$, respectively, where $\varepsilon \in (0, 0.5)$ is a NOMA power allocation parameter. UE_1 is assumed to be with a better normalized channel gain. UE_2 is assumed to be with a worse normalized channel gain. The two users are selected randomly in NOMA network. P_J denotes the power of jammer. BS-transmitted signals to UE1 and UE2 are expressed as x_1 and x_2, respectively. Since UE1 and UE2 form a NOMA group, x_1 and x_2 are encoded as the composite signal at the BS_0 [12]:

$$\overline{x} = \sqrt{P_1} x_1 + \sqrt{P_2} x_2. \tag{1}$$

The received signal at $UE_i, i \in \{1, 2\}$ can be expressed as

$$y_i = \sqrt{h_i r_i^{-a}} \overline{x} + n_i, \tag{2}$$

where h_i is the Rayleigh fading gain between BS_0 and UE_i, which follows an exponential distribution with mean 1. All h_i are assumed to be i.i.d. r_i is the distance between BS_0 and UE_i. n_i is the additive noise.

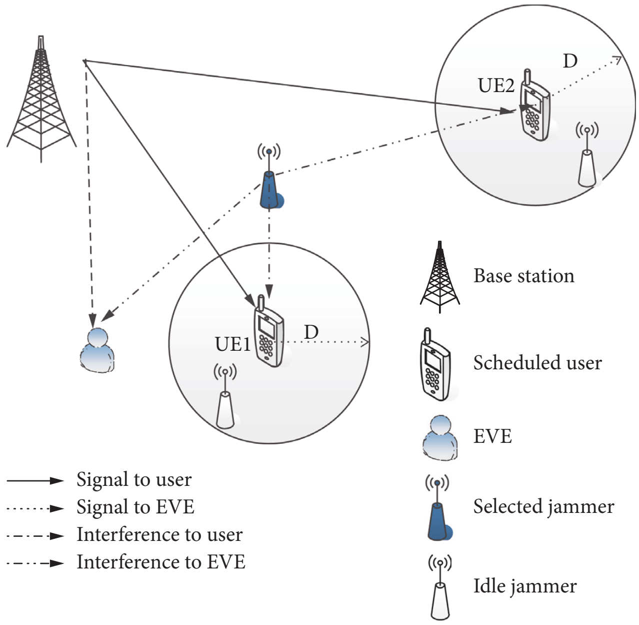


Figure 1: NOMA wireless network with the selected jammer.

3. NOMA User Outage Probability

We assume UE_1 has a better channel condition. At the receiver side, successive interference cancellation (SIC) is used to decode the intended message. UE_1 first decodes the UE_2 signal x_2 and removes it from the received composite signal; after that, UE_1 can further decode its signal x_1. UE_2 decodes x_2 directly by treating x_1 as interference. We consider the possible SIC error propagation, which is caused by decoding unsuccessfully in the first step, and thus, error is carried over to the next-level decoding. Let β be the fraction of NOMA interference due to SIC error propagation. Noise can be safely neglected in a dense interference limited wireless system. The signal to interference ratio (SIR) of UE_1 can be represented as $\mathrm{SIR}_{U_1} = ((P_1 h_1 r_1^{-a})/(I_{B_1} + I_{JS_1} + I_{W_1}))$, where $I_{B_1} = \sum_{j\in\Phi_B\backslash BS_0} P_b g_{1,j} R_{1,j}^{-a}$ denotes the cumulative downlink intercell interference from the all other cells and $I_{JS_1} = \sum_{y\in\Phi_{JS}} P_j h_{1,y} R_{1,y}^{-a}$ denotes cumulative downlink interference from the selected jammers. $I_{W_1} = \beta P_2 h_1 r_1^{-a}$ denotes the interference from SIC error propagation. $g_{1,j}$ is the Rayleigh fading an exponential distribution with mean 1, $g_{1,j} \sim \exp(1)$. $\Phi_B\backslash BS_0$ represents the set of all BSs excluding BS_0.

The achievable rate of UE_1 on each subband in NOMA network is given as

$$\begin{aligned}\tau_1 &= \log\left(1 + SIR_{U_1}\right)\\ &= \log\left(1 + \frac{c_1 P_1}{\beta c_1 P_2 + 1}\right),\end{aligned} \tag{3}$$

where $c_1 = ((h_1 r_1^{-a})/(I_{B_1} + I_{JS_1}))$ is the UE_1 channel gain including pathloss and fast fading normalized by two kinds of interferences. The signal to interference ratio of UE_2 can be represented as $\mathrm{SIR}_{U_2} = ((P_2 r_2^{-a} h_2)/(I_{B_2} + I_{JS_2} + P_1 r_2^{-a} h_2))$, where $I_{B_2} = \sum_{j\in\Phi_B\backslash BS_0} P_b g_{2,j} R_{2,j}^{-a}$ is the cumulative downlink intercell interference from all the other cells. $I_{JS_2} = \sum_{y\in\Phi_{JS}} P_j h_{2,y} R_{2,y}^{-a}$ denotes cumulative downlink interference from the selective jammers. $P_1 r_2^{-a} h_2$ is the interference from UE_1.

The achievable rate of UE_2 on each subband in NOMA network is given as

$$\begin{aligned}\tau_2 &= \log\left(1 + \mathrm{SIR}_{U_2}\right)\\ &= \log\left(1 + \frac{c_2 P_2}{c_2 P_1 + 1}\right),\end{aligned} \tag{4}$$

where $c_2 = ((h_2 r_2^{-a})/(I_{B_2} + I_{JS_2}))$. We assume that two users are randomly selected among all scheduled users. Two users are marked as UE_n and UE_m. The normalized channel gains of UE_n and UE_m are denoted as c_n and c_m, respectively. Let $UE_1 = \{UE_i \mid UE_i \in \{UE_n, UE_m\}, c_i = \max(c_n, c_m)\}$, and $UE_2 = \{UE_i \mid UE_i \in \{UE_n, UE_m\}, c_i = \min(c_n, c_m)\}$, $z = \max(x, y)$, and $\varpi = \min(x, y)$. The CDF of z and ϖ can be represented as $F_z(z) = F_{xy}(z, z)$; $F_\varpi(\varpi) = F_x(\varpi) + F_y(\varpi) - F_{xy}(\varpi, \varpi)$ [18]. Thus, CDFs of c_1 and c_2 can be derived as follows:

$$F_{c_1}(C) = F_{c_n c_m}(C, C) = F_c(C)^2, \tag{5}$$

$$\begin{aligned}F_{c_2}(C) &= F_{c_n}(C) + F_{c_m}(C) - F_{c_n c_m}(C, C)\\ &= 2F_c(C) - F_c(C)^2,\end{aligned} \tag{6}$$

where $F_c(C) = 1 - P(c > C)$ and $P(c > C)$ denotes the probability of $c > C$. According to (5) and (6), $F_{c_1}(C)$ and $F_{c_2}(C)$ can be given as (7) and (8), respectively:

$$F_{c_1}(C) = F_c(C)^2 = (1 - P(c > C))^2, \tag{7}$$

$$\begin{aligned}F_{c_2}(C) &= 2F_c(C) - F_c(C)^2\\ &= 2(1 - P(c > C)) - (1 - P(c > C))^2.\end{aligned} \tag{8}$$

For a given normalized channel gain to UE_1 or UE_2, $c = ((h_i r_i^{-a})/(I_B + I_{JS}))$ and $P(c > C)$ can be derived as follows:

$$\begin{aligned}P(c > C) &= \mathrm{E}_{r_i}\left[P(c > C) \mid r_i\right]\\ &= \int_{r_i > 0} P\left(\frac{h_i r_i^{-\alpha}}{I_B + I_{JS}} > C \mid r_i\right) f(r_i)\mathrm{d}r_i\\ &= \int_{r_i > 0} E_{I_B, I_{JS}}\left[\exp\left(-C r_i^{\alpha}\left(I_B + I_{JS}\right)\right)\right] f(r_i)\mathrm{d}r_i\\ &= \int_{r_i > 0} L_{I_B}(C r_i^{\alpha}) L_{I_{JS}}(C r_i^{\alpha}) f(r_i)\mathrm{d}r_i.\end{aligned} \tag{9}$$

In (9), the second term follows from $h_i \sim \exp(1)$ [13]. The Laplace transform of I_B is given by

$$\begin{aligned} L_{I_B}(s) &= E_{\Phi_B,g}\left[-\exp\left(-s\sum_{j\in\Phi_B/BS0} g_{i,j}R_j^{-a}P_B\right)\right] \\ &= \exp\left(-2\pi\lambda_B\int_{r_i}^{\infty}\left(1-\frac{1}{1+sv^{-a}P_B}\right)v\mathrm{d}v\right) \qquad (10) \\ &= \exp\left(-2\pi\lambda_B(sP_B)^{\delta}\int_{r_i^2/(sP_B)^{\delta}}^{\infty}\frac{1}{1+u^{\delta}}\mathrm{d}u\right), \end{aligned}$$

where $\delta = 2/a$.The Laplace transform of I_{JS} is given by

$$\begin{aligned} L_{I_{JS}}(s) &= \mathrm{E}_{\Phi_{JS},h}\left[-\exp\left(-s\sum_{j\in\Phi_{JS}} h_{i,j}R_{i,j}^{-a}P_J\right)\right] \\ &= \mathrm{E}_{\Phi_J}\left(\prod_{j\in\Phi_J\setminus B(UE_i,D)} L_{h_{i,j}}\left(sR_{i,j}^{-a}P_J\right)\right) \\ &\overset{(a)}{=} \mathrm{E}_{\Phi_J}\left(\exp\left(-\lambda_J\int_{j\in\Phi_J\setminus B(UE_i,D)}\left(1-L_{h_{i,j}}\left(sP_Jx^{-a}\right)\mathrm{d}x\right)\right)\right) \\ &\overset{(b)}{\approx} \exp\left(-2\pi\lambda_J D^{2-a}P_J s(a-2)^{-1}{}_2F_1 \cdot\left(1,1-\frac{2}{a};2-\frac{2}{a};-\frac{sP_J}{D^a}\right)\right). \end{aligned} \qquad (11)$$

In step (a), $B(UE_i,D)$ is a hole of radius D centered at UE_i, $\Phi_J\setminus B(UE_i,D)$ denotes the active jammers location, and Φ_J is the jammer baseline PPP from which the hole is carved out. In step (b), we only discuss the hole around the UE_i. The step (b) follows from the probability generating functional of PPP [13], where ${}_2F_1(a,b;c;d)$ is the Gauss hypergeometric function.

When all jammers are active without jammer selection (NO JS scheme), $\delta = (2/a)$. $L_{I_{\mathrm{NOJS}}}(s)$ denotes the Laplace transform of interference from all jammers without selection to UE_i in NO JS scheme. We can derive $L_{I_{NOJS}}(s)$ as [13]

$$L_{I_{\mathrm{NOJS}}}(s) = \exp\left(-\pi\lambda_J\frac{(sP_J)^{\delta}}{\mathrm{sinc}(\delta)}\right). \qquad (12)$$

By plugging (10) and (11) into (9), $P(c>C)$ with jammer selection in NOMA network is given as

$$\begin{aligned} P(c>C) = \int_{r_i>0} & \exp\left(-2\pi\lambda_B(sP_B)^{\delta}\int_{r_i^2/(sP_B)^{\delta}}^{\infty}\frac{1}{1+u^{\delta}}\mathrm{d}u\right) \\ & \times\exp\left(-2\pi\lambda_J D^{2-a}P_J s(a-2)^{-1}\times{}_2F_1 \cdot\left(1,1-\frac{2}{a};2-\frac{2}{a};-\frac{sP_J}{D^a}\right)\right) \\ & \times\ 2\pi\lambda_B r_i\exp\left(-\pi\lambda_B r_i^2\right)\mathrm{d}r_i\Big|_{s=Cr_i^a}. \end{aligned} \qquad (13)$$

When $a=4$,

$$\begin{aligned} P(c>C) = \int_{r_i>0} & \exp\%\left[-2\pi\lambda_B r_i^2(CP_B)^{1/2} \cdot\left(\frac{\pi}{2}-\arctan\left(\frac{1}{(CP_B)^{1/2}}\right)\right)\%\right] \\ & \times\exp\left(-\pi\lambda_J D^{-2}P_J Cr_i^4\,{}_2F_1\left(1,0.5;1.5;-\frac{Cr_i^4P_J}{D^4}\right)\right) \\ & \times 2\pi\lambda_B r_i\exp\left(-\pi\lambda_B r_i^2\right)\mathrm{d}r_i. \end{aligned} \qquad (14)$$

The outage probability of UE1 with jammer selection in NOMA network can be evaluated as follows:

$$\begin{aligned} P_1(\overline{\tau}_1,\overline{\tau}_2) &= 1-P(\tau_1>\overline{\tau}_1,\tau_{1\longrightarrow 2}>\overline{\tau}_2) \\ &= 1-P\left(\frac{c_1P_1}{\beta c_1P_2}>\gamma_1,\frac{c_1P_2}{c_1P_1+1}>\gamma_2\right) \\ &= \begin{cases} 1; & \text{if } \gamma_1\geq\dfrac{P_1}{\beta P_2} \text{ or } \gamma_2\geq\dfrac{P_2}{P_1}, \\ F_{c_1}(\max(\theta_1,\theta_2)); & \text{otherwise,} \end{cases} \end{aligned} \qquad (15)$$

where $P(\tau_1>\overline{\tau}_1,\tau_{1\longrightarrow 2}>\overline{\tau}_2)$ denotes the connection probability of UE_1, γ_1 and γ_2 denote the SIRs of UE_1 and UE_2, respectively. $\gamma_1 = 2^{\overline{\tau}_1}-1$ and $\gamma_2 = 2^{\overline{\tau}_2}-1$. $\overline{\tau}_1$ and $\overline{\tau}_2$ are the target rate thresholds for UE_1 and UE_2, respectively. $\tau_{1\longrightarrow 2}$ is the rate of decoding UE_2 signal x_2 in the UE_1 receiver, which must be greater than the QoS requirement of UE_2. $\tau_{1\longrightarrow 2}>\overline{\tau}_2$ can ensure that UE_1 is able to remove UE_2's signal from interference.

$\theta_1 = (\gamma_1/(p_1-\gamma_1\beta P_2))$, and $\theta_2 = (\gamma_2/(p_2-\gamma_2P_1))$. Plugging $\max(\theta_1,\theta_2)$ into (7), we get $F_{c_1}(\max(\theta_1,\theta_2))$ in (15).

The outage probability of UE_2 with jammer selection in NOMA network can be evaluated as follows:

$$P_2(\tau_2\leq\overline{\tau}_2) = \begin{cases} 0; & \text{if } \gamma_2\geq\dfrac{P_2}{P_1}. \\ F_{c_2}(\theta_2); & \text{otherwise.} \end{cases} \qquad (16)$$

Taking θ_2 into (8), we can easily get $F_{c_2}(\theta_2)$ as shown in (16).

4. NOMA User Secrecy Probability

We investigate the secrecy probability of a randomly located NOMA user. In this work, the user secrecy probability corresponds to the probability that a secret message for the schedule user cannot be decoded by any noncolluding eavesdroppers, because UE_1's and UE_2's signals are derived by eavesdroppers in the similar way. Here, we only discuss the secrecy performance of UE_1. Hence, the secrecy probability can be expressed as

$$\begin{aligned} P_{\mathrm{Sec}}(\gamma_s) &= P\left(\max_{x\in\Phi_e} \mathrm{SIR}(x) < \gamma_s\right) \\ &= P\left(\bigcap_{x\in\Phi_e} \mathrm{SIR}(x) < \gamma_s\right) \\ &= E\left(\prod_{x\in\Phi_e} P\left(\mathrm{SIR}(x) < \gamma_s \mid x\right)\right) \\ &= E_{\Phi_e}\left(\prod_{x\in\Phi_e} \left(1 - \exp\left(-P_1^{-1}\gamma_s r_x^a I_E(x)\right)\right)\right) \\ &= \exp\left(-2\pi\lambda_e \int_0^\infty L_{I_E(x)}\left(P_1^{-1}\gamma_s r_x^a\right) r_x \mathrm{d}r_x\right), \end{aligned} \tag{17}$$

where $\mathrm{SIR}(x)$ of the typical EVE is given by

$$\mathrm{SIR}(x) = \frac{P_1 h_x r_x^{-a}}{I_{B\longrightarrow E} + I_{JS\longrightarrow E}}, \tag{18}$$

where γ_s is the target secrecy SIR, h_x is the Rayleigh fading gain between BS_0 and EVE, and h_x follows an exponential distribution with mean 1. r_x is the distance between BS_0 and EVE. $L_{I_E}(s) = L_{I_{B\longrightarrow E}}(s) L_{I_{JS\longrightarrow E}}(s)$, where $L_{I_{B\longrightarrow E}}(s)$ and $L_{I_{JS\longrightarrow E}}(s)$ denote the Laplace transform of $I_{B\longrightarrow E}$ and $I_{JS\longrightarrow E}$, respectively. $I_{B\longrightarrow E}$ is the interference from the other cell BSs to EVE. $I_{JS\longrightarrow E}$ is the interference from the selective jammers to EVE. The detailed derivation of $L_{I_{JS\longrightarrow E}}(s)$ is provided in Appendix A. We can derive the following:

$$\begin{aligned} L_{I_E}(s) &= L_{I_{B\longrightarrow E}}(s) L_{I_{JS\longrightarrow E}}(s) \\ &= \exp\left(-\frac{\pi s^2 P_1^\delta \lambda_B}{\mathrm{sinc}(\delta)}\right) \exp\left(-\pi\lambda_J \frac{(sP_J)^\delta}{\mathrm{sinc}(\delta)}\right) \\ &\quad \times \int_0^\infty H(v,s) g(v) \mathrm{d}v. \end{aligned} \tag{19}$$

Inserting (19) into (17), we can easily have the expression of $P_{\mathrm{Sec}}(\gamma_s)$.

When all jammers are active without jammer selection, $L_{I_E}(s)$ is given by

$$\begin{aligned} L_{I_E}(s) &= L_{I_{B\longrightarrow E}}(s) L_{I_{J\longrightarrow E}}(s) \\ &= \exp\left(-\pi\lambda_B \frac{(sP_1)^\delta}{\mathrm{sinc}(\delta)}\right) \exp\left(-\pi\lambda_J \frac{(sP_J)^\delta}{\mathrm{sinc}(\delta)}\right). \end{aligned} \tag{20}$$

5. Simulation Results and Discussion

In this section, we present Monte Carlo simulations to evaluate the performance of the proposed scheme, and analytical results are illustrated and validated with extensive simulations in NOMA network. The default parameters are listed in Table 1 unless otherwise stated.

Our first proposed scheme is that all jammers are active without jammer selection in NOMA network, which is marked as "NO JS scheme." Our second proposed scheme is that some jammers are active with jammer selection in NOMA network, which is marked "JS scheme." There are no jammers in the traditional scheme in NOMA network. As expected, our proposed schemes provide a better security performance compared with the traditional scheme. The JS scheme provides a good balance between the user outage probability and the user secrecy probability. Figure 2 shows UE_1 outage probability $P_1(\overline{\tau}_1, \overline{\tau}_2)$ and UE_2 outage probability $P_2(\tau_2 \le \overline{\tau}_2)$ versus different target rates $\overline{\tau}_1$, where $\overline{\tau}_2$ is fixed to 0.1 bits/s/subband.

Table 1: Parameter assumptions.

Parameter	Meaning	Default value
λ_B	Density of BS	1/km^2
λ_J	Density of jammer	10/km^2
λ_E	Density of eavesdropper	11/km^2
λ_U	Density of user	100/km^2
P_B	Transmission power of BS	46 dBm
P_J	Transmission power of jammer	23 dBm
ε	NOMA power allocation parameter	0.3
α	Pathloss exponent	4
D	Jammer exclusion circle radius	0.1 km

In Figure 2, "ana" (the dashed curves) and "sim" (the curves with circle marks) are the abbreviation of analysis and simulation, respectively. "UE1 NO JS ana" denotes the analytical result of UE1 outage probability using the first proposed scheme, where all jammers are active. "UE1 NO JS sim" denotes the simulation result of UE1 outage probability. "UE1 JS ana" denotes the analytical result of UE1 in the second proposed scheme, where some selective jammers are active. From Figure 2, we can observe that the analytical results match well with the simulation results, which validate the accuracy of the analysis.

In Figure 2, all jammers are active in the first proposed scheme. Jammers transmit artificial noise to legitimate NOMA users and the eavesdroppers. While transmitting noise to eavesdroppers, the jammer also transmits artificial noise to legitimate NOMA users in the proposed scheme. The noise is the interference for NOMA users. When the interference increases, the SIR decreases. Compared with the traditional scheme without jointing the jammer, the outage probability increases in our proposed scheme with jointing jammers in NOMA network. Compared to the first scheme, the outage probability decreases for the selective jammer scheme. In other words, the user connective performance improves. In Figure 2, we can see that $P_1(\overline{\tau}_1, \overline{\tau}_2)$ remains constant when $\overline{\tau}_1 \le 0.04$ bit/s/subband. This is due to the fact that UE_1 needs to decode the signal intended to UE_2 first before it can decode the signal for itself. When $\overline{\tau}_1$ is below 0.04, the outage is always remained by failing to decode UE_2 signal. The result also can be explained by the definition of outage probability of $UE_1 P_1(\overline{\tau}_1, \overline{\tau}_2) = 1 - P_1(\tau_1 > \overline{\tau}_1, \tau_{1\longrightarrow 2} > \overline{\tau}_2)$; $P_1(\overline{\tau}_1, \overline{\tau}_2)$ is related to $\overline{\tau}_1$ and $\overline{\tau}_2$. If $\overline{\tau}_2$ is fixed, when $\overline{\tau}_1$ is quite small, $\tau_{1\longrightarrow 2} > \overline{\tau}_2$ can guarantee $\tau_1 > \overline{\tau}_1$ and $P_1(\tau_1 > \overline{\tau}_1, \tau_{1\longrightarrow 2} > \overline{\tau}_2)$ becomes $P_1(\tau_{1\longrightarrow 2} > \overline{\tau}_2)$, so $P_1(\overline{\tau}_1, \overline{\tau}_2)$ is not a function of $\overline{\tau}_1$ and it remains constant

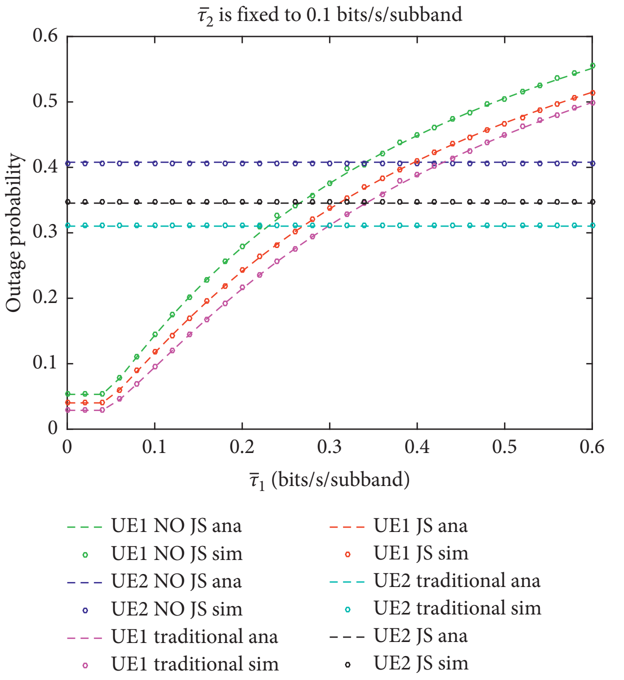


Figure 2: Outage probability of NOMA when $\overline{\tau}_2$ is fixed to 0.1 bits/s/subband.

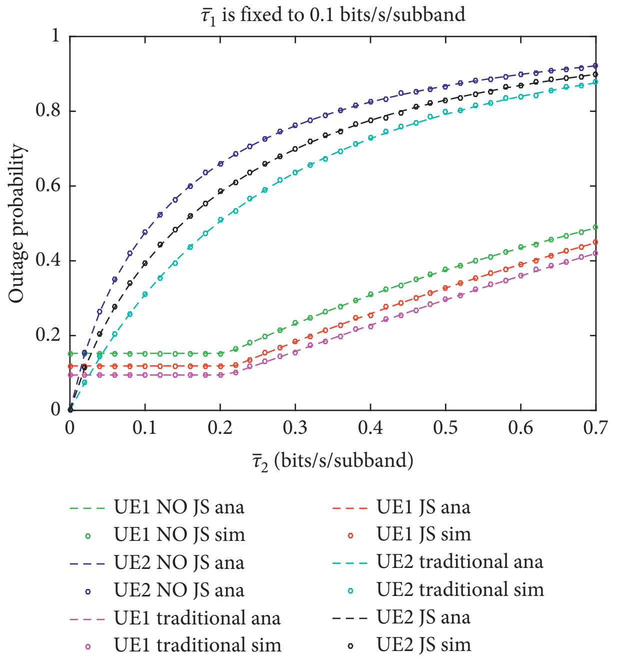


Figure 3: Outage probability of NOMA when $\overline{\tau}_1$ is fixed to 0.1 bits/s/subband.

when $\overline{\tau}_1$ is quite small. When $\overline{\tau}_1 > 0.04$, the outage probability reduces as $\overline{\tau}_1$ increases. $P_2(\tau_2 \leq \overline{\tau}_2)$ remains constant as $\overline{\tau}_1$ increases due to the fact that $P_2(\tau_2 \leq \overline{\tau}_2)$ is not a function of $\overline{\tau}_1$.

Figure 3 shows the outage probability of UE_1 and UE_2 when τ_1 is fixed to $\tau_1 = 0.1$ bit/s/subband. We can observe $P_1(\overline{\tau}_1, \overline{\tau}_2)$ remains constant at first and then increases in the same way as shown in Figure 2. When $\overline{\tau}_2$ is small, $P_1(\overline{\tau}_1, \overline{\tau}_2)$ is only a function of $\overline{\tau}_1$, which is not affected by $\overline{\tau}_2$. As $\overline{\tau}_2$ continues to increase, both $\overline{\tau}_1$ and $\overline{\tau}_2$ will affect $P_1(\overline{\tau}_1, \overline{\tau}_2)$.

Figure 4 shows that outage probability of UE_1 in three schemes versus $\overline{\tau}_1$ with different ε in NOMA network. The allocation power of UE_1 increases as ε increases; we can see that while ε increases in these schemes; $P_1(\overline{\tau}_1, \overline{\tau}_2)$ does not necessarily decrease. This outcome can be explained that more transmit power allocated to UE_1 also means less power allocated to UE_2, so it is difficult for UE_1 to decode UE_2 signal x_2. But the lower bound of outage probability of UE_1 can be improved, which is related by successfully decoding UE_2's signal x_2.

Figure 5 shows that UE_2 outage probability of three schemes versus $\overline{\tau}_2$ with different ε in NOMA network. We can observe that the outage probability decreases whsen ε is decreasing from 0.5 to 0.3. This is because more power allocated to UE_2 will result in a better outage performance of UE_2.

Figure 6 shows the impact of imperfect SIC of three schemes with different β. From the SIR of UE_1, $((c_1 P_1)/(\beta c_1 P_2 + 1))$, we can see SIR decreases as β increases. When $\beta = 0.02$, compared to perfect SIC $\beta = 0$, the outage probability of UE_1 increases.

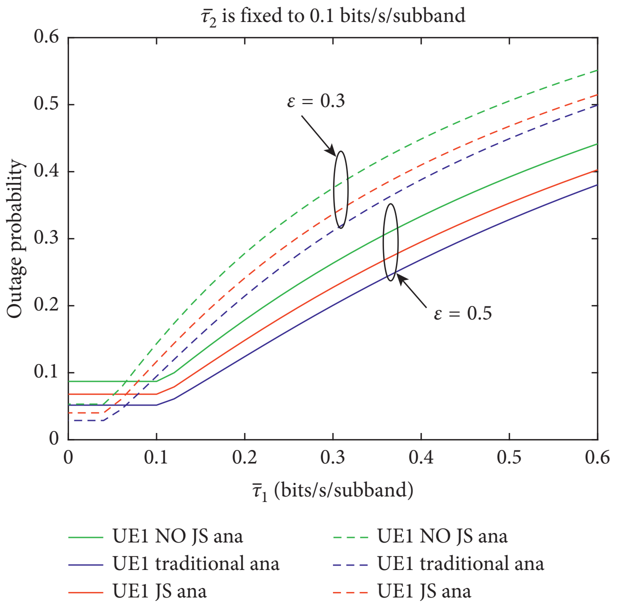


Figure 4: Outage probability of UE_1 three schemes versus $\overline{\tau}_1$ with different ε in NOMA network.

Figure 7 shows that the UE_1 secrecy probability of our proposed scheme versus SIR threshold γ_s with different D exclusion zone radii. We can see that our proposed scheme has a better performance than the traditional scheme in secrecy probability in NOMA network. "NO JS scheme" will obtain the highest secrecy probability. But the outage probability of "NO JS scheme" is the worst. Secrecy probability of "JS scheme" with small jammer

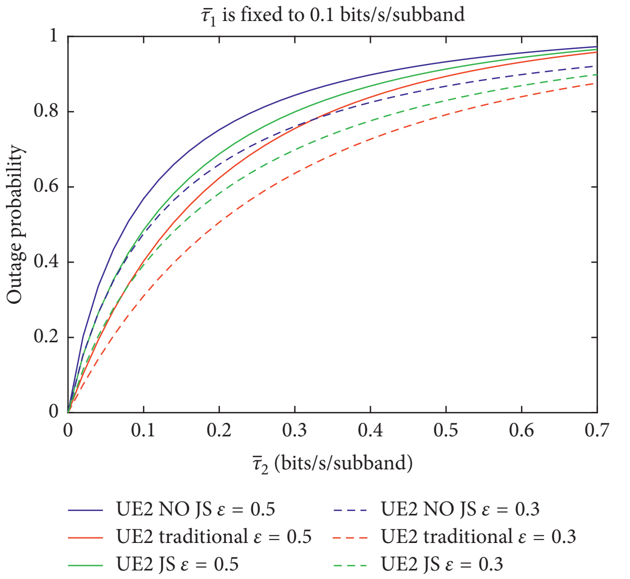


Figure 5: Outage probability of UE_2 in three schemes versus $\overline{\tau}_2$ with different ε in NOMA network.

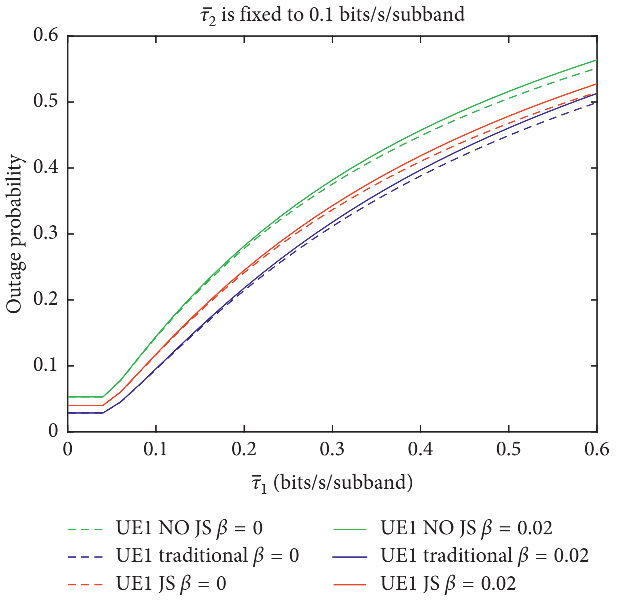


Figure 6: The impact of imperfect SIC of three schemes on NOMA with different β.

exclusion zone is better. When the exclusion zone radius increases, the small jammers transmit noise to interfere the eavesdropper, so secrecy probability decrease. Our proposed jammer selection scheme provides a good balance between the user outage probability and secrecy probability.

Figure 8 compares the connection probability performance of UE_1 versus jammer density λ_J. We can observe that simply deploying more jammers cannot enhance the connection probability. When jammer density λ_J increases, the connection probability of JS scheme increases. But the connection probability of NO JS scheme

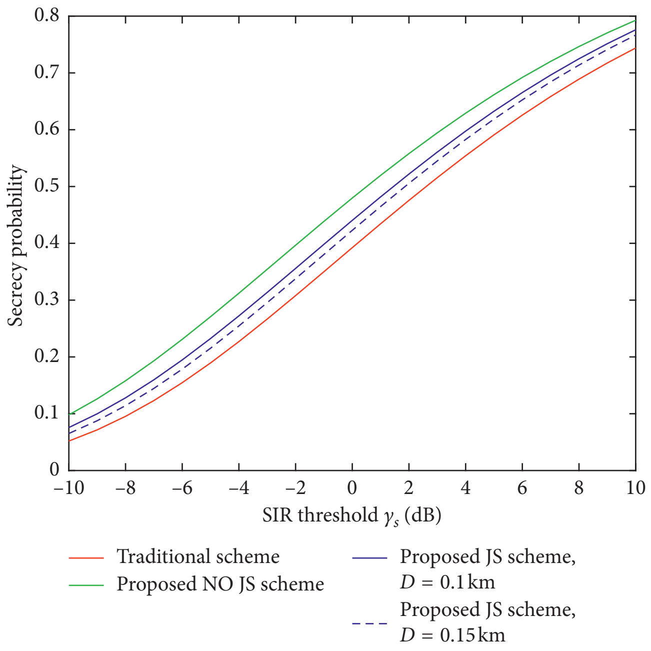


Figure 7: The UE1 secrecy probability versus SIR threshold γ_s.

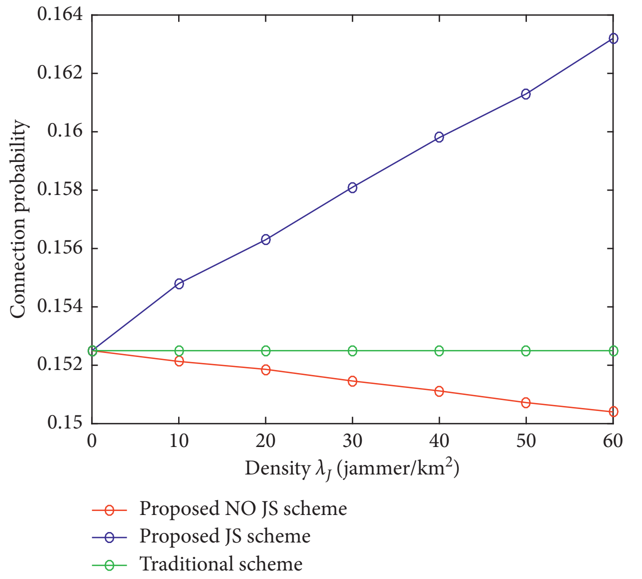
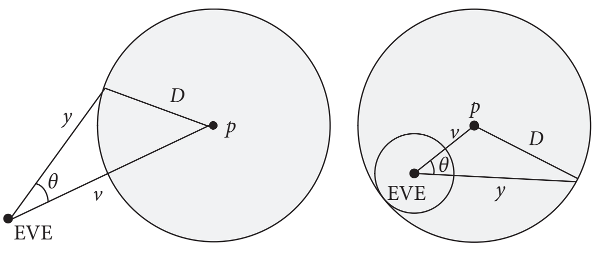


Figure 8: The connection probability performance of UE_1 versus jammer density λ_J in three schemes.

decreases, as λ_J increases. The connection probability of traditional scheme without jointing jammer remains constant. This is because the jammers whose interference on any scheduled user is stronger than a threshold are prevented from being active. When λ_J increases, there are more jammers around the eavesdropper, but the interference level suffered by the legitimate user from jammers is mitigated, and the interference level remains low in the jammer selection scheme. When $\lambda_J = 0$, the performance is the same between our proposed schemes and the traditional scheme.



(a)

(b)

FIGURE 9: Illustration of the closest jammer hole to the eavesdropper. (a) $V \leq D$. (b) $v < D$.

6. Conclusion

This paper analyzes the outage and secrecy performances of NOMA network using stochastic geometry theory. The analytical expressions of outage and secrecy probabilities are derived. Compared with the “NO JS scheme” and traditional scheme (without jointing jammer), the jammer selection scheme provides a good balance between the user outage probability and secrecy probability. Simulation results show that the expressions can provide sufficient precision to evaluate the system performance. We can optimize jammer selection exclusion zone radius and NOMA power allocation to realize a secrecy transmission in future study.

Appendix

A. Derivation of $L_{I_{JS\longrightarrow E}}(s)$

To derive the $L_{I_{JS\longrightarrow E}}(s)$, we use the approach in [20] (see Figure 9).

Point-p is the closest hole location to the EVE as in [20]. V is the distance between the jammer and EVE. Y and v have a cosine-law relation: $D^2 = y^2 + v^2 - 2yv\cos(\theta)$. $L_{I_{JS\longrightarrow E}}(s)$ can be given as

$$\begin{aligned} L_{I_{JS\longrightarrow E}}(s) &= E_{\Phi_{JS},h}\left[-\exp\left(-s\sum_{j\in\Phi_{JS}} P_J h_{e,j} R_{e,j}^{-a}\right)\right] \\ &= E_{\Phi_J}\left(\prod_{j\in\Phi_J\backslash B(p,D)} L_{h_{e,j}}\left(sP_J R_{e,j}^{-a}\right)\right) \\ &\overset{(c)}{=} \exp\left(-\pi\lambda_J\frac{\left(sP_J\right)^{\delta}}{\operatorname{sinc}(\delta)}\right) \\ &\quad \times E_p\left(\exp\left(\lambda_J\int_{B(p,\mathrm{D})}\left(1-L_{h_{e,j}}\left(sP_J y^{-a}\right)\right)\mathrm{d}y\right)\right) \\ &= \exp\left(-\pi\lambda_J\frac{\left(sP_J\right)^{\delta}}{\operatorname{sinc}(\delta)}\right)\times\int_0^{\infty} H(v,s)g(v)\mathrm{d}v. \end{aligned} \tag{A.1}$$

In step ©, $R_{e,j} = y$ denotes the distance between selective jammers with EVE. The final step follows from the probability-generating functional of PPP [13, 19] and cosine-law $D^2 = y^2 + v^2 - 2yv\cos(\theta)$ and some geometry derivation [20]:

$$H(v,s) = \begin{cases} \exp\left(\int_{v-D}^{v+D} 2y\lambda_{Je}\left(1+\frac{y^a}{sP_J}\right)^{-1}\mathrm{d}y\right), & v > D, \\ \exp\left(\pi\lambda_J(D-v)^2{}_2F_1\left(1, 1-\frac{2}{a}; 1+\frac{2}{a}; \frac{-(D-v)^a}{sP_J}\right)\right) & \\ \times\exp\left(\int_{v-D}^{v+D} 2y\lambda_{Je}\left(1+\frac{y^a}{sP_J}\right)^{-1}\mathrm{d}y\right), & v \leq D. \end{cases} \tag{A.2}$$

where

$$\lambda_{Je}(y) = \lambda_J \arccos\left(\frac{y^2+v^2-D^2}{2yv}\right), \tag{A.3}$$

$$g(v) = 2\pi\lambda_{U_s}(r_x, v)v\exp\left(-2\pi\int_0^{v}\lambda_{U_s}(r_x, v)y\mathrm{d}y\right), \tag{A.4}$$

$$\lambda_{U_s}(r_x, v) = \lambda_B\left(1-\exp\left(-\pi(r_x+y)^2\lambda_B\right)\right), \tag{A.5}$$

This completes the proof.

Data Availability

The data that support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This study was supported by the Natural Science Foundation of China (Grant nos. 61801006 and 61603003), Key Laboratory of Intelligent Perception and Computing of Anhui Province, Anqing Normal University, China, Key Project on Anhui Provincial Natural Science Study by Colleges and Universities (Grant nos. KJ2017A356 and KJ2018A0361), and Natural Science Foundation of Anhui Province (Grant nos. 1608085 and 1908085MF194).

References

[1] B. Dai, Z. Ma, Y. Luo, X. Liu, Z. Zhuang, and M. Xiao, "Enhancing physical layer security in internet of things via feedback: a general framework," *IEEE Internet of Things Journal*, p. 1, 2019.

[2] Z. Wang, R. F. Schaefer, M. Skoglund, M. Xiao, and H. V. Poor, "Strong secrecy for interference channels based on channel resolvability," *IEEE Transactions on Information Theory*, vol. 64, no. 7, pp. 5110–5130, 2018.

[3] B. Dai, Z. Ma, M. Xiao, X. Tang, and P. Fan, "Secure communication over finite state multiple-access wiretap channel with delayed feedback," *IEEE Journal on Selected Areas in Communications*, vol. 36, no. 4, pp. 723–736, 2018.

[4] J. Chen, Y. Liang, and M. S. Alouini, "Physical layer security for cooperative NOMA systems," *IEEE Transactions on Vehicular Technology*, vol. 67, no. 5, pp. 4645–4649, 2018.

[5] Z. Ding, Z. Yang, P. Fan, and H. V. Poor, "On the performance of non-orthogonal multiple access in 5G systems with randomly deployed users," *IEEE Signal Processing Letters*, vol. 21, no. 12, pp. 1501–1505, 2014.

[6] L. Dai, B. Wang, Y. Yuan, S. Han, C.-l. I, and Z. Wang, "Non-orthogonal multiple access for 5G: solutions, challenges, opportunities, and future research trends," *IEEE Communications Magazine*, vol. 53, no. 9, pp. 74–81, 2015.

[7] Y. Liu, Z. Qin, M. Elkashlan, Y. Gao, and L. Hanzo, "Enhancing the physical layer security of non-orthogonal multiple access in large-scale networks," *IEEE Transactions on Wireless Communications*, vol. 16, no. 3, pp. 1656–1672, 2017.

[8] G. Gomez, F. J. Martin-Vega, F. Javier Lopez-Martinez, Y. Liu, and M. Elkashlan, "Physical layer security in uplink NOMA multi-antenna systems with randomly distributed eavesdroppers," *IEEE Access*, vol. 7, pp. 70422–70435, 2019.

[9] Y. Tao, Y. Lei, Y. J. Guo et al., "A non-orthogonal multiple-access scheme using reliable physical-layer network coding and cascade-computation decoding," *IEEE Transactions on Wireless Communications*, vol. 16, no. 3, pp. 1633–1645, 2017.

[10] C. Wang and H. M. Wang, "Opportunistic jamming for enhancing security: stochastic geometry modeling and analysis," *IEEE Transactions on Vehicular Technology*, vol. 65, no. 12, pp. 10213–10217, 2016.

[11] A. H. Abdel-Malek, A. M. Salhab, S. A. Zummo et al., "Power allocation and cooperative jamming for enhancing physical layer security in opportunistic relay networks in the presence of interference," *Transactions on Emerging Telecommunications Technologies*, vol. 28, no. 11, p. e3178, 2017.

[12] W. Tang, S. Feng, Y. Ding et al., "Physical layer security in heterogeneous networks with jammer selection and full-duplex users," *IEEE Transactions on Wireless Communications*, vol. 16, no. 12, pp. 7982–7995, 2017.

[13] H. S. Jo, Y. J. Sang, P. Xia et al., "Heterogeneous cellular networks with flexible cell association: a comprehensive downlink SINR analysis," *IEEE Transactions on Wireless Communications*, vol. 11, no. 10, pp. 3484–3495, 2011.

[14] A. He, L. Wang, M. Elkashlan et al., "Spectrum and energy efficiency in massive MIMO enabled HetNets: a stochastic geometry approach," *IEEE Communications Letters*, vol. 19, no. 12, pp. 2294–2297, 2015.

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

[16] M. D. Renzo, "Stochastic geometry modeling and analysis of multi-tier millimeter wave cellular networks," *IEEE Transactions on Wireless Communications*, vol. 14, no. 9, pp. 5038–5057, 2015.

[17] Y. Sun, Z. Ding, X. Dai et al., "On the performance of network NOMA in uplink CoMP systems: a stochastic geometry approach," 2018, http://arxiv.org/abs/1803.00168.

[18] Z. Zhang, H. Sun, and R. Q. Hu, "Downlink and uplink non-orthogonal multiple access in a dense wireless network," *IEEE Journal on Selected Areas in Communications*, vol. 35, no. 12, pp. 2771–2784, 2017.

[19] M. Haenggi, *Wireless Security and Cryptography: Specifications and Implementations*, Cambridge University Press, Cambridge, UK, 2012.

[20] Z. Yazdanshenasan, H. S. Dhillon, M. Afshang, and P. H. J. Chong, "Poisson hole process: theory and applications to wireless networks," *IEEE Transactions on Wireless Communications*, vol. 15, no. 11, pp. 7531–7546, 2016.

Journal of Engineering
The Scientific World Journal
International Journal of Rotating Machinery
Journal of Sensors
Advances in Multimedia
Advances in Civil Engineering
Journal of Control Science and Engineering
Journal of Robotics
Journal of Electrical and Computer Engineering
Advances in OptoElectronics
VLSI Design
International Journal of Navigation and Observation
Modelling & Simulation in Engineering
International Journal of Aerospace Engineering
International Journal of Chemical Engineering
International Journal of Antennas and Propagation
Active and Passive Electronic Components
Shock and Vibration
Advances in Acoustics and Vibration
Hindawi