Hindawi
Wireless Communications and Mobile Computing
Volume 2018, Article ID 4359261, 11 pages
https://doi.org/10.1155/2018/4359261

Research Article

On the Secrecy Capacity of 5G New Radio Networks

Ke Xiao, Shaowei Zhang, and Yunhua He

School of Computer Science and Technology, North China University of Technology, Beijing 100144, China

Correspondence should be addressed to Ke Xiao; zehan_xiao@163.com

Received 30 November 2017; Accepted 2 April 2018; Published 7 May 2018

Academic Editor: Gui-Ling Sun

The new radio technology for the fifth-generation wireless system has been extensively studied all over the world. Specifically, the air interface protocols for 5G radio access network will be standardized by the 3GPP in the coming years. In the next-generation 5G new radio (NR) networks, millimeter wave (mmWave) communications will definitely play a critical role, as new NR air interface (AI) is up to 100 GHz just like mmWave. The rapid growth of mmWave systems poses a variety of challenges in physical layer (PHY) security. This paper investigates those challenges in the context of several 5G new radio communication technologies, including multiple-input multiple-output (MIMO) and nonorthogonal multiple access (NOMA). In particular, we introduce a ray-tracing (RT) based 5G NR network channel model and reveal that the secrecy capacity in mmWave band widely depends on the richness of radio frequency (RF) environment through numerical experiments.

1. Introduction

Cellular mobile network has been arranged for several years. In the past, this kind of networks was designed to mainly facilitate a specific service, while other services were always supported as by-products (e.g., Internet browsing and Internet of Things deployment). However, many applications are urgently needed in the coming decades, to name a few, driverless car and intelligent transportation system. In order to make these emerging applications offering more convenience for people's lives, a significant shift is needed in the development of fifth-generation (5G) mobile networks [1].

Instead of simply increasing the data rates to improve the transmission efficiency, the International Telecommunication Union Radiocommunications Standardization Sector (ITU-R) has announced multiple design goals of 5G mobile networks [2], which include strong security, ultrahigh reliability, ultralow latency, extreme data rates, and extreme capacity. In order to achieve these design goals, the 3rd-Generation Partnership Project (3GPP) launched a canonical work plan in 2016, which is the beginning of 5G NR.

Due to the successful development of a large number of advanced techniques in current generation 3GPP standard [3], the 5G system is expected to consist of a number of 5G, including the 4G LTE and new NR AIs at carrier frequencies from below 1 GHz up to 100 GHz (e.g., mmWave) [4]. To meet the challenging service demands and related key performance indicators (KPIs), a highly flexible design of 5G AI is needed; we therefore are driving technology innovation to mobilize mmWave.

MmWave communication will play a key role in the next-generation 5G new radio networks. MmWave generally corresponds to the band of spectrum between frequencies of 30 GHz and 300 GHz, with the wavelength ranging from 1 to 10 millimeters. Unlike traditional sub-6 GHz frequency bands, mmWave bands have plenty available chunks, which suffer from additional high path loss though [5]. Moreover, mmWave has other merits, including limited intercell interference, low transmission latency, and improved security. As a result, it has been adopted by some commercial standards, for example, IEEE 802.11ad.

MmWave is intensively investigated by academia, standard organizations, regulatory commissions, and industry. Many researchers have remarked that, as a key enabler of 5G new radio communication, mmWave infrastructure poses new security challenges, particularly in PHY. PHY security has attracted enormous attention from researchers, since Wyner proposed a new type of channel named wiretap channel in 1975. Wiretap channel formulates a PHY model, where

a transmitter (Alice) communicates with a legitimate receiver (Bob) menaced by an eavesdropper (Eve) [6]. Wyner, the developer of wiretap channel, justified that a perfect secure communication can be achieved at a nonzero rate, referred to as secrecy rate, if Bob's channel condition overweighs Eve's [7].

Previous study of PHY security usually concentrated on large-scale MIMO. MIMO was introduced to achieve the best tradeoff between energy efficiency (EE) and spectral efficiency (SE) [8]. Reducing circuit power helps to improve EE in the low SE area while introducing more antennas benefits the EE in the high SE area. Using a given number of antennas, the optimal number of transceivers can maximize each SE value. When taking security into account, MIMO optimization becomes an even more complex problem, which considers three metrics, EE, SE, and secrecy capacity [9].

MmWave technology is a burgeoning technology that offers multi-Gbps wireless connectivity to electronic devices in short distance. Compared to lower frequencies, mmWave makes the RF environment too complicated to handle secrecy capacity using MIMO channel matrix [10]. For example, in urban area, a channel can easily have hundreds of rays, making channel matrix too large to calculate. To overcome this challenge, researchers apply RT models to solve mmWave propagation problems. A survey of current propagation modeling tools shows that RT has been a backbone of many of these tools because of its less reliance on computer memory and the ability to solve the three-dimensional problems on modern desktop computers [11]. When RT is concerned, determining the ray type from a point source to a field point in an urban setting is not a simple task, but a hot research topic since the 1990s [12]. For example, in [13], site-specific models based on two-ray models were developed for real-time prediction of the received power from waves propagating through urban street canyons. These models are used to predict small-area average received power for radio communication in urban environment. The RT method, on the other hand, is based on the high frequency regime to solve Maxwell's equations ray optics [14]. The RT method is a generic propagation modeling tool that provides estimation of path loss, arrival/departure angle, and delays [15].

The ray concept becomes valid in mmWave communications; thus we can formulate the mmWave propagation using several mechanisms. Imagine that many rays are emitted from the point source. Consider one of the rays and according to the behavior of this ray we can perform the security analysis profoundly [16].

To study the secrecy capacity of mmWave systems, we depend on the correlation matrix to reflect the relevance of legitimate receiver's rays and eavesdropper's rays. Moreover, the RF environment decides the elements of correlation matrix. In our proposed 5G new radio network architecture, we have considered two propagation environments, with rich RF and poor RF, respectively. In rich RF setup, such as urban area, the distribution of buildings is very dense; thus the eavesdroppers will receive more paths and have more correlations. In poor RF setup, such as rural area, the distribution of the buildings is sparse; thus the eavesdroppers will receive less paths and have less correlations.

The rest of the paper is organized as follows. We first introduce the different mmWave propagation mechanisms and 5G mmWave wiretap channel in Section 2. We then analyze the secrecy capacity of 5G new radio communication systems in different RF environments in Section 3. Section 4 presents a variety of simulation setups and justifies the system security performance that we have derived. Finally, Section 5 concludes the paper.

2. Ray-Tracing Channel Model for mmWave Security

Ray-tracing channel model is an effective way to formulate mmWave system. In particular, the rays are generated based on the following four phenomena.

Direct Rays. This ray is also called line of sight (LoS), where a ray goes from the source to the destination directly.

Reflected and Transmitted Rays. A reflected (transmitted) ray corresponds to the reflection (transmission) of mmWave at interfaces between different mediums [17].

Diffracted Rays. In this case, one incident ray can spawn many diffracted rays. A typical example is the diffraction from a wedge that results in a continuum cone of rays.

Scattering. A general physical process where some forms of mmWave radiation are forced to deviate from a straight trajectory by one or more paths due to localized nonuniformities in the medium through which they pass [18].

The wavelength of mmWave is short enough to mimic the propagation characteristic of light. As a result, the phenomenon of reflection, diffraction, and scattering often comes at the same time in 5G new radio networks. As shown in Figure 1, the RF environment of city is more complex than rural and venues, with more transmission paths.

As a trend of 5G new radio network research, ray-tracing model has been recently used to derive mmWave path loss and perform multidimensional channel characterization. The higher operating frequency makes the ray optics approximations less intense and allows for unprecedented accuracy. When designing the radio interface of 5G new radio communication systems, ray-tracing model goes often in combination with measurements.

Ray tracing is considered to be the best model to help design future short-range, mmWave wireless systems. The most critical part of ray tracing is to predict the rays from a source to a destination. The simplest case is for the free space, where only one ray passes through a straight line from the source to the destination. A more complicated scenario is an urban environment, where there may exist many rays from a source location to a receiving point, with each ray undergoing different number of reflections, diffractions, or scattering.

At each transmitter and receiver link, there will be several effect rays which have different departure and arrival angles [19], and the path loss is just calculated from the path loss and the phase of all effective rays.

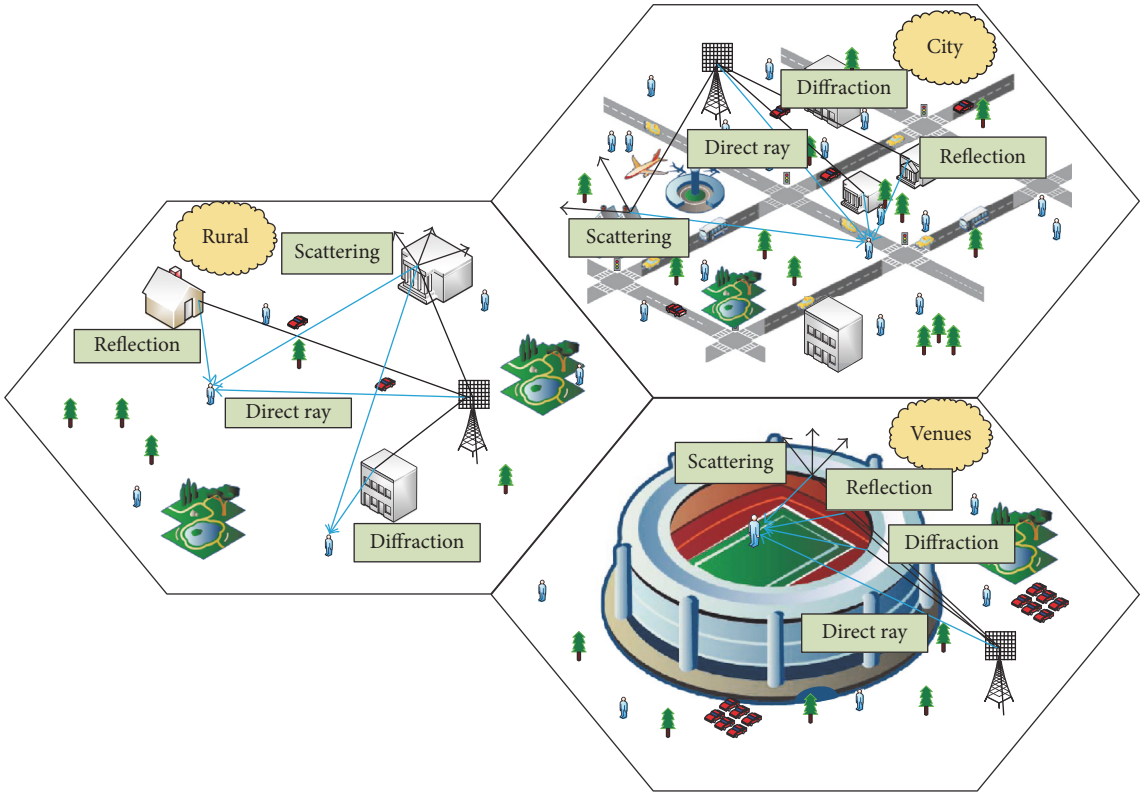

FIGURE 1: Different mmWave propagation environment.

Direction of arrival of the mth subpath of the nth cluster at building ($\theta_{n,m,\mathrm{AoA}}$) is given as

$$\theta_{n,m,\mathrm{AoA}} = \theta_{\mathrm{building}} + \delta_{n,\mathrm{AoA}} + \Delta_{n,m,\mathrm{AoA}}, \quad (1)$$

where $\theta_{\mathrm{building}}$ is the line-of-sight (LoS) angle between building and BS, $\delta_{n,\mathrm{AoA}}$ is the AoA of the main path, and $\Delta_{n,m,\mathrm{AoA}}$ is the offset angle of the mth subpath.

Direction of departure at the BS ($\theta_{n,m,\mathrm{AoD}}$) is given as

$$\theta_{n,m,\mathrm{AoD}} = \theta_{\mathrm{BS}} + \delta_{n,\mathrm{AoD}} + \Delta_{n,m,\mathrm{AoD}}, \quad (2)$$

where θ_{BS} is the LoS angle between BS and building, $\delta_{n,\mathrm{AoD}}$ is the angle of departure (AoD) of the main path, and $\Delta_{n,m,\mathrm{AoD}}$ is the offset angle of the mth subpath.

Path Loss Fitting Method and Shading Fading. In order to better understand the specific path loss, we use two kinds of fitting models based on the data measurement [19]: one is called "floating intercept model" which is expressed as follows:

$$\overline{\mathrm{PL}(d)} = \alpha + 10\beta \log_{10}(d) + \mathrm{SF}, \quad (3)$$

where α is the intercept and β is the path loss exponent and SF is the lognormal shadowing. In general, the floating intercept and the path loss exponent are extracted by the least square method to fit the measurement data.

$$\sum_{i,j} \left[P\left(d_{i,j}\right) - \overline{\mathrm{PL}\left(d_{i,j}\right)} \right]^2, \quad (4)$$

where i and j are the transmitter and receiver index. This model is difficult to give physical meaning, but it can provide the minimum SF standard deviation of the existing measurement data. The disadvantage of this model is that the distance extension beyond the measurement range is limited and requires a large number of samples. Shadow fading (SF) is the measured standard deviation of path loss and estimated path loss.

$$\mathrm{SF} = \sqrt{\frac{1}{N-1} \sum_{i,j} \left(\mathrm{PL}_{i,j} - \overline{\mathrm{PL}_{i,j}} \right)^2}, \quad (5)$$

where N is the transmitter and receiver link number.

Another is close-in-reference method as follows:

$$P_r\,(\mathrm{dBm}) = P_0\,(\mathrm{dBm}) - 10n \log\left(\frac{d}{d_0}\right) + \mathrm{SF}, \quad (6)$$

where P_0 is the path loss at reference distance d_0 and n is the path loss exponent. Valid d should be larger than far-field distance of the transmitter antenna.

For a smooth surface, the reflected wave is coherent with the incident wave and is calculated by the means of reflection coefficient. If the surface becomes slightly rough, this specular component decays due to the scattering in all directions. This effect is caused by a reduction factor.

$$\chi = \exp\left(-2k^2 \Delta h_0^2 \cos^2 \theta_i\right), \quad (7)$$

where k is the wavenumber, Δh_0 is the standard deviation of surface height, and θ_i is the incidence angle. Hence, the specular reflected power can be expressed as follows:

$$P_{\text{ref}} = P_T \left(\frac{\lambda}{4\pi}\right)^2 \frac{G_T G_R}{(s+s')^2} R^2 \chi^2, \tag{8}$$

where P_T is the transmitted power, s is the path length between the transmitter and reflection point, s' is the path length between the reflection point and receiver, R is the Fresnel reflection coefficient, and G_T and G_R are the transmitter/receiver antenna gains.

We can suppose a reasonable command. The usual length of the brick wall is on the order of a few centimeters and the diffuse power is scattered in all directions θ_s, with ϕ_s denoting the angle between the planes of incidence and scattering, and can be calculated as

$$P_{\text{ref}} = P_T \left(\frac{\lambda}{4\pi}\right)^2 \int_S \frac{\sigma_{\text{sca}} G_T G_R}{4\pi r r'} ds, \tag{9}$$

where r is the path length between transmitter and surface s, r' is the path length between surface s and receiver, and σ_{sca} is the scattering cross section per unit area of rough surface, which can be estimated using the Kirchhoff approximation.

For the study of mmWave physical layer security, most researchers consider ray-tracing model as a good candidate to assist as well. Due to their intrinsic capability to simulate multipath propagation, ray-tracing models can provide a multidimensional characterization of radio propagation for a variety of RF environment. Figure 2 illustrates a 5G new radio communication wiretap channel model, where the signal passes the legitimate channel to reach a receiver (Bob) and the illegitimate channel to reach an eavesdropper (Eve). $\mathbf{H}$, $\mathbf{G}$, $\mathbf{Z}$, $\mathbf{Z}_b$, and $\mathbf{Z}_e$ are legitimate receiver channel, eavesdropper channel, noise, legitimate receiver noise, and eavesdropper noise, respectively.

In typical wiretap channel model, the eavesdropper is located near to the legitimate receiver, which is a common case in low frequency. In 5G new radio networks, however, the eavesdropper could be far from the legitimate receiver as shown in the bottom of Figure 2. In this case, the rays go through the buildings and undergo scattering, diffraction, and reflection, before finally arriving at "Eve" and "Bob."

A more complicated scenario includes one legitimate receiver and multiple eavesdroppers. As we can see from Figure 2, there is a set of "Eve," and it demonstrates such an example in a rich RF environment. It will grow up to a huge menace, if multiple eavesdroppers can cooperatively steal the legitimate information.

3. Secrecy Capacity Analysis in mmWave RF Environment

3.1. Previous Works. Previously, the study of wiretap channel model is based on the traditional system model, with large-scale antenna arrays. The large space freedom provided by the large-scale antenna arrays can be used to improve the secrecy performance [20]. In physical layer security, in order to hide their presence, eavesdroppers (Eves) are usually considered to be passive, so that their channel state information (CSI) is unknown at both the transmitter (Alice) and the legitimate receiver (Bob). Therefore, it is advantageous to confuse the eavesdropper with generated artificial noise (AN) by using multiantenna techniques [21]. Specifically, in order to mask the information to be transmitted to Bob, AN radiates isotropically. If the perfect CSI between Alice and Bob can be used in Alice, then the AN can be made invisible to Bob while reducing the decoding performance of potentially eavesdroppers [22].

In order to better understand the traditional wiretap channel model, some formulas will be introduced [23]. Assuming that the access point is equipped with N antennas for downlink large-scale MIMO systems serving K single-antenna users, $N, K \in \mathbb{N}_+$, $N \geq K$. The channel model can be formulated as

$$\mathbf{G} = \mathbf{HD}, \tag{10}$$

where $\mathbf{G} = [\mathbf{g}_1, \mathbf{g}_2, \ldots, \mathbf{g}_K]$ represents the channel matrix and $\mathbf{D} = \text{diag}\{\sqrt{\beta_1}, \sqrt{\beta_2}, \ldots, \sqrt{\beta_K}\}$ is the large-scale propagation matrix.

In the mutual coupling channel model, $\mathbf{H} = [\mathbf{H}_1, \mathbf{H}_2, \ldots, \mathbf{H}_K]$ denotes the fast fading matrix, and the vector $\mathbf{H}_k \in \mathbb{C}^{1\times N}$ $(k = 1, 2, \ldots, K)$ is described by the following [24]:

$$\mathbf{H}_k = \mathbf{Z}\mathbf{R}_k\mathbf{v}_k, \tag{11}$$

where $\mathbf{R}_k$ is the steering matrix and $\mathbf{v}_k$ denotes the Gaussian stochastic factor. $\mathbf{Z} \in \mathbb{C}^{N\times N}$ is the constant mutual coupling matrix related to antenna configuration in the form of

$$\mathbf{Z} = (Z_A + Z_L)(\mathbf{\Gamma} + Z_L\mathbf{I})^{-1}, \tag{12}$$

where

$$\mathbf{\Gamma} = \begin{bmatrix} Z_A & Z_M & 0 & \cdots & 0 \\ Z_M & Z_A & Z_M & \cdots & 0 \\ 0 & Z_M & Z_A & \cdots & 0 \\ \vdots & \vdots & \ddots & \ddots & \vdots \\ 0 & 0 & \cdots & Z_M & Z_A \end{bmatrix}. \tag{13}$$

The complex value of Z_L, Z_A, and Z_M denotes the load impedance, antenna impedance, and mutual impedance, respectively.

However, many natural as well as man-made factors make the propagation very random in both time and space; microwave, optical, and acoustic waves are good examples; they will be scattered by atmospheric turbulence, rain, fog, vegetation, snow, biological media, and composite materials [25]. These fluctuations may affect communications, identification, and remote-sensing of objects to some extent through these media.

Therefore, the phenomenon of reflection, diffraction, and scattering often come at the same time in 5G new radio networks. Because of the complexity of the propagation environment, it is definitely easier for eavesdroppers to catch the

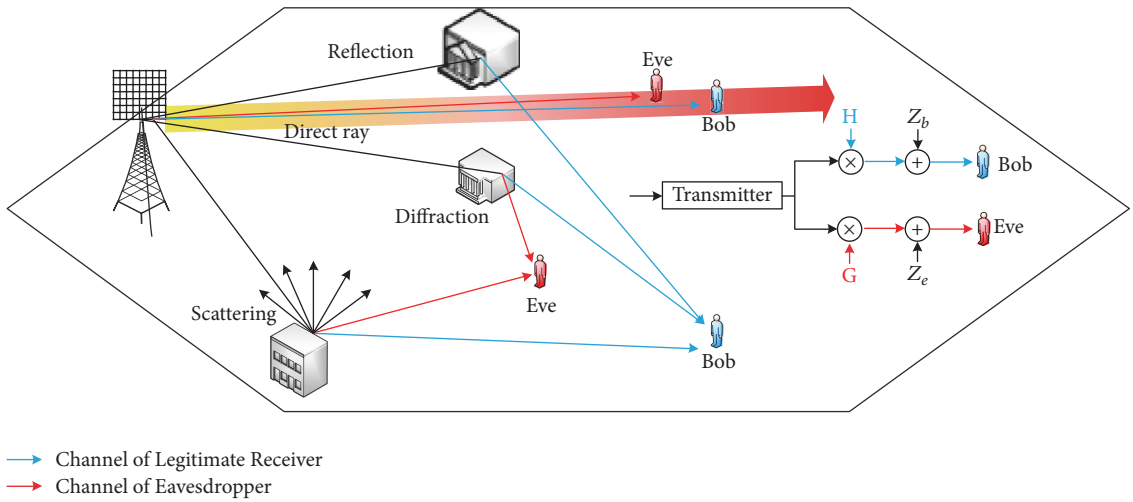

Figure 2: The wiretap channel model in 5G new radio networks.

transmission paths. Thereby in 5G new radio networks, the study based on the channel matrix will be inaccurate, but the ray-based study will lead to more prepared conclusions and results.

3.2. The Concept of Correlation Matrix. In our analysis, capacity refers to the transmission paths that are received by legitimate receiver without considering eavesdroppers, and the secrecy capacity refers to the paths that are received in consideration of eavesdroppers. And those paths which are received by both legitimate receiver and eavesdroppers can be called "shared path," which is the main reason for the decrease of security capacity. And we define the channel matrix generated by the shared paths as the "correlation matrix."

We can suppose a rectangular antenna array scenario [23]; the kth user has A_k different azimuths of arrival (AoAs) and elevations of arrival (EoAs). The ith azimuth of arrival (AoA) and the ith elevation of arrival (EoA) of the kth user are written as $\theta_{k,i}$ and $\phi_{k,i}$, respectively. Then the column steering vectors in $\mathbf{R}_k = [\mathbf{r}_{k,1}, \mathbf{r}_{k,2}, \ldots, \mathbf{r}_{k,A_k}]$ is described by

$$\begin{aligned}\mathbf{r}_{k,l} = \frac{1}{A_k} \times \mathrm{vec}\left[\mathbf{a}\left(\theta_{k,l}\right) \otimes \mathbf{a}\left(\phi_{k,l}\right)^T\right] = \frac{1}{A_k} \times \mathrm{vec}\left\{\left[1,\right.\right. \\ e^{(j2\pi d/\lambda)\sin\theta_{k,l}}, e^{(j2\pi d/\lambda)2\sin\theta_{k,l}}, \ldots, e^{(j2\pi d/\lambda)(N-1)\sin\theta_{k,l}}\Big] \\ \otimes \left[1, e^{(j2\pi d/\lambda)\sin\phi_{k,l}}, e^{(j2\pi d/\lambda)2\sin\phi_{k,l}}, \ldots,\right. \\ \left.\left. e^{(j2\pi d/\lambda)(N-1)\sin\phi_{k,l}}\right]\right\},\end{aligned} \tag{14}$$

where $\otimes$ is the Kronecker product of matrices and the vec$(\cdot)$ function represents vectorization of matrix.

As shown in Figure 3, the transmitter has N transmit antennas in this system, the receivers have M receiving antennas, and $M < N$. We assume that there are K legitimate receivers, J eavesdroppers, and $M = K + J$.

$$\mathbf{G}_{\mathbf{M\times N}} = \left[\mathbf{h}_1, \mathbf{h}_2, \ldots, \mathbf{h}_K, \mathbf{g}_1, \mathbf{g}_2, \ldots, \mathbf{g}_J\right]^T, \tag{15}$$

where $\mathbf{G}_{\mathbf{M\times N}}$ represents the channel matrix of the system, where $\mathbf{h}_k$ $(k = 1, 2, \ldots, K)$ is the kth legitimate receiver, and $\mathbf{g}_j$ $(j = 1, 2, \ldots, J)$ is the jth eavesdropper.

$$\mathbf{h}_\mathrm{k} = \left[\mathbf{h}_{k,1} + \mathbf{h}_{k,2} + \cdots + \mathbf{h}_{k,I}\right]^T, \tag{16}$$

besides, $\mathbf{h}_{k,i}$ $(i = 1, 2, \ldots, I)$ represents the channel vector of the ith ray of the kth legitimate receiver, and $\mathbf{g}_{j,i}$ $(i = 1, 2, \ldots, I)$ represents the channel vector of the ith ray of the jth eavesdropper.

$$\mathbf{g}_j = \left[\mathbf{g}_{j,1} + \mathbf{g}_{j,2} + \cdots + \mathbf{g}_{j,I}\right]^T. \tag{17}$$

We can define as follows: $\mathbf{h}$, $\mathbf{g}$, and $\mathbf{f} = \{\mathbf{h} \cap \mathbf{g}\}$ denote a set of legitimate receiver channel matrices, a set of eavesdropping channel matrices, and a set of correlation matrices, respectively. The set of new legitimate receiver channel vectors and new eavesdropper channel vectors are as follows:

$$\begin{aligned}\check{\mathbf{h}} &= \mathrm{sum}\left\{\mathbf{h} - \mathbf{f}\right\}, \\ \check{\mathbf{g}} &= \mathrm{sum}\left\{\mathbf{g} - \mathbf{f}\right\}.\end{aligned} \tag{18}$$

The correlation matrix is

$$\mathbf{G}_f = \mathbf{H}_f \mathbf{D}_f, \tag{19}$$

where $\mathbf{G}_f = [\mathbf{f}_1, \mathbf{f}_2, \ldots, \mathbf{f}_L]$ with $\mathbf{f}_l$ $(l = 1, 2, \ldots, L)$ is the correlation vector of the lth shared path, $\mathbf{H}_f = [\mathbf{h}_1, \mathbf{h}_2, \ldots, \mathbf{h}_L]$ is the fast fading matrix, and $\mathbf{D}_f = \mathrm{diag}\{\sqrt{\beta_1}, \sqrt{\beta_2}, \ldots, \sqrt{\beta_L}\}$ is the large-scale propagation matrix.

The correlation vector is

$$\mathbf{h}_l = \mathbf{R}_l \mathbf{v}_l, \quad (l = 1, 2, \ldots, L), \tag{20}$$

where $\mathbf{R}_l \in \mathbb{C}^{N\times D_l}$ contains D_l steering vectors with different AoAs for the lth user and $\mathbf{v}_l$ denotes the Gaussian stochastic factor.

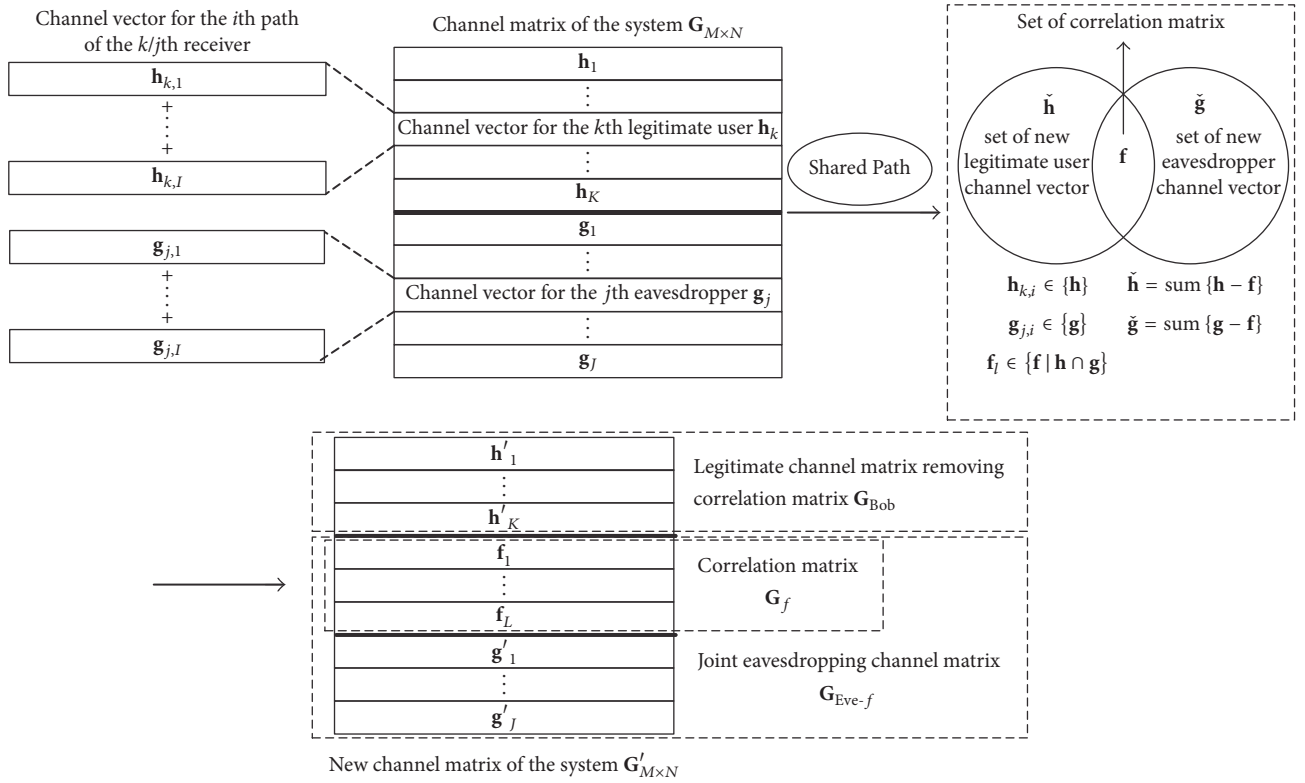

Figure 3: The formation process for correlation matrix.

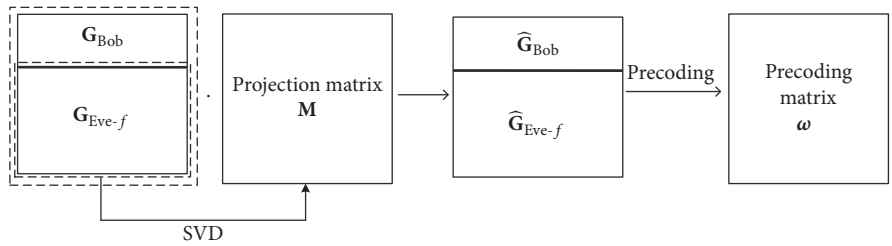

Figure 4: The formation process for projection matrix $\mathbf{M}$, mapping and precoding.

When the rectangular antenna array is assumed at the BS, the steering matrix $\mathbf{R}_l$ can be written as

$$\mathbf{R}_l = \frac{1}{D_l} \times \text{vec}\left[\mathbf{a}\left(\theta_{l,i}\right) \otimes \mathbf{a}\left(\phi_{l,i}\right)^T\right], \tag{21}$$

where $\theta_{l,i}$ is the ith AoA of the lth user and the steering vector $\mathbf{a}(\theta_{l,i})$ is given as

$$\mathbf{a}\left(\theta_{l,i}\right) = \left[1, e^{(j2\pi d/\lambda)\sin\theta_{l,i}}, e^{(j2\pi d/\lambda)2\sin\theta_{l,i}}, \ldots, e^{(j2\pi d/\lambda)(N-1)\sin\theta_{l,i}}\right], \tag{22}$$

and $\phi_{l,i}$ is the ith EoA of the lth user and the steering vector $\mathbf{a}(\phi_{l,i})$ is given as

$$\mathbf{a}\left(\phi_{l,i}\right) = \left[1, e^{(j2\pi d/\lambda)\sin\phi_{l,i}}, e^{(j2\pi d/\lambda)2\sin\phi_{l,i}}, \ldots, e^{(j2\pi d/\lambda)(N-1)\sin\phi_{l,i}}\right], \tag{23}$$

where d is the distance between the adjacent antennas and λ is the carrier wavelength.

The new channel matrix is

$$\mathbf{G}'_{M\times N} = \left[\mathbf{h}'_1, \ldots, \mathbf{h}'_K, \mathbf{f}_1, \ldots, \mathbf{f}_L, \mathbf{g}'_1, \ldots, \mathbf{g}'_J\right]^T, \tag{24}$$

where $\mathbf{h}'_k$ $(k = 1, 2, \ldots, K)$, $\mathbf{f}_l$ $(l = 1, 2, \ldots, L)$, and $\mathbf{g}'_j$ $(j = 1, 2, \ldots, J)$ represent the new channel vector of the kth legitimate receiver, the correlation vector of the lth shared path, and the new channel vector of the jth eavesdropper.

3.3. Projection Matrix. We implement the null-space method in the system. To eliminate the eavesdropping signal of the eavesdroppers, we propose a projection matrix and we can explain the process for obtaining projection matrix $\mathbf{M}$, mapping and precoding, as shown in Figure 4.

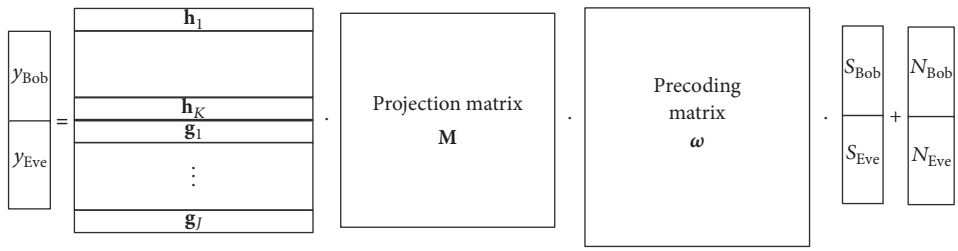

Figure 5: The signal transmission process in 5G new radio networks.

The joint eavesdropping channel matrix $\mathbf{G}_{\text{Eve-}f} = [\mathbf{f}_1, \ldots, \mathbf{f}_L, \mathbf{g}'_1, \ldots, \mathbf{g}'_J]^T$. To calculate $\mathbf{M}$ by singular value decomposition (SVD) [26], the projection matrix is derived from the following equations:

$$\begin{aligned} \mathbf{G}_{\text{Eve-}f} &= \mathbf{U}_{\text{Eve-}f} \boldsymbol{\Lambda}_{\text{Eve-}f} \mathbf{V}_{\text{Eve-}f}, \\ \mathbf{M} &= \mathbf{V}^0_{\text{Eve-}f} \left(\mathbf{V}^0_{\text{Eve-}f}\right)^H, \end{aligned} \tag{25}$$

where $\mathbf{U}_{\text{Eve-}f} \in \mathbb{C}^{N \times N}$, $\boldsymbol{\Lambda}_{\text{Eve-}f} \in \mathbb{C}^{N \times (K-K_m)}$, and $\mathbf{V}_{\text{Eve-}f} \in \mathbb{C}^{(K-K_m) \times (K-K_m)}$ are SVD factor matrices. $\mathbf{V}^0_{\text{Eve-}f} \in \mathbb{C}^{(K-K_m) \times N}$ is a subspace of column vector space of $\mathbf{V}_{\text{Eve-}f}$. By multiplying $\mathbf{M}$ and precoding, the precoding matrix ω is shown in Figure 4.

3.4. 5G New Radio Network Signal Transmission Process. Figure 5 illustrates that the eavesdropping signal is cancelled by the full view of entire system, which is equivalent to system formula in equation. After manipulation, eavesdropping signals can be eliminated from eavesdroppers and shared paths to ensure the security of transmission.

$$\begin{aligned} \mathbf{Y} &= \mathbf{GM}\boldsymbol{\omega}\mathbf{S} + \mathbf{N}, \\ \mathbf{N} &= \left[\mathbf{N}_{\text{Bob}}, \mathbf{N}_{\text{Eve}}\right]^T, \\ \mathbf{S} &= \left[\mathbf{s}_{\text{Bob}}, \mathbf{s}_{\text{Eve}}\right]^T, \\ \mathbf{G} &= \mathbf{G}_{M \times N}, \\ \mathbf{Y} &= \left[\mathbf{y}_{\text{Bob}}, \mathbf{y}_{\text{Eve}}\right]^T. \end{aligned} \tag{26}$$

After the receiving signal has been processed by the projection matrix $\mathbf{M}$ and precoding matrix $\boldsymbol{\omega}$, we can get the expecting result, where $\mathbf{Y}$ demonstrates the receiving signal of the transmitted signal $\mathbf{S}$ and $\mathbf{N}$ denotes the White Gaussian noise.

According to the investigation of the wiretap channel model above, it is easy to notice that correlation matrix has a lot to do with secrecy capacity. However, sometimes the correlation matrix can be largely affected by the RF environment. For example, in a rich RF environment, like urban area, the distribution of buildings is more complex; thus the eavesdroppers will be more likely to receive more paths, and there will be more correlations. However, in a poor RF environment, like rural area, the distribution of the buildings is monotonous; thus the eavesdroppers will less likely to receive paths, and there will be less correlations.

3.5. The Different RF Environment In 5G New Radio Networks. As shown in Figure 6, the signal passes the legitimate channel to reach a receiver and the illegitimate channel to reach an eavesdropper, and these related rays that are received by both can be called "correlation matrix." We simulated the urban area here; there are massive eavesdroppers and more buildings, and these eavesdroppers can be called "distributed deployment." The more the buildings here are, the more the rays can be received, not only for legitimate receiver, but also for eavesdroppers. As a result, these eavesdroppers can form a cluster, and each terminal has a few paths of the legitimate receiver, and the more the paths are, the more the paths can cooperate to decode the information.

Figure 7 simulates the rural area; there are only two ordinary houses and still a lot of eavesdroppers. Because the distribution of the buildings is not so complicated, thereby only two eavesdroppers can receive the paths, and there will be less correlation matrix here.

As a result, we can get the conclusion from our proposed 5G new radio network architecture. In urban area, the distribution of buildings is more complex, then the legitimate receiver will receive more paths, and the capacity of the receiver will become larger. At the same time, the probability of capturing the shared paths for the eavesdroppers will increase, and the growth is also reflected in the correlation matrix, which will lead to the decrease of the secrecy capacity of urban area. However, in rural area, the distribution of buildings is monotonous, then the legitimate receiver will get less paths, and normally the capacity of receiver will become smaller. For the eavesdroppers, they have less opportunities to get shared paths, and the elements of correlation matrix will decrease accordingly.

4. Simulation Result

As mmWave can provide multi-Gbps wireless connectivity for electronic devices, it has gradually become a burgeoning technology. However, mmWave makes the RF environment too complicated to deal with the secrecy capacity. Thus, using traditional massive MIMO channel matrix based on mmWave is not feasible any more. Based on our study of correlation matrix, the ray-tracing method is a generic propagation modeling tool which can provide estimates of path loss, arrival/departure angles, and time delay. Thereby, the ray-based study will lead to more prepared results.

As for the complexity for theoretical analysis of the capacity and the nonclosed form solution of the result,

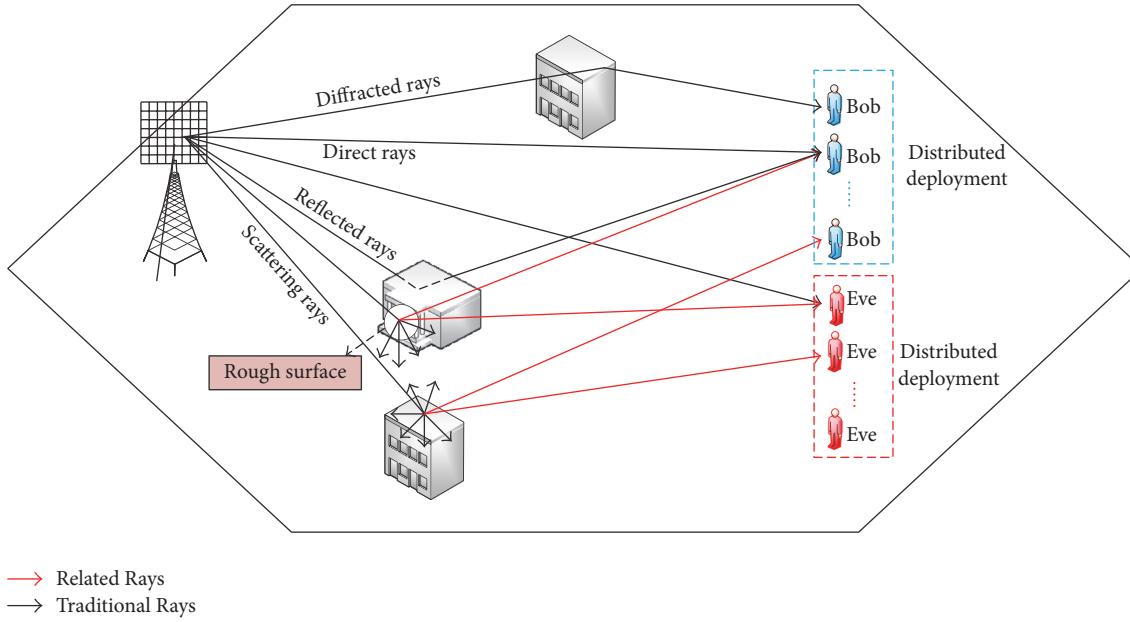

Figure 6: Ray-tracing channel model for physical layer security in urban area.

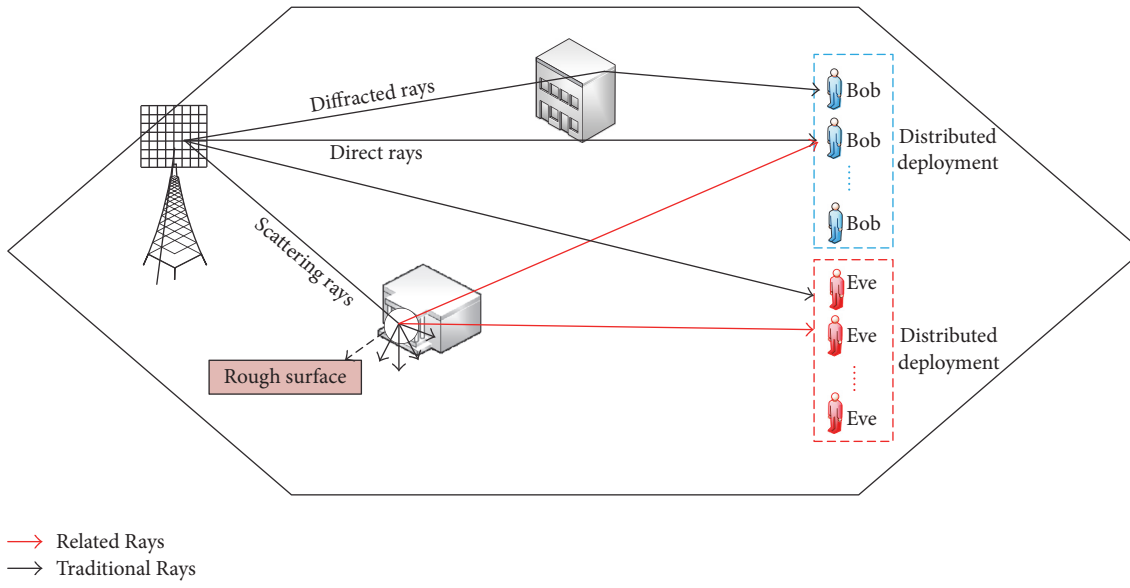

Figure 7: Ray-tracing channel model for physical layer security in rural area.

simulation is used to describe the feasibility of our proposed method.

We evaluate the performance of the proposed ray-tracing based 5G new radio communication channel model separately using MATLAB simulation. The simulation parameters are shown in Table 1.

4.1. Analysis of Each Capacity for Urban Area. In Figure 8, the impact of the number of eavesdroppers on each capacity of urban area is investigated. It is observed that the security capacity gradually decreased, and wiretap capacity gradually increased with the rising in the number of eavesdroppers. As the transmission paths that are received by legitimate receiver are certain, capacity is immutable.

Under the circumstance that the total number of legitimate receivers of urban area is fixed at 80, Figure 9 shows the trend of each capacity with the change of distance between eavesdroppers and legitimate receiver. As the distance goes farther, the probability of capturing the shared paths for eavesdroppers will decrease, and when the distance is far enough, no transmission paths can be received, which reflects zero wiretap capacity in the figure. In contrast, secrecy capacity will be relatively increased, and it will be equal to the capacity finally.

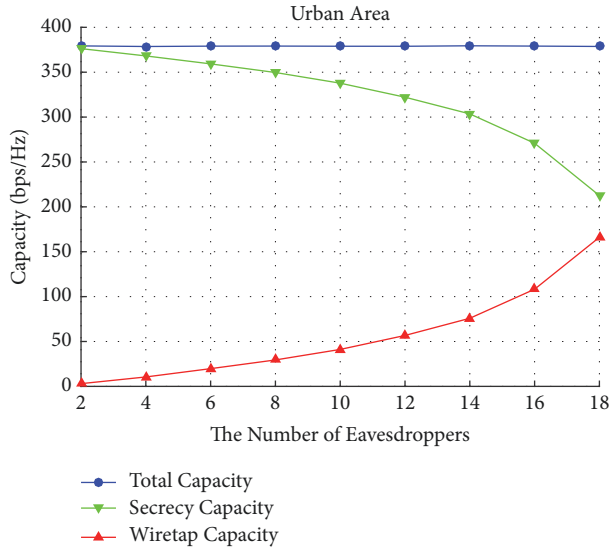

Figure 8: Impact of the number of eavesdroppers on each capacity of urban area.

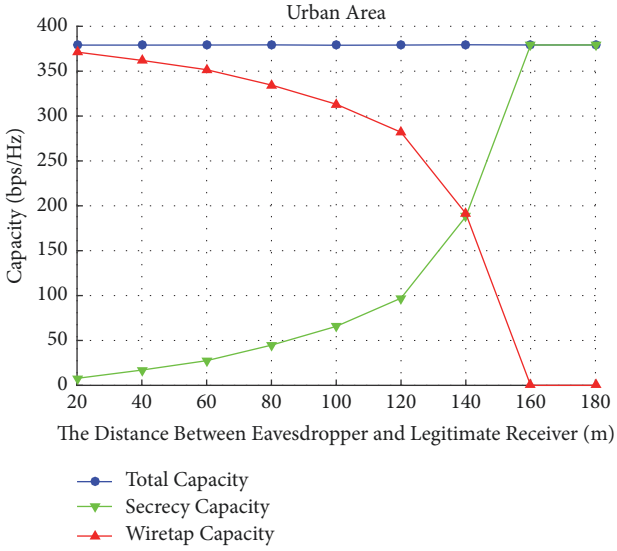

Figure 9: Impact of the distance between eavesdropper and legitimate receiver on each capacity of urban area.

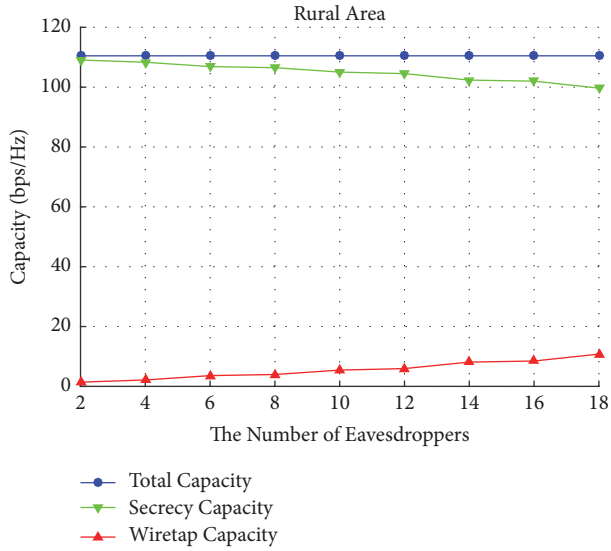

Figure 10: Impact of the number of eavesdroppers on each capacity of rural area.

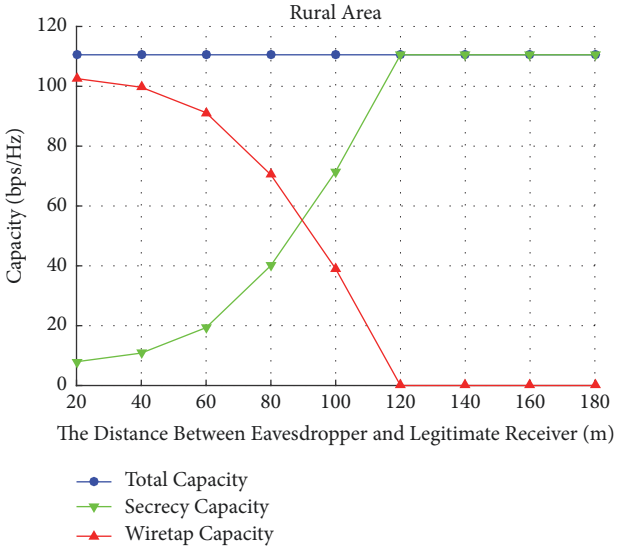

Figure 11: Impact of the distance between eavesdropper and legitimate receiver on each capacity of rural area.

4.2. Analysis of Each Capacity for Rural Area. Figure 10 illustrates the trend of capacity in rural area. As the distribution of buildings is monotonous, less transmission paths can be received; thus the trend in Figure 10 is less pronounced, but, with the increase in the number of eavesdroppers, the secrecy capacity and the wiretap capacity also showed stable changes.

Compared to Figure 8, as the complexity of rural area is lower than that of urban area, the shared paths of rural are less than that of urban area, which means that the secrecy capacity in rural area will not fall as much as that of urban area.

As can be observed from Figure 11, the distance value which makes the secrecy capacity and the wiretap capacity tend to be constant is smaller. As the distribution of buildings is not complex in rural area, so when the distance reaches a marginal value, no transmission paths can be received by eavesdroppers, as the zero wiretap capacity shown in figure.

Compared to Figure 9, as the complexity of rural area is lower than that of urban area, the probability of catching shared paths for eavesdroppers is smaller. Thus, under the condition of increasing the same distance, the wiretap capacity of rural area decreases more rapidly. On the other hand, the secrecy capacity of rural area increases more rapidly, and when the initial value is 20 meters, rural area has a certain secrecy capacity, while the secrecy capacity of urban area is almost zero.

Table 1: Simulation parameters.

Parameters	Values
Transmit antenna number	128
Legitimate receiver number (urban/rural)	80/30
Path number (urban/rural)	70/40
Eavesdropper number	2 to 18
Shared path obtain probability (urban/rural)	70%/20%
Distance between eavesdropper and legitimate user	20 to 180 m
Frequency	38 GHz
Tx/Rx antenna height	36/1.5 m
Tx/Rx antenna gain	25/13.3 dB
Scenario	Urban/rural area

5. Conclusion

This work develops a ray-tracing based security channel model for 5G new radio communications. In particular, we rely on the concept of correlation matrix to reflect the relevance of rays between legitimate receiver and eavesdroppers. As the RF environment decides the elements of correlation matrix, we investigate both rich RF environment, such as urban area, and poor RF environment, such as rural area in our proposed architecture, and if the RF environment is more complex, the eavesdroppers are more easily to obtain the correlation paths. Our simulation results indicate that the secrecy capacity reduces faster in urban area than in rural area with the growth of cooperative eavesdroppers. Besides, with the distance between eavesdropper and legitimate receiver increased, the secrecy capacity of both urban and rural area will increase but the rate of growth in urban area is less than that in rural area. In addition, when the distance reaches a certain value, the secrecy capacity and the total capacity in urban and rural area are consistent, and the capacity is equal to the sum of secrecy capacity and wiretap capacity.

Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this paper.

Acknowledgments

This work is supported by the National Key R&D Program of China under Grant 2017YFB0802300.

References

[1] S.-Y. Lien, S.-L. Shieh, Y. Huang, B. Su, Y.-L. Hsu, and H.-Y. Wei, "5G New Radio: Waveform, Frame Structure, Multiple Access, and Initial Access," *IEEE Communications Magazine*, vol. 55, no. 6, pp. 64–71, 2017.

[2] ITU-R Rec: ITU-R M, "IMT Vision - Framework and Overall Objectives of the Future Development of IMT for 2020 and Beyond," 2015.

[3] H. Miao and M. Faerber, "Physical Downlink Control Channel for 5G New Radio," *IEEE EuCNC*, pp. 1–5, June 2017.

[4] C. Kilinc, J. F. Monserrat, M. C. Filippou et al., "New radio 5G user plane design alternatives: One 5G air interface framework supporting multiple services and bands," in *Proceedings of the 2016 IEEE Globecom Workshops, GC Wkshps 2016*, USA, December 2016.

[5] X. Ma, F. Yang, S. Liu, J. Song, and Z. Han, "Design and Optimization on Training Sequence for mmWave Communications: A New Approach for Sparse Channel Estimation in Massive MIMO," *IEEE Journal on Selected Areas in Communications*, vol. 35, no. 7, pp. 1486–1497, 2017.

[6] C. Wang and H.-M. Wang, "Physical layer security in millimeter wave cellular networks," *IEEE Transactions on Wireless Communications*, vol. 15, no. 8, pp. 5569–5585, 2016.

[7] Y. Zou and G. Wang, "Intercept Behavior Analysis of Industrial Wireless Sensor Networks in the Presence of Eavesdropping Attack," *IEEE Transactions on Industrial Informatics*, vol. 12, no. 2, pp. 780–787, 2016.

[8] D. Zhang, Z. Zhou, C. Xu, Y. Zhang, J. Rodriguez, and T. Sato, "Capacity Analysis of NOMA with mmWave Massive MIMO Systems," *IEEE Journal on Selected Areas in Communications*, vol. 35, no. 7, pp. 1606–1618, 2017.

[9] P. Krishna, T. A. Kumar, and K. K. Rao, "Multiuser MIMO systems: Spectral and energy efficiencies, estimations and capacity limits," in *Proceedings of the 2015 Twelfth International Conference on Wireless and Optical Communications Networks (WOCN)*, pp. 1–6, Bangalore, India, September 2015.

[10] M. Hashemi, C. E. Koksal, and N. B. Shroff, "Hybrid RF-mmWave communications to achieve low latency and high energy efficiency in 5G cellular systems," in *Proceedings of the 15th International Symposium on Modeling and Optimization in Mobile, Ad Hoc, and Wireless Networks, WiOpt 2017*, France, May 2017.

[11] S. Y. Lim, Q. P. Soo, A. Adam, D. W. G. Lim, Z. Yun, and M. F. Iskander, "Towards a comprehensive ray-tracing modeling of an urban city with open-trench drains for mobile communications," *IEEE Access*, vol. 5, pp. 2300–2307, 2017.

[12] Z. Yun and M. F. Iskander, "Ray tracing for radio propagation modeling: Principles and applications," *IEEE Access*, vol. 3, pp. 1089–1100, 2015.

[13] J. S. Lu, H. L. Bertoni, K. A. Remley, W. F. Young, and J. Ladbury, "Site-specific models of the received power for radio communication in urban street canyons," *IEEE Transactions on Antennas and Propagation*, vol. 62, no. 4, pp. 2192–2200, 2014.

[14] G.-Y. Wang, Y.-J. Liu, S.-D. Li, X.-J. Zhang, and Z.-P. Chen, "Study on the outdoor wave propagation at 28GHz by ray tracing method," in *Proceedings of the 9th International Conference on Microwave and Millimeter Wave Technology, ICMMT 2016*, pp. 476–478, China, June 2016.

[15] B. Ai, K. Guan, R. He et al., "On Indoor Millimeter Wave Massive MIMO Channels: Measurement and Simulation," *IEEE Journal on Selected Areas in Communications*, vol. 35, no. 7, pp. 1678–1690, 2017.

[16] E. M. Vitucci, F. Mani, and T. Mazloum, "Ray Tracing Simulations of Indoor Channel Spatial Correlation for Physical Layer Security," *IEEE EuCAP*, p. 1, April 2015.

[17] B. Lee, J.-B. Lim, C. Lim, B. Kim, and J.-Y. Seol, "Reflected self-interference channel measurement for mmwave beamformed full-duplex system," in *Proceedings of the IEEE Globecom Workshops, GC Wkshps 2015*, USA, December 2015.

[18] P. Pongsilamanee and H. L. Bertoni, "Specular and nonspecular scattering from building facades," *IEEE Transactions on Antennas and Propagation*, vol. 52, no. 7, pp. 1879–1889, 2004.

[19] S. Sasmal, S. Mishra, B. R. Behera, and S. Bandopadhaya, "Ray tracing channel model for millimeter-(mm-) wave systems," in *Proceedings of the 2016 International Conference on Advanced Communication Control and Computing Technologies, ICACCCT 2016*, pp. 281–284, India, May 2016.

[20] A. Hyadi, Z. Rezki, and M.-S. Alouini, "Secure Multiple-Antenna Block-Fading Wiretap Channels with Limited CSI Feedback," *IEEE Transactions on Wireless Communications*, vol. 16, no. 10, pp. 6618–6634, 2017.

[21] X. Mu, L. Guo, and C. Dong, "Downlink secure transmission with base station cooperation using artificial noise," in *Proceedings of the 2017 IEEE Wireless Communications and Networking Conference, WCNC 2017*, USA, March 2017.

[22] P. Mu, Z. Li, and B. Wang, "Secure On-Off Transmission in Slow Fading Wiretap Channel with Imperfect CSI," *IEEE Transactions on Vehicular Technology*, vol. 66, no. 10, pp. 9582–9586, 2017.

[23] K. Zheng, S. L. Ou, and X. F. Yin, "Massive MIMO channels: a survey," *International Journal of Antennas and Propagation*, vol. 2014, Article ID 848071, 10 pages, 2014.

[24] C. Masouros, M. Sellathurai, and T. Ratnarajah, "Large-scale MIMO transmitters in fixed physical spaces: the effect of transmit correlation and mutual coupling," *IEEE Transactions on Communications*, vol. 61, no. 7, pp. 2794–2804, 2013.

[25] M. Shaik, A. Kabanni, and N. Nazeema, "Millimeter wave propagation measurments in forest for 5G Wireless sensor communications," in *Proceedings of the 16th Mediterranean Microwave Symposium, MMS 2016*, UAE, November 2016.

[26] S. Sodagari, "On effects of imperfect channel state information on null space based cognitive MIMO communication," in *Proceedings of the 2015 International Conference on Computing, Networking and Communications, ICNC 2015*, pp. 438–444, USA, February 2015.