IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received September 3, 2018, accepted October 1, 2018, date of publication October 10, 2018, date of current version October 31, 2018.

Digital Object Identifier 10.1109/ACCESS.2018.2875118

Enhancing the Physical Layer Security of Uplink Non-Orthogonal Multiple Access in Cellular Internet of Things

SHUAI ZHANG[1], XIAOMING XU[1], (Student Member, IEEE), HUIMING WANG[2], (Senior Member, IEEE), JIANHUA PENG[1], DI ZHANG [3], (Member, IEEE), AND KAIZHI HUANG[1]

[1]National Digital Switching System Engineering and Technological Research Center, Zhengzhou 450002, China
[2]School of Electronic and Information Engineering, Xi'an Jiaotong University, Xi'an 710049, China
[3]School of Information Engineering, Zhengzhou University, Zhengzhou 450001, China

Corresponding author: Jianhua Peng (2012301200229@whu.edu.cn)

This work was supported in part by the National Natural Science Foundation of China under Grants 61501516, 61671364, 61701538, and 61801435, in part by the Project funded by the China Postdoctoral Science Foundation under Grant 2018M633733, in part by the Scientific and Technological Key Project of Henan Province under Grant 182102210449, in part by the Outstanding Young Research Fund of Shaanxi Province under Grant 2018JC-003, and in part by the Scientific Key Research Project of Henan Province for Colleges and Universities under Grant 19A510024.

ABSTRACT This paper investigates the physical-layer security of uplink non-orthogonal multiple access (NOMA) in the cellular Internet of Things (IoT) with invoking stochastic geometry. Poisson cluster process-based model is applied to characterize the NOMA uplink transmission scenario, where IoT terminals are located around the serving base station. Considering the severe interference brought by a large number of IoT terminals, inter-cell interference is also taken into account. To enhance the physical-layer security of uplink NOMA transmission with limited overhead increment at IoT terminals, the base stations not only receive the signals from IoT terminals but also keep emitting jamming signals all the time to degrade the performance of any potential eavesdroppers. In order to characterize the physical-layer security performances, we derive expressions of coverage probability and secrecy outage probability. To obtain further insights, network-wide secrecy throughput (NST) and network-wide secrecy energy efficiency (NSEE) are analyzed. It is demonstrated that the security performance can be improved by the proposed full-duplex base station jamming scheme at the cost of reliable performance. The analytical and simulation results show the effects of BS intensity and jamming power on network performances. We also verify that NST and NSEE can be significantly enhanced by our proposed scheme. Using these results, the security of confidential information transmitted by low-complexity IoT terminals can be protected from overhearing.

INDEX TERMS Full-duplex receiver, Internet of Things, non-orthogonal multiple access, physical layer security, uplink.

I. INTRODUCTION

A. BACKGROUND

The internet of things (IoT) promises ubiquitous connectivity of everything everywhere, which represents a new technology trend in the years to come. Cellular networks are expected to play a fundamental role to provide first mile connectivity for a big sector of IoT terminals [1], [2]. As expected, there will be over 25 billion devices connected to cellular networks by 2020, far beyond the number of devices in current wireless networks [3], [4]. Therefore, it is a great challenge for cellular IoT to provide connectivity to such large number of IoT terminals. Among all existing technologies, techniques for the forthcoming fifth generation (5G) system will be the important enablers for the development of IoT. Non-orthogonal multiple access (NOMA), which is the potential access technology for 5G, allows serving multiple users simultaneously using the same resource block (RB) at the cost of increased intra-cell interference. NOMA thus is deemed to have a superior spectral efficiency than the traditional orthogonal multiple access (OMA) [5]. It has also shown great potentials to be applied in cellular IoT.

Using NOMA in uplink cellular IoT scenario, a set of user equipments (UEs) transmit signals to their associated base station (BS) using the same RB. In order to minimize the

intra-cell interference, the BS may apply successive interference cancelation (SIC) to decode signals. SIC technique in IoT uplink NOMA transmission works as follows [6]: The BS first decodes the strongest signal by considering the signals from other users as noise. That is, the decoding of the strongest signal experiences interference from all users in the same RB, whereas the decoding of the the weakest signal receives zero interference in its cluster (considering ideal conditions). A general concept of uplink NOMA transmission was firstly analyzed in [7], in which minimum mean squared error (MMSE)-based SIC decoding is applied at the BS. There are many benefits when NOMA is applied to uplink cellular IoT. Besides the spectral efficiency gains, BS can serve a group of UEs using the same RB, which enable BS to serve a great number of IoT terminals. The random access (RA) process is not needed to access the network, leading to a significant reduction on signaling overhead [3], [8].

With ubiquitous UEs in IoT adopted in everywhere, an unprecedented amount of private and sensitive data is transmitted over wireless channels. The security problem of IoT is therefore of great importance. Traditionally, security problem is treated mostly in upper layers, and most of the security solutions primarily focus on cryptographic technologies. However, the ultra-low hardware complexity of IoT terminals poses a great challenge to adopt conventional computational complexity based encryption algorithm [9]. Fortunately, physical layer security has emerged as an appealing approach to provide information theoretically unbreakable secrecy. The basic thought of physical layer security exploits the open and time-varying nature of wireless channel. Numerous researches have been made based on the concept of physical layer security, such as network performances analysis [10], [11], cooperative communication [12], [13], signal processing [14], [15] and cache-enabled communication [16] [17]. As for the secrecy problem in IoT, an overview of low-complexity physical layer security schemes that are suitable for the IoT such as ON-OFF switching and space-time block codes are presented [18]. The secrecy problem of NOMA has also been considered from the physical layer security perspective, in which most of the existing works are based on the assumption that perfect SIC can be achieved. The optimal design of point-to-point NOMA transmission were studied in [19] and [20]. Considering large-scale networks, the application of NOMA in multi-user network with mixed multicasting and unicasting traffic was studied in [21], in which spectral efficiency and security gain are analyzed. In [22], physical layer security of downlink NOMA in large-scale networks was investigated, taking both single-antenna and multiple-antenna BS scenarios into consideration. The physical layer security of uplink NOMA in large-scale networks was analyzed in [23], where fixed and adaptive transmission schemes were considered.

B. MOTIVATION AND CONTRIBUTION

To date, the most of framework analyzing physical layer security in NOMA system cannot be applied directly to uplink NOMA system in IoT. The reason is that the inter-cell interference in IoT can be quite severe owing to the large number of IoT terminals. However, inter-cell interference is either not considered or simply treated as a constant value in most of the existing work studying physical layer security for NOMA system, such as [22] and [23]. The lack of a realistic inter-cell interference model makes it difficult to analyze the impact of some key system parameters, such as transmit power, BS/UE densities, and secure scheme, on the secrecy performance of NOMA system in IoT. Besides, compared to downlink transmission, we note that the characterize of inter-cell interference in uplink NOMA transmission is particularly more challenging due to the mathematical structure of the inter-cell interferences. Also, as IoT terminals have limited hardware complexity, power and computing ability, the overhead at IoT terminals is extremely important when designing the physical layer security scheme, which poses a great challenge in improving the physical layer security of IoT uplink NOMA transmissions.

To this end, we dedicate to safeguard the uplink NOMA transmissions in IoT from overhearing. Inter-cell interference is taken into account in the considered uplink transmissions scenario, where multiple IoT terminals are more likely to be located around the serving BS. Besides, the full-duplex (FD) BS jamming scheme is proposed, which requires little power consumption and computing ability at IoT terminals. Importantly, we adopt a practical assumption that the SIC at BS is imperfect, i.e., the error is propagated to all remaining messages if there exists a SIC failure. In order to avoid sophisticated high-complexity message detection at the receivers, 2-UEs NOMA has been included in the 3rd Generation Partnership Project (3GPP) Long Term Evolution Advanced (LTE-A) [24]. In this work, a random user pairing technique is adopted to ensure that only two users share a specific orthogonal RB, which can be readily separated by low-complexity SIC [25], [26]. The major contributions of this paper are summarized as follows:

- We model the uplink NOMA transmissions in IoT using the theory of stochastic geometry. Particularly, the Poisson Cluster Process (PCP) model is applied to depict the scenario where multiple IoT terminals are located around the serving BS. Besides, eavesdroppers (Eves) with uncertain locations are modeled by the Poisson Point Process (PPP) model.
- Based on the proposed model, we provide a physical layer security characterization of uplink NOMA in IoT. As the inter-cell interference in IoT can be quite severe, the influence of inter-cell interference is taken into consideration. We obtain expressions for coverage probabilities and secrecy outage probability of the most detrimental Eve. Besides, network-wide secrecy throughput (NST) and network-wide secrecy energy efficiency (NSEE) are also analyzed, which reflects the comprehensive secrecy performances from a network-wide perspective.

- In order to enhance the physical layer security of the considered network, the FD BS jamming scheme is proposed, which is suitable for improving IoT secrecy performances considering the constrains of hardware complexity and power in IoT terminals. Besides, the security enhancement brought by the proposed scheme is also analyzed.
- Based on the proposed analysis and simulations, several important observations are reached: 1) BS intensity and jamming power introduce a tradeoff between reliability and security, which can be improved by a proper design of BS intensity and jamming power. 2) NST and NSEE can be significantly enhanced by our proposed FD BS jamming scheme.

C. ORGANIZATION

The rest of the paper is organized as follows. In Section II, the system model and performance metrics are introduced. In Section III, we obtain analytical results of the performances metrics. In Section IV, the FD BS jamming scheme is introduced. Analytical and simulation results are presented in Section V and conclusions are drawn in Section VI.

Notation: Throughout this paper, bold lowercase letters denote vectors, $\mathrm{E}[\cdot]$ stands for the expectation operator and $\mathrm{P}(\cdot)$ for the probability measure, $\|\cdot\|$ denotes Euclidean norm. $\mathcal{CN}(u, v)$ denotes the circularly symmetric complex Gaussian distribution with mean u and variance v The key symbols used in the paper are listed in Table 1.

TABLE 1. Key symbols used in the paper.

Symbols	Notations
λ_b	Intensity of BSs
λ_e	Intensity of Eves
$h_{u_1u_2}$	small-scale channel gain between node u_1 and node u_2
R_B, R_S	Codewords rate and secrecy rate
P_u, P_C	Transmit power and other power consumption at UE
P_n, P_B	Jamming power and other power consumption at BS
$d_{(1)}/r_1$	Distance between UE_1 and serving BS.
$d_{(2)}/r_2$	Distance between UE_2 and serving BS.
$p_{u,1}$, $p_{u,1}$	Coverage probability of UE_1 and UE_2

II. SYSTEM MODEL

As shown in Fig. 1, we consider an uplink cellular IoT network composed of BSs surrounded by UEs. The locations of BSs and UEs are distributed according to a Matern cluster process [27], [28]. In detail, the locations of BSs are modeled by a parent homogeneous PPP $\varphi_b = \{b_1, b_2, \cdots\}$ in the Euclidean plane with density λ_b. Each BS forms the center of a cluster around which a fixed number of daughter points (UEs) $\bar{c}$ are uniformly spatially distributed in a circle of radius R with density function $f(z)$ given by

$$f(z) = \begin{cases} \dfrac{1}{\pi R^2} & \text{if } \|z\| \le R \\ 0 & \text{otherwise} \end{cases} \tag{1}$$

where z is the two dimensional coordinates relative to the cluster center, $\|\cdot\|$ is the Euclidean norm. Besides, $\bar{c}$ UEs are assumed to be randomly divided into $\bar{c}/2$ orthogonal pairs

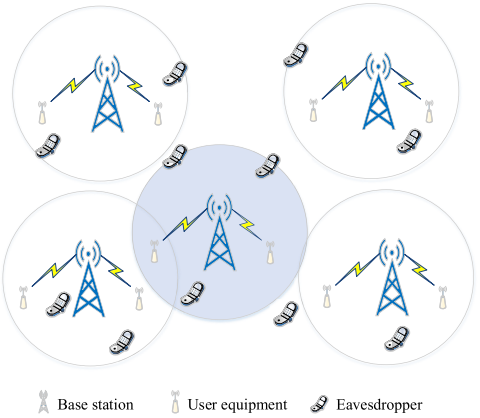


FIGURE 1. Network model for secure uplink NOMA transmission with $\bar{c} = 2$.

using different RBs, such as a time slot or an orthogonal frequency band. For simplicity, we focus our attention on investigating a typical pair of UEs, denoted by UE_1 and UE_2. A number of passive non-colluding Eves are distributed along the whole plane, which are assumed to have powerful detection capabilities and can overhear the messages of all orthogonal RB. The spatial distribution of Eves are modeled using a homogeneous PPP distributed in $\mathbb{R}^2$, which is denoted by φ_e and associated with a density λ_e. We note that the PPP model is adopted to model randomness of Eves' spatial distribution as the locations of the passive Eves are difficult to get, e.g., [9], [22].

We assume that each UE and BS is equipped with a single antenna. Eves are also considered to be equipped with a single antenna to disguise themselves to UEs. Wireless channels are assumed to suffer a large-scale path loss governed by the exponent $\alpha > 2$ together with a quasi static Rayleigh fading with fading coefficients independent and identically distributed (i.i.d.) obeying $\mathcal{CN}(0, 1)$. We denote $h_{u_1u_2}$ as the Rayleigh fading channel gain between node u_1 and node u_2, which can be modeled by the exponential random variable with unit mean. Considering a typical cell, 2 UEs transmit confidential messages s_i to the serving BS $b \in \varphi_b$ with power P_u such that the superposed NOMA signal at BS b or Eve e can be given by:

$$y_x = \sum_{i=1,2} \sqrt{P_u h_{u_i x} \|u_i - x\|^{-\alpha}} s_i + n, \quad x \in \{b, e\} \tag{2}$$

where n is additive noise, which obeys complex Gaussian distributed with mean zero and variance δ^2.

Considering the hardware complexity of UEs, adaptive transmission rate scheme is difficult to be used. Thus, we utilize fixed rate Wyners wiretap encoding scheme [29] to encode secret information. Let R_B and R_E denote the rates of the transmitted codewords and redundant information respectively, and $R_S = R_B - R_E$ denotes the secrecy rate. According to Shannon theorem, if the channel from the UE to connected BS can accommodate rate R_B, the BS can decode the confidential information. Otherwise, if none of the channels from

the BS to Eves can accommodate the redundant rate R_E, the information is deemed to be protected against wiretapping, i.e., secrecy is achieved. Based on Wyners encode, the following outage based metrics are analyzed in this paper.

- **Coverage Probability:** Coverage probability of UEs, denoted as $p_{u,i}, i \in \{1, 2\}$, quantifies the probability that the message can be decoded at the intended receiver without error. The reliability performance can be measured by coverage probability.
- **Secrecy Outage Probability:** The secrecy performance is measured by secrecy outage probability (SOP), denoted as p_{so}. SOP quantifies the probability that perfect secrecy can not be guaranteed. We consider the Eve which has the best channel to the UE. If the Eve fails to decode the confidential message, information secrecy is achieved. Otherwise, a secrecy outage occurs.

In order to analyze the network-wide secrecy performances, we focus our study on the following two items:

1) NST. To assess the efficiency of secure transmissions, we use the metric named NST (bps/m^2/Hz) [30], which is defined as average rate of message reliably and securely uplink transmitted by UEs per unit bandwidth and per unit area. As the intensities of UE_1 and UE_2 are the same as λ_b, NST denoted by Ω will be

$$\Omega = \lambda_b \sum_{i=1,2} R_s \left(1 - p_{so}\right) p_{u,i}. \tag{3}$$

Here, we clarify that the NST takes both reliability and security into consideration.

2) NSEE. To evaluate the energy efficiency of secure transmissions, we use the metric named NSEE (bps/m^2/Hz/W) [31], which is defined as the ratio of NST to the power consumed by UEs and BSs per unit bandwidth and per unit area. Mathematically, NSEE denoted by Ψ is expressed as $\Psi = \frac{\Omega}{P_{total}}$, where P_{total} denotes the total power consumption for UEs and BSs per unit area. We note that NSEE can reflect comprehensive performances of network reliability, network security and power consumption.

III. PHYSICAL LAYER SECURITY OF UPLINK NOMA IN CELLULAR IoT

In this section, we analyze the physical layer security of the considered IoT uplink NOMA networks. The typical cluster assumption is adopted in the sequel.

A. COVERAGE PROBABILITIES

We first derive the coverage probabilities of 2 UEs in the typical cluster to analyze the reliability performance of the network. In the considered scenario, the BS in typical cell is vulnerable to two kinds of interference, i.e.,

- **Intra-cluster interference:** Intra-cluster interference is the interference caused by UEs in the same NOMA pair using the same RB. Some of the intra-cluster interference can also be removed by performing SIC.
- **Inter-cluster interference:** Inter-cluster interference is the interference caused by the UEs outside the typical cell using the same RB.

In order to remove intra-cluster interference with SIC, the BS needs to order the received power from 2 UEs. As the impact of the path-loss is generally the dominant factor compared to the channel fading effects [27], it is assumed that the order of the received signal powers is equal to the order of the distances from the UEs to their serving BS.[1] The distance from UE_1 and UE_2 to the serving BS are denoted by d_1 and d_2. We thus order the distances as $\{d_{(1)}, d_{(2)}\}$, in which $d_{(1)} < d_{(2)}$. Note that d_1 and d_2 are i.i.d. While $d_{(1)}$ and $d_{(2)}$ are interdependent with different distribution from d_1 and d_2. Without loss of generality, UE_1 is assumed to be closer to the BS and the distance from UE_1 to the serving BS is $d_{(1)}$. According to the principle of uplink NOMA, the signal from UE_1 is decoded first by treating the received signal from UE_2 as interference. If the UE_1's signal can be successfully decoded, the serving BS can removes UE_1's signal from the composite received signal and then decodes UE_2's signal without intra-user interference. Otherwise, UE_2 will experience the interference from UE_1's signal, which is referred to as SIC error propagation (the imperfect SIC) [27]. The signal-to-interference-plus-noise ratio (SINR) of UE_1 and UE_2 after SIC can be respectively expressed as

$$\begin{aligned} \gamma_1 &= \frac{P_u h_{u_1 b_0} {d_{(1)}}^{-\alpha}}{I^1_{\text{intra}} + I^u_{\text{inter}} + \delta^2}, \\ \gamma_2 &= \frac{P_u h_{u_2 b_0} {d_{(2)}}^{-\alpha}}{(1 - b(1)) I^2_{\text{intra}} + I^u_{\text{inter}} + \delta^2}, \end{aligned} \tag{4}$$

where

$$\begin{aligned} I^1_{\text{intra}} &= P_u h_{u_2 b_0} {d_{(2)}}^{-\alpha}, \\ I^2_{\text{intra}} &= P_u h_{u_1 b_0} {d_{(1)}}^{-\alpha}, \\ I^u_{\text{inter}} &= \sum_{b \in \varphi_b \setminus b_0} \sum_{u \in \{u_1, u_2\}} P_u h_{u b_0} \|u - b_0\|^{-\alpha}. \end{aligned} \tag{5}$$

We note that the successful decode of UE_1's signal is represented by a binary digit $b(1) = 1$ whereas the SIC failure is given by $b(1) = 0$. Therefore, $b(1)$ obeys the Bernoulli distribution with parameter $p_{u,1}$. When decoding the signal of UE_1, it will suffer the intra-cell interference and inter-cell interference. Thus, the coverage probability of UE_1 is evaluated as

$$p_{u,1} = P\left(\log_2\left(1 + \gamma_1\right) > R_b\right). \tag{6}$$

Considering the SIC error propagation at UE_2, the coverage probability of UE_2 is evaluated as

$$\begin{aligned} p_{u,2} &= P\left(\log_2\left(1 + \gamma_2\right) > R_b\right) \\ &= p_{u,1} P\left(\frac{P_u h_{u_2 b_0} {d_{(2)}}^{-\alpha}}{I^u_{\text{inter}} + \delta^2} > 2^{R_b} - 1\right) \\ &\quad + \left(1 - p_{u,1}\right) P\left(\frac{P_u h_{u_2 b_0} {d_{(2)}}^{-\alpha}}{I^2_{\text{intra}} + I^u_{\text{inter}} + \delta^2} > 2^{R_b} - 1\right). \end{aligned} \tag{7}$$

[1] We note that the SIC based on long-term channel states is more practically feasible since it requires less overheads for channel estimation. Thus, this SIC method provides us a tradeoff between SIC effect and channel estimation overheads. Besides, the SIC error brought by this method has also been consideration in this paper.

In order to get the coverage probabilities of 2 UEs, we first derive the Laplace transform of the intra-cluster interference. Then we derive the Laplace transform of the inter-cluster interference incurred at the representative BS. Finally, the coverage probability expressions for 2 UEs can be derived.

Lemma 1: The Laplace transform of the intra-cluster interference experienced by the transmissions of UE_1 and UE_2 can be given as follows:

$$\begin{aligned}\mathcal{L}^1_{\text{intra}}(s) &= \frac{F(R) - F(r_1)}{sP_u\left(\frac{\alpha}{2}+1\right)\left(R^2 - {r_1}^2\right)},\\ \mathcal{L}^2_{\text{intra}}(s) &= \frac{2F(r_2)}{sP_u(\alpha+2){r_2}^2},\end{aligned} \tag{8}$$

where

$$F(r) = r^{2+\alpha}\,{}_2F_1\left[1, 1+\frac{2}{\alpha}, 2+\frac{2}{\alpha}, -\frac{r^\alpha}{sP_u}\right]. \tag{9}$$

Here, ${}_2F_1[\cdot]$ denotes the Gauss hypergeometric function, r_1 denotes the distance between BS and UE_1, r_2 denotes the distance between BS and UE_2.

Proof: See Appendix A.

As for the Laplace transform of the inter-cluster interference, the definition expression in (5) can be rewritten as

$$I^u_{\text{inter}} = \sum_{b\in\varphi_b\setminus b_0}\sum_{u\in\{u_1,u_2\}} P_u h_{ub}\|\boldsymbol{x}+\boldsymbol{y}\|^{-\alpha}, \tag{10}$$

where $\boldsymbol{x}$ denotes two-dimensional vector from the representative BS b_0 to the other BS $b \in \varphi_b\setminus b_0$, $\boldsymbol{y}$ denotes two-dimensional vector from the interfering UEs to serving BS in other cluster. Then, the Laplace transform of the inter-cluster interference can be derived in the following lemma.

Lemma 2: The Laplace transform of the inter-cluster interference for the representative BS can be given as follows:

$$\begin{aligned}\mathcal{L}^u_{\text{inter}}(s) = \exp\Bigg(-2\pi\lambda_b\Bigg(&\int_0^R\left(1-{\mathcal{D}_1}^2\right)v dv\\ &+\int_R^\infty\left(1-{\mathcal{D}_2}^2\right)v dv\Bigg)\Bigg),\end{aligned} \tag{11}$$

where

$$\begin{aligned}\mathcal{D}_1 = &\int_{R-v}^{R+v}\frac{\frac{u}{R^2}-\frac{2u}{\pi R^2}\sin^{-1}\left(\frac{v^2-R^2+u^2}{2uv}\right)}{1+sP_u u^{-\alpha}}du\\ &+\int_0^{R-v}\frac{2u}{R^2\left(1+sP_u u^{-\alpha}\right)}du,\end{aligned} \tag{12}$$

and

$$\mathcal{D}_2 = \int_{v-R}^{R+v}\frac{\frac{u}{R^2}-\frac{2u}{\pi R^2}\sin^{-1}\left(\frac{v^2-R^2+u^2}{2uv}\right)}{1+sP_u u^{-\alpha}}du \tag{13}$$

Proof: See Appendix B.

Using the Laplace transform of the intra-cluster interference and inter-cluster interference, we can obtain the coverage probabilities in the typical cluster, which is given by the following Lemma.

Lemma 3: The coverage probabilities of 2 UEs are given by

$$\begin{aligned}p_{u,1} &= \int_0^R \exp\left(-\delta^2 c_1\right)\mathcal{L}^1_{\text{intra}}(c_1)\,\mathcal{L}^u_{\text{inter}}(c_1) f_{d(1)}(r_1)\,dr_1\\ p_{u,2} &= (1-p_{u,1})\int_0^R \exp\left(-\delta^2 c_2\right)\mathcal{L}^2_{\text{intra}}(c_2)\,\mathcal{L}^u_{\text{inter}}(c_2)\\ &\quad\times f_{d(2)}(r_2)\,dr_2 + p_{u,1}\int_0^R \exp\left(-\delta^2 c_2\right)\mathcal{L}^u_{\text{inter}}(c_2)\\ &\quad\times f_{d(2)}(r_2)\,dr_2\end{aligned} \tag{14}$$

where

$$\begin{aligned}c_i &= {P_u}^{-1}\left(2^{R_b}-1\right){r_i}^\alpha, \quad i\in\{0,1\},\\ f_{d(1)}(r_1) &= \frac{4r_1}{R^2}\left(1-\frac{{r_1}^2}{R^2}\right), \quad r_1 < R,\\ f_{d(2)}(r_2) &= \frac{4{r_2}^3}{R^4}, \quad r_2 < R.\end{aligned} \tag{15}$$

Proof: See Appendix C.

Here, we note that coverage probabilities for 2 UEs decrease with the increasing λ_b because the larger λ_b brings severer inter-cell interference.

B. SECRECY OUTAGE PROBABILITY

In this subsection, we analyze the secrecy outage probability of a typical UE. We consider the worst-case scenario of the IoT cellular networks, in which Eves are assumed to have enough detection capabilities to distinguished multiuser data stream in the same cluster by applying multiuser detection techniques [22], [23]. It is also assumed that the received signal power from other cluster is too small that the data stream can not be distinguished. Specifically, Eves will not be interfered by intra-cluster interference upon subtracting interference generated by the superposed signals from each other and will still suffer from inter-cluster interference. We note that this assumption may overestimate Eve's multi-user detection capabilities and leads to the lower bound of the network secrecy performances. Similarly to typical cluster assumption, a typical UE is chosen arbitrarily as all UEs are equal from the perspective of Eves. We thus consider the most detrimental Eve which has the best channel to the typical UE. Therefore, the received SINR at the most detrimental Eve (with respect with typical UE) can be expressed as follows:

$${\gamma_e}^* = \max_{e\in\varphi_e}\frac{P_u h_{ue}\|e-u\|^{-\alpha}}{I^e_{\text{inter}}+\delta^2}, \tag{16}$$

where

$$I^e_{\text{inter}} = \sum_{b\in\varphi_b\setminus b_0}\sum_{u\in\{u_1,u_2\}} P_u h_{ue}\|u-e\|^{-\alpha}. \tag{17}$$

Then, SOP can be expressed as follows:

$$p_{so} = P\left(\log_2\left(1+{\gamma_e}^*\right) > R_b - R_s\right). \tag{18}$$

In order to derive the SOP, Laplace transform of the inter-cluster interference $\mathcal{L}^e_{\text{inter}}$ for the most detrimental Eve

is derived first. Using the Plam measure [28] and bounding technology, an upper bound on $\mathcal{L}^{e}_{inter}$ can be given in the following lemma.

Lemma 4: An upper bound on Laplace transform of the inter-cluster interference for the most detrimental Eve can be given as follows:

$$\mathcal{L}^{e}_{\text{inter}}(s) = \exp\left(-2\pi\lambda_b (sP_u)^{\frac{2}{\alpha}} B\left[1-\frac{2}{\alpha}, 2+\frac{2}{\alpha}\right]\right), \tag{19}$$

where $B(x, y)$ is the Beta function.

Proof: See Appendix D.

Note that Tabassum *et al.* [27] use the same bounding technique to derive analytical bound and numerically studied the accuracy of the derived bounds. The analytical and simulation results also validate the accuracy of our approximation on the Laplace transform of the inter-cluster interference.

Then, the SOP of the most detrimental eavesdropper can be computed as follows:

Lemma 5: The upper bound of SOP for the most detrimental eavesdropper is given by

$$p_{so} = 1-\exp\left(-2\pi\lambda_e \int_0^{\infty} \exp\left(-\delta^2 c_e\right) \mathcal{L}^{e}_{\text{inter}}(c_e)\, r_e dr_e\right), \tag{20}$$

where $c_e = \left(2^{R_b-R_s}-1\right) {P_u}^{-1} {r_e}^{\alpha}$, and $\mathcal{L}^{e}_{inter}$ are given in Lemma 4.

Proof: Substituting (14) into (16), we thus obtain SOP for the most detrimental eavesdropper as follows:

$$\begin{aligned} p_{so} &= \mathrm{P}\left(\max_{e\in\varphi_e} \frac{P_u h_{ue} {r_e}^{-\alpha}}{I^{e}_{fer}+\delta^2} > 2^{R_b-R_s}-1\right) \\ &= 1-\mathrm{E}_{\varphi_e}\left(\prod_{e\in\varphi_e} \mathrm{P}\left(h_{ue} < c_e\left(I^{e}_{\text{inter}}+\delta^2\right)\right)\right) \\ &\le 1-\exp\left(-2\pi\lambda_e \int_0^{\infty} \mathrm{P}\left(h_{ue} > c_e\left(I^{e}_{\text{inter}}+\delta^2\right)\right) r_e dr_e\right), \end{aligned} \tag{21}$$

where the last line follows the PPP distribution of Eves and Jensen's inequality [9], [10]. Then SOP in Lemma 5 can be derived.

We note that the upper bound p_{so} in (21) gives an accurate approximation of the exact SOP over the entire range of $p_{so} \in [0,1]$ [9], [29]. Therefore, we adopt the upper bound in (21) as the approximation of p_{so}, which is also validated by our simulation results. It is obvious that SOP decreases with the increasing λ_b because the inter-cell interference at Eves increases with larger λ_b.

C. NST AND NSEE ANALYSIS

Finally, we evaluate NST and NSEE of the considered network. Having $p_{u,i}$, $i \in \{1, 2\}$ in Lemma 3 and p_{so} in Lemma 5, a lower bound of NST can be given as follows:

$$\Omega = \lambda_b R_s (1-p_{so})\left(p_{u,1}+p_{u,2}\right). \tag{22}$$

As for the power model, we assume that the power consumption includes the signal transmission power consumption, dynamic circuit power consumption of transmit chains and the static power consumption in transmit modes [32]. Then, the total power consumption can be given by

$$P_{total} = 2\lambda_b \left(P_u + P_C\right), \tag{23}$$

where P_C combines the dynamic circuit power consumption of transmit chains and the static power consumption in transmit modes. Having Ω in (20) and P_{total} in (21), a lower bound of NSEE is given by

$$\Psi = \frac{R_s (1-p_{so})\left(p_{u,1}+p_{u,2}\right)}{2\left(P_u+P_C\right)}. \tag{24}$$

Remark 1: From the analysis of considered network, intensity λ_b, code rate R_b and R_s are key parameters which have a great impact on network reliability and security. The secrecy performance can be improved at the cost of reliable performance by setting a larger value of λ_b. Therefore, λ_b triggers a trade-off between reliability and security, and plays a key role in improving NST and NSEE. However, the set of λ_b in practical network design depends on various factors, such as the real demand and economic considerations, which may lead to poor secrecy performances. As for R_b and R_s, although they can be optimized to maximize NST and NSEE, the channel differences between legitimate channel and wiretap channel has not been widen. As a result, the optimal design of R_b and R_s only has a limited capability of security enhancement. Thus, design of effective protocols is still needed to enhance the physical layer security of the considered network. Note that our analysis can also be extended to k-UE NOMA case.[2]

IV. ENHANCING SECURITY WITH THE AID OF FULL-DUPLEX BS JAMMING

In this section, we present a method to further improve the physical layer security of the considered network. Recently, great progress has been made in FD technology, in which self interference (SI) can be efficiently mitigated in the analog circuit domain [33], digital circuit domain [34], and spatial domain [35], respectively. Based on efficient SI cancelation, we enable BS to radiate jamming signals upon their information receptions. By doing so, additional degrees of freedom can be gained to improve the network security.

The general idea of FD receiver jamming has been introduced in point-to-point and network transmission scenarios [34]–[36]. Specifically, Zheng *et al.* [36] and Chen *et al.* [37] consider a single-input multi-output (SIMO) channel with the receiver using single- and multi-antenna jamming, respectively. Zheng *et al.* [38] investigate the potential benefits of FD receiver jamming techniques in

[2] As for k-UE NOMA case, the main difference is the intra-cell interference model. The probability density function of the distance between BS and the k-th UE is needed when deriving the Laplace transform of intra-cell interference. Then, the network performances can also be analyzed using the same analytical framework.

enhancing information security from a network perspective. When it comes to our considered scenarios, it is a good way of thinking to improve the secrecy performance with the aid of BS, considering the constrains of hardware complexity and power in IoT. In this work, we consider to enhance security of uplink NOMA in cellular IoT with the aid of FD BS jamming. In the following, physical layer security in the considered network are analyzed.

A. COVERAGE PROBABILITIES

In addition to the intra-cell interference and inter-cell interference, the representative BS is also interfered by self-interference and mutual-jamming from the neighboring cells. As SI depends on the transmit power, we assume a linearly increasing SI associating with the transmit power in this paper [35], [39]. Thus, the SINR of UE_1 and UE_2 can be respectively expressed as

$$\gamma_1 = \frac{P_u h_{u_1 b_0} d_{(1)}{}^{-\alpha}}{I^1_{\text{intra}} + I^u_{\text{inter}} + I_f + \eta P_n + \delta^2},$$
$$\gamma_2 = \frac{P_u h_{u_2 b_0} d_{(2)}{}^{-\alpha}}{(1-b(1)) I^2_{\text{intra}} + I^u_{\text{inter}} + I_f + \eta P_n + \delta^2}, \quad (25)$$

where

$$I_f = \sum\nolimits_{b \in \varphi_b \setminus b_0} P_n h_{bb_0} \|b - b_0\|^{-\alpha}, \quad (26)$$

P_n is the transmit power of the jamming signal, η is the parameter that reflects the SI cancelation capability, and $\eta = 0$ refers to the perfect SI cancelation while $0 < \eta \leq 1$ corresponds to different levels of SI cancelation. The coverage probabilities in the typical cluster with FD BS jamming can be derived using the following Lemma.

Lemma 6: The coverage probabilities of 2 UEs are given by

$$p_{u,1} = \int_0^R \exp\left(-\left(\delta^2 + \eta P_n\right) c_1\right) \times \mathcal{L}^1_{\text{intra}}(c_1)\, \mathcal{L}^u_{\text{inter}}(c_1)\, \mathcal{L}_f(c_1) f_{d(1)}(r_1)\, dr_1,$$
$$p_{u,2} = p_{u,1} \int_0^R \exp\left(-\left(\delta^2 + \eta P_n\right) c_2\right) \mathcal{L}^u_{\text{inter}}(c_2)\, \mathcal{L}_f(c_2) \times f_{d(2)}(r_2)\, dr_2 + (1 - p_{u,1}) \int_0^R \exp\left(-\left(\delta^2 + \eta P_n\right) c_2\right) \times \mathcal{L}^2_{\text{intra}}(c_2)\, \mathcal{L}^u_{\text{inter}}(c_2)\, \mathcal{L}_f(c_2) f_{d(2)}(r_2)\, dr_2, \quad (27)$$

where

$$\mathcal{L}_f(c) = \exp\left(-\pi \lambda_b (cP_n)^{2/\alpha} \Gamma\left(1 + \frac{2}{\alpha}\right) \Gamma\left(1 - \frac{2}{\alpha}\right)\right). \quad (28)$$

$\mathcal{L}^1_{\text{intra}}(c)$ is given in Lemma 1, $\mathcal{L}^u_{\text{inter}}$ is given in Lemma 2, $c_i, i \in \{1, 2\}$, $f_{d(1)}(r_1)$ and $f_{d(2)}(r_2)$ is given in Lemma 3.

Proof: The Laplace transform of FD BS jamming interference can be given as follows:

$$\mathcal{L}_f(c) = E\left[\exp\left(-cI_f\right)\right] = E\left[\prod_{b \in \varphi_b \setminus b_0} E_{h_{bb_0}}\left[\exp\left(-cP_n h_{bb_0} \|b - b_0\|^{-\alpha}\right)\right]\right]$$
$$\overset{a}{=} \exp\left(-2\pi\lambda_b \int_0^\infty \left(1 - \frac{1}{1 + cP_n y^{-\alpha}}\right) y dy\right) = \exp\left(-\pi \lambda_b (cP_n)^{2/\alpha} \Gamma\left(1 + \frac{2}{\alpha}\right) \Gamma\left(1 - \frac{2}{\alpha}\right)\right). \quad (29)$$

The equation (a) follows the probability generating functional (PGFL) of PPP. Using the same approach in Lemma 3, the coverage probabilities in Lemma 6 can be derived.

Note that coverage probabilities will decrease when using FD BS jamming because it brings self-interference and mutual-jamming to BS. It can also be inferred that coverage probabilities decrease with the increasing P_n.

B. SECRECY OUTAGE PROBABILITY

Using the same assumption in Section III.B, Eves are interfered by inter-cell interference and jamming signals, where inter-cell interference is given in (15). Considering the typical cell, UE u transmit confidential message to the BS b_0. Jamming signals at Eve e can be expressed as follows:

$$I^e_f = \sum_{b \in \varphi_b} P_n h_{eb} \|e - b\|^{-\alpha} = \sum_{b \in \varphi_b \setminus b_0} P_n h_{eb} \|e - b\|^{-\alpha} + P_n h_{eb_0} \|e - b_0\|^{-\alpha}. \quad (30)$$

Let r and r_e denote the distance between the typical UE and BS and the distance between the typical UE and Eve, respectively. Therefore, the distance between the BS and Eve can be expressed as:

$$\|e - b_0\| = \sqrt{r^2 + {r_e}^2 - 2 r r_e \cos\theta}, \quad (31)$$

where the angle θ is uniformly distributed in the range $[0, 2\pi]$ [38]. Therefore, the received SINR at the most detrimental Eve can be expressed as follows:

$$\gamma_e{}^* = \max_{e \in \varphi_e} \frac{P_u h_{ue} {r_e}^{-\alpha}}{I^e_{\text{inter}} + I^e_f + \delta^2}. \quad (32)$$

Then, SOP can be derived in the following Lemma.

Lemma 7: The upper bound of SOP for the most detrimental eavesdropper is given by

$$p_{so} = 1 - \exp(-2\pi\lambda_e \times \int_0^\infty \exp\left(-c_e \delta^2\right) L^e_{\text{inter}}(c_e)\, L^e_{f/b_0}(c_e)\, \mathcal{C} r_e dr_e), \quad (33)$$

where

$$\mathcal{L}^e_{f/b_0}(c_e) = \exp\left(-\pi \lambda_b (c_e P_n)^{2/\alpha} \Gamma\left(1 + \frac{2}{\alpha}\right) \Gamma\left(1 - \frac{2}{\alpha}\right)\right),$$
$$\mathcal{C} = \frac{1}{\pi R^2} \int_0^{2\pi} \int_0^R \frac{r}{1 + c_e P_n \left(r^2 + {r_e}^2 - 2 r r_e \cos\theta\right)^{-\frac{\alpha}{2}}} dr d\theta \quad (34)$$

c_e, and $\mathcal{L}^e_{\text{inter}}(c_e)$ can be derived in Lemma 4.

TABLE 2. Simulation parameters.

Parameters	Values
Codeword rate R_b	1bps/Hz
Secrecy rate R_s	0.5bps/Hz
Radius of BS $\mathcal{R}$	$200m$
Path loss coefficient α	4
Noise power δ^2	-120dBm
Intensity of Eves λ_e	10^{-5}unit/m^2
SI cancellation parameter η	-100dB
Transmit power at UE P_u	20dBm
Other power consumption at UE P_C	12dBm
Other power consumption at BS P_B	12dBm

Proof: See Appendix E

It is shown that SOP decreases with the increasing P_n. Thus the secrecy performance can be improved by using FD BS jamming.

C. NST AND NSEE ANALYSIS

Similarly, substituting $p_{u,i}, i \in \{1, 2\}$ in Lemma 6 and p_{so} in Lemma 7 into (3), NST can be derived. As for the power model in NSEE, extra power is consumed to radiate jamming signal, thus the total power consumption is $P_{total} = \lambda_b (2P_u + 2P_C + P_n + P_B)$, where P_B combines the dynamic circuit power consumption of transmit chains and the static power consumption in transmit modes at BS. Therefore, NSEE can be given by

$$\Psi = \frac{R_s (1 - p_{so}) \left(p_{u,1} + p_{u,2}\right)}{(2P_u + 2P_C + P_n + P_B)}. \tag{35}$$

Remark 2: It can be inferred that radiating jamming signals at BS can largely interfere the information overhearing at Eves which benefits the secrecy. Whereas the increased jamming signals also interfere with legitimate receivers and thus harm the reliability. Thus, P_n arouses a tradeoff between reliability and security. In order to maximize NST, P_n should be optimized to balance the tradeoff between the reliability and security. In order to maximize NSEE, P_n should be optimized not only to balance the tradeoff between the security and reliability, but also to reduce the total power consumption as much as possible. As NST and NSEE can not be maximized simultaneously, P_n also arouses a tradeoff between NST and NSEE.

V. NUMERICAL RESULTS

In this section, we employ the Monte Carlo based simulations to verify the correctness of our analysis. Additionally, performance of the considered uplink NOMA IoT system is also evaluated. The simulation parameters are configured in Table 2. Besides, we adopt the PPP model on a square [0, 1000] m × [0, 1000] m for BSs and Eves and Rayleigh channel fading model with unit mean value, as done in the analytical model.

A. COVERAGE PROBABILITIES AND SECRECY OUTAGE PROBABILITY

In this subsection, the effects of BS intensity and the jamming power on reliability and security performance are examined.

We illustrate coverage probabilities and SOP, i.e., $p_{u,1}$, $p_{u,2}$ and p_{so}, over different intensity λ_b in Fig. 2 without

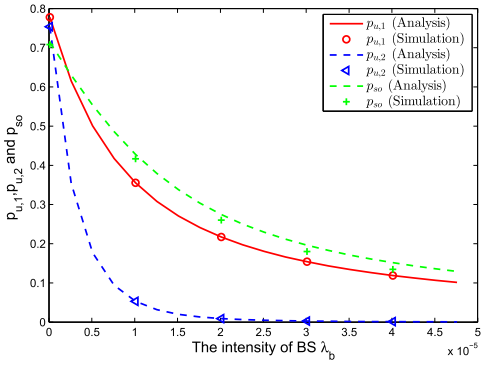


FIGURE 2. $p_{u,1}$, $p_{u,2}$ and p_{so} versus λ_b.

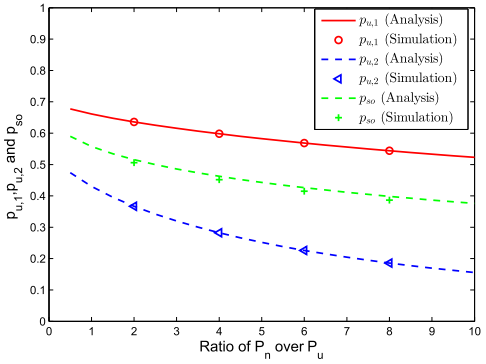


FIGURE 3. $p_{u,1}$, $p_{u,2}$ and p_{so} versus ratio of P_n over P_u with $\lambda_b = 10^{-5}$unit/m^2.

the FD BS jamming. It is obvious that $p_{u,1}$, $p_{u,2}$ and p_{so} are decreasing functions of λ_b, which is consistent with the analytical results in (12) and (18). This implies that security performance can be improved at the cost of reliable performances with larger λ_b. However, the value of λ_b is highly related to the real demand, which may lead to a poor secrecy performance. Thus, the design of security scheme is of great importance to improve the secrecy performances of the considered network. The coverage probabilities and SOP over different jamming power P_n is shown in Fig. 3, in which η is fixed at -100dB. It is obvious that $p_{u,1}$, $p_{u,2}$ and p_{so} are decreasing functions of P_n. Therefore, the secrecy performance can be improved while the reliable performance will be reduced with larger P_n. Besides, the energy efficiency will also be reduced as $p_{u,1}$ and $p_{u,2}$ decreasing and power consumption increasing with larger P_n. This implies that P_n introduces not only a tradeoff between reliability and security, but also a tradeoff between the energy efficiency and security. In Fig. 2 and Fig. 3, it can be observed from the curves and the corresponding markers, the analytical results of the coverage probabilities are in quite good agreement with corresponding simulation results. This fact validates the correctness of our analytical results. As for the secrecy outage probabilities, the simulation results are a little smaller than analytical results, which is explained as follows: 1) we make an approximation to derive the upper bound of Laplace

transform of the inter-cluster interference for the most detrimental Eve; 2) Jensen's inequality is utilized to derive SOP. The observations from the Fig. 2 and Fig. 3 can help the designers of IoT uplink NOMA networks to appropriately select the intensity of BS and the jamming power according to the performances for different requirements.

B. NST AND NSEE

In this subsection, we first analyze the effects of BS intensity and the jamming power on NST and NSEE. Then, we compare the normalized NST with NSEE to get further insights.

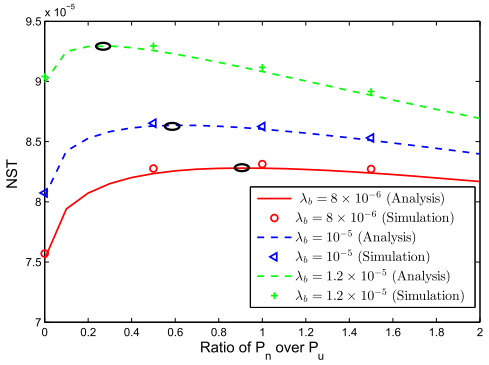


FIGURE 4. NST versus ratio of P_n over P_u.

Fig. 4 depicts NST versus P_n for different values of λ_b. It is obvious that as P_n increases, NST first increases and then decreases. The underlying reason is that too small jamming power lead to poor secrecy performance whereas too large jamming power leads to poor reliable performance; both aspects result in small NST. This also implies that proposed FD BS jamming scheme can largely improve the network-wide security performance with a proper set of P_n. Besides, the optimal P_n is tagged in the figure. We find that the optimal P_n which maximizes NST is related to λ_b. The optimal P_n will be smaller with larger λ_b because more inter-cell interference are introduced with larger λ_b, leading to less jamming power demand.

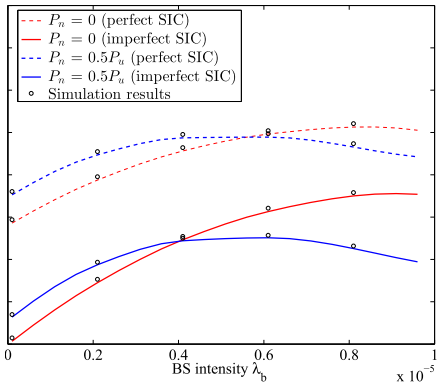


FIGURE 5. NSEE versus λ_b for different SIC assumption.

Fig. 5 shows NSEE versus λ_b for different SIC assumption. We observe that the imperfect SIC will degrade the network performance. Also, we note that the effect of FD BS jamming scheme on NSEE is largely related to λ_b. NSEE is enhanced when λ_b is small. Otherwise, NSEE may be degraded. Then, we analyze NSEE with two conditions: $P_n = 0$ and $P_n = 0.5P_u$. When NSEE with $P_n = 0$ is the same as NSEE with $P_n = 0.5P_u$, the IoT terminal intensity is denoted as λ_b^*. It is implied that λ_b^* in perfect SIC assumption is larger than that in imperfect SIC assumption. The underlay reason is that the effect of interference on reliable performance is weakened for perfect SIC assumption. This fact indicates that the ignorance of imperfect SIC will lead to error in the network parameter design.

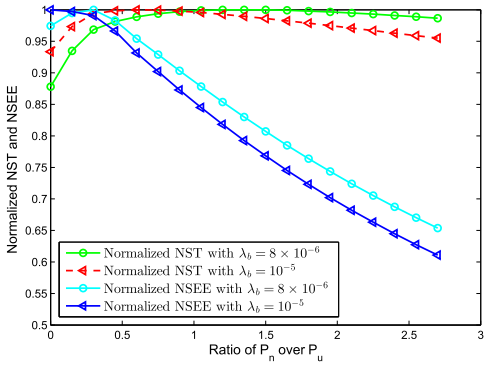


FIGURE 6. Normalized NST and NSEE versus ratio of P_n over P_u with different λ_b.

We compare normalized NST and NSEE in Fig. 6. We observe that the optimal P_n which maximizes NSEE is smaller than the optimal P_n which maximizes NST for a given λ_b. As maximizing NST and NSEE cannot be achieved simultaneously, different value of P_n is applied in different reality scenarios. When the network is in the busy condition, i.e., NST is preferred, P_n which maximizes NST should be selected. When the network is in the idle condition, i.e., NSEE is preferred, P_n which maximizes NSEE should be selected.

VI. CONCLUSION

In this paper, we analyze the physical layer security performances of uplink NOMA-IoT. We consider the uplink transmission scenario where UEs are located around the serving BS. Passive non-colluded Eves are assumed to be randomly distributed with uncertain locations. Both intra-cell interference and inter-cell interference are considered in our analysis. The FD BS jamming scheme is proposed to enhance the network physical layer security performance. The impact of imperfect SIC is also considered in our analysis.

We obtain expressions of coverage probabilities and SOP. Additionally, NST and NSEE are also derived to analyze the network-wide secrecy performances. The effects of λ_b and P_n on network performances are analyzed. It is proved that λ_b and P_n have an opposite effect on coverage probability and secrecy outage probability, which introduces a tradeoff between reliability and security. Besides, P_n also introduces a NST-NSEE tradeoff. It is worth mentioning that the results in this paper are theoretically oriented and offer a useful

design guide for uplink NOMA transmission in IoT. We also note that our work only gives a rough solution to balance the tradeoff between NST and NSEE, this tradeoff will be analyzed in detail in our future work.

APPENDIX A
PROOF OF LEMMA 1

Conditioned on $d_{(1)} = r_1$, the Laplace transform of the intra-cluster interference of UE_1 as defined in (5), can be derived as follows:

$$\begin{aligned}\mathcal{L}^1_{intra}(s) &= \mathrm{E}\left[\exp\left(-sI^1_{intra}\right)\right]\\ &= \mathrm{E}_{d_{(2)}}\left[\mathrm{E}_{h_{u_2b_0}}\left[\exp\left(-sP_u h_{u_2b_0} {d_{(2)}}^{-\alpha}\right)\right]|d_{(1)}=r_1\right]\\ &\overset{(a)}{=} \mathrm{E}_{d_{(2)}}\left[\frac{1}{1+sP_u {d_{(2)}}^{-\alpha}}\,|d_{(1)}=r_1\right]\\ &\overset{(b)}{=} \int_{r_1}^{R}\frac{1}{1+sP_u {r_2}^{-\alpha}}\frac{2r_2}{R^2-{r_1}^2}dr_2. \end{aligned} \tag{36}$$

Note that (a) follows the Laplace transform of random variable $h_{u_2b_0}$ which is exponentially distributed with unit mean and (b) follows the probability density function of $d_{(2)}$ conditioned on $d_{(1)} = r_1$.

Similarly, the Laplace transform of the intra-cluster interference of UE_2 conditioned on $d_{(2)} = r_2$, can be derived as follows:

$$\begin{aligned}\mathcal{L}^2_{intra}(s) &= \mathrm{E}\left[\exp\left(-sI^2_{intra}\right)\right]\\ &= \mathrm{E}_{d_{(1)}}\left[\frac{1}{1+sP_u {d_{(1)}}^{-\alpha}}\,|d_{(2)}=r_2\right]\\ &= \int_0^{r_2}\frac{2r_1}{{r_2}^2\left(1+sP_u {r_1}^{-\alpha}\right)}dr_1. \end{aligned} \tag{37}$$

Then, Lemma 1 can be derived by solve the integrals above.

APPENDIX B
PROOF OF LEMMA 2

We can write the Laplace transform of the inter-cluster interference as follows:

$$\begin{aligned}&\mathcal{L}^u_{inter}(s)\\ &= \mathrm{E}\left[\exp\left(-sI^u_{inter}\right)\right]\\ &= \mathrm{E}\left[\prod_{b\in\varphi_b\setminus b_0}\prod_{u\in\mathcal{N}^b}\mathrm{E}_{h_{bu}}\left[\exp\left(-sP_u h_{bu}\|\boldsymbol{x}+\boldsymbol{y}\|^{-\alpha}\right)\right]\right]\\ &\overset{(a)}{=} \mathrm{E}\left[\prod_{b\in\varphi_b\setminus b_0}\left(\mathrm{E}_y\left[\frac{1}{1+sP_u\|\boldsymbol{x}+\boldsymbol{y}\|^{-\alpha}}\right]\right)^2\right]\\ &\overset{(b)}{=} \exp\left[-\lambda_b\underbrace{\int_{\mathbb{R}^2}\left(1-\left(\mathrm{E}_y\left[\frac{1}{1+sP_u\|\boldsymbol{x}+\boldsymbol{y}\|^{-\alpha}}\right]\right)^2\right)dx}_{\mathcal{B}}\right] \end{aligned} \tag{38}$$

where (a) follows the Laplace transform of random variable h_{ub} which is exponentially distributed with unit mean, (b) follows from the PGFL of PPP since all cluster centers follow a homogeneous PPP [40]. Let $u = \|\boldsymbol{x}+\boldsymbol{y}\|$ denotes the distance from the representative BS to a UE at other cluster, $v = \|\boldsymbol{x}\|$ denotes the distance from the representative BS to the other BS, $\mathcal{B}$ in (b) can be further expressed as

$$\mathcal{B} = 2\pi\int_0^\infty\left(1-\left(\int_u\frac{1}{1+sP_u u^{-\alpha}}f_U(u|v)\,du\right)^2\right)vdv \tag{39}$$

where $f_U(u|v)$ can be attained in [41] as:

when (i) $v \geq R$, $v-R \leq u \leq R+v$; (ii) $v < R$, $R-v \leq u \leq R+v$,

$$f_U(u|v) = \frac{u}{R^2} - \frac{2u}{\pi R^2}\sin^{-1}\left(\frac{v^2-R^2+u^2}{2uv}\right), \tag{40}$$

when (i) $v < R$, $0 \leq u \leq R-v$,

$$f_U(u|v) = \frac{2u}{R^2}. \tag{41}$$

Therefore, the Laplace transform of the inter-cluster interference can be given as Lemma 2.

APPENDIX C
PROOF OF LEMMA 3

We first derive the probability density functions of $d_{(1)}$ and $d_{(2)}$. Considering the independent random variables d_1 and d_2, it can be ordered as $\{d_{(1)}, d_{(2)}\}$ where $d_{(1)} < d_{(2)}$. Then, the probability density functions of $d_{(1)}$ and $d_{(2)}$ can be derived as

$$\begin{aligned}f_{d(1)}(r) &= \frac{\mathrm{d}\left(1-\mathrm{P}\left(\min(d_1,d_2)>r\right)\right)}{\mathrm{d}r}\\ &= \frac{4r}{R^2}\left(1-\frac{r^2}{R^2}\right), \quad r<R \end{aligned} \tag{42}$$

and

$$\begin{aligned}f_{d(2)}(r) &= \frac{\mathrm{d}\left(\mathrm{P}\left(\max(d_1,d_2)<r\right)\right)}{\mathrm{d}r}\\ &= \frac{4r^3}{R^4}, \quad r<R. \end{aligned} \tag{43}$$

Substituting (4) into (6), the coverage probability of UE_1 is given by

$$\begin{aligned}p_{u,1} &= \mathrm{P}\left(\frac{P_u h_{u_1b_0} {d_{(1)}}^{-\alpha}}{I^1_{intra}+I^u_{inter}+\delta^2} > 2^{R_b}-1\right)\\ &= \exp\left(-\frac{{d_{(1)}}^\alpha\left(2^{R_b}-1\right)\left(I^1_{intra}+I^u_{inter}+\delta^2\right)}{P_u}\right)\\ &= \int_0^R\exp\left(-\delta^2 c_1\right)\mathcal{L}^1_{intra}(c_1)\,\mathcal{L}^u_{inter}(c_1)f_{d(1)}(r_1)\,dr_1, \end{aligned} \tag{44}$$

where $c_1 = {P_u}^{-1}\left(2^{R_b}-1\right){r_1}^\alpha$. Similarly, the coverage probability of UE_2 can also be derived.

APPENDIX D
PROOF OF LEMMA 4

Let z denotes two-dimensional vector from Eve to the represent BS, y denotes two-dimensional vector from typical UE to serving BS. The Laplace transform of the inter-cluster interference of the detrimental Eve can be written as follows:

$$\begin{aligned}
&\mathcal{L}^{e}_{\text{inter}}(s)\\
&= \mathrm{E}\left[\exp\left(-sI^{e}_{\text{inter}}\right)\right]\\
&= \mathrm{E}\left[\prod_{b\in\varphi_b\setminus b_0}\prod_{u\in\mathcal{N}^b}\mathrm{E}_{h_{bu}}\left[\exp\left(-sP_u h_{bu}\|z+y\|^{-\alpha}\right)\right]\right]\\
&\overset{(a)}{=} \exp\left[-\lambda_b\int_{\mathbb{R}^2}\left(1-\left(\mathrm{E}_y\left[\frac{1}{1+sP_u\|z+y\|^{-\alpha}}\right]\right)^2\right)dz\right]\\
&\overset{(b)}{\leq} \exp\left[-\lambda_b\underbrace{\int_{\mathbb{R}^2}\left(1-\mathrm{E}_y\left[\frac{1}{\left(1+sP_u\|z+y\|^{-\alpha}\right)^2}\right]\right)dz}_{\mathcal{A}}\right]
\end{aligned} \tag{45}$$

where (a) follows from the PGFL of Matern cluster process [27] and (b) follows Jensen inequality $\mathrm{E}_y[a]^b \leq \mathrm{E}_y\left[a^b\right], b \geq 1$. Substituting m for $\|z+y\|$, $\mathcal{A}$ can be expressed as

$$\begin{aligned}
\mathcal{A} &= \int_{\mathbb{R}^2} f_Y(y)\int_{\mathbb{R}^2}\left[1-\left(\frac{m^\alpha}{sP_u+m^\alpha}\right)^2\right]dmdy\\
&\overset{c}{=} (sP_u)^{\frac{2}{\alpha}}\int_{\mathbb{R}^2}\left[1-\left(\frac{n^\alpha}{1+n^\alpha}\right)^2\right]dn\\
&\overset{d}{=} 2\pi(sP_u)^{\frac{2}{\alpha}}\int_0^\infty\frac{t^{-\frac{2}{\alpha}}}{(1+t)^3}dt\\
&\overset{e}{=} 2\pi(sP_u)^{\frac{2}{\alpha}}B\left(1-\frac{2}{\alpha},2+\frac{2}{\alpha}\right).
\end{aligned} \tag{46}$$

Note that (c) is derived by substituting $(sP_u)^{\frac{1}{\alpha}}n$ for m and $(sP_u)^{\frac{2}{\alpha}}$ in (c) is due to the two dimensional integral. (d) is derived by performing integral by parts and (e) follows the definition of the Beta function.

APPENDIX E
PROOF OF LEMMA 7

Let $I^{e}_{f/b_0} = \sum_{b\in\varphi_b\setminus b_0}P_n h_{bb_0}\|e-b\|^{-\alpha}$, $I_{b_0} = P_n h_{eb_0}\|e-b_0\|^{-\alpha}$, thus $I^{e}_{f} = I_{b_0} + I^{e}_{f/b_0}$. Substituting (31) into (17) and using the same approach in Lemma 5, we can express SOP for the most detrimental eavesdropper as follows:

$$\begin{aligned}
&p_{so}\\
&= P\left(\max_{e\in\varphi_e}\frac{P_u h_{ue} {r_e}^{-\alpha}}{I^{e}_{\text{inter}}+I^{e}_{f/b_0}+I_{b_0}+\delta^2} > 2^{R_b-R_s}-1\right)\\
&= 1-\exp\left(-2\pi\lambda_e\right.\\
&\quad\left.\times\int_0^\infty\underbrace{P\left(\frac{P_u h_{ue} {r_e}^{-\alpha}}{I^{e}_{\text{inter}}+I^{e}_{f/b_0}+I_{b_0}+\delta^2} > 2^{R_b-R_s}-1\right)}_{\mathcal{D}} r_e dr_e\right)
\end{aligned} \tag{47}$$

Using the same way as (38), $\mathcal{D}$ can be calculate as

$$\mathcal{D} = \exp\left(-c_e\delta^2\right)\mathcal{L}^{e}_{\text{inter}}(c_e)\,\mathcal{L}^{e}_{f/b_0}(c_e)\,\mathcal{L}^{e}_{b_0}(c_e) \tag{48}$$

where $c_e = \left(2^{R_b-R_s}-1\right){P_u}^{-1}{r_e}^{\alpha}$. Then, $\mathcal{L}^{e}_{b_0}(c_e)$ and $\mathcal{L}^{e}_{f/b_0}(c_e)$ can be calculate as:

$$\begin{aligned}
&\mathcal{L}^{e}_{b_0}(c_e)\\
&= E\left[\exp\left(-c_e I_{b_0}\right)\right]\\
&= E\left[\frac{1}{1+c_e P_n\left(r^2+{r_e}^2-2rr_e\cos\theta\right)^{-\alpha/2}}\right]\\
&= \frac{1}{\pi R^2}\int_0^{2\pi}\int_0^R\frac{r}{1+c_e P_n\left(r^2+{r_e}^2-2rr_e\cos\theta\right)^{-\frac{\alpha}{2}}}drd\theta
\end{aligned} \tag{49}$$

$$\begin{aligned}
&\mathcal{L}^{e}_{f/b_0}(c_e)\\
&= E\left[\exp\left(-c_e I^{e}_{f}\right)\right]\\
&= E\left[\prod_{b\in\varphi_b\setminus b_0}E_{h_{eb}}\left[\exp\left(-c_e P_n h_{eb}\|b-e\|^{-\alpha}\right)\right]\right]\\
&= \exp\left(-\pi\lambda_b(c_e P_n)^{2/\alpha}\Gamma\left(1+\frac{2}{\alpha}\right)\Gamma\left(1-\frac{2}{\alpha}\right)\right)
\end{aligned} \tag{50}$$

Substituting (46), (47) and (48) into (45), Lemma 7 can be derived.

REFERENCES

[1] K. Zheng, F. Hu, W. Wang, W. Xiang, and M. Dohler, "Radio resource allocation in LTE-Advanced cellular networks with M2M communications," *IEEE Commun. Mag.*, vol. 50, no. 7, pp. 184–192, Jul. 2012.

[2] D. Zhang, Z. Zhou, S. Mumtaz, J. Rodriguez, and T. Sato, "One integrated energy efficiency proposal for 5G IoT communications," *IEEE Internet Things J.*, vol. 3, no. 6, pp. 1346–1354, Dec. 2016.

[3] M. Shirvanimoghaddam *et al.*, "Massive non-orthogonal multiple access for cellular IoT: Potentials and limitations," *IEEE Commun. Mag.*, vol. 55, no. 9, pp. 55–61, Sep. 2017.

[4] M. R. Palattella *et al.*, "Internet of Things in the 5G era: Enablers, architecture, and business models," *IEEE J. Sel. Areas Commun.*, vol. 34, no. 3, pp. 510–527, Mar. 2016.

[5] Z. Zhang, H. Sun, R. Q. Hu, and Y. Qian, "Stochastic geometry based performance study on 5G non-orthogonal multiple access scheme," in *Proc. IEEE GLOBECOM*, Dec. 2016, pp. 1–6.

[6] D. Zhang, Y. Liu, Z. Ding, Z. Zhou, A. Nallanathan, and T. Sato, "Performance analysis of non-regenerative massive-MIMO-NOMA relay systems for 5G," *IEEE Trans. Commun.*, vol. 65, no. 11, pp. 4777–4790, Nov. 2017.

[7] Y. Endo, Y. Kishiyama, and K. Higuchi, "Uplink non-orthogonal access with MMSE-SIC in the presence of inter-cell interference," in *Proc. Int. Symp. Wireless Commun. Syst.*, 2012, pp. 261–265.

[8] H. Tabassum, M. S. Ali, E. Hossain, M. J. Hossain, and I. K. Dong. (2016). "Non-orthogonal multiple access (NOMA) in cellular uplink and downlink: Challenges and enabling techniques." [Online]. Available: https://arxiv.org/abs/1608.05783

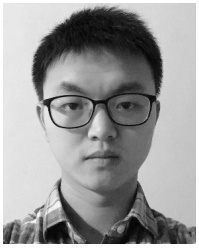
[9] X. Xu, W. Yang, Y. Cai, and S. Jin, "On the secure spectral-energy efficiency tradeoff in random cognitive radio networks," *IEEE J. Sel. Areas Commun.*, vol. 34, no. 10, pp. 2706–2722, Oct. 2016.

[10] S. Zhang, J. Peng, K. Huang, X. Xu, and Z. Zhong, "Physical layer security in IoT: A spatial-temporal perspective," in *Proc. Wireless Commun. Signal Process.*, Nanjing, China, Dec. 2017, pp. 1–6.

[11] Y. Zhang, Y. Shen, H. Wang, J. Yong, and X. Jiang, "On secure wireless communications for IoT under eavesdropper collusion," *IEEE Trans. Autom. Sci. Eng.*, vol. 13, no. 3, pp. 1281–1293, Jul. 2016.

[12] D. Chen, W. Yang, J. Hu, Y. Cai, and X. Tang, "Energy-efficient secure transmission design for the internet of things with an untrusted relay," *IEEE Access*, vol. 6, pp. 11862–11870, 2018.

[13] Q. Xu, P. Ren, H. Song, and Q. Du, "Security enhancement for IoT communications exposed to eavesdroppers with uncertain locations," *IEEE Access*, vol. 4, pp. 2840–2853, 2016.
[14] B. He, Y. She, and V. K. N. Lau, "Artificial noise injection for securing single-antenna systems," *IEEE Trans. Veh. Technol.*, vol. 66, no. 10, pp. 9577–9581, Oct. 2017.
[15] L. Hu *et al.*, "Cooperative jamming for physical layer security enhancement in Internet of Things," *IEEE Internet Things J.*, vol. 5, no. 1, pp. 219–228, Feb. 2018.
[16] X. Lai, J. Xia, M. Tang, H. Zhang, and J. Zhao, "Cache-aided multiuser cognitive relay networks with outdated channel state information," *IEEE Access*, vol. 6, pp. 21879–21887, 2018.
[17] J. Xia *et al.*, "Cache aided decode-and-forward relaying networks: From the spatial view," *Wireless Commun. Mobile Comput.*, vol. 2018, nos. 3–4, 2018, Art. no. 5963584.
[18] A. Mukherjee, "Physical-layer security in the Internet of Things: Sensing and communication confidentiality under resource constraints," *Proc. IEEE*, vol. 103, no. 10, pp. 1747–1761, Oct. 2015.
[19] Y. Zhang, H.-M. Wang, Q. Yang, and Z. Ding, "Secrecy sum rate maximization in non-orthogonal multiple access," *IEEE Commun. Lett.*, vol. 20, no. 5, pp. 930–933, May 2016.
[20] B. He, A. Liu, N. Yang, and V. K. N. Lau, "On the design of secure non-orthogonal multiple access systems," *IEEE J. Sel. Areas Commun.*, vol. 35, no. 10, pp. 2196–2206, Oct. 2017.
[21] Z. Ding, Z. Zhao, M. Peng, and H. V. Poor, "On the spectral efficiency and security enhancements of NOMA assisted multicast-unicast streaming," *IEEE Trans. Commun.*, vol. 65, no. 7, pp. 3151–3163, Jul. 2017.
[22] 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 Trans. Wireless Commun.*, vol. 16, no. 3, pp. 1656–1672, Mar. 2017.
[23] G. Gomez, F. J. Martin-Vega, F. J. Lopez-Martinez, Y. Liu, and M. Elkashlan. (2017). "Physical layer security in uplink NOMA multi-antenna systems with randomly distributed eavesdroppers." [Online]. Available: https://arxiv.org/abs/1709.04693
[24] *Study on Downlink Multiuser Superposition Transmission for LTE*, document, 3rd Generation Partnership Project, Mar. 2015.
[25] Z. Zhang and R. Q. Hu, "Uplink non-orthogonal multiple access with fractional power control," in *Proc. IEEE Wireless Commun. Netw. Conf. (WCNC)*, Mar. 2017, pp. 1–6.
[26] Z. Zhang, H. Sun, and R. Q. Hu, "Downlink and uplink non-orthogonal multiple access in a dense wireless network," *IEEE J. Sel. Areas Commun.*, vol. 35, no. 12, pp. 2771–2784, Dec. 2017.
[27] H. Tabassum, E. Hossain, and M. J. Hossain, "Modeling and analysis of uplink non-orthogonal multiple access in large-scale cellular networks using poisson cluster processes," *IEEE Trans. Commun.*, vol. 65, no. 8, pp. 3555–3570, Aug. 2017.
[28] Y. J. Chun, M. O. Hasna, and A. Ghrayeb, "Modeling heterogeneous cellular networks interference using Poisson cluster processes," *IEEE J. Sel. Areas Commun.*, vol. 33, no. 10, pp. 2182–2195, Oct. 2015.
[29] H.-M. Wang, T.-X. Zheng, J. Yuan, D. Towsley, and M. H. Lee, "Physical layer security in heterogeneous cellular networks," *IEEE Trans. Commun.*, vol. 64, no. 3, pp. 1204–1219, Mar. 2016.
[30] X. Zhou, R. K. Ganti, J. G. Andrews, and A. Hjørungnes, "On the throughput cost of physical layer security in decentralized wireless networks," *IEEE Trans. Wireless Commun.*, vol. 10, no. 8, pp. 2764–2775, Aug. 2011.
[31] T. X. Zheng, H. M. Wang, J. Yuan, Z. Han, and M. H. Lee, "Physical layer security in wireless Ad Hoc networks under a hybrid full-/half-duplex receiver deployment strategy," *IEEE Trans. Wireless Commun.*, vol. 16, no. 6, pp. 3827–3839, Jun. 2017.
[32] O. Arnold, F. Richter, G. Fettweis, and O. Blume, "Power consumption modeling of different base station types in heterogeneous cellular networks," in *Proc. Future Netw. Mobile Summit*, Florence, Italy, Jun. 2010, pp. 1–8.
[33] M. Duarte, C. Dick, and A. Sabharwal, "Experiment-driven characterization of full-duplex wireless systems," *IEEE Trans. Wireless Commun.*, vol. 11, no. 12, pp. 4296–4307, Dec. 2012.
[34] D. W. K. Ng, E. S. Lo, and R. Schober, "Dynamic resource allocation in MIMO-OFDMA systems with full-duplex and hybrid relaying," *IEEE Trans. Commun.*, vol. 60, no. 5, pp. 1291–1304, May 2012.
[35] T. Riihonen, S. Werner, and R. Wichman, "Hybrid full-duplex/half-duplex relaying with transmit power adaptation," *IEEE Trans. Wireless Commun.*, vol. 10, no. 9, pp. 3074–3085, Sep. 2011.
[36] G. Zheng, I. Krikidis, J. Li, A. P. Petropulu, and B. Ottersten, "Improving physical layer secrecy using full-duplex jamming receivers," *IEEE Trans. Signal Process.*, vol. 61, no. 20, pp. 4962–4974, Oct. 2013.
[37] G. Chen, Y. Gong, P. Xiao, and J. A. Chambers, "Physical layer network security in the full-duplex relay system," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 3, pp. 574–583, Mar. 2015.
[38] T.-X. Zheng, H.-M. Wang, Q. Yang, and M. H. Lee, "Safeguarding decentralized wireless networks using full-duplex jamming receivers," *IEEE Trans. Wireless Commun.*, vol. 16, no. 1, pp. 278–292, Jan. 2017.
[39] B. P. Day, A. R. Margetts, D. W. Bliss, and P. Schniter, "Full-duplex MIMO relaying: Achievable rates under limited dynamic range," *IEEE J. Sel. Areas Commun.*, vol. 30, no. 8, pp. 1541–1553, Sep. 2012.
[40] S. N. Chiu, D. Stoyan, W. S. Kendall, and J. Mecke, *Stochastic geometry and Its Applications*, 3rd ed. New York, NY, USA: Wiley, 2013.
[41] F. Adelantado, J. Pérez-Romero, and O. Sallent, "Nonuniform traffic distribution model in reverse link of multirate/multiservice WCDMA-based systems," *IEEE Trans. Veh. Technol.*, vol. 56, no. 5, pp. 2902–2914, Sep. 2007.



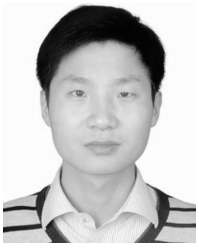
SHUAI ZHANG received the B.E. degree in communication engineering from Wuhan University, Wuhan, China, in 2016. He is currently pursuing the M.S. degree with the National Digital Switching System Engineering and Technological Research Center, China. His major research interests include physical-layer security and Internet of Things.

XIAOMING XU (S'13) received the B.S. and Ph.D. degrees in communication engineering from the College of Communications Engineering, PLA University of Science and Technology, Nanjing, China, in 2011 and 2016, respectively. He is currently an Assistant Research Fellow with the National Digital Switching System Engineering and Technological Research Center, Zhengzhou, China. His research interests include stochastic geometry, cooperative communications, and physical-layer security of wireless communications.

HUIMING WANG (S'07–M'10–SM'16) received the B.S. and Ph.D. degrees in electrical engineering from Xi'an Jiaotong University, Xi'an, China, in 2004 and 2010, respectively. From 2007 to 2008, and 2009 to 2010, he was a Visiting Scholar at the Department of Electrical and Computer Engineering, University of Delaware, USA. He is currently a Full Professor with Xi'an Jiaotong University. His research interests include 5G communications and networks, physical-layer security of wireless communications, and covert communications.

He has co-authored the book *Physical Layer Security in Random Cellular Networks* (Springer, 2016) and has authored or co-authored over 120 IEEE journal and conference papers. Nine of his papers are the ESI Highly Cited papers and one is ESI Hot Paper. He received the National Excellent Doctoral Dissertation Award in China in 2012 and the Best Paper Award from the IEEE/CIC International Conference on Communications in China in 2014. He is currently an Associate Editor of the IEEE TRANSACTIONS ON COMMUNICATIONS and the IEEE ACCESS.

JIANHUA PENG received the M.S. degree in computer application from the National Digital Switching System Engineering and Technological Research Center in 1995. He is currently a Professor and a Doctoral Supervisor and also a Deputy Chief Engineer with the National Digital Switching System Engineering and Technological Research Center, China. His major research interests include network switching and wireless mobile communication.



DI ZHANG (M'17) has been an Assistant Professor with Zhengzhou University, Zhengzhou, China in 2017. He was a Visiting Researcher with Seoul National University, Seoul, South Korea from 2017 to 2018. He has engaged in two international projects in wireless communications and networking funded by the European FP-7, H2020. His research interests include V2X, vehicle communications, and 5G and signal processing. He served as a TPC Member for the IEEE ICC, WCNC, PIMRC, VTC, and CCNC. He served as the Guest Editor for the IEEE NETWORK, the IEEE ACCESS, the *IET Intelligent Transport Systems*.

KAIZHI HUANG received the Ph.D. degree in communication and information system from Tsinghua University, Beijing, China. She is currently a Professor and a Supervisor of postgraduate student with the National Digital Switching System Engineering and Technological Research Center, China. She is also a Leader of the Wireless Mobile Communication Innovation Technology Team. Her major research interests include wireless mobile communication network and information secrecy.