Hindawi
Wireless Communications and Mobile Computing
Volume 2018, Article ID 6869189, 14 pages
https://doi.org/10.1155/2018/6869189

*Research Article*

# On Secrecy Outage Probability and Average Secrecy Rate of Large-Scale Cellular Networks

**Liwei Tao, Weiwei Yang, Yueming Cai, and Dechuan Chen**

*College of Communication Engineering, Army Engineering University of PLA, 210007 Nanjing, China*

Correspondence should be addressed to Weiwei Yang; wwyang1981@163.com

Received 14 February 2018; Revised 22 April 2018; Accepted 30 April 2018; Published 7 June 2018

Academic Editor: Lu Wei

We investigate the secrecy performance in large-scale cellular networks, where both Base Stations (BSs) and eavesdroppers follow independent and different homogeneous Poisson point processes (PPPs). Based on the distances between the BS and user, the intended user selects the nearest BS as serving BS to transmit the confidential information. We first derive closed-formed expressions of secrecy outage probability and average secrecy rate of a single-antenna system for both noncooperative and cooperative eavesdroppers scenarios. Then, to further improve the secrecy performance through additional spatial degrees of freedom, the above analyses generalize to the multiantenna scenario, where BSs employ the transmit antenna selection (TAS) scheme. Finally, the results show the small-scale fading has a considerable effect on the secrecy performance in certain density of eavesdroppers and small path loss exponent environment, and when the interference caused by BS is considered, the secrecy performance will be reduced. Moreover, the gap of secrecy performance between noncooperative and cooperative eavesdroppers cases is nearly invariable as the number of antennas increases.

## 1. Introduction

Due to the broadcast nature of physical propagation channel, wireless communication networks are particularly vulnerable to be wiretapped and attacked by malicious users. Traditionally, protecting the secret information transmission relies heavily on cryptographic encryption and decryption technologies. However, because of the high complexity caused by key distribution and management, cryptographic technologies may not be suitable for large-scale wireless networks. Against this background, physical layer security (PLS), which takes advantage of the inherent randomness of wireless channels, including noise, channel fading, and interference to achieve secure transmission for wireless networks, has aroused wide attention after Shannon and Wyner's pioneering works [1, 2].

*1.1. Background.* A significant amount of PLS techniques in wireless networks, such as artificial-noise-aided security [3], security-oriented beamforming [4], cooperation based secure transmission [5], and power control and resource allocation [6], has been developed by researchers. An important information conveyed by [7, 8] is that PLS techniques have enormous potential in future 5th-generation (5G) secure communications. However, most of these works are based on point-to-point communications, where the node locations and topology of networks are determined and static. Moreover, these works only consider small-scale fading in the process of information transmission. However, in reality, the uncertain node locations has significant impact on the secure communication, especially in future 5G wireless networks where the node locations and topological structure are becoming more and more randomized and dynamic. The difficulty of researching the secrecy performance in such wireless networks is how to model the random locations distribution of nodes accurately. Fortunately, stochastic geometry has provided a powerful tool to address this difficulty and achieved great success in ad hoc networks [9, 10], random cognitive radio networks [11, 12], and large-scale cellular networks [13–19].

Stochastic geometry has facilitated the investigation of the influence of randomly located eavesdroppers on secrecy performance. Specially, for describing the locations distribution of unknown eavesdroppers, the Poisson point process (PPP) is an efficient model. In [13], the authors derived the secrecy outage probability in the scenario where a transmitter transmits confidential information to an intended receiver in the presence of PPP distributed eavesdroppers. In order to further enhance physical layer security of networks, the researchers exploited various signal processing technologies, e.g., beamforming [14], transmit antenna selection (TAS) [15], regularized channel inversion linear precoding [16], and artificial noise (AN) [17], and designed different transmission schemes, e.g., on-off transmission [18] and secrecy guard zone [19]. It is worth noting that [14, 15] simultaneously considered the noncooperative and cooperative eavesdroppers cases and analyzed the secrecy performance under various network factors. Comparing the two different eavesdropping cases, it can be concluded that cooperative eavesdroppers had more serious damage to the security of networks. The recently work [20] investigated the secrecy outage probability in random wireless networks, and the authors utilized TAS to enhance secrecy performance and proposed two metrics to order the users.

The aforementioned papers only take the single cell into account. Considering the mobility of users, users may communicate with different BSs in different locations. Hence, in order to conform to more realistic scenes, it is necessary to consider the impacts caused by the multiple cells in large-scale cellular networks. Due to the uneven distribution of BSs, particularly in remote areas, the cellular structure presents the irregular features. It has proved that the BSs modeled as PPP can track in real deployment as accurately as the traditional grid model [21]. Based on [21], the placement of BSs and eavesdroppers was modeled as mutually independent PPPs in [22, 23]. The authors in [23] specially evaluated the secrecy rate in large-scale cellular networks where BSs can exchange partial or complete information according to the eavesdroppers' location information. This work was extended to [24, 25] which proposed a regularized channel inversion linear precoding approach to improve the average secrecy rate. Furthermore, [26] considered the PLS in heterogeneous cellular networks where the BSs in every tier are spatially distributed according to a homogeneous PPP with different density.

*1.2. Motivation.* In large-scale cellular networks where BSs and eavesdroppers are random distribution [22, 23], only the large-scale fading is considered. In fact, small-scale fading caused by multipath components produces the harmful or even fatal impact for wireless communications. Hence, considering small-scale fading is more practical for analyzing secrecy performance. On the other hand, when the density of BSs is large enough, the distance between BSs and user will become small. For this short distance transmission, small-scale fading may be the main factor that affects the secrecy performance. Therefore, it is significant to research the effects on secrecy performance caused by the small-scale fading in addition to the large-scale fading in large-scale cellular networks. This work has been studied partly in our prior work [27]. However, the system that it considered is a single-antenna system, and the interference caused by BS has been ignored. In this paper, the influence of interference has been considered in single-antenna scenario. In addition, in future cellular networks, the BS may equip multiple antennas to enhance information transmission. Therefore, we extend the research to multiantenna scenario.

TAS technology with low-cost and low-computational can effectively enhance secrecy performance, and it achieves full diversity while maintaining low feedback overhead and requiring minimal transceiver circuitry. Although it has been applied in [15], it is important to know that [15] considered such a scenario where a transmitter communicated with an intended user in the presence of randomly distributed eavesdroppers. However, we focus on a more realistic and complex cellular network where BSs and eavesdroppers both are randomly distributed. It is significant to study how the network parameters, i.e., node density, the number of antennas, and path loss exponent, affect the secrecy performance, especially the performance difference between noncooperative and cooperative eavesdroppers cases, and these are beneficial for understanding and designing such wireless networks.

*1.3. Contributions.* In this paper, we investigate the secrecy outage probability and average secrecy rate of large-scale cellular networks subject to Rayleigh fading, coexisting with PPP distributed BSs and eavesdroppers. Comparing the work with [23], we consider both large-scale and small-scale fading simultaneously in the process of transmitting confidential information. Hence, our results in this paper are more general and realistic. In addition, through analyzing the secrecy performance in the large-scale cellular networks, we find that the results of [23] can be regarded as the bound of our results, and it can be concluded that the small-scale fading has a considerable effect on secrecy performance in certain density of eavesdroppers and small path loss exponent. And the impact on secrecy performance caused by the small-scale fading will decrease with the increasing of path loss exponent.

Especially, on the basis of considering the small-scale fading, we consider the interference caused by BS in the single-antenna scenario. In such case, the closed-form expressions of the secrecy outage probability and average secrecy rate are derived and the numerical results are also given in simulation section. On the other hand, we consider both noncooperative and cooperative eavesdroppers cases and derive an accurate expression as well as a closed-form bound on secrecy performance for the noncooperative eavesdroppers case and a closed-form solution for the cooperative eavesdroppers case, respectively. In the simulations section, the effects on secrecy performance in various network parameters have been given, which can help us design and optimize the network performance. An interesting finding is that increasing of the number of antennas has a little effect on the difference between noncooperative and cooperative eavesdroppers cases.

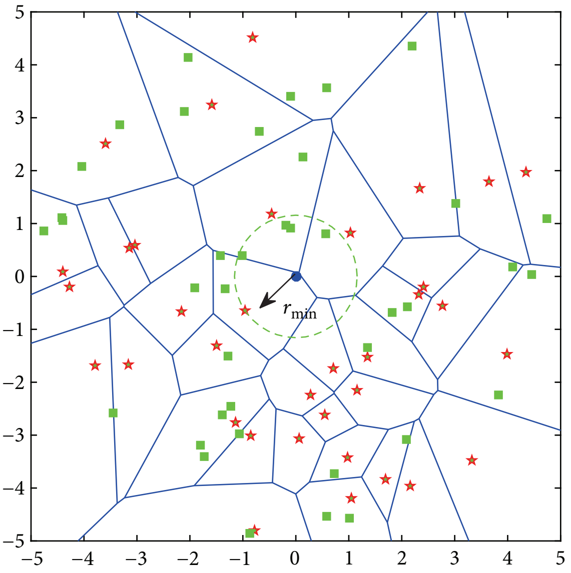


Figure 1: Illustration of Poisson distributed BSs cell boundaries. A typical user chooses the nearest BS to be the serving BS. BSs and eavesdroppers (respectively, represented by red five-pointed star and green squares) are distributed according to homogeneous PPPs.

## 2. System and Channel Model

As shown in Figure 1, we consider a downlink secure transmission in large-scale cellular networks, where one of stochastic distributed BSs is chosen to serve an intended mobile user in the presence of multiple malicious eavesdroppers. Without loss of generality, the intended mobile user is located at the origin in $\mathrm{R}^2$ as the typical user by Slivnyak theorem [28]. In this paper, both the locations of BSs and eavesdroppers are modeled as independent homogeneous PPPs $\Phi_b$ and $\Phi_e$ of intensity $\lambda_b$ and $\lambda_e$, respectively. First of all, we assume the BSs, the typical user, and eavesdroppers are equipped with a single antenna each. Furthermore, in Section 5, we extend to the multiantenna scenario where BSs are equipped with multiple antennas and use TAS technology to further enhance the secrecy performance.

We consider both large-scale and small-scale fading for the wireless channels. For the large-scale fading, we adopt the standard path loss model $l_{xy}^{-\alpha}$, where $l_{xy}$ denotes the distance between transmitter $x$ and receiver $y$, and $\alpha > 2$ is path loss exponent. Small-scale fading is caused by the coherent superposition of a great number of multipath components at the receiver. It heavily leads to the fragility of wireless communication. For the small-scale fading, a quasi-static Rayleigh fading is assumed, which is ignored by prior research in this research field [23]. And in the scenario of passive eavesdroppers, it is difficult to obtain the instantaneous channel state information (CSI) and locations of eavesdroppers. Nevertheless, we assume that their small-scale channel distributions are available. Let $h_{ij}$ represent the Rayleigh fading coefficient between node $i$ and node $j$ in the cellular network. Meanwhile, we assume that the Rayleigh fading coefficient follows a zero-mean complex Gaussian distribution with unit variance, i.e., $\mathscr{CN}(0,1)$.

Similar to [15, 23], in order to reduce feedback and computational complexity, we select the serving BS for the intended user only depending on the large-scale fading, i.e., $l_{B_iU}^{-\alpha}$. For a given $\alpha$ and channel model, serving BS is equivalent as the nearest BS. Hence the serving BS can be selected as $B^* = \arg\min_{B_i \in \Phi_b}(l_{B_iU})$. Based on [29], the probability density function (PDF) of $l_{B^*U}$ is $f_{l_{B^*U}}(l) = 2\pi\lambda_b l e^{-\pi\lambda_b l^2}$, where $l_{B^*U}$ is the distance between the serving BS and the typical user.

In this work, we adopt two assumptions; one is that the downlink receiver has no in-band interference [23]. It is justifiable when the interfering BSs are far away from the serving BS, so that a carefully planned frequency reuse pattern can be adopted. Moreover, the constant noise power can comprise interference of networks. Another assumption is that the interference caused by BS is considered in the process of information transmission [24, 25].

## 3. Secrecy Performance of Single-Antenna System

In this section, we investigate the secrecy outage probability and average secrecy rate at the typical user under the assumption that all nodes are equipped with a single antenna. The received signal-noise-ratio (SNR) at the typical user can be expressed as $\gamma_{B^*U} = P_{BS}|h_{B*U}|^2 l_{B*U}^{-\alpha}/\sigma^2$, and the SNR of an arbitrary eavesdropper $e$ is $\gamma_{B^*e} = P_{BS}|h_{B^*e}|^2 l_{B^*e}^{-\alpha}/\sigma^2$, where $\sigma^2$ is the variance of zero-mean Additive White Gaussian Noise (AWGN) at each receiver, and $P_{BS}$ is the transmit power of the serving BS.

### 3.1. Noncooperative Eavesdroppers

*3.1. Noncooperative Eavesdroppers.* In this subsection, considering that there is no cooperation among eavesdroppers and each eavesdropper decodes information independently, in such case, we evaluate the secrecy outage probability and average secrecy rate of the intended user in cellular networks.

*3.1.1. Secrecy Outage Probability.* The secrecy outage probability is defined as the probability that the achievable secrecy rate is less than a given secrecy code rate which is nonnegative.

Based on the model described above, the channel capacity of the serving BS to the typical user can be written as

$$\begin{aligned} C_{B^*U} &= \log_2\left(1+\gamma_{B^*U}\right) \\ &= \log_2\left(1+\frac{P_{BS}\left|h_{B^*U}\right|^2 l_{B^*U}^{-\alpha}}{\sigma^2}\right). \end{aligned} \tag{1}$$

In order to design the optimal network parameters to achieve the maximum level of security in the presence of multiple noncooperative eavesdroppers, we consider the most detrimental eavesdropper which has the worst impact on secrecy performance of networks. The channel capacity at the most detrimental eavesdropper can be expressed as

$$\begin{aligned} C_{B^*e} &= \log_2\left(1 + \max_{e\in\Phi_e}\left(\gamma_{B^*e}\right)\right) \\ &= \log_2\left(1 + \max_{e\in\Phi_e}\left(\frac{P_{BS}\left|h_{B^*e}\right|^2 l_{B^*e}^{-\alpha}}{\sigma^2}\right)\right). \end{aligned} \tag{2}$$

The achievable maximum secrecy rate at the typical user is given by $R_s = [C_{B^*U} - C_{B^*e}]^+$, so the secrecy outage probability can be given as

$$\begin{aligned} P_{so}^{NC}\left(R_0\right) &= \mathbb{P}\left(R_s < R_0\right) = \mathbb{P}\left(C_{B^*U} - C_{B^*e} < R_0\right) \\ &= \mathbb{P}\left(\log_2\left(\frac{1 + P_{BS}\left|h_{B^*U}\right|^2 l_{B^*U}^{-\alpha}/\sigma^2}{1 + \max_{e\in\Phi_e}\left(P_{BS}\left|h_{B^*e}\right|^2 l_{B^*e}^{-\alpha}/\sigma^2\right)}\right)\right. \\ &\left. < R_0\right) \overset{a}{\simeq} \mathbb{P}\left(\frac{\left|h_{B^*U}\right|^2 l_{B^*U}^{-\alpha}}{\max_{e\in\Phi_e}\left(\left|h_{B^*e}\right|^2 l_{B^*e}^{-\alpha}\right)} < 2^{R_0}\right), \end{aligned} \tag{3}$$

where $[X]^+ = \max(0, x)$ and $R_0 \geq 0$ denotes the secrecy rate threshold. Step (a) is based on that the typical user and eavesdroppers operate in moderate-to-high SNR regime [18, 23].

**Proposition 1.** *The secrecy outage probability for the scenario of noncooperative eavesdroppers can be expressed as*

$$\begin{aligned} &P_{so}^{NC}\left(R_0\right) \\ &\quad \simeq \sum_{k=1}^{\infty}\left(\frac{-\lambda_b\alpha}{2\lambda_e\Gamma\left(2/\alpha\right)\left(2^{R_0}\right)^{2/\alpha}}\right)^{k-1}\Gamma\left(\frac{2}{\alpha}\left(k-1\right)+1\right). \end{aligned} \tag{4}$$

*Proof.* According to the definition of the secrecy outage probability in (3), we can derive the secrecy outage probability as

$$\begin{aligned} P_{so}^{NC}\left(R_0\right) &\simeq \mathbb{P}\left(\frac{\left|h_{B^*U}\right|^2 l_{B^*U}^{-\alpha}}{\max_{e\in\Phi_e}\left(\left|h_{B^*e}\right|^2 l_{B^*e}^{-\alpha}\right)} < 2^{R_0}\right) \\ &= \mathbb{E}_{\Phi_b,\Phi_e}\left(\mathbb{P}\left(\max_{e\in\Phi_e}\left(\left|h_{B^*e}\right|^2 l_{B^*e}^{-\alpha}\right) > \frac{\left|h_{B^*U}\right|^2 l_{B^*U}^{-\alpha}}{2^{R_0}} \mid \Phi_b,\right.\right. \\ &\left.\left.\Phi_e\right)\right) = 1 - \mathbb{E}_{\Phi_b,\Phi_e}\left(\prod_{e\in\Phi_e}\mathbb{P}\left(\left|h_{B^*e}\right|^2\right.\right. \\ &\left.\left.< \frac{\left|h_{B^*U}\right|^2 l_{B^*U}^{-\alpha}}{2^{R_0}} l_{B^*e}^{\alpha} \mid \Phi_b, \Phi_e\right)\right) \overset{a}{=} 1 \\ &- \mathbb{E}_{\Phi_b}\left(\exp\left(-\lambda_e\int_0^{2\pi}\int_0^{\infty} e^{(|h_{B^*U}|^2 l_{B^*U}^{-\alpha}/2^{R_0})r^{\alpha}} rdrd\theta\right) \mid\right. \\ &\left.\Phi_b\right) \overset{b}{=} 1 - \mathrm{E}_{\Phi_b}\left(\exp\left(-\frac{2\pi\lambda_e 2^{R_0}}{\alpha\left|h_{B^*U}\right|^{2/\alpha} l_{B^*U}^{-2}}\Gamma\left(\frac{2}{\alpha}\right)\right) \mid\right. \\ &\left.\Phi_b\right) = 1 \\ &- \mathrm{E}_{|h_{B^*U}|^2}\left(\int_0^{\infty}\exp\left(-\frac{2\pi\lambda_e\left(2^{R_0}\right)^{2/\alpha}}{\alpha\left|h_{B^*U}\right|^{2/\alpha} l_{B^*U}^{-2}}\times\Gamma\left(\frac{2}{\alpha}\right)\right)\right. \\ &\left.\cdot f_{l_{B^*U}}\left(l\right)dl \mid \left|h_{B^*U}\right|^2\right) \\ &\overset{c}{=} \int_0^{\infty}\left(\frac{2\lambda_e\Gamma\left(2/\alpha\right)\left(2^{R_0}\right)^{2/\alpha} e^{-x}}{\lambda_b\alpha x^{2/\alpha} + 2\lambda_e\Gamma\left(2/\alpha\right)\left(2^{R_0}\right)^{2/\alpha}}\right)dx \\ &\overset{d}{=} \sum_{k=1}^{\infty}\left(-\frac{\lambda_b\alpha}{2\lambda_e\Gamma\left(2/\alpha\right)\left(2^{R_0}\right)^{2/\alpha}}\right)^{k-1}\Gamma\left(\frac{2}{\alpha}\left(k-1\right)+1\right), \end{aligned} \tag{5}$$

where step (a) is based on the probability generating functional (PGFL) of PPPs $\Phi_b$ and $\Phi_e$ [30], and step (b) holds by using [31, eq. (3.326.2)]. In addition, step (c) is based on the exponential distribution of channel gain $|h_{B^*U}|^2$ and the PDF of $l_{B^*U}$, and step (d) follows polynomial expansion [31, eq. (1.112.1)] and integral formula [31, eq. (3.326.2)].

From (4), we know that if the density of eavesdroppers increases or the density of BSs decreases, the secrecy outage probability will increase. Additionally, the secrecy outage probability increases as the threshold value $R_0$ or $\alpha$ increases. In order to make the result easy to analyze, we derive the lower bound of the secrecy outage probability as

$$P_{so}^{NC}\left(R_0\right) \geq P_{so}^{NC-lower}\left(R_0\right) = \frac{\lambda_e\left(2^{R_0}\right)^{2/\alpha}}{\lambda_b + \lambda_e\left(2^{R_0}\right)^{2/\alpha}} \tag{6}$$

□

*Proof.* Beginning with the basic definition of the secrecy outage probability, it can be derived as follows:

$$\begin{aligned}
P_{so}^{NC}\left(R_0\right) &= \mathbb{E}_{\Phi_b,\Phi_e}\left(\mathbb{P}\left(l_{B^*U} > \left(\frac{\left|h_{B^*U}\right|^2}{\max_{e\in\Phi_e}\left(\left|h_{B^*e}\right|^2 l_{B^*e}^{-\alpha}\right)} \times \frac{1}{2^{R_0}}\right)^{1/\alpha} \mid \Phi_b, \Phi_e\right)\right) \\
&\overset{a}{\geq} \mathbb{E}_{l_{B^*U},l_{B^*e}}\left(\mathbb{P}\left(l_{B^*U} > \left(\mathbb{E}_{|h_{B^*U}|^2,|h_{B^*e}|^2}\left(\frac{1}{2^{R_0}} \times \frac{\left|h_{B^*U}\right|^2}{\max_{e\in\Phi_e}\left(\left|h_{B^*e}\right|^2 l_{B^*e}^{-\alpha}\right)} \mid \left|h_{B^*U}\right|^2, \left|h_{B^*e}\right|^2\right)\right)^{1/\alpha}\right) \mid l_{B^*U,}l_{B^*e}\right) \\
&= \mathbb{E}_{l_{B^*U,}l_{B^*e}}\left(\mathbb{P}\left(l_{B^*U} > \frac{1}{\max_{e\in\Phi_e}\left(l_{B^*e}^{-\alpha}\right)\left(2^{R_0}\right)^{1/\alpha}}\right) \mid l_{B^*U,}l_{B^*e}\right) \\
&= \mathbb{E}_{l_{B^*U,}l_{B^*e}}\left(\mathbb{P}\left(\min_{e\in\Phi_e}\left(l_{B^*e}\right) < \left(2^{R_0}\right)^{1/\alpha} l_{B^*U}\right) \mid l_{B^*U,}l_{B^*e}\right) \overset{b}{=} 1 - \int_0^\infty \exp\left(-\pi\lambda_e\left(2^{R_0}\right)^{2/\alpha} y^2\right) f_{l_{B^*U}}(l)\, dl \\
&= \frac{\lambda_e\left(2^{R_0}\right)^{2/\alpha}}{\lambda_b + \lambda_e\left(2^{R_0}\right)^{2/\alpha}},
\end{aligned} \tag{7}$$

where step (a) is derived by employing the Jensen inequality $E(\varphi(x)) \geq \varphi(E(x))$, and step (b) follows the PPPs void probability and the PDF of $l_{B^*\text{U}}$. □

*Remark 2.* It should be noticed that the result in (6) can be compared with scenario 1 in [23] where mobile users to be served by the nearest BS and the full location information of eavesdroppers can be obtained by BS. In that paper, it gave the complementary cumulative distribution function (CCDF) of $R_s$ as $\overline{F}_{R_s}(R_0) = \mathbb{P}(R_s > R_0)$ without considering the impact of the small-scale fading. We can find that the result in [23] is the same as the lower bound in essence. Therefore, it provides a bound for our result. Because we take the small-scale fading into account, the result presented in this paper is more realistic and general.

*3.1.2. Average Secrecy Rate.* In the following, we study the average secrecy rate $\overline{R}_s$ of the cellular network in the presence of noncooperative eavesdroppers. By calculating the expectation of secrecy rate, we can derive the expression of average secrecy rate as

$$\begin{aligned}
\overline{R}_s &= \int_0^\infty R_s f\left(R_s\right) dR_s = \int_0^\infty \left(\int_0^{R_s} dy\right) f\left(R_s\right) dR_s \\
&= \int_0^\infty \int_y^\infty f\left(R_s\right) dR_s dy = \int_0^\infty \left(1 - F\left(R_s\right)\right) dy,
\end{aligned} \tag{8}$$

where $f(R_s)$ and $F(R_s)$ are the PDF and the cumulative distribution function (CDF) of $R_s$, respectively. And, the secrecy outage probability can be regarded as the distribution function of the achievable maximum secrecy rate $R_s$. Therefore, based on Proposition 1, we can derive the expression of average secrecy rate as $\overline{R}_s = \int_0^\infty (1 - P_{so}(R_0))dR_0$.

**Corollary 3.** *The average secrecy rate is provided by*

$$\overline{R}_s^{NC} = \sum_{k=1}^\infty \frac{(-1)^{k+1}\alpha}{2k\ln 2}\left(\frac{\alpha\lambda_b}{2\lambda_e\Gamma(2/\alpha)}\right)^k \Gamma\left(\frac{2}{\alpha}k + 1\right) \tag{9}$$

*Proof.* From Proposition 1 and the definition of $\overline{R}_s$, the average secrecy rate can be expressed as

$$\begin{aligned}
\overline{R}_s^{NC} &= \int_0^\infty \int_0^\infty \left(\frac{\lambda_b \alpha x^{2/\alpha} e^{-x}}{\lambda_b \alpha x^{2/\alpha} + 2\lambda_e \Gamma(2/\alpha)\left(2^{R_0}\right)^{2/\alpha}}\right) dx dR_0 \\
&\overset{a}{=} \int_0^\infty \frac{e^{-x}}{\ln\left(2^{2/\alpha}\right)}\left[\ln\left(\frac{\exp\left(\ln\left(2^{2/\alpha}\right) R_0\right)}{\lambda_b \alpha x^{2/\alpha} + 2\lambda_e \Gamma(2/\alpha)} \times \frac{\lambda_b \alpha x^{2/\alpha}}{\exp\left(\ln\left(2^{2/\alpha}\right) R_0\right)}\right)\right]_0^\infty dx \\
&= \int_0^\infty \left(\frac{\alpha e^{-x}}{2\ln 2}\ln\left(1 + \frac{\alpha\lambda_b x^{2/\alpha}}{2\lambda_e \Gamma(2/\alpha)}\right)\right) dx \overset{b}{=} \frac{\alpha^2 \lambda_b}{4\ln 2\lambda_e \Gamma(2/\alpha)} \int_0^\infty \frac{e^{-t^{2/\alpha}}}{1 + \left(\alpha\lambda_b/2\lambda_e\Gamma(2/\alpha)\right) t} dt \\
&\overset{c}{=} \sum_{k=1}^\infty \frac{(-1)^{k+1}}{\ln 2}\left(\frac{\alpha\lambda_b}{2\lambda_e\Gamma(2/\alpha)}\right)^k \Gamma\left(\frac{2k}{\alpha} + 1\right),
\end{aligned} \tag{10}$$

where step (a) follows the integral result based on the integrand herein [32, eq. (5.1.2.4.2)], and step (b) is based on the integration by parts. In addition, step (c) uses the power of binomials [31, eq. (1.112.1)].

From (9), the average secrecy rate $\overline{R}_s$ at the typical user decreases when the value $\lambda_e$ increases. Also, with the increasing of path loss exponent $\alpha$, the average secrecy rate increases. So the large path loss exponent has a positive impact on the average secrecy rate. □

*Remark 4.* Utilizing the lower bound of secrecy outage probability in Proposition 1, the upper bound of the average secrecy rate is written as

$$\begin{aligned}\overline{R}_s^{NC} \leq \overline{R}_s^{NC\text{-}upper} &= \int_0^{\infty} \left(1 - P_{so}^{NC\text{-}lower}(R_0)\right) dR_0 \\ &= \frac{\alpha}{2\ln 2} \ln\left(1 + \frac{\lambda_b}{\lambda_e}\right).\end{aligned} \tag{11}$$

We can find that the upper bound of the average secrecy rate is the same with the result in [23] where it considered a noncooperative eavesdroppers case and only taken lager-scale fading into account but ignored the effect caused by the small-scale fading. From (11), it is obvious that the large $\alpha$ and $\lambda_b/\lambda_e$ are beneficial to improve the secrecy performance in the large-scale cellular network.

*3.1.3. Security Outage Probability When Considering Interference.* In this section, we consider the typical user will be interfered by the other BSs except the serving BS. In addition, the secrecy indeed becomes better when the eavesdropping channel is degraded under the effect of interference. In this paper, we focus on the worst-case scenario of eavesdropping, where all the eavesdroppers can mitigate the interference. In fact, eavesdroppers are usually assumed to have strong ability, and they may cooperate to cancel the interference, as seen in [33]. In this scenario, the security outage probability at the typical user is written as

$$\begin{aligned}P_{so}^{I}(R_0) &= \mathbb{P}(C_s < R_0) = \mathbb{P}(C_{B^*U} - C_{B^*e} < R_0) \\ &= \mathbb{P}\left(\log_2 \frac{1+\gamma_{B^*U}}{1+\gamma_{B^*e}} < R_0\right) \simeq \mathbb{P}\left(\frac{\gamma_{B^*U}}{\gamma_{B^*e}} < \beta\right) \\ &= \int_0^{\infty}\int_0^{\beta\gamma_{B^*e}} f_{\gamma_{B^*U}}(x) f_{\gamma_{B^*e}}(y)\,dx\,dy \\ &= \int_0^{\infty} F_{\gamma_{B^*U}}(\beta y) f_{\gamma_{B^*e}}(y)\,dy,\end{aligned} \tag{12}$$

where $\beta = 2^{R_0}$.

The CDF of $\gamma_{B^*U}$ is derived as

$$\begin{aligned}F_{\gamma_{B^*U}}(x) &= \mathbb{P}(\gamma_{B^*U} < x) \\ &= \mathbb{P}\left(\frac{P_{BS}h_{B^*U}l_{B^*U}^{-\alpha}}{\sum_{i\in\Phi_b/\{s\}} P_{BS}h_{B_iU}l_{B_iU}^{-\alpha} + \sigma^2} < x\right) \\ &= \mathbb{P}\left(\frac{P_{BS}h_{B^*U}l_{B^*U}^{-\alpha}}{I+\sigma^2} < x\right) \\ &\overset{a}{\approx} \mathbb{P}\left(\frac{P_{BS}h_{B^*U}l_{B^*U}^{-\alpha}}{I} < x\right) = 1 - \mathrm{E}_{\Phi_b}\left(e^{-(xI/P_{BS})l_{B^*U}^{-\alpha}}\right) \\ &= 1 - L_I\left(\frac{l_{B^*U}^{\alpha}x}{P_{BS}}\right) \\ &\overset{b}{=} 1 - \exp\left(-\pi l_{B^*U}^2 \lambda_b \Gamma\left(1+\frac{2}{\alpha}\right)\Gamma\left(1-\frac{2}{\alpha}\right)x^{2/\alpha}\right),\end{aligned} \tag{13}$$

where $I = \sum_{i\in\Phi_b/\{s\}} P_{BS}h_{B_iU}l_{B_iU}^{-\alpha}$. Step (a) is based on the the assumption that this is an interference limited system, and step (b) follows the Laplace transform of $I$ [34].

Next, we can give the CDF of $\gamma_{B^*e}$ as

$$\begin{aligned}F_{\gamma_{B^*e}}(x) &= \mathbb{P}(\gamma_{B^*e} < x) = \mathbb{P}\left(\max_{e\in\Phi_e} P h_{B^*e} l_{B^*e}^{-\alpha} < x\right) \\ &= \mathbb{E}_{\Phi_e}\left(\prod\left(P\left(h_{B^*e} < \frac{x l_{B^*e}^{\alpha}}{P}\right)\right)\right) \\ &= \exp\left(-2\pi\lambda_e \int_0^{\infty} e^{-xr^{\alpha}/P} r\,dr\right) \\ &= \exp\left(-2\pi\lambda_e \frac{\Gamma(2/\alpha)P^{2/\alpha}}{\alpha x^{2/\alpha}}\right),\end{aligned} \tag{14}$$

where $P = P_{BS}/\sigma^2$. Then, the PDF is

$$\begin{aligned}f_{\gamma_{B^*e}}(x) &= -\frac{4\pi\lambda_e\Gamma(2/\alpha)P^{2/\alpha}}{\alpha^2} x^{-2/\alpha-1} \\ &\quad \cdot \exp\left(-2\pi\lambda_e \frac{\Gamma(2/\alpha)P^{2/\alpha}}{\alpha x^{2/\alpha}}\right),\end{aligned} \tag{15}$$

Submit (15) and (13) to (12), we can get the expression of secrecy outage probability

$$\begin{aligned}P_{so}^{I}(R_0) &\simeq \int_0^{\infty} 1 - \exp\left(-\pi l_0^2 \lambda_b \Gamma\left(1+\frac{2}{\alpha}\right)\Gamma\left(1-\frac{2}{\alpha}\right)(\beta \mathrm{y})^{2/\alpha}\right) \times f_{\gamma_{B^*e}}(y)\,dy \\ &= \int_0^{\infty}\int_0^{\infty} \left(1 - \exp\left(-\pi l_0^2 \lambda_b \Gamma\left(1+\frac{2}{\alpha}\right)\Gamma\left(1-\frac{2}{\alpha}\right)(\beta \mathrm{y})^{2/\alpha}\right)\right) \times 2\pi\lambda_b l_0 e^{-\pi\lambda_b l_0^2 d_{l_0} f_{\gamma_e}(y)} dy \\ &= \int_0^{\infty} \left(1 - 2\pi\lambda_b l_0 e^{-\pi\lambda_b l_0^2 - \pi l_0^2 \lambda_b \Gamma(1+2/\alpha)\Gamma(1-2/\alpha)(\beta \mathrm{y})^{2/\alpha}}\right) d_{l_0} f_{\gamma_e}(y)\,dy\end{aligned}$$

$$\begin{aligned} &= 1 - \int_0^\infty \left( \frac{1}{1 + (\beta y)^{2/\alpha} \Gamma(1 + 2/\alpha) \Gamma(1 - 2/\alpha)} \right) f_{\gamma_e}(y)\, dy \\ &= 1 + C_1 \int_0^\infty \frac{1}{1 + C_2 y^{2/\alpha}} \times \frac{1}{y^{2/\alpha+1}} \exp\left(-C_3 y^{-2/\alpha}\right) dy, \end{aligned} \tag{16}$$

where $C_1 = 4\pi\lambda_e\Gamma(2/\alpha)P^{2/\alpha}/\alpha^2$, $C_2 = \beta^{2/\alpha}\Gamma(1 + 2/\alpha)\Gamma(1 - 2/\alpha)$, and $C_3 = 2\pi\lambda_e(\Gamma(2/\alpha)P^{2/\alpha}/\alpha)$.

Using the approach of equivalent substitution, the expression can be simplified as

$$\begin{aligned} P_{so}^{I}(R_0) &= 1 + C_1 \int_0^\infty \frac{1}{1 + C_2 t} \\ &\quad \times \frac{1}{t^{1+2/\alpha}} \exp\left(-C_3 t^{-1}\right) \frac{dt}{(2/\alpha)(t)^{1-\alpha/2}} = 1 + \frac{\alpha}{2} \\ &\quad \cdot C_1 \int_0^\infty \frac{1}{1 + C_2 t} \frac{1}{t^2} \exp\left(-C_3 t^{-1}\right) dt = 1 - \frac{\alpha}{2} \\ &\quad \cdot C_1 \int_0^\infty \frac{x}{\mathrm{x} + C_2} \exp\left(-C_3 x\right) dx \overset{a}{=} 1 - \frac{\alpha}{2} \\ &\quad \cdot C_1 C_2 e^{C_2 C_3} \Gamma(2) \Gamma\left(-1, C_2 C_3\right), \end{aligned} \tag{17}$$

where $\Gamma(\alpha, x)$ is the incomplete gamma function and step (a) is based on [31, eq. (3.381.10)].

*3.1.4. Average Secrecy Rate When Considering Interference.* In this section, the average secrecy rates are derived when the interference caused by BSs is considered. According to the expression of average secrecy rate $\overline{R}_s = \int_0^\infty (1 - P_{so}(R_0))dR_0$, the average secrecy rate can be calculated as follows:

$$\begin{aligned} \overline{R}_s^{I} &= \int_0^\infty \left( \frac{\alpha}{2} C_1 C_2 e^{C_2 C_3} \Gamma(2) \Gamma\left(-1, C_2 C_3\right) \right) dR_0 \\ &= \frac{\alpha \Gamma(2)}{2} C_4 C_1 \int_0^\infty \left( \beta^{2/\alpha} e^{\beta^{2/\alpha} C_0} \Gamma\left(-1, \beta^{2/\alpha} C_0\right) \right) dR_0 \\ &= \frac{\alpha \Gamma(2)}{2 \ln 2} C_4 C_1 \int_0^\infty \left( \beta^{2/\alpha - 1} e^{\beta^{2/\alpha} C_0} \Gamma\left(-1, \beta^{2/\alpha} C_0\right) \right) d\beta \\ &\overset{a}{=} \frac{\alpha^2 \Gamma(2)}{4 \ln 2} C_4 C_1 \int_0^\infty e^{C_0 t} \Gamma\left(-1, C_0 t\right) dt \\ &= \frac{\alpha^2 \Gamma(2)}{4 \ln 2} C_4 C_1 F\left(C_0\right), \end{aligned} \tag{18}$$

where $C_0 = (2\pi\lambda_e\Gamma(2/\alpha)P^{2/\alpha}/\alpha)\Gamma(1 + 2/\alpha)\Gamma(1 - 2/\alpha)$, $C_4 = \Gamma(1 + 2/\alpha)\Gamma(1 - 2/\alpha)$, and $F(x) = \int_0^\infty e^{xt}\Gamma(-1, xt)dt$. Step (a) is based on the variable substitution.

*3.2. Cooperative Eavesdroppers.* In this subsection, for a strongly robust analysis, we consider the worst case that all eavesdroppers can share the message with each other, and eavesdroppers are capable of combining their signals in an optimal manner to decode confidential information.

*3.2.1. Secrecy Outage Probability.* It is easy to know that the main channel capacity $C_{B^*U}$ is the same as the scenario of noncooperative eavesdroppers. In cooperative eavesdroppers case, multiple eavesdroppers can be regarded as a single eavesdropper with multiple distributed antennas. Considering that the maximal ratio combining (MRC) scheme is employed, the equivalent eavesdropping channel capacity can be derived as

$$\begin{aligned} C_{B^*e} &= \log_2 \left( 1 + \sum_{e \in \Phi_e} \left( \gamma_{B^*e} \right) \right) \\ &= \log_2 \left( 1 + \sum_{e \in \Phi_e} \left( \frac{P_{BS} \left| h_{B^*e} \right|^2 l_{B^*e}^{-\alpha}}{\sigma^2} \right) \right). \end{aligned} \tag{19}$$

The secrecy outage probability $P_{so}^{C}(R_0)$ in the presence of multiple cooperative eavesdroppers can be calculated by

$$\begin{aligned} P_{so}^{C}(R_0) &= \mathbb{P}\left(C_{B^*U} - C_{B^*e} < R_0\right) \\ &= \mathbb{P}\left( \log_2 \left( \frac{1 + P_{BS} \left| h_{B*U} \right|^2 l_{B*U}^{-\alpha} / \sigma^2}{1 + \sum_{e \in \Phi_e} \left( P_{BS} \left| h_{B^*\mathrm{e}} \right|^2 l_{B^*e}^{-\alpha} / \sigma^2 \right)} \right) \right. \\ &\quad \left. < R_0 \right) \simeq \mathbb{P}\left( \frac{\left| h_{B^*U} \right|^2 l_{B^*U}^{-\alpha}}{\sum_{e \in \Phi_e} \left( \left| h_{B^*e} \right|^2 l_{B^*e}^{-\alpha} \right)} < 2^{R_0} \right) \end{aligned} \tag{20}$$

**Proposition 5.** *The secrecy outage probability for the scenario of cooperative eavesdroppers can be given as*

$$P_{so}^{C}(R_0) \simeq \frac{2\lambda_e \left(2^{R_0}\right)^{2/\alpha} \Gamma(1 - 2/\alpha) \Gamma(2/\alpha)}{\alpha\lambda_b + 2\lambda_e \left(2^{R_0}\right)^{2/\alpha} \Gamma(1 - 2/\alpha) \Gamma(2/\alpha)} \tag{21}$$

*Proof.* Based on the definition of the secrecy outage probability (10) of the cooperative eavesdroppers case, the secrecy outage probability can be obtained as follows:

$$\begin{aligned} P_{so}^{C}(R_0) &\simeq \mathbb{P}\left(\frac{|h_{B^*U}|^2 l_{B^*U}^{-\alpha}}{\Sigma_{e\in\Phi_e}\left(|h_{B^*e}|^2 l_{B^*e}^{-\alpha}\right)} < 2^{R_0}\right) \\ &\overset{a}{=} \int_0^\infty \mathbb{E}_{\Phi_e}\left(\mathbb{P}\left(|h_{B^*U}|^2 < 2^{R_0} l_{B^*U}^{\alpha} Z_{\Phi_e} \mid \Phi_e\right)\right) \\ &\cdot f_{l_{B*U}}(l)\,dl = \int_0^\infty \mathbb{E}_{\Phi_e}\Big(1 \\ &- \exp\left(-2^{R_0} l_{B^*U}^{\alpha} Z_{\Phi_e}\right)\Big) f_{l_{B*U}}(l)\,dl \overset{b}{=} 1 \\ &- \int_0^\infty \exp\left(\frac{-2\pi\lambda_e \left(2^{R_0}\right)^{2/\alpha}\Gamma(1-2/\alpha)\Gamma(2/\alpha)}{\alpha}\right. \\ &\left.\cdot\, l_{B^*U}^2\right) f_{l_{B^*U}}(l)\,dl \\ &\overset{c}{=} \frac{2\lambda_e \left(2^{R_0}\right)^{2/\alpha}\Gamma(1-2/\alpha)\Gamma(2/\alpha)}{\alpha\lambda_b + 2\lambda_e \left(2^{R_0}\right)^{2/\alpha}\Gamma(1-2/\alpha)\Gamma(2/\alpha)} \end{aligned} \tag{22}$$

where $Z_{\Phi_e} = \Sigma_{e\in\Phi_e}|h_{B^*e}|^2 l_{B^*e}^{-\alpha}$. Step (a) is derived based on the independence between $\Phi_b$ and $\Phi_e$, and step (b) is the Laplace transform of $Z_{\Phi_e}$ given by $\mathbb{E}_{\Phi_e}(e^{-sZ_{\Phi_e}}) = \exp(-2\pi\lambda_e s^{2/\alpha}\Gamma(1-2/\alpha)\Gamma(2/\alpha)/\alpha)$ [34]. Step (c) utilizes the integral of exponential functions [31, eq. (3.326.2)].

From (21), it is easy to know that, with the increasing of the density of eavesdroppers, the secrecy outage probability increases, and the secrecy outage probability increases as the threshold $R_0$ increases. □

*3.2.2. Average Secrecy Rate.* In the scenario of cooperative eavesdroppers, the average secrecy rate at the typical user $\overline{R}_s^C$ can also be calculated by the integral over all possible values of $R_s$ as stated in Proposition 5. Thus, we obtain $\overline{R}_s^C = \int_0^\infty (1 - P_{so}^{C}(\mathrm{R}_0))dR_0$.

**Corollary 6.** *The average secrecy rate at the typical user is provided by*

$$\begin{aligned} \overline{R}_s^C &= \int_0^\infty \frac{\alpha\lambda_b}{\alpha\lambda_b + 2\lambda_e \left(2^{R_0}\right)^{2/\alpha}\Gamma(1-2/\alpha)\Gamma(2/\alpha)} dR_0 \\ &= \int_0^\infty \frac{\alpha\lambda}{\alpha\lambda_b + 2\lambda_e\Gamma(1-2/\alpha)\Gamma(2/\alpha)\, e^{(2\ln 2/\alpha)R_0}} dR_0 \\ &\overset{a}{=} \frac{\alpha}{2\ln 2} \cdot \ln\left(1 + \frac{\alpha\lambda_b}{2\lambda_e\Gamma(1-2/\alpha)\Gamma(2/\alpha)}\right), \end{aligned} \tag{23}$$

*where step (a) follows the integral result for the form of integrand herein, which can be found in [32, eq. (5.1.2.4.2)].*

*When α increases, the typical user will achieve a larger average secrecy rate from formula (23). It is the same as the scenario of noncooperative eavesdropping. And the large density of eavesdroppers can reduce the average secrecy rate.*

## 4. Secrecy Performance of Multiantenna System

In this section, comparing with the single-antenna system, we assume that the BS are equipped with multiple antennas and the typical user and each eavesdropper are equipped with a single antenna. Furthermore, we assume that the serving BS employs the TAS scheme to enhance secrecy performance in the cellular network. In this case, the typical user first gives feedback to the index of the antenna that maximizes its SNR. Then, the serving BS uses the selected antenna to broadcast the signal. Therefore, the selected $s^{th}$ antenna can be expressed as

$$s = \arg\max_{k\in[1,L]}\left(\left|h_{B_k^*U}\right|^2\right), \tag{24}$$

where $h_{B_k^*U}$ is the channel between the $k^{th}$ antenna at the serving BS and the typical user [35].

We consider that all the channels undergo independent Rayleigh fading channels. Thus, the PDF of $|h_{B_k^*U}|^2$ follows the form of exponential distribution, i.e.,

$$f_{|h_{B_k^*U}|^2}(x) = \frac{1}{\overline{\gamma}}\exp\left(-\frac{x}{\overline{\gamma}}\right), \tag{25}$$

where $\overline{\gamma} = \mathbb{E}[|h_{B_k^*U}|^2]$. Furthermore, we can derive the CDF of $|h_{B_k^*U}|^2$ as

$$F_{|h_{B_k^*U}|^2}(x) = 1 - \exp\left(-\frac{x}{\overline{\gamma}}\right). \tag{26}$$

According to the relationship given in (24), the CDF of $|h_{B_s^*U}|^2$ can be found using order statistics, i.e., $F_{|h_{B_s^*U}|^2}(x) = [F_{|h_{B_k^*U}|^2}(x)]^L$, which can be derived by (26) Relying on the binomial theorem, followed by some algebraic manipulations; the CDF of $|h_{B_s^*U}|^2$ can be reexpressed as

$$F_{|h_{B_s^*U}|^2}(x) = \sum_{n=0}^{L}(-1)^n\binom{L}{n}\exp\left(-\frac{nx}{\overline{\gamma}}\right). \tag{27}$$

Hence, the PDF of $|h_{B_s^*U}|^2$ can be calculated as

$$f_{|h_{B_s^*U}|^2}(x) = \sum_{n=0}^{L}(-1)^{n+1}\frac{n}{\overline{\gamma}}\binom{L}{n}\exp\left(-\frac{nx}{\overline{\gamma}}\right). \tag{28}$$

In the following analysis, we assume $\overline{\gamma} = 1$ to simplify calculation.

*4.1. Noncooperative Eavesdroppers.* In this section, we still use two secrecy performance metrics, i.e., the secrecy outage probability and average secrecy rate, to evaluate the security of cellular network.

*4.1.1. Secrecy Outage Probability.* The secrecy outage probability under the TAS scheme can be calculated by

$$P_{so}^{NC}\left(R_0\right) = \mathbb{P}\left(\frac{\left|h_{B_s^*U}\right|^2 l_{B^*U}^{-\alpha}}{\max_{e\in\Phi_e}\left(\left|h_{B^*e}\right|^2 l_{B^*e}^{-\alpha}\right)} < 2^{R_0}\right) \tag{29}$$

**Proposition 7.** *The secrecy outage probability for the scenario of noncooperative eavesdroppers can be expressed as*

$$\begin{aligned} &P_{so}^{NC}\left(R_0\right) \\ &\simeq \sum_{n=0}^{L}\sum_{k=1}^{\infty}(-1)^{n+1}\binom{L}{n}\frac{\Gamma\left(\left(2/\alpha\right)\left(k-1\right)+1\right)}{n^{(2/\alpha)(k-1)}} \\ &\times\left(\frac{-\lambda_b\alpha}{2\lambda_e\Gamma\left(2/\alpha\right)\left(2^{R_0}\right)^{2/\alpha}}\right)^{k-1} \end{aligned} \tag{30}$$

*Proof.* Based on the definition of the secrecy outage probability, the secrecy outage probability can be obtained as follows:

$$\begin{aligned} &P_{so}^{NC}\left(R_0\right) \simeq \mathbb{P}\left(\frac{\left|h_{B_s^*U}\right|^2 l_{B^*U}^{-\alpha}}{\max_{e\in\Phi_e}\left(\left|h_{B^*e}\right|^2 l_{B^*e}^{-\alpha}\right)} < 2^{R_0}\right) = 1 \\ &- \mathbb{E}_{\Phi_b,\Phi_e}\left(\prod_{e\in\Phi_e}\left(\left|h_{B^*e}\right|^2\right.\right. \\ &\left.\left.< \frac{\left|h_{B_s^*U}\right|^2 l_{B^*U}^{-\alpha}}{2^{R_0}} l_{B^*e}^{\alpha} \mid \Phi_b, \Phi_e\right)\right) \overset{a}{=} 1 \\ &- \mathrm{E}_{\Phi_b}\left(\exp\left(-\frac{2\pi\lambda_e 2^{R_0}}{\alpha\left|h_{B^*U}\right|^{2/\alpha} l_{B^*U}^{-2}}\Gamma\left(\frac{2}{\alpha}\right)\right) \mid \Phi_b\right) \\ &= 1 \\ &- \mathrm{E}_{\left|h_{B^*U}\right|^2}\left(\int_0^{\infty}\exp\left(-\frac{2\pi\lambda_e\left(2^{R_0}\right)^{2/\alpha}}{\alpha\left|h_{B^*U}\right|^{2/\alpha} l_{B^*U}^{-2}}\times\Gamma\left(\frac{2}{\alpha}\right)\right)\right. \\ &\left.\cdot f_{l_{B^*U}}\left(l\right)dl \mid \left|h_{B^*U}\right|^2\right) \overset{b}{=} \sum_{n=0}^{L}(-1)^{n+1} \\ &\cdot n\binom{L}{n} \\ &\cdot \int_0^{\infty}\left(\frac{2\lambda_e\Gamma\left(2/\alpha\right)\left(2^{R_0}\right)^{2/\alpha}e^{-nx}}{\lambda_b\alpha x^{2/\alpha}+2\lambda_e\Gamma\left(2/\alpha\right)\left(2^{R_0}\right)^{2/\alpha}}\right)dx \\ &\overset{c}{=} \sum_{n=0}^{L}\sum_{k=1}^{\infty}\frac{\binom{L}{n}}{(-1)^{-n+1}} \\ &\cdot \frac{\Gamma\left(\left(2/\alpha\right)\left(k-1\right)+1\right)}{n^{(2/\alpha)(k-1)}}\left(\frac{-\lambda_b\alpha}{2\lambda_e\Gamma\left(2/\alpha\right)\left(2^{R_0}\right)^{2/\alpha}}\right)^{k-1}, \end{aligned} \tag{31}$$

where step (a) is based on the PGFL of PPPs $\Phi_e$, and step (b) follows the PDF of $l_{B^*U}$ and $|h_{B_s^*U}|^2$. Step (c) is derived by the exponential function [31, eq. (1.211.1)]. □

*4.1.2. Average Secrecy Rate.* Based on the $P_{so}^{NC}(R_0)$ in Proposition 7, the average secrecy rate at the typical user can be derived by $\overline{R}_s^{NC} = \int_0^{\infty}(1 - P_{so}^{NC}(R_0))dR_0$.

**Corollary 8.** *The average secrecy rate is provided by*

$$\begin{aligned} &\overline{R}_s^{NC} \\ &= \sum_{n=0}^{L}\sum_{k=1}^{\infty}\binom{L}{n}\frac{(-1)^{n+k}}{n^{2k/\alpha-1}\ln 2}\left(\frac{\alpha\lambda_b}{2\lambda_e\Gamma\left(2/\alpha\right)}\right)^k\Gamma\left(\frac{2k}{\alpha}\right) \end{aligned} \tag{32}$$

*Proof.* With the help of (25), the desired results can be easily derived by following the similar procedures as the single-antenna scenario. □

*4.2. Cooperative Eavesdroppers.* In this subsection, the effect of cooperative eavesdroppers on secrecy performance under different network parameters is given for the multiantenna scenario.

*4.2.1. Secrecy Outage Probability.* Similar to (20), the secrecy outage probability $P_{so}^{C}(R_0)$ under the TAS scheme can be calculated by

$$P_{so}^{C}\left(R_0\right) = \mathbb{P}\left(\frac{\left|h_{B_s^*U}\right|^2 l_{B*U}^{-\alpha}}{\sum_{e\in\Phi_e}\left(\left|h_{B^*e}\right|^2 l_{B^*e}^{-\alpha}\right)} < 2^{R_0}\right) \tag{33}$$

**Proposition 9.** *The secrecy outage probability for the scenario of cooperative eavesdroppers can be given as*

$$\begin{aligned} P_{so}^{C}\left(R_0\right) &\simeq \sum_{n=0}^{L}\left(\binom{L}{n}(-1)^n\right. \\ &\left.\times\frac{\alpha\lambda_b}{\alpha\lambda_b+2\lambda_e\Gamma\left(1-2/\alpha\right)\Gamma\left(2/\alpha\right)n^{2/\alpha}\left(2^{R_0}\right)^{2/\alpha}}\right) \end{aligned} \tag{34}$$

*Proof.* In multiantenna system, the secrecy outage probability can be expressed as (21). From the definition, we can derive the secrecy outage probability as follows:

$$\begin{aligned} P_{so}^{C}\left(R_0\right) &\simeq \mathbb{P}\left(\frac{\left|h_{B_s^*U}\right|^2 l_{B^*U}^{-\alpha}}{\sum_{e\in\Phi_e}\left(\left|h_{B^*e}\right|^2 l_{B^*e}^{-\alpha}\right)} < 2^{R_0}\right) \\ &= \int_0^{\infty}\mathbb{E}_{\Phi_e}\left(\mathbb{P}\left(\left|h_{B_s^*U}\right|^2 < 2^{R_0} l_{B^*U}^{\alpha} Z_{\Phi_e} \mid \Phi_e\right)\right) \\ &\cdot f_{l_{B^*U}}\left(l\right)dl \overset{a}{=} \mathbb{E}_{\Phi_e}\left(1 - e^{-2^{R_0} l_{B^*U}^{\alpha} Z_{\Phi_e}}\right)^L \end{aligned}$$

$$\overset{b}{=} \sum_{n=0}^{L} \binom{L}{n} (-1)^n \mathbb{E}_{\Phi_e} \left( e^{-2^{R_0} l_{B^* U}^{\alpha} Z_{\Phi_e} n} \right)$$

$$\overset{c}{=} \sum_{n=0}^{L} \binom{L}{n} (-1)^n$$

$$\cdot \frac{\alpha\lambda_b}{\alpha\lambda_b + 2\lambda_e \Gamma(1-2/\alpha)\Gamma(2/\alpha) n^{2/\alpha} \left(2^{R_0}\right)^{2/\alpha}} \tag{35}$$

where $Z_{\Phi_e} = \Sigma_{e\in\Phi_e} |h_{B^* e}|^2 l_{B^* e}^{-\alpha}$. Step (a) is derived based on the CDF of $|h_{B_s^* U}|^2$, and according to the polynomial expansion [32, eq. (1.1.10)], step (b) can be obtained. In addition, step (c) is the Laplace transform of $Z_{\Phi_e}$ [34]. □

*4.2.2. Average Secrecy Rate.* Combining Proposition 9 and the integral formula in [32, eq. (5.1.2.4.2)], we can obtain the average secrecy rate at the typical user as follows.

**Corollary 10.** *The average secrecy rate is provided by*

$$\overline{R}_s^C = \sum_{n=1}^{L} \binom{L}{n}$$

$$\cdot \frac{(-1)^{n+1} \alpha}{2 \ln 2} \ln \left( 1 + \frac{\alpha\lambda_b}{2\lambda_e \Gamma(1-2/\alpha)\Gamma(2/\alpha) n^{2/\alpha}} \right) \tag{36}$$

*Proof.* Using the definition of the average secrecy rate, we can obtain the expression as follows:

$$\overline{R}_s^C = \int_0^{\infty} \sum_{n=0}^{L} \frac{(-1)^n \binom{L}{n} \alpha\lambda_b}{\alpha\lambda_b + 2\lambda_e \Gamma(1-2/\alpha)\Gamma(2/\alpha) n^{2/\alpha} \left(2^{R_0}\right)^{2/\alpha}} dR_0$$

$$= \sum_{n=0}^{L} \frac{\binom{L}{n}}{(-1)^{-n}}$$

$$\cdot \int_0^{\infty} \frac{\alpha\lambda_b dR_0}{\alpha\lambda_b + 2\lambda_e \Gamma(1-2/\alpha)\Gamma(2/\alpha) n^{2/\alpha} \left(2^{R_0}\right)^{2/\alpha} e^{(2\ln 2/\alpha)R_0}} \tag{37}$$

$$\overset{a}{=} \sum_{n=0}^{L} \binom{L}{n} \frac{(-1)^{n+1} \alpha}{2 \ln 2}$$

$$\cdot \ln \left( 1 + \frac{\alpha\lambda_b}{2\lambda_e \Gamma(1-2/\alpha)\Gamma(2/\alpha) n^{2/\alpha}} \right)$$

where step (a) is based on the integral formula in [32, eq. (5.1.2.4.2)].

For the secrecy outage probability, we find that $P_{so}^{NC}$ and $P_{so}^{C}$ are a function of various factors, e.g., $L$, $\lambda_e$, $\lambda_b$, $R_0$, $\alpha$. For any given $L$, $\lambda_b$, $R_0$, $\alpha$, the secrecy outage probability solely depends on eavesdroppers' density. And a large $\alpha$ and $L$ can decrease the secrecy outage probability in both cooperative and noncooperative eavesdroppers. As to the average secrecy rates $\overline{R}_S^{NC}$ and $\overline{R}_S^{C}$, the more number of antennas $L$ and large path loss exponent $\alpha$ is also beneficial for improving the average secure transmission rate. Detailed analysis on the impacts of these factors to the security can be seen in Section 5. □

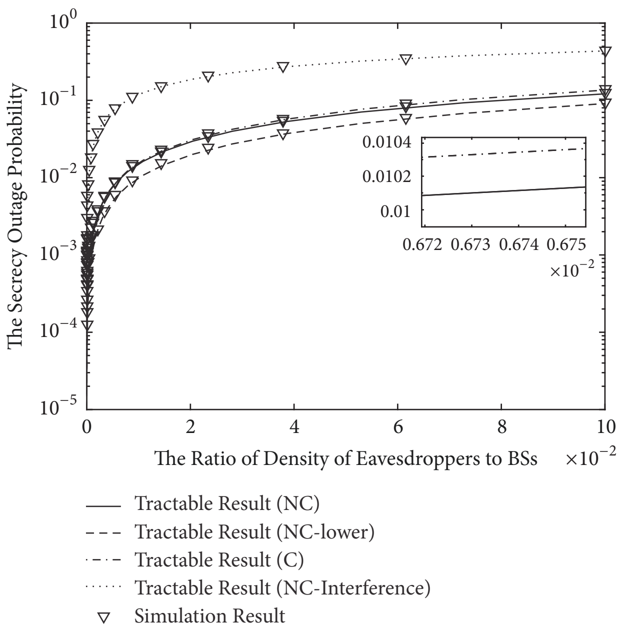


Figure 2: The secrecy outage probability as a function of $\lambda_e/\lambda_b$.

## 5. Numerical Results and Discussion

In this section, we provide simulation results to verify our analyses for different scenarios as mentioned above. We show the secrecy outage probability and the average secrecy rate as functions of $\lambda_e/\lambda_b$, $\alpha$, $R_0$, and $L$. In the simulation analysis, we assume the transmit SNR $P_{BS}/\sigma^2 = 20dB$. In the following figures, NC and C denote the noncooperative eavesdroppers and cooperative eavesdroppers, respectively. In addition, the NC-lower and NC-upper corresponded, respectively, to the lower bound of the secrecy outage probability and the upper bound of the average secrecy rate under the noncooperative eavesdroppers scenarios, and NC-Interference is the secrecy performance in the noncooperative eavesdropping case with considering interference.

Figure 2 verifies the secrecy outage probability for two different scenarios as a function of $\lambda_e/\lambda_b$. We observe that the secrecy outage probability increases as the density of eavesdroppers increases. This is because large $\lambda_e$ can reduce the distance between eavesdropper and BS. When the interference is considered, the secrecy outage probability has a large increase comparing to the noninterference case in noncooperative eavesdropping scenario. This indicates that the interference has an important effect for the secrecy performance in such a scenario. Moreover, with the increasing of $\lambda_e$, the lower bound of the secrecy outage probability is different from the performance of the exact analytical expression in (4). This difference shows that the impact of small-scale fading is considerable in certain $\lambda_e$ regime. And the secrecy outage probability of the scenario of noncooperative eavesdroppers is always lower than that of cooperative eavesdroppers, because sharing information among eavesdroppers makes it easier to decode the confidential message.

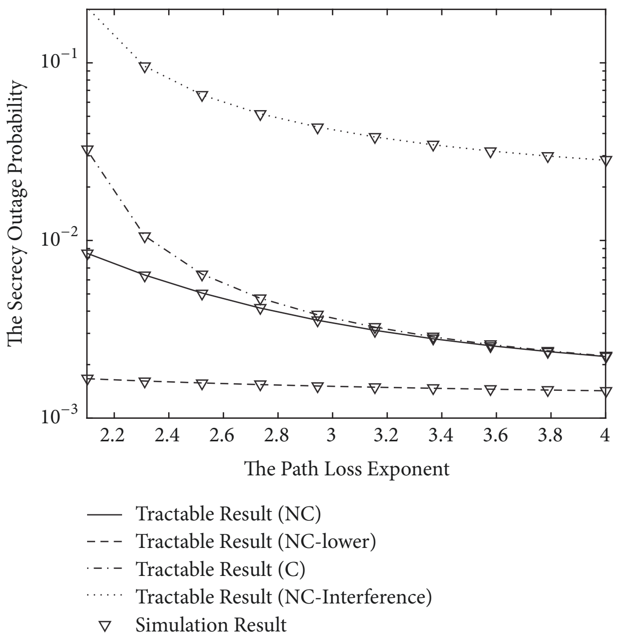


Figure 3: The secrecy outage probability as a function of $\alpha$.

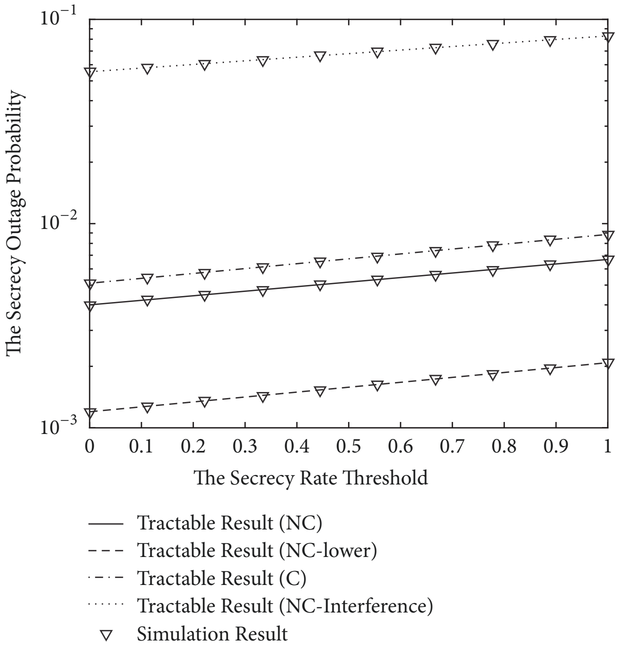


Figure 4: The secrecy outage probability as a function of $R_0$.

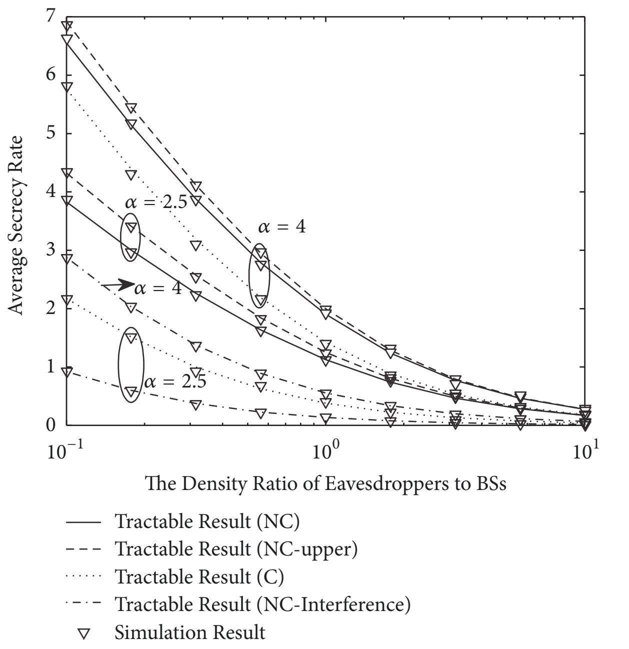


Figure 5: The average secrecy rate as a function of $\lambda_e/\lambda_b$ for two different scenarios.

Figures 3 and 4 demonstrate the secrecy outage probability as a function of path loss exponent $\alpha$ and threshold $R_0$, respectively. It is easy to find that the secrecy outage probability decreases with the increasing of $\alpha$ and increases with the increasing of $R_0$. This is because larger path loss exponent indicates worse signal condition for both eavesdroppers and the typical user, whereas the impact on the former is turned out to be more influential on the secrecy outage probability. And the large threshold $R_0$ requires larger channel difference between legal and illegal links, so it is more likely to be easily interrupted for the transmission. Another fact is that the large value of $\alpha$ makes the difference on secrecy performance between the lower bound and the exact analytical expression become small. This explains that the effect of secrecy performance caused by small-scale fading cannot be ignored in small $\alpha$ environment. In addition, when the interference caused by BSs is considered, the secrecy performance is the worst in these scenarios.

Figure 5 shows the average secrecy rate as a function of $\lambda_e/\lambda_b$ under various path loss exponents $\alpha$. The result shows that the average secrecy rate decreases as the density of eavesdroppers $\lambda_e/\lambda_b$ increases. For a given $\lambda_e/\lambda_b$, the large path loss exponent $\alpha$ can improve the average secrecy rate. And the average secrecy rate is the lowest when interference is considered. This is because the interference reduces the channel capacity of legal link. At the same time, we can observe that the gap of the average secrecy rate between the scenarios of noncooperative eavesdroppers and cooperative eavesdroppers is becoming narrower with the increasing of $\lambda_e/\lambda_b$, especially the gap between the upper bound of the average secrecy rate with the exact analytical expression in (9). The reason is that the large-scale fading is gradually becoming the main cause on secrecy performance. Moreover, because eavesdroppers can exchange information with each other in the scenario of cooperative eavesdroppers, the secrecy performance is always worse than the scenario of noncooperative eavesdroppers.

Figure 6 illustrates the secrecy outage probability as a function of the number of antennas $L$. We can know that a slight increase of $L$ effectively decreases the secrecy outage probability. This is because more antennas make BS transmit message in a better channel quality with a large probability. When $\lambda_e$ becomes very small or large, the gap of secrecy

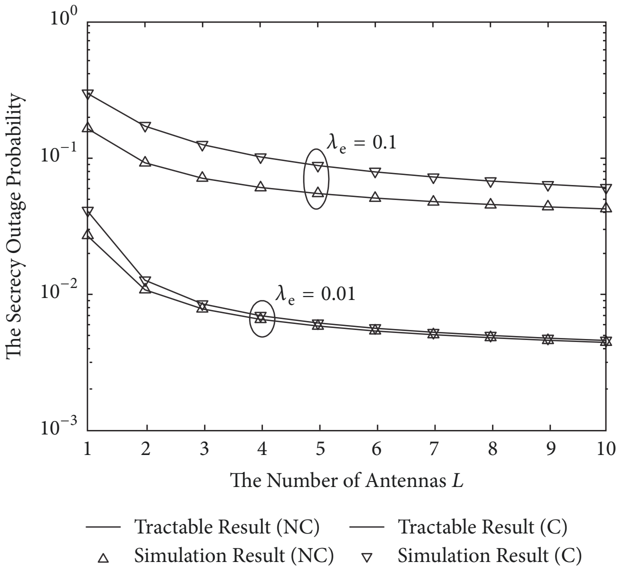


FIGURE 6: The secrecy outage probability as a function of $L$ with $\lambda_e = 0.01$, $\lambda_e = 0.1$.

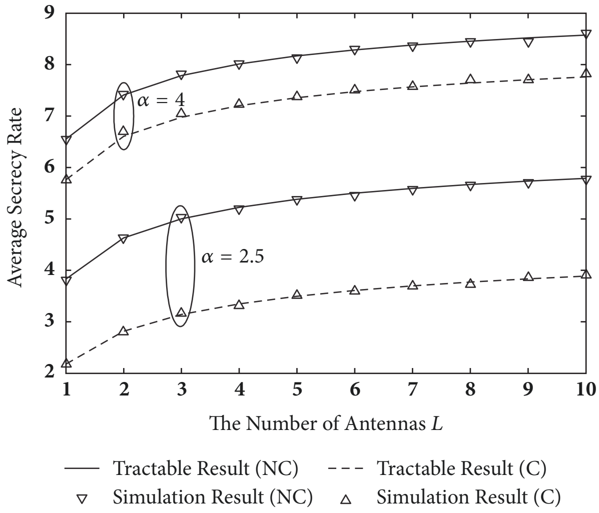


FIGURE 7: The average secrecy rate as a function of $L$ with $\alpha = 2.5$, $\alpha = 4$.

outage probability between the scenarios of noncooperative and cooperative eavesdroppers will become narrower. This can be explained as follows: a smaller $\lambda_e$ decreases the average number of eavesdroppers in a certain area, which naturally makes fewer eavesdroppers share information. In addition, a larger $\lambda_e$ means eavesdroppers are closer to BSs, which leads to the worst eavesdropper being capable enough of intercepting the information transmission. In this case, whether or not eavesdroppers can cooperate has no significant effect on secrecy performance. Moreover, an interesting finding is that the gap between cooperative and noncooperative eavesdroppers does not change obviously as $L$ increases. When the density of eavesdroppers is large, increasing the number of antennas has litter improvement on the secrecy outage probability. This is because the number of eavesdroppers has become the main influence factor to damage the secrecy performance.

In Figure 7, the average secrecy rate $\overline{R}_S^{NC}$ in (32) and $\overline{R}_S^{C}$ in (36) versus the number of antennas $L$ with different path loss exponent $\alpha$ is presented. Both average secrecy rate in noncooperative and cooperative eavesdroppers scenarios monotonically increase with the increasing of $L$, with the benefit being brought by multiple antennas. But there is no obvious change in the gap between $\overline{R}_S^{NC}$ and $\overline{R}_S^{C}$ for $\alpha = 4$ and $\alpha = 2.5$ with an increasing of $L$, which indicates that multiple antenna has equal effects on the improvement of the secrecy rate in noncooperative and cooperative eavesdroppers scenarios. We also find that the average secrecy rate is smaller than that with $\alpha = 4$, which is the same as shown in Figure 4. Comparing to a small $\alpha = 2.5$, the average secrecy rate $\overline{R}_S^{NC}$ is closer to $\overline{R}_S^{C}$ when $\alpha = 4$. In other words, the cooperative eavesdroppers provides less additional degradation on the secrecy performance compared with the noncooperative eavesdroppers when $\alpha$ becomes larger. The reason is that more severe path loss makes the influence of the worst eavesdroppers more significant compared with other eavesdroppers, which has weakened the impact of eavesdroppers' cooperation.

## 6. Conclusion

In this paper, the exact expressions for the secrecy outage probability and average secrecy rate at the typical user are presented by using the tool of stochastic geometry in large-scale cellular networks. These results are represented by numerical simulations. Our results show that, with the increasing of density ratio of eavesdroppers to BSs, the secrecy performance decreases in both scenarios of noncooperative and cooperative eavesdroppers, and the typical user can achieve better secrecy performance in the environment with large path loss exponent. Furthermore, the secrecy performance in the scenario of noncooperative eavesdroppers is always better than that of cooperative eavesdroppers, and the interference caused by BS will damage the secrecy performance. Moreover, we give more accurate results than predecessors, because of considering both of the large-scale and small-scale fading. At the same time, we know that the small-scale fading cannot be ignored in eavesdroppers with certain density regime and small loss path exponent environment. Finally, using the TAS technology can effectively enhance the secrecy performance compared to single-antenna system, but it cannot obviously improve the difference on secrecy performance between the scenarios of noncooperative and cooperative eavesdroppers.

## Data Availability

The data used to 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 work was supported by the National Natural Science Foundation of China (no. 61471393 and no. 61771487). This paper was presented in part at the IEEE 3rd International Conference on Computer and Communications (ICCC 2017), Chengdu, China, Dec. 2017.

## References

[1] C. E. Shannon, "Communication theory of secrecy systems," *Bell Labs Technical Journal*, vol. 28, pp. 656–715, 1949.

[2] A. D. Wyner, "The wire-tap channel," *Bell Labs Technical Journal*, vol. 54, no. 8, pp. 1355–1387, 1975.

[3] D. Goeckel, S. Vasudevan, D. Towsley, S. Adams, Z. Ding, and K. Leung, "Artificial noise generation from cooperative relays for everlasting secrecy in two-hop wireless networks," *IEEE Journal on Selected Areas in Communications*, vol. 29, no. 10, pp. 2067–2076, 2011.

[4] N. Romero-Zurita, M. Ghogho, and D. McLernon, "Outage probability based power distribution between data and artificial noise for physical layer security," *IEEE Signal Processing Letters*, vol. 19, no. 2, pp. 71–74, 2012.

[5] L. Dong, Z. Han, A. P. Petropulu, and H. . Poor, "Improving wireless physical layer security via cooperating relays," *IEEE Transactions on Signal Processing*, vol. 58, no. 3, part 2, pp. 1875–1888, 2010.

[6] B. He and X. Zhou, "Secure On-Off transmission design with channel estimation errors," *IEEE Transactions on Information Forensics and Security*, vol. 8, no. 12, pp. 1923–1936, 2013.

[7] Y. Zou, J. Zhu, X. Wang, and L. Hanzo, "A survey on wireless security: technical challenges, recent advances, and future trends," *Proceedings of the IEEE*, vol. 104, no. 9, pp. 1727–1765, 2016.

[8] L. Sun and Q. Du, "Physical layer security with its application in 5g networks: A review," *China Comunications*, vol. 14, no. 12, p. 14, 2017.

[9] S. Weber, J. G. Andrews, and N. Jindal, "The effect of fading, channel inversion, and threshold scheduling on ad hoc networks," *IEEE Transactions on Information Theory*, vol. 53, no. 11, pp. 4127–4149, 2007.

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

[11] X. Xu, B. He, W. Yang, X. Zhou, and Y. Cai, "Secure Transmission Design for Cognitive Radio Networks With Poisson Distributed Eavesdroppers," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 2, pp. 373–387, 2016.

[12] X. Xu, W. Yang, Y. Cai, and S. Jin, "Secure Transmission Design for Cognitive Radio Networks With Poisson Distributed Eavesdroppers," *IEEE Transactions on Information Forensics and Security*, vol. 34, no. 10, pp. 2706–2722, 2016.

[13] S. Vuppala and G. Abreu, "Secrecy outage in random wireless networks subjected to fading," in *Proceedings of the 2013 IEEE 24th Annual International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC)*, pp. 446–450, London, September 2013.

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

[15] G. Chen, J. P. Coon, and M. Di Renzo, "Secrecy Outage Analysis for Downlink Transmissions in the Presence of Randomly Located Eavesdroppers," *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 5, pp. 1195–1206, 2017.

[16] H. Chen, X. Tao, N. Li, and X. Li, "Secrecy performance of the artificial noise assisted broadcast channel with confidential messages and external eavesdroppers," in *Proceedings of the ICC 2016 - 2016 IEEE International Conference on Communications*, pp. 1–6, Kuala Lumpur, Malaysia, May 2016.

[17] T. Zheng, H. Wang, R. Huang, and P. Mu, "Adaptive artificial noise transmission against randomly distributed eavesdroppers," in *Proceedings of the 2015 10th International Conference on Communications and Networking in China (ChinaCom)*, pp. 248–253, Shanghai, China, August 2015.

[18] 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, 2015.

[19] L. Zhang, H. Zhang, D. Wu, and D. Yuan, "Improving Physical Layer Security for MISO Systems via Using Artificial Noise," in *Proceedings of the GLOBECOM 2015 - 2015 IEEE Global Communications Conference*, pp. 1–6, San Diego, CA, USA, December 2015.

[20] G. Chen and J. P. Coon, "Secrecy Outage Analysis in Random Wireless Networks with Antenna Selection and User Ordering," *IEEE Wireless Communications Letters*, vol. 6, no. 3, pp. 334–337, 2017.

[21] J. G. Andrews, F. Baccelli, and R. K. Ganti, "A tractable approach to coverage and rate in cellular networks," *IEEE Transactions on Communications*, vol. 59, no. 11, pp. 3122–3134, 2011.

[22] H. Wang, X. Zhou, and M. C. Reed, "On the physical layer security in large scale cellular networks," in *Proceedings of the 2013 IEEE Wireless Communications and Networking Conference, WCNC 2013*, pp. 2462–2467, chn, April 2013.

[23] H. Wang, X. Zhou, and M. C. Reed, "Physical layer security in cellular networks: A stochastic geometry approach," *IEEE Transactions on Wireless Communications*, vol. 12, no. 6, pp. 2776–2787, 2013.

[24] G. Geraci, H. S. Dhillon, J. G. Andrews, J. Yuan, and I. B. Collings, "A new model for physical layer security in cellular networks," in *Proceedings of the 2014 1st IEEE International Conference on Communications, ICC 2014*, pp. 2147–2152, aus, June 2014.

[25] G. Geraci, H. S. Dhillon, J. G. Andrews, J. Yuan, and I. B. Collings, "Physical layer security in downlink multi-antenna cellular networks," *IEEE Transactions on Communications*, vol. 62, no. 6, pp. 2006–2021, 2014.

[26] H.-M. Wang, T.-X. Zheng, J. Yuan, D. Towsley, and M. H. Lee, "Physical layer security in heterogeneous cellular networks," *IEEE Transactions on Communications*, vol. 64, no. 3, pp. 1204–1219, 2016.

[27] L. Tao, W. Yang, Y. Cai, and D. Chen, "Secrecy performance analysis in large-scale cellular networks via stochastic geometry," in *Proceedings of the 2017 3rd IEEE International Conference on Computer and Communications (ICCC)*, pp. 1444–1449, Chengdu, December 2017.

[28] D. Stoyan, W. S. Kendall, and J. Mecke, *Stochastic geometry and its applications*, Wiley Series in Probability and Mathematical Statistics: Applied Probability and Statistics, John Wiley & Sons, Ltd., Chichester, New York, NY, USA, 1995.

[29] M. Haenggi, “On distances in uniformly random networks,” *Institute of Electrical and Electronics Engineers Transactions on Information Theory*, vol. 51, no. 10, pp. 3584–3586, 2005.

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

[31] I. S. Gradshteyn and I. M. Ryzhik, *Table of Integrals, Series, and Products*, Academic Press, New York, NY, USA, 7th edition, 2007.

[32] A. Jeffrey and H.-H. Dai, *Handbook of Mathematical Formulas and Integrals*, Academic Press of Elsevier, Burlington, Amsterdam, Netherlands, 4th edition, 2008.

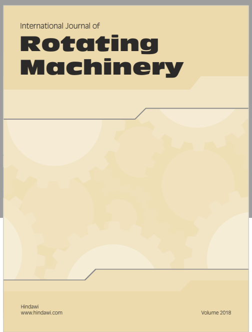
[33] Y. Zhu, L. Wang, K. Wong, and R. W. Heath, “Physical Layer Security in Large-Scale Millimeter Wave Ad Hoc Networks,” in *Proceedings of the GLOBECOM 2016 - 2016 IEEE Global Communications Conference*, pp. 1–6, Washington, DC, USA, December 2016.

[34] C. Cai, Y. Cai, X. Zhou, W. Yang, and W. Yang, “When does relay transmission give a more secure connection in wireless ad hoc networks?” *IEEE Transactions on Information Forensics and Security*, vol. 9, no. 4, pp. 624–632, 2014.

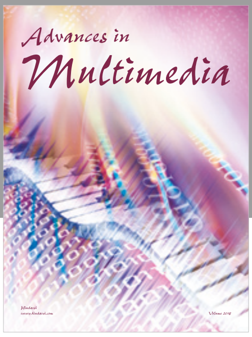
[35] N. S. Ferdinand, D. B. Da Costa, A. L. F. De Almeida, and M. Latva-Aho, “Physical layer secrecy performance of TAS wiretap channels with correlated main and eavesdropper channels,” *IEEE Wireless Communications Letters*, vol. 3, no. 1, pp. 86–89, 2014.

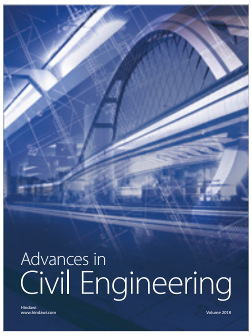
Journal of
Engineering

The Scientific
World Journal

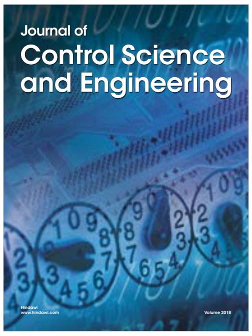

International Journal of
Rotating
Machinery

Journal of
Sensors

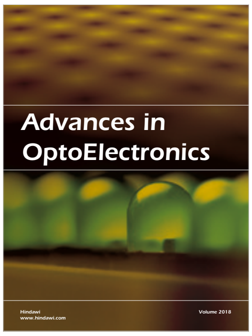

Advances in
Multimedia


Advances in
Civil Engineering

Journal of
Robotics

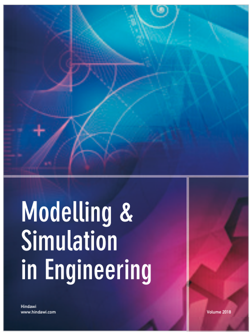

Journal of
Control Science
and Engineering

Journal of
Electrical and Computer
Engineering

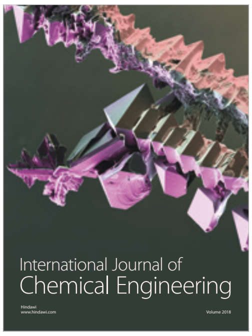

Advances in
OptoElectronics

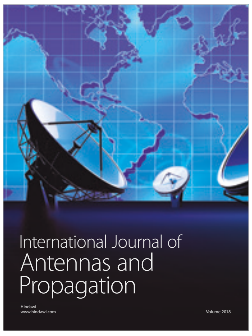
VLSI Design

International Journal of
Navigation and
Observation

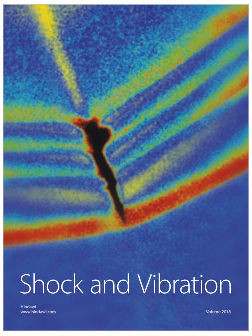

Modelling &
Simulation
in Engineering

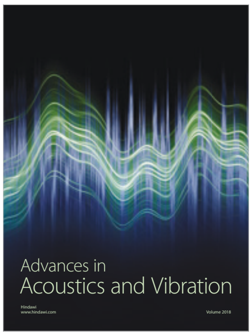
International Journal of
Aerospace
Engineering


International Journal of
Chemical Engineering


International Journal of
Antennas and
Propagation

Active and Passive
Electronic Components


Shock and Vibration


Advances in
Acoustics and Vibration