Covert Wireless Communication in IoT Network: From AWGN Channel to THz Band

Zhihong Liu, Jiajia Liu, *Member, IEEE,* Yong Zeng, and Jianfeng Ma

***Abstract*—Covert communication can prevent an adversary from knowing that a transmission has occurred between two users. In this paper, we consider covert wireless communications in an IoT network with dense deployment, where an IoT device experiences not only the background noise, but also the aggregate interference from other Tx devices. Our results show that, in a dense IoT network with lower frequency AWGN channels, when the distance between Alice and the adversary Willie $d_{a,w} = \omega(n^{1/(2\alpha)})$, Alice can reliably and covertly transmit $\mathcal{O}(\log_2 \sqrt{n})$ bits to Bob in n channel uses. In an IoT network with THz (Terahertz) Band, covert communication is more difficult because Willie can simply place a receiver in the narrow beam between Alice and Bob in order to detect or block their LOS communications. We demonstrated that covert communication is still possible in this occasion by utilizing the reflection or diffuse scattering from a rough surface. From the physical-layer security perspective, covert communication can enhance the security of IoT network from the bottom layer.**

***Index Terms*—Internet of Things; Physical-layer Security; Covert Communication; AWGN Channel; THz Band.**

I. Introduction

The Internet of Things (IoT) is dramatically changing our daily lives [1]. Meanwhile, security issue is becoming one of the primary tasks of IoT in the coming years [2][3][4]. Traditional cryptography methods for network security cannot solve all security problems. If a user wishes to communicate covertly (without being detected by other detectors), encryption to preventing eavesdropping is not enough [5]. Even if a message is encrypted, the metadata, such as network traffic pattern, can reveal some sensitive information [6]. In a battlefield, soldiers hope to hide their tracks so they need to communicate stealthy. Furthermore, if an adversary cannot detect the transmissions, he has no chance to launch the "eavesdropping and decoding" attack even if he has boundless computing and storage capabilities.

Covert communication at physical-layer has a long history. It is always related with "wireless steganography", i.e., hidden information is embedded into a cover signal to construct a covert channel, such as encoding information on top of the training sequences of WiFi [7], the cyclic prefix of WiFi OFDM symbols [8], or a dirty WiFi QPSK constellation [9]. In this paper, we consider physical-layer covert communication that employs the background noise and the aggregate interference in a dense IoT network to hide user's transmission attempts. Consider a scenario that a transmitter Alice would like to send a message to a receiver Bob covertly over a wireless channel in order to not being detected by a warden Willie. Alice can use the noise in the channel instead of the statistical properties of the cover signal to hide information. Seminal work of Bash *et al.* [10] initiated the research on how the covert throughput scales with n, the number of channel uses in AWGN channel. It is shown that using a pre-shared key between Alice and Bob, it is possible to transmit $\mathcal{O}(\sqrt{n})$ bits reliably and covertly to Bob over n channel uses such that Willie is not aware of the existence of the communication.

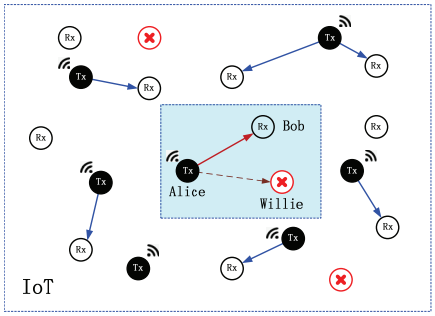


Fig. 1. System configuration of covert wireless communication in an IoT network with AWGN channels.

Since covert wireless communication can provide stronger security protection, significant effort in the last few years has been devoted to achieve covertness in various network settings. However, previous research works on covert wireless communication mainly focus on the covert throughout of a simple system model with a transmitter, a receiver, and a warden, while the performance of covert communication in noisy wireless networks remains largely unknown. This triggers a pertinent question: "Does the interference indeed affect the covert performance and how much benefit can Alice or Willie gain?" In this work, we consider covert communication in a dense IoT network with two kinds of wireless channel: lower frequency AWGN channel and THz (Terahertz) Band. AWGN channel is the standard model for a free-space RF channel. As depicted in Fig.1, although the noise is unpredictable to some extent, the aggregate interference in a noisy IoT network is more difficult to be predicted. In a dense IoT network with lower frequency AWGN channels, we found that covert communication is still possible. Alice can reliably and covertly transmit $\mathcal{O}(\log_2 \sqrt{n})$ bits in n channel uses when the distance between Alice and Willie $d_{a,w} = \omega(n^{1/(2\alpha)})$ (α is path loss

Zhihong Liu, Yong Zeng, and Jianfeng Ma are with the School of Cyber Engineering, Xidian University, Xi'an, 710071, China.

Jiajia Liu is with the School of Cybersecurity, Northwestern Polytechnical University, Xi'an, 710072, China.

Corresponding author Jiajia Liu, e-mail: liujiajia@nwpu.edu.cn

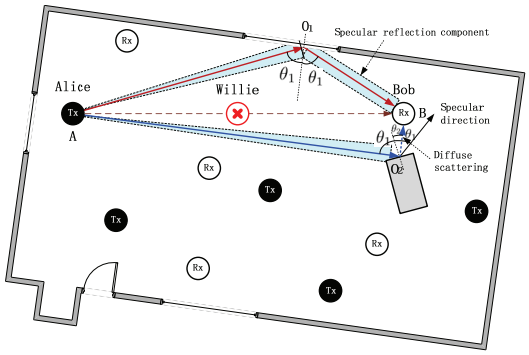


Fig. 2. Covert communication in a THz Band IoT network.

exponent).

Increasing demand for larger bandwidths for IoT network has turned the interest from lower frequency UHF (0.3-3GHz) towards higher frequencies, mmWaves (30-300GHz) [11] and THz Band (0.1-10THz)[12]. THz Band signals are often assumed to be more secure than lower frequency signals due to the more directional transmission and the more narrow beams. However this makes covert communication more difficult. In THz Band, Willie can simply place a receiver in the LOS (Line-of-Sight) path between Tx and Rx to find or block their communications. Hence Alice and Bob need resorting to the aggregate interference and the NLOS (Non-Line-of-Sight) communication to improve the security and hiding. In a THz Band IoT network, although the LOS communications can be detected easily by Willie, we found that the communication based on reflection or diffuse scattering is a feasible information hiding method. As depicted in Fig. 2, the communication via specular reflection $\overrightarrow{AO_1B}$ or diffuse scattering $\overrightarrow{AO_2B}$ can evade the detection. The scattering signals Willie eavesdropping are masked by the background noise and the aggregate interference in a dense IoT network.

II. Related Work

Bash, Goeckel, and Towsley's work [10] is the first work that puts information theoretic bound on covert wireless communication. A square root law is found over noisy AWGN channels and quantum channels [13]. In a different model, if Alice transmits only once in a long sequence of possible transmission slots and Willie does not know the time of transmission attempts, Alice can reliably transmit $\mathcal{O}(\min\{\sqrt{n\log(T(n))}, n\})$ bits to Bob with a slotted AWGN channel [14]. To improve the performance of covert communication, Lee *et al.* [15] found that, Willie has measurement uncertainty about its noise level due to the existence of SNR wall, then they obtained an asymptotic privacy rate which approaches a non-zero constant. Following Lee's work, He *et al.* [16] defined new metrics to gauge covertness of communication, and Liu *et al.* [17] took the interference measurement uncertainty into considerations.

In general, the covertness is due to the existence of noise, and Willie cannot accurately distinguish it from user's signals. Cooperative jamming is regarded as a prevalent physical-layer security approach [18][19] which can increase the measurement uncertainty of the adversary. Sobers *et al.* [20] utilized cooperative jamming to carry out covert communications. To achieve the transmission of $\mathcal{O}(n)$ bits covertly to Bob over n uses of channel, they added a "jammer" to the environment to help Alice for security objectives. Soltani *et al.* [21] considered a network scenario where multiple "friendly" nodes generate artificial noise to hide the transmission from multiple adversaries. He *et al.* [22] studied covert communication in wireless networks in which Bob and Willie are subject to uncertain shot noise from interferers.

In this paper we seek to understand what are the factors that affect the covert communication in a dense IoT network with AWGN or THz Band channels, and how much impact does the interference exactly has on covert communication.

III. System Models

A. AWGN Channel

1) Channel Model: Wireless channels are assumed to suffer from discrete-time AWGN with real-valued symbols. Alice transmits n real-valued symbols $\{s_i^{(a)}\}_{i=1}^n$. Bob observes a vector $\{y_i^{(b)}\}_{i=1}^n$, where $y_i^{(b)} = s_i^{(a)} + z_i^{(b)}$, and $z_i^{(b)}$ is the noise Bob experiences which can be expressed as $z_i^{(b)} = z_{i,0}^{(b)} + I_i^{(b)}$, $z_{i,0}^{(b)} \sim \mathcal{N}(0, \sigma_{b,0}^2)$ is the AWGN at Bob, $I_i^{(b)}$ is the aggregate interference Bob experiences. Similarly, Willie observes a vector $\{y_i^{(w)}\}_{i=1}^n$, and $z_{i,0}^{(w)} \sim \mathcal{N}(0, \sigma_{w,0}^2)$, $I_i^{(w)}$ are the AWGN and the aggregate interference at Willie in the i-th channel use, and $\sigma_{b,0}^2 = \sigma_{w,0}^2$.

Suppose each IoT device is equipped with an omnidirectional antenna. The wireless channel is modeled by the large-scale fading with path loss exponent α. The channel gain $\mathbf{h}_{i,j}$ from i to j is static over the signaling period, all links experience unit mean Rayleigh fading.

2) Network Model: Consider an IoT network with dense deployment, where the locations of transmitter Tx form a stationary Poisson point process (PPP) $\Pi = \{X_i\}$ on the plane $\mathbb{R}^2$ with the density λ. Suppose the transmit power employed for each Tx is a constant[1] P_t, the Euclidean distance between node i and node j is denoted as $d_{i,j}$. The aggregate interferences seen by Bob and Willie are the functional of the underlying PPP $\Pi = \{X_i\}$ and the channel gain

$$I_i^{(b)} \equiv \sum_{k\in\Pi} \sqrt{\frac{P_t}{d_{b,k}^{\alpha}}} \mathbf{h}_{b,k} \cdot s_i^{(k)} \sim \mathcal{N}(0, \sigma_{I_b}^2) \quad (1)$$

$$I_i^{(w)} \equiv \sum_{k\in\Pi} \sqrt{\frac{P_t}{d_{w,k}^{\alpha}}} \mathbf{h}_{w,k} \cdot s_i^{(k)} \sim \mathcal{N}(0, \sigma_{I_w}^2) \quad (2)$$

where $s_i^{(k)}$ is Gaussian random variable $\mathcal{N}(0,1)$ which represents the signal of k-th transmitter in i-th channel use, and

$$\sigma_{I_b}^2 = \sum_{k\in\Pi} \frac{P_t}{d_{b,k}^{\alpha}} |\mathbf{h}_{b,k}|^2 = \sum_{k\in\Pi} \frac{P_t}{d_{b,k}^{\alpha}} \Psi_{b,k} \quad (3)$$

$$\sigma_{I_w}^2 = \sum_{k\in\Pi} \frac{P_t}{d_{w,k}^{\alpha}} |\mathbf{h}_{w,k}|^2 = \sum_{k\in\Pi} \frac{P_t}{d_{w,k}^{\alpha}} \Psi_{w,k} \quad (4)$$

[1]Any other channel models with power control or threshold scheduling will have similar results with some scale factors.

are shot noise (SN) processes, representing the powers of the interference at Bob and Willie, respectively. $\Psi_{i,j} = |\mathbf{h}_{i,j}|^2$ is exponentially distributed with its mean $\mathbf{E}[\Psi_{i,j}] = 1$.

3) Hypothesis Testing: To find whether or not Alice is transmitting, Willie has to distinguish between the following two hypotheses

$$\mathbf{H_0} \quad : \quad y_i^{(w)} = I_i^{(w)} + z_{i,0}^{(w)} \tag{5}$$

$$\mathbf{H_1} \quad : \quad y_i^{(w)} = \sqrt{\frac{P_t}{d_{a,w}^{\alpha}}}\mathbf{h}_{a,w} \cdot s_i^{(a)} + I_i^{(w)} + z_{i,0}^{(w)} \tag{6}$$

based on the vector $\mathbf{y} = \{y_i^{(w)}\}_{i=1}^n$. Willie employs a radiometer as his detector and does the following statistic test

$$T(\mathbf{y}) = \frac{1}{n}\mathbf{y}^H\mathbf{y} = \frac{1}{n}\sum_{k=1}^{n} y_k^{(w)} * y_k^{(w)} \underset{\mathbf{H_1}}{\overset{\mathbf{H_0}}{\lessgtr}} \gamma \tag{7}$$

where γ is Willie's detection threshold.

Let $\mathbb{P}_{FA}$ and $\mathbb{P}_{MD}$ be the probability of false alarm and missed detection. Willie wishes to minimize his probability of error $\mathbb{P}_e^{(w)} = (\mathbb{P}_{FA} + \mathbb{P}_{MD})/2$, but Alice's objective is to guarantee that the average probability of error $\mathbf{E}[\mathbb{P}_e^{(w)}] = \mathbf{E}[\mathbb{P}_{FA} + \mathbb{P}_{MD}]/2 > 1/2 - \epsilon$ for any small positive ϵ.

B. THz Band

Next we briefly look into the THz Band model, network and blocking model, and rough surface scattering theory.

1) Channel Model [23]: Suppose each device in THz Band is equipped with a directional antenna, and the antenna radiation pattern is the cone model, i.e., a single cone-shaped beam, whose width determines the antenna directivity. The antenna gain G_k for the main lobe of device k is given by

$$G_k = \frac{2}{1 - \cos(\phi/2)} \tag{8}$$

where ϕ is the directivity angle of antenna.

When Alice transmits a message, the power of received signal at Bob is given by

$$P_{Rx} = A d_{a,b}^{-2} \exp(-K d_{a,b}) \tag{9}$$

where K is the overall absorption coefficient of the medium, $d_{a,b}$ is the distance between Alice and Bob, and

$$A = P_{Tx} G_{Tx} G_{Rx} \frac{c^2}{16\pi^2 f^2} = H G_{Tx} G_{Rx} \tag{10}$$

where P_{Tx} is the transmit power of Tx, G_{Tx} and G_{Rx} are the antenna gain of Tx and Rx, c is the speed of EM wave, and f is the operating frequency, $H = P_{Tx} c^2/(16\pi^2 f^2)$.

In addition to path loss, any receiver will suffer from Johnson-Nyquist noise generated by thermal agitation of electrons in conductors, which can be represented as

$$S_{JN}(f) = \frac{hf}{\exp(hf/k_B T) - 1} \tag{11}$$

where h is Planck's constant, k_B is Boltzmann constant, and T is the temperature in Kelvin.

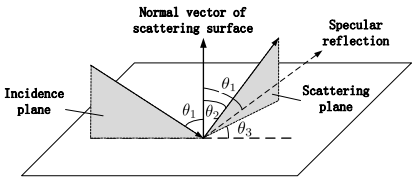


Fig. 3. The model of scattering at a rough surface.

2) Network and Blocking Model: In a dense THz Band IoT network, transmitters form a stationary PPP $\Pi = \{X_i\}$ with the density λ, receivers experience not only the noise, but also the aggregate interference from other transmitters. However, due to the directionality of antenna in THz Band, users themselves may act as blockers to interference. We use the blocking model proposed in [23] to analyze the aggregate interference. For any interferer located at a distance x from the receiver Bob, the blocking probability of the interference from this interferer can be estimated as follows

$$\mathbb{P}_B(x) = 1 - \exp[-\lambda(x - r_B) r_B] \tag{12}$$

where r_B is the blocker radius.

Besides, if Bob is not in the coverage of an interferer J, then J does not contribute to the aggregate interference at Bob. Given the antenna directivity angle ϕ, the probability that Bob is located in coverage of an interferer is

$$\mathbb{P}_C = \frac{\phi}{2\pi} \tag{13}$$

then the aggregate interference at Bob is

$$I_{THz}^{(b)} = A \sum_{i=1}^{\infty} \left[r_i^{-2} \exp(-K r_i) \cdot \mathbf{1}_{\{I_i > 0\}} \right] \tag{14}$$

where r_i is the distance between i-th interferer and Bob. $\mathbf{1}_{\{I_i>0\}}$ is an indicator function, $\mathbf{1}_{\{I_i>0\}} = 0$ if the signal from this interferer is blocked, or Bob's antenna directivity is not in coverage of this interferer, $\mathbf{1}_{\{I_i>0\}} = 1$ if Bob is interfered by i-th interferer, $\mathbb{P}\{\mathbf{1}_{\{I_i>0\}} = 1\} = \mathbb{P}_C(1 - \mathbb{P}_B)$.

3) Rough Surface Scattering Model: The general surface scattering model is shown in Fig. 3. A wave, which is incident on a rough surface under an angle θ_1, is scattered into the direction given by the angles θ_2 and θ_3. Kirchhoff scattering model [24] gives the expression of the scattering path gain, $G(f, \sigma_h, l_c, \theta_1, \theta_2, \theta_3)$, describing the scattered with respect to the incident power. In the expression of Kirchhoff approximation, parameters l_c (the surface correlation length) and σ_h (the standard deviation of surface height variation) describe the surface properties. Fig. 4 shows the path gain at $f = 500$GHz as a function of angles θ_1 and θ_2 with $\theta_3 = 0$.

4) Assessment Metric: To quantify the detection ability of Willie, we assess a normalized secrecy capacity [25], which relates the strength of Willie's signal to Bob's signal as follows

$$\bar{c}_s = \frac{\log(1 + SINR_B) - \log(1 + SINR_W)}{\log(1 + SINR_B)} \tag{15}$$

where $SINR_B$ and $SINR_W$ represent Bob and Willie's signal to interference plus noise ratio on linear scale, respectively. Given the reflecting path gain of Bob G_B and the

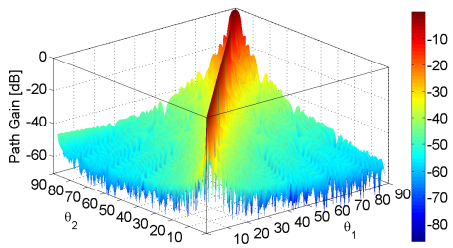


Fig. 4. Path gain at 500 GHz frequency as a function of angles θ_1 and θ_2. $\theta_1, \theta_2 = 0^\circ \cdots 90^\circ$ in steps of 1°, and θ_3 is set to 0°. The illuminated area is approximately 4cm^2, the surface correlation length $l_c = 0.1$mm, the surface height variation $\sigma_h = 0.01$mm.

scattering path gain of Willie G_W, $SINR_B$ and $SINR_W$ can be estimated as follows

$$SINR_B = \frac{Ad_{a,b}^{-2}\exp(-Kd_{a,b})\cdot G_B}{S_{JN}(f)+I_{THz}^{(b)}} \quad (16)$$

$$SINR_W = \frac{Ad_{a,w}^{-2}\exp(-Kd_{a,w})\cdot G_W}{S_{JN}(f)+I_{THz}^{(w)}} \quad (17)$$

The quantity $\bar{c}_s$ is a metric which can be used to assess the likelihood of a successful covert communication. If $\bar{c}_s$ is above a predefined threshold, we presume that covert communication is feasible. On the other hand, $SINR_W$ can also be used to quantify the Willie's detection ability. If $SINR_W \ll 0$ dB, the signal Willie eavesdropped will be overwhelmed by the noise and the aggregate interference.

IV. Covert Communication in AWGN Channel

In this section, we first analyze Willie's probability of detection error $\mathbb{P}_e^{(w)}$ in a dense IoT network with AWGN channel, then estimate the upper bound of Alice's covert throughout, the amount of bits that Alice can reliably and covertly transmit to Bob over n uses of channel.

A. Willie's Probability of Detection Error

Let $\mathbf{P}_0$ be the probability density function (PDF) of $\mathbf{y} = \{y_i^{(w)}\}_{i=1}^n$ when $\mathbf{H_0}$ is true, $\mathbf{P}_1$ be the PDF of $\mathbf{y}$ when $\mathbf{H_1}$ is true. Using the same analysis method and the results from [10][21], if Willie employs the optimal hypothesis test to minimize his probability of detection error $\mathbb{P}_e^{(w)}$, then

$$\mathbb{P}_e^{(w)} \geq \frac{1}{2} - \sqrt{\frac{1}{8}D(\mathbf{P}_1||\mathbf{P}_0)} \quad (18)$$

where $D(\mathbf{P}_1||\mathbf{P}_0)$ is the relative entropy between $\mathbf{P}_1$ and $\mathbf{P}_0$, and the lower bound of $\mathbb{P}_e^{(w)}$ can be estimated as follows [21]

$$\begin{aligned}\mathbb{P}_e^{(w)} &\geq \frac{1}{2} - \sqrt{\frac{n}{8}}\cdot\frac{P_t\Psi_{a,w}}{2\sigma_w^2 d_{a,w}^{\alpha}} \\ &\overset{(a)}{=} \frac{1}{2} - \sqrt{\frac{n}{8}}\cdot\frac{P_t\Psi_{a,w}}{2d_{a,w}^{\alpha}}\cdot\frac{1}{\sigma_{w,0}^2+\sigma_{I_w}^2} \\ &\geq \frac{1}{2} - \sqrt{\frac{n}{8}}\cdot\frac{P_t\Psi_{a,w}}{2d_{a,w}^{\alpha}}\cdot\frac{1}{\sigma_{I_w}^2}\end{aligned} \quad (19)$$

where Eq. (a) holds because the total noise power at Willie is $\sigma_w^2 = \sigma_{w,0}^2 + \sigma_{I_w}^2$, here $\sigma_{w,0}^2$ is the power of the noise, $\sigma_{I_w}^2$ is the power of the aggregate interference (defined in Eq. (4)). Then the mean of $\mathbb{P}_e^{(w)}$ is

$$\begin{aligned}\mathbf{E}[\mathbb{P}_e^{(w)}] &\geq \frac{1}{2} - \sqrt{\frac{n}{8}}\cdot\frac{P_t\mathbf{E}[\Psi_{a,w}]}{2d_{a,w}^{\alpha}}\cdot\mathbf{E}\left[\frac{1}{\sigma_{I_w}^2}\right] \\ &= \frac{1}{2} - \sqrt{\frac{n}{8}}\cdot\frac{P_t}{2d_{a,w}^{\alpha}}\cdot\mathbf{E}\left[\frac{1}{\sigma_{I_w}^2}\right]\end{aligned} \quad (20)$$

since links experience unit mean Rayleigh fading with $\mathbf{E}[\Psi_{a,w}] = 1$.

To estimate $\mathbf{E}[1/\sigma_{I_w}^2]$, we should have the closed-form expression of the distribution of $\sigma_{I_w}^2$. However, $\sigma_{I_w}^2$ is an RV whose randomness originates from PPP Π and the fading channels. It obeys a stable distribution without closed-form expression. We then use the Taylor expansion technique ([23], Appendix. B) to obtain the approximation of the mean of $1/\sigma_{I_w}^2$. Particularly, the mean of an RV $Y = g(X)$, where X is another RV with mean $\mathbf{E}[X]$ and variance $\mathbf{Var}[X]$, can be estimated as

$$\mathbf{E}[Y] = g(\mathbf{E}[X]) + \frac{g''(\mathbf{E}[X])}{2}\cdot\mathbf{Var}[X] \quad (21)$$

Next we have to estimate the mean and variance of $\sigma_{I_w}^2$. However, its mean is not exist if we employ the unbounded path loss law. We then use a bounded path loss law, $l(r) \equiv r^{-\alpha}\mathbf{1}_{r\geq\rho}$ for $\rho \geq 0$. This law truncates around the origin and thus removes the singularity of unbounded path loss law $l(r) \equiv r^{-\alpha}$. For relatively small ρ, this model yields rather accurate results, its mean and variance are finite and can be given as [26]

$$\mathbf{E}[\sigma_{I_w}^2] = \frac{\lambda d c_d}{\alpha - d}\mathbf{E}[\Psi]\mathbf{E}[P_t]\rho^{d-\alpha} \quad (22)$$

$$\mathbf{Var}[\sigma_{I_w}^2] = \frac{\lambda d c_d}{2\alpha - d}\mathbf{E}[\Psi^2]\mathbf{E}[P_t^2]\rho^{d-2\alpha} \quad (23)$$

where d is the spatial dimension of the network, the relevant values of c_d are: $c_1 = 2$, $c_2 = \pi$, $c_3 = 4\pi/3$. In the following analysis, we set $\rho = 1$, all links experience unit mean Rayleigh fading with $\mathbf{E}[\Psi] = 1$ and $\mathbf{E}[\Psi^2] = 2$.

Therefore using Eq. (21), (22), and (23), given the constant transmit power P_t, $\mathbf{E}[1/\sigma_{I_w}^2]$ can be estimated as follows

$$\begin{aligned}\mathbf{E}\left[\frac{1}{\sigma_{I_w}^2}\right] &= \frac{1}{\mathbf{E}[\sigma_{I_w}^2]} + \frac{1}{(\mathbf{E}[\sigma_{I_w}^2])^3}\cdot\mathbf{Var}[\sigma_{I_w}^2] \\ &= \frac{\alpha-d}{\lambda d c_d P_t} + \left(\frac{\alpha-d}{\lambda d c_d P_t}\right)^3\cdot\frac{2\lambda d c_d}{2\alpha-d}\cdot P_t^2 \\ &= \frac{1}{P_t}\cdot f(\lambda)\end{aligned} \quad (24)$$

where $f(\lambda)$ is a function of λ as follows

$$f(\lambda) = \frac{1}{\lambda}\cdot\frac{\alpha-d}{dc_d}\left[1 + \frac{2(\alpha-d)^2}{(2\alpha-d)dc_d}\cdot\frac{1}{\lambda}\right] \quad (25)$$

Eq. (20) and (24) yield the lower bound of $\mathbf{E}[\mathbb{P}_e^{(w)}]$ as

$$\begin{aligned}\mathbf{E}[\mathbb{P}_e^{(w)}] &\geq \frac{1}{2} - \sqrt{\frac{n}{8}}\cdot\frac{P_t}{2d_{a,w}^{\alpha}}\cdot\frac{1}{P_t}\cdot f(\lambda) \\ &= \frac{1}{2} - \sqrt{\frac{n}{8}}\cdot\frac{f(\lambda)}{2d_{a,w}^{\alpha}}\end{aligned} \quad (26)$$

Suppose $\mathbf{E}[\mathbb{P}_e^{(w)}] \geq \frac{1}{2} - \epsilon$ for any $\epsilon > 0$, then we should set

$$d_{a,w} > \left[\frac{1}{4\sqrt{2}\epsilon} \cdot f(\lambda)\right]^{1/\alpha} \cdot n^{1/(2\alpha)}. \tag{27}$$

Therefore, as long as $d_{a,w} = \omega(n^{1/(2\alpha)})$, we can get $\mathbf{E}[\mathbb{P}_e^{(w)}] \geq \frac{1}{2} - \epsilon$ for any $\epsilon > 0$. This implies that there is no limitation on the transmit power P_t (if all potential transmitters employ the same transmit power P_t), the critical factor is the distance between Alice and Willie, which is related with n and λ. This theoretical result is also verified in Section IV-C. In brief, if Alice has more information to send to Bob covertly (n is larger), she should be farther away from Willie. Besides, in a sparse IoT network with less interference, we should put Alice farther away from Willie to guarantee the covertness.

B. Covert Throughput

In this subsection, we estimate the upper bound of Alice's covert throughout, i.e., the amount of bits that Alice can reliably and covertly transmit to Bob over n uses of channel. First we estimate Bob's decoding error probability. Let the total noise power that Bob experiences is $\sigma_b^2 = \sigma_{b,0}^2 + \sigma_{I_b}^2$, where $\sigma_{b,0}^2$ is the power of the background noise at Bob, $\sigma_{I_b}^2$ is the power of the aggregate interference from other Tx. By utilizing the same approach in [10][21], Bob's decoding error probability can be lower bounded as follows,

$$\begin{aligned}
\mathbb{P}_e^{(b)}(\sigma_b^2) &\leq 2^{nR - \frac{n}{2}\log_2\left(1+\frac{P_t}{2\sigma_b^2}\right)} \\
&= 2^{nR - \frac{n}{2}\log_2\left[1+\frac{P_t}{2(\sigma_{b,0}^2+\sigma_{I_b}^2)}\right]} \\
&= 2^{nR}\left[1 + \frac{P_t}{2(\sigma_{b,0}^2 + \sigma_{I_b}^2)}\right]^{-n/2} \\
&\leq 2^{nR}\left[1 + \frac{P_t}{2(\sigma_{b,0}^2 + \sigma_{I_b}^2)}\frac{n}{2}\right]^{-1}
\end{aligned} \tag{28}$$

where R (bits/symbol) is the rate of encoder, and the last step is obtained by the following inequality [21]: $(1+x)^{-r} \leq (1+rx)^{-1}$, for any $r \geq 1$ and $x > -1$.

To estimate the mean of $\mathbb{P}_e^{(b)}(\sigma_b^2)$, we should have the closed-form expression of the distribution of $\sigma_{I_b}^2$. However, $\sigma_{I_b}^2$ does not have a closed-form expression for its PDF or CDF. To address wireless network capacity, Weber *et al.* [27] employed tools from stochastic geometry to obtain asymptotically tight bounds on the distribution of the signal-to-interference (SIR) level in a wireless network, yielding tight bounds on its complementary cumulative distribution function (CCDF). Define a random variable

$$\mathbf{Y} = \frac{\Sigma_{k\in\Pi} P_t \Psi_{k,b} d_{k,b}^{-\alpha}}{P_t \Psi_{a,b} d_{a,b}^{-\alpha}} = \frac{\sigma_{I_b}^2}{P_t \Psi_{a,b} d_{a,b}^{-\alpha}} \tag{29}$$

then, the upper bound on the CCDF of RV $\mathbf{Y}$, $\bar{F}_{\mathbf{Y}}^u(y)$, can be expressed as ([27], Eq. 27),

$$\bar{F}_{\mathbf{Y}}^u(y) = \frac{2}{2-\delta}\kappa\lambda y^{-\delta} + \mathcal{O}(y^{-2\delta}) \tag{30}$$

where $\kappa = \pi \mathbf{E}[\Psi^\delta]\mathbf{E}[\Psi^{-\delta}]\mathbf{E}[d_{a,b}^2]$, λ is the intensity of Tx in PPP Π, and $\delta = 2/\alpha$. When $\Psi \sim \text{Exp}(1)$, $\kappa = \pi\Gamma(1+\delta)\Gamma(1-\delta)d_{a,b}^2 = \frac{\pi^2\delta}{\sin(\pi\delta)}d_{a,b}^2$.

Because $\sigma_{I_b}^2$ is a linear function of $\mathbf{Y}$, we can get the upper bound on CCDF of RV $\sigma_{I_b}^2$ as follows

$$\begin{aligned}
\bar{F}_{\sigma_{I_b}^2}^u(x) &= \mathbb{P}\{\sigma_{I_b}^2 > x\} = \mathbb{P}\{P_t\Psi_{a,b}d_{a,b}^{-\alpha}\mathbf{Y} > x\} \\
&= \mathbb{P}\{\mathbf{Y} > \frac{x}{P_t\Psi_{a,b}d_{a,b}^{-\alpha}}\} \\
&= \frac{2}{2-\delta}\kappa\lambda\beta^\delta x^{-\delta} + \mathcal{O}(x^{-2\delta}) \\
&= \eta\lambda\beta^\delta x^{-\delta} + \mathcal{O}(x^{-2\delta})
\end{aligned} \tag{31}$$

where $\eta = \frac{2}{2-\delta}\kappa$, $\beta = P_t\Psi_{a,b}d_{a,b}^{-\alpha}$.

Now define an RV $\bar{\sigma}_{I_b}^2$ who obeys the CCDF distribution of Eq. (31). Because Eq. (31) is the upper bound on CCDF of the RV $\sigma_{I_b}^2$, then we have $\mathbb{P}\{\bar{\sigma}_{I_b}^2 > x\} > \mathbb{P}\{\sigma_{I_b}^2 > x\}$ which implies that the RV $\bar{\sigma}_{I_b}^2$ stochastically dominates RV $\sigma_{I_b}^2$. According to the theory of stochastic orders [28], $\mathbf{E}[g(\bar{\sigma}_{I_b}^2)] > \mathbf{E}[g(\sigma_{I_b}^2)]$ if $g(x)$ is a non-decreasing function.

Hence the mean of Bob's decoding error probability can be estimated as follows

$$\begin{aligned}
\mathbf{E}[\mathbb{P}_e^{(b)}(\sigma_b^2)] &\leq \mathbf{E}\left[2^{nR}\left(1 + \frac{nP_t/4}{\sigma_{b,0}^2 + \sigma_{I_b}^2}\right)^{-1}\right] \\
&\overset{(a)}{<} \mathbf{E}\left[2^{nR}\left(1 + \frac{nP_t/4}{\sigma_{b,0}^2 + \bar{\sigma}_{I_b}^2}\right)^{-1}\right] \\
&\overset{(b)}{=} \int_0^\infty 2^{nR}\left(1 + \frac{nP_t/4}{\sigma_{b,0}^2 + x}\right)^{-1} f_{\bar{\sigma}_{I_b}^2}^u(x)\mathrm{d}x \\
&= 2^{nR}\int_{(\eta\lambda)^{\frac{1}{\delta}}\beta}^\infty \left(1 + \frac{nP_t/4}{\sigma_{b,0}^2 + x}\right)^{-1} \\
&\quad \times \eta\lambda\beta^\delta\delta x^{-(\delta+1)}\mathrm{d}x
\end{aligned} \tag{32}$$

here Eq. (a) holds because the RV $\bar{\sigma}_{I_b}^2$ stochastically dominates the RV $\sigma_{I_b}^2$, and the function $g(x) = \left(1 + \frac{nP_t/4}{\sigma_{b,0}^2+x}\right)^{-1}$ is non-decreasing. In Eq. (b), $f_{\bar{\sigma}_{I_b}^2}^u(x)$ is PDF of RV $\bar{\sigma}_{I_b}^2$ whose CCDF is expressed in Eq. (31),

$$f_{\bar{\sigma}_{I_b}^2}^u(x) = \eta\lambda\beta^\delta\delta x^{-(\delta+1)}, \quad x \in [(\eta\lambda)^{1/\delta}\beta, +\infty) \tag{33}$$

here we set $x \in [(\eta\lambda)^{1/\delta}\beta, +\infty)$ to normalize the function to be a PDF of an RV.

Define $a = nP_t/4$, Eq. (32) can be calculated as follows

$$\begin{aligned}
&\mathbf{E}[\mathbb{P}_e^{(b)}(\sigma_b^2)] \\
&< 2^{nR}\int_{(\eta\lambda)^{\frac{1}{\delta}}\beta}^\infty \left(1 + \frac{a}{\sigma_{b,0}^2 + x}\right)^{-1} \eta\lambda\beta^\delta\delta x^{-(\delta+1)}\mathrm{d}x \\
&= 2^{nR}\eta\lambda\beta^\delta\delta\Bigg[\frac{\pi a}{(a+\sigma_{b,0}^2)^{3/2}} - \frac{2a\tan^{-1}\left(\frac{\eta\lambda\beta^\delta}{\sqrt{a+\sigma_{b,0}^2}}\right)}{(a+\sigma_{b,0}^2)^{3/2}} \\
&\quad + \frac{2\sigma_{b,0}^2}{\eta\lambda\beta^\delta(a+\sigma_{b,0}^2)}\Bigg].
\end{aligned}$$

When n is large enough, we have $a = nP_t/4 \gg \sigma_{b,0}^2$, $a + \sigma_{b,0}^2 \approx a$.

Let the path loss exponent $\alpha = 4$, then $\delta = 1/2$, $\eta = \frac{2}{2-\delta}\kappa = \frac{2}{2-\delta}\frac{\pi^2\delta}{\sin(\pi\delta)}d_{a,b}^2 = \frac{2\pi^2}{3}d_{a,b}^2$, and

$$\frac{2a\tan^{-1}\left(\frac{\eta\lambda\beta^\delta}{\sqrt{a+\sigma_{b,0}^2}}\right)}{(a+\sigma_{b,0}^2)^{3/2}} > \frac{2\sigma_{b,0}^2}{\eta\lambda\beta^\delta(a+\sigma_{b,0}^2)} \tag{34}$$

provided that the transmit power P_t satisfies the following condition[2],

$$P_t > \frac{9}{4\pi^4\lambda^2\Psi_{a,b}} \cdot \sigma_{b,0}^2 \tag{35}$$

Therefore we have

$$\begin{aligned}
\mathbf{E}[\mathbb{P}_e^{(b)}(\sigma_b^2)] &\overset{(a)}{<} 2^{nR}\eta\lambda\beta^\delta\delta\left[\frac{\pi a}{(a+\sigma_{b,0}^2)^{3/2}}\right] \\
&\overset{(b)}{<} 2^{nR}\eta\lambda\beta^\delta\delta\frac{\pi}{\sqrt{a}} \\
&= 2^{nR}\eta\lambda\beta^\delta\delta\frac{2\pi}{\sqrt{nP_t}} \\
&= 2^{nR}\frac{2\pi^2}{3}d_{a,b}^2\lambda P_t^{1/2}\mathbf{E}[\Psi^{1/2}]d_{a,b}^{-\alpha/2}\delta\frac{2\pi}{\sqrt{nP_t}} \\
&= 2^{nR}\frac{\pi^{7/2}\lambda}{3\sqrt{n}}
\end{aligned} \tag{36}$$

where Eq. (a) holds because we have Eq. (34), Eq. (b) is due to $a+\sigma_{b,0}^2 \approx a$. $\mathbf{E}[\Psi^{1/2}] = \Gamma(1+1/2) = \sqrt{\pi}/2$ for $\Psi \sim \text{Exp}(1)$.

Let $\mathbf{E}[\mathbb{P}_e^{(b)}(\sigma_b^2)] \leq \epsilon$ for any $\epsilon > 0$, then we have

$$nR \leq \log_2\left(\frac{3\epsilon}{\pi^{7/2}\lambda} \cdot \sqrt{n}\right) \tag{37}$$

which implies that Alice can send $\mathcal{O}(\log_2\sqrt{n})$ bits reliably in n channel uses in the case that $\alpha = 4$, and this covert throughout decreases as the density λ becomes larger.

C. Discussions

1) Spatial Throughput: The spatial throughput is the expected spatial density of successful transmissions in a wireless network [27], $\tau(\lambda) = \lambda(1-q(\lambda))$, where $q(\lambda)$ is the probability of transmission outage when the density of interferers is λ for a given SINR requirement ξ.

In the work of Bash [10], only the background noise is taken into account, Alice can transmit $\mathcal{O}(\sqrt{n})$ bits reliably and covertly to Bob over n uses of AWGN channel. Soltani [21] introduced the friendly node closest to Willie to produce artificial noise. This method allows Alice to reliably and covertly send $\mathcal{O}(\min\{n, \lambda^{\alpha/2}\sqrt{n}\})$ bits to Bob in n channel uses when there is only one adversary. However Alice must set her average symbol power $P_a = \mathcal{O}(\frac{c\lambda^{\alpha/2}}{\sqrt{n}})$ to avoid being detected by Willie. Thus, given the SINR threshold ξ, $\sigma_{b,0}^2 \geq 1$, and Rayleigh fading with $\Psi \sim \text{Exp}(1)$, the outage probability of Soltani's method is

$$\begin{aligned}
q^J(\lambda) &= \mathbb{P}\left\{\text{SINR} = \frac{P_a\Psi d_{a,b}^{-\alpha}}{\sigma_{b,0}^2 + P_f\Psi d_{a,f}^{-\alpha}} < \xi\right\} \\
&\geq \mathbb{P}\{P_a\Psi d_{a,b}^{-\alpha} < \xi\} \\
&\geq \mathbb{P}\left\{\frac{c\lambda^{\alpha/2}}{\sqrt{n}}\Psi d_{a,b}^{-\alpha} < \xi\right\} \\
&= \mathbb{P}\left\{\Psi < \frac{1}{c\lambda^{\alpha/2}}d_{a,b}^{\alpha}\xi\sqrt{n}\right\} \\
&= 1 - \exp\left\{-\frac{1}{c\lambda^{\alpha/2}}d_{a,b}^{\alpha}\xi\sqrt{n}\right\}
\end{aligned} \tag{38}$$

[2]This inequality can be easily derived, mainly because $\lim_{n\to\infty}\sqrt{n}\tan^{-1}(\frac{c}{\sqrt{n}}) = c$ for a given constant c, and $a + \sigma_{b,0}^2 \approx a$ when $n \to \infty$.

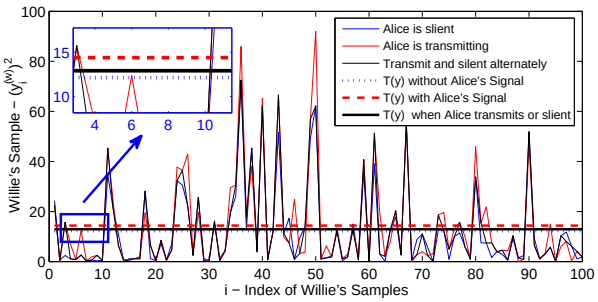


Fig. 5. Sequences of 100 Willie's samples $[y_1^{(w)}]^2, ..., [y_n^{(w)}]^2$ when Alice is silent, transmitting, or transmitting with probability $p = 0.5$ in each time slot. Here $T(\mathbf{y}) = \frac{1}{n}\sum_{k=1}^{n}[y_k^{(w)}]^2$, a bounded path loss law is used, $l(x) = \min\{1, r^{-\alpha}\}$, the transmit power P_t is unity, channels experience unit mean Rayleigh fading, $\Psi \sim \text{Exp}(1)$, $\alpha = 4$, and $\sigma_{w,0}^2 = 1$. Willie is located at the center of a square area 100m×100m with $d_{a,w} = 1$. Interferers deployed in this area form a PPP on the plane with $\lambda = 1$.

Then the spatial throughput of the network is

$$\tau^J(\lambda) = \lambda(1-q^J(\lambda)) \leq \lambda\exp\left\{-\frac{1}{c\lambda^{\alpha/2}}d_{a,b}^{\alpha}\xi\sqrt{n}\right\} \tag{39}$$

If we hide communications in the aggregate interference of a noisy IoT network with randomized transmissions in Rayleigh fading channel and the SINR threshold is set to ξ, the spatial throughput is [27] ($\delta = 2/\alpha$)

$$\tau^I(\lambda) = \lambda\exp\{-\pi\lambda\xi^\delta d_{a,b}^2\Gamma(1+\delta)\Gamma(1-\delta)\} \tag{40}$$

As a result of Eq. (39) and (40), as $n \to \infty$, the spatial throughput of the jamming scheme $\tau^J(\lambda)$ reduces to zero, and the covert communication in a noisy network can achieve a constant spatial throughput $\tau^I(\lambda)$. Hence, although this approach has a lower covert throughput for any pair of nodes, it has a higher spatial throughput from the network perspective.

2) Simulation Results: In the previous analysis, when Willie samples the noise to determine the threshold of his detector, we presuppose that Willie knows whether Alice is transmitting or not, and he knows the power level of $\sigma_{I_w}^2$. In practice, Willie has no prior knowledge on whether Alice is transmitting or not during his sampling process. This implies that Willie's sample $y_i^{(w)}$ follows the following distribution

$$y_i^{(w)} \sim \mathcal{N}\left(\sqrt{\frac{P_t}{d_{a,w}^{\alpha}}}\mathbf{h}s_i^{(a)}\cdot\mathbf{1}_A + \sum_{k\in\Pi}\sqrt{\frac{P_t}{d_{k,w}^{\alpha}}}\mathbf{h}s_i^{(k)}, \sigma_{w,0}^2\right) \tag{41}$$

where $\mathbf{1}_A$ is an indicator function, $\mathbf{1}_A = 1$ if Alice is transmitting, $\mathbf{1}_A = 0$ if Alice is silent, and the transmission probability $\mathbb{P}\{\mathbf{1}_A = 1\} = p$.

To confuse Willie, Alice can divide the time into slots, then sends a packet in a slot with a predefined transmission probability p. Fig. 5 illustrates an example of sequences of 100 Willie's samples $[y_1^{(w)}]^2, ..., [y_n^{(w)}]^2$ when Alice is silent, transmitting with probability 1, or transmitting with probability $p = 0.5$ in a slot. Clearly, if the transmission probability p is small, Alice's signals will resemble the noise in the channel.

With the same simulation settings as Fig. 5, we evaluate Willie's sample values $T(\mathbf{y})$ by varying the transmit power P_t. As displayed in Fig. 6, when Alice employs the random

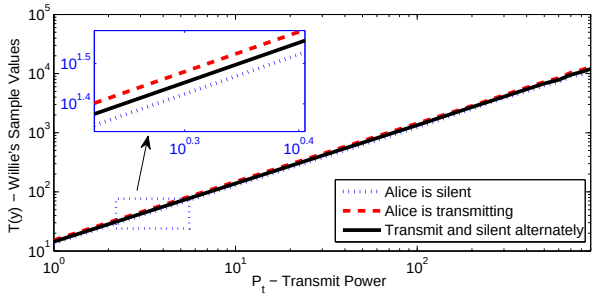


Fig. 6. The transmit power P_t versus Willie's sample values $T(\mathbf{y})$ which are the average of 100 experiment runs, each with the number of samples $n = 500$. During each run of simulation, a random wireless network obeying PPP on the plane is generated.

transmission method, Willie's sample values decrease. The result is consistent with the previous analysis, which indicates that increasing the transmit power P_t does not increase the risk of being detected by Willie in a noisy wireless network.

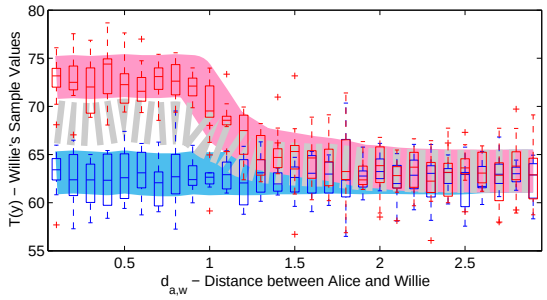
Further, one of critical factors affecting covert communication is the parameter $d_{a,w}$, the distance between Alice and Willie, which should satisfy $d_{a,w} = \omega(n^{1/(2\alpha)})$ to ensure communication covertly. Fig. 7 shows the tendency of $T(\mathbf{y})$ with respect to the distance $d_{a,w}$ when $n = 1000$ and $n = 3000$. As can be seen, the discreteness of $T(\mathbf{y})$ decreases with increasing the number of samples n. To detect Alice's transmission attempts, Willie has to distinguish three lines in the figures with relatively low probability of error. The only way to decrease the probability of error is increasing the number of samples. By choosing a larger n, Willie's uncertainty decreases, hence he can stay farther away from Alice to detect her transmission attempts. Overall, this result agrees with the previous theoretical derivation, i.e., given the value n, the distance between Alice and Willie should be greater than a bound to ensure the covertness, and the bound of $d_{a,w}$ increases with n.

As described in Eq.(37), Alice can send $\mathcal{O}(\log_2 \sqrt{n})$ bits reliably in n channel uses. However, how to approach this bound is still unknown. The key point is how to choose an appropriate coding scheme to achieve the covertness in a specific target network. This code should be reliably and computationally efficiently designed according to the specific interference model and can make it impossible for Willie to distinguish between interference and hidden information. Because random coding has a high complexity, polar coding may be an appropriate coding scheme to achieve good performance.

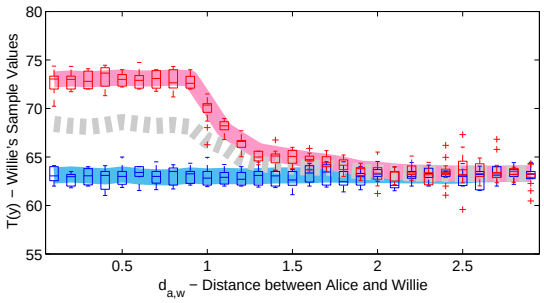
V. Covert Communication in THz Band

THz Band is envisioned as a key technology to satisfy the increasing demand for higher speed wireless communication. It can be used in classical networking scenarios as well as in nano-scale communication paradigms, such as wireless nano-sensor networks for health monitoring and the Internet of Nano-Things (IoNT) [12].

In THz Band, devices always use directional channels with a beam divergence angle much smaller than that used by existing mobile networks. Intuitively, the narrow, razor-sharp beam of



(a) n=1000



(b) n=3000

Fig. 7. The discreteness of Willie's sample values $T(\mathbf{y})$ versus the distance $d_{a,w}$ when the number of samples $n = 1000$ and $n = 3000$. Three simulation curves are given (from top to bottom): Alice is transmitting, transmitting with probability $p = 0.5$, and silent. For each occasion, we implement 20 experiment runs to obtain 20 sample values $T(\mathbf{y})$, and depict the discreteness of $T(\mathbf{y})$ in boxplot form. The width of curves represents the dispersion degree of Willie's sample values.

THz Band can drastically limit the eavesdropping probability and can improve the data security. However, an eavesdropper can place an object in the path of the transmission to scatter radiation towards the eavesdropper [25]. Covert communication is more difficult than anti-eavesdropping.

A. Covert Communication in THz Band

In THz Band IoT network (as depicted in Fig.2), Willie is located in the path of LOS link between Alice and Bob, and tries to detect the possible transmission between them. To bypass the detection of Willie, Alice and Bob should resort to the reflection or diffuse scattering NLOS transmission link,

- **Specular Reflection**: At first, Alice and Bob try to find a surface in the surroundings that the THz beam from Alice can be specularly reflected to the antenna of Bob, i.e., the specular reflection path $\overrightarrow{AO_1}$ and $\overrightarrow{O_1B}$ in Fig. 2, and SINR at Bob is above a predefined threshold.
- **Diffuse Scattering**: If a specular reflection path does not exist, Alice and Bob find a diffuse scattering path so that Bob's received signal strength is above a threshold, such as the scattering path $\overrightarrow{AO_2}$ and $\overrightarrow{O_2B}$ in Fig. 2.

B. Analysis

In this subsection we use the normalized secrecy capacity $\bar{c}_s$ to assess the likelihood of covert communication. To estimate $\bar{c}_s$, we need to calculate $I_{THz}^{(b)}$, $I_{THz}^{(w)}$ and $SINR_B$, $SINR_W$.

Next, we estimate the mean of the aggregate interference $I_{THz}^{(b)}$ Bob observed (in Eq. (14)) as follows,

$$\begin{aligned}\mathbf{E}[I_{THz}^{(b)}] &= \mathbf{E}\left[A\sum_{i=1}^{\infty} r_i^{-2}e^{-Kr_i}\cdot\mathbf{1}_{\{I_i>0\}}\right]\\ &\overset{(a)}{=} A\lambda\int_{X_i\in\Pi} r_i^{-2}e^{-Kr_i}\cdot\mathbb{P}_C(1-\mathbb{P}_B)\mathrm{d}X_i\\ &= A\lambda\int_0^{2\pi}\mathrm{d}\theta\int_{r_B}^{R} r^{-2}e^{-Kr}\frac{\phi}{2\pi}\cdot e^{-\lambda(r-r_B)r_B}r\mathrm{d}r\\ &= A\lambda\phi e^{\lambda {r_B}^2}\int_{r_B}^{R}\frac{1}{r}e^{-(K+\lambda r_B)r}\mathrm{d}r\\ &= A\lambda\phi e^{\lambda {r_B}^2}\Big[Ei(-R(K+\lambda r_B))\\ &\quad -Ei(-r_B(K+\lambda r_B))\Big] \end{aligned}\tag{42}$$

where $Ei(\cdot)$ is the exponential integral function, R is the radius of the zone that the signal that comes from Tx farther than R is considered as the background noise. Eq. (a) follows directly after Campbell's theorem [26] for the mean of a sum function of a stationary PPP $\Pi=\{X_i\}$.

Similarly, the variance of the aggregate interference $I_{THz}^{(b)}$ can be obtained as follows,

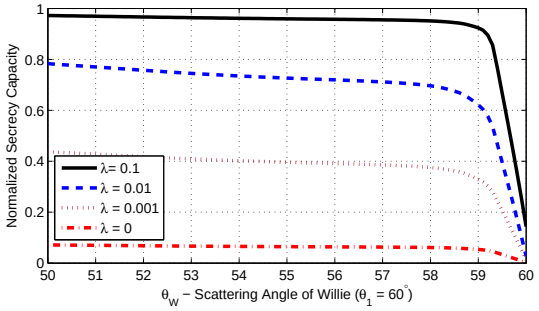
$$\begin{aligned}&\mathbf{Var}[I_{THz}^{(b)}]\\ =\ &\mathbf{Var}\left[\sum_{i=1}^{\infty} Ar_i^{-2}e^{-Kr_i}\cdot\mathbf{1}_{\{I_i>0\}}\right]\\ \overset{(a)}{=}\ &\lambda\int_{X_i\in\Pi}\left[Ar_i^{-2}e^{-Kr_i}\cdot\mathbb{P}_C(1-\mathbb{P}_B)\right]^2\mathrm{d}X_i\\ =\ &\lambda\int_0^{2\pi}\mathrm{d}\theta\int_{r_B}^{R}\left[Ar^{-2}e^{-Kr}\cdot\frac{\phi}{2\pi}\cdot e^{-\lambda(r-r_B)r_B}\right]^2 r\mathrm{d}r\\ =\ &A^2\lambda\frac{\phi^2}{2\pi}e^{2\lambda {r_B}^2}\int_{r_B}^{R}\frac{1}{r^3}e^{-(2K+2\lambda r_B)r}\mathrm{d}r\\ =\ &A^2\lambda\frac{\phi^2}{2\pi}e^{2\lambda {r_B}^2}\Big\{2(K+\lambda r_B)^2Ei\big[-2(K+\lambda r_B)\big]\\ &+e^{-2(K+\lambda r_B)r}\cdot\Big(\frac{K+\lambda r_B}{r}-\frac{1}{2r^2}\Big)\Big\}\Big|_{r_B}^{R}\end{aligned}\tag{43}$$

here Eq. (a) also follows directly after Campbell's theorem for the variance of a sum function of a stationary PPP $\Pi=\{X_i\}$.

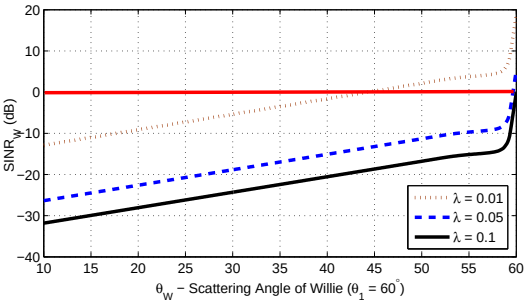
Next we estimate the mean of $SINR_B$ by Taylor expansion technique [23] as follows,

$$\begin{aligned}\mathbf{E}[SINR_B] &= \mathbf{E}\left[\frac{P_{Rx}}{S_{JN}(f)+I_{THz}^{(b)}}\right]\\ &= \frac{P_{Rx}}{S_{JN}(f)+\mathbf{E}[I_{THz}^{(b)}]}\\ &\quad +\frac{P_{Rx}}{(S_{JN}(f)+\mathbf{E}[I_{THz}^{(b)}])^3}\cdot\mathbf{Var}[I_{THz}^{(b)}]\end{aligned}\tag{44}$$

here P_{Rx} is the received signal strength of Bob, $P_{Rx}=Ad_{a,b}^{-2}\exp(-Kd_{a,b})\cdot G_B$, G_B is the reflecting path gain of Bob, which is obtained from Kirchhoff scattering model [24], and $S_{JN}(f)$ is Johnson-Nyquist noise, described in Eq. (11). Similarly, we can get the approximation of the mean of $SINR_W$ in the same way.



(a) Normalized secrecy capacity $\bar{c}_s$



(b) $SINR_W$ (dB)

Fig. 8. (a) The normalized secrecy capacity $\bar{c}_s$ and (b) $SINR_W$ versus the scattering angle of Willie θ_W for different network density λ. Here the incidence angle of Alice $\theta_1 = 60°$, the surface height variation $\sigma_h = 0.088$mm, and the operating frequency $f = 500$GHz.

Now we assess the effects of the operating frequency, network density, the surface roughnesses, and the scattering angle on the normalized secrecy capacity $\bar{c}_s$. Throughout this subsection, we assume that interference coming from the nodes $R = 10$m away is zero, the coefficient H introduced in Eq. (10) is set to 1. The blocker radius of every node $r_B = 0.1$m, the distance between Alice and Bob $d_{a,b} = 5$m, the absorption coefficient is assumed to be a constant $K = 0.01$. All devices in the IoT network are equipped with directional antennas (Tx and Rx) with directivity angle $\phi = \pi/18$. Also, the illuminated area of the reflection surface is approximately 4cm^2, the surface correlation length $l_c = 1.8$mm.

1) The Effect of Network Density λ: As illustrated in Fig. 8(a), if the incident angle of Alice $\theta_1 = 60°$ and Bob's antenna is located exactly at the specular reflection direction of Alice's signal, the closer Willie's scattering angle θ_W to θ_1, the smaller $\bar{c}_s$ we can get. This is obvious because the scattering coefficient G_W approximates to G_B when $\Delta = \theta_1 - \theta_W$ is very small. On the other hand, the higher the network density λ, the larger the normalized secrecy capacity and the covert communication is more likely to succeed. Indeed, if there is no interferer in the surroundings ($\lambda = 0$), the normalized secrecy capacity is so small that covert communication is practically impossible for a predefined threshold. Fig. 8(b) also confirms this result from another aspect. The smaller the density λ is, the higher the $SINR_W$, which means the reduction of the interference will increase the likelihood of exposure. This also implies that the interference is helpful to covert communication.

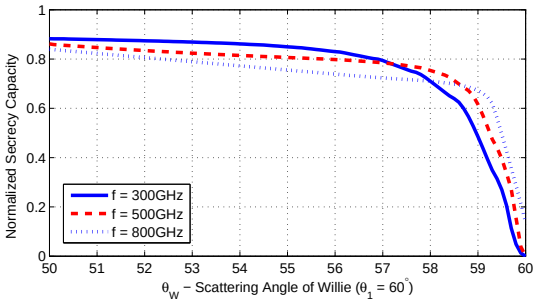


Fig. 9. The normalized secrecy capacity $\bar{c}_s$ versus the scattering angle of Willie θ_W for different operating frequencies. Here the incidence angle $\theta_1 = 60°$, $\sigma_h = 0.058$mm, and $\lambda = 0.01$.

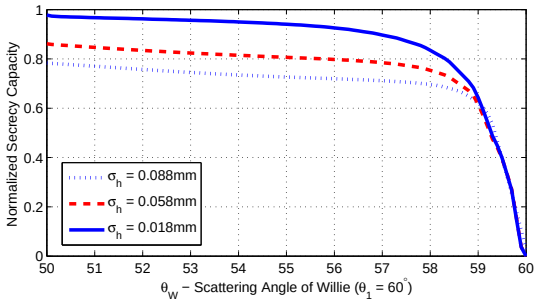


Fig. 10. The normalized secrecy capacity $\bar{c}_s$ versus the scattering angle of Willie θ_W for different surface roughnesses σ_h. Here the incidence angle $\theta_1 = 60°$, $f = 500$GHz, and $\lambda = 0.01$.

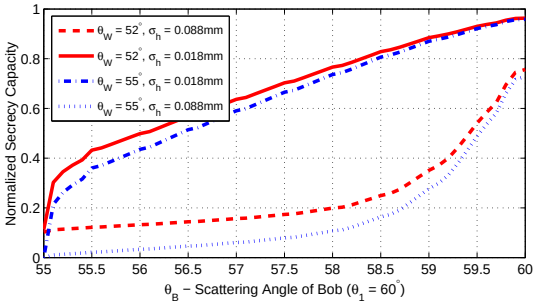


Fig. 11. The normalized secrecy capacity $\bar{c}_s$ versus the scattering angle of Bob θ_B for different surface roughness σ_h. Here $\theta_1 = 60°$, $f = 500$GHz, and $\lambda = 0.01$.

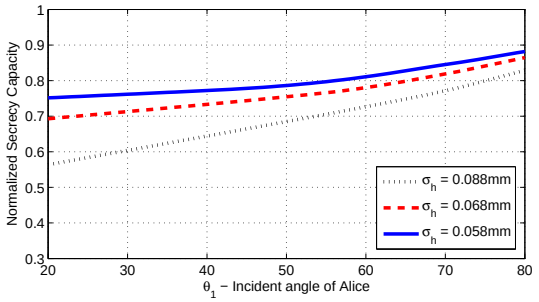


Fig. 12. The normalized secrecy capacity $\bar{c}_s$ versus the incident angle of signal θ_1 for different surface roughnesses σ_h. Here the scattering angle of Willie $\theta_W = \theta_1 - 5°$, $f = 500$GHz, $\lambda = 0.01$.

2) The Effect of Operating Frequency: Fig. 9 shows the comparison when different operating frequencies are taken into account. One can notice that $\bar{c}_s$ increases with the frequency when the scattering angle is close to the specular reflection direction, but decreases when the receiver angle of Willie gradually deviates from the reflection direction. This is reasonable since the scattering always increases with the operating frequency [29].

3) The Effect of Surface Roughness: The effect of surface roughness on $\bar{c}_s$ is illustrated in Fig. 10. In this measurement, we fix the surface correlation length l_c, only change the standard deviation of the surface height distribution σ_h. We notice that the larger value of σ_h results in lower $\bar{c}_s$. The underlying reason is that, for smaller value of σ_h, the surface is a more smooth surface with a purely specular reflection, a larger value of σ_h represents a relatively more rough surface with a stronger diffuse scattering contribution [30].

4) The Effect of Bob's Scattering Angle: In practice, Alice and Bob cannot always find a specular reflection path to perform their NLOS communication. As an alternative, Alice and Bob use diffuse scattering to communicate covertly. Fig. 11 demonstrates the effect of Bob's scattering angle θ_B on $\bar{c}_s$. Given the incidence angle $\theta_1 = 60°$, we fix the receiver angle of Willie θ_W at $52°$ and $55°$, then calculate the value $\bar{c}_s$ at different scattering angle of Bob $\theta_B(55° \cdots 60°)$. The results show that, the closer Bob's scattering direction to the specular reflection direction, the larger the value of $\bar{c}_s$. On the other hand, a more smooth surface (with less σ_h) will have less scattering strength and therefore will have larger $\bar{c}_s$. However, if the scattering angle deviates from the direction of reflection for several degrees, the value of $\bar{c}_s$ will decrease rapidly, especially when the surface is rougher.

5) The Effect of Incident Angle: Fig. 12 depicts the tendency of $\bar{c}_s$ with the incident angle θ_1. In the measurement setup, we assume Bob is located in the reflected direction ($\theta_B = \theta_1$), and Willie's receiver angle is fixed to be $\theta_W = \theta_B - 5°$. When the incident angle θ_1 increases, the value of $\bar{c}_s$ increases as well. However, this growth is slow. Besides, the more smooth the surface, the higher the value of $\bar{c}_s$. This is due to the fact that a smooth surface has a stronger specular reflection component.

C. Discussions

1) The Selection of Reflection Points: If Alice and Bob can find several specular reflection paths to perform NLOS communication, they should select the path whose reflection point is closest to Bob. As depicted in Fig. 13, Alice and Bob have two specular reflection paths, i.e., $A \Rightarrow O_1 \Rightarrow B$ (with O_1 as the reflection point) and $A \Rightarrow O_2 \Rightarrow B$ (with O_2 as the reflection point). The shaded areas represent the scattering areas that Willie can eavesdrop Alice's signal. If we choose O_1 as the reflection point, the scattering area is smaller.

If there are several reflection points with the same distance to Bob, the point with the largest incident angle θ_1 is the best choice, since the larger the incident angle, the higher the normalized secrecy capacity.

In the case that no specular reflection path can be found. Alice and Bob have to use a scattering NLOS to communicate.

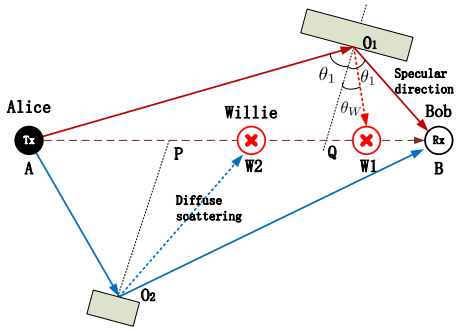


Fig. 13. The selection of reflection points. O_1 and O_2 are two reflection points, $\overline{O_1B}$ and $\overline{O_2B}$ are their specular reflection directions, $\overline{O_1Q}$ and $\overline{O_2P}$ are the normal vectors of two scattering surfaces, respectively.

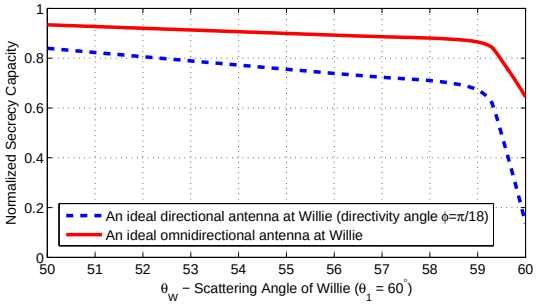


Fig. 14. The normalized secrecy capacity $\bar{c}_s$ versus the scattering angle of Willie θ_W for different antennas of Willie. Here $\theta_1 = 60°$, $\sigma_h = 0.058$mm, and $f = 800$GHz.

Because the diffuse scattering field is very weak in comparison to the specular direction, they should find a scattering point to Bob as close as possible. Additionally, a more rough surface with larger value of σ_h is preferred because it provides a stronger diffuse scattering contribution.

2) Willie's Detection Strategy: In general, Willie should put himself in the LOS path between Alice and Bob, and aim his antenna at Alice. After all, the LOS transmission is the most reasonable and effective channel in THz band. However, if Willie has no information about NLOS channels between Alice and Bob, or does not know which reflected path they utilize at a particular time, a better way is to adopt an omnidirectional antenna to receive Alice's signal. But this method also has some drawbacks. At first the gain of an omnidirectional antenna is much lower than a directional antenna with a small directivity angle. Then, the omnidirectional antenna will experience more interference from other Tx in the vicinity. Fig. 14 also shows the normalized secrecy capacity Alice and Bob can get when Willie adopts an omnidirectional or directional antenna. It is important to note that the omnidirectional antenna has relatively lower detection capability compared with the directional antenna. However, if Willie has no knowledge about the direction of Alice's signal, a wrong receiving direction of his directional antenna would be counterproductive. Therefore, Willie is faced with a dilemma of how to determine the type of antenna.

The best-case scenario to Willie is that he knows the NLOS transmission path between Alice and Bob. However it is extremely unwise for Willie to abandon the LOS path and leave to the possible NLOS path. In THz Band, as a result of the transmission at very high data rates, the time consumed in transmitting a packet can be expectedly several orders of magnitude lower than in classical wireless networks. Placing himself in the place between Alice and Bob, Willie can not only block the LOS transmission, but also keep watch on other possible NLOS transmissions.

VI. Conclusions

Security is the foundation for the development of IoT network. However, how to protect IoT is a challenging task and many related issues need to be solved. From the physical-layer security perspective, this paper introduces covert communication into IoT network to enhance the security from the bottom layer. If the adversary cannot detect user's transmission behavior, he has no chance to launch other attacks. What he sees is merely a shadow noisy wireless network.

Acknowledgments

This work is supported by the National Natural Science Foundation of China (61771374, 61941105, and 61671360), and in part by China 111 Project (B16037).

References

[1] J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, and W. Zhao, "A survey on internet of things: Architecture, enabling technologies, security and privacy, and applications," *IEEE Internet of Things Journal*, vol. 4, no. 5, pp. 1125–1142, October 2017.

[2] M. Frustaci, P. Pace, G. Aloi, and G. Fortino, "Evaluating critical security issues of the iot world: Present and future challenges," *IEEE Internet of Things Journal*, vol. 5, no. 4, pp. 2483–2495, August 2018.

[3] Y. Lu and L. D. Xu, "Internet of things (iot) cybersecurity research: A review of current research topics," *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 2103–2115, April 2019.

[4] Y. Miao, X. Liu, K. R. Choo, R. H. Deng, H. Wu, and H. Li, "Fair and dynamic data sharing framework in cloud-assisted internet of everything," *IEEE Internet of Things Journal*, vol. 6, no. 4, pp. 7201–7212, Aug 2019.

[5] B. A. Bash, D. Goeckel, D. Towsley, and S. Guha, "Hiding information in noise: Fundamental limits of covert wireless communication," *IEEE Communications Magazine*, vol. 52, no. 12, pp. 26–31, December 2015.

[6] J. Hu, C. Lin, and X. Li, "Relationship privacy leakage in network traffics," in *25th International Conference on Computer Communication and Networks, ICCCN*, August 2016, pp. 1–9.

[7] J. Classen, M. Schulz, and M. Hollick, "Practical covert channels for wifi systems," in *2015 IEEE Conference on Communications and Network Security (CNS)*, Sep. 2015, pp. 209–217.

[8] S. Grabski and K. Szczypiorski, "Steganography in ofdm symbols of fast ieee 802.11n networks," in *2013 IEEE Security and Privacy Workshops*, May 2013, pp. 158–164.

[9] S. DOro, F. Restuccia, and T. Melodia, "Hiding data in plain sight: Undetectable wireless communications through pseudo-noise asymmetric shift keying," in *IEEE INFOCOM 2019*, April 2019, pp. 1585–1593.

[10] B. Bash, D. Goeckel, and D. Towsley, "Limits of reliable communication with low probability of detection on awgn channels," *IEEE Journal on Selected Areas in Communications*, vol. 31, no. 9, pp. 1921–1930, September 2013.

[11] W. Wu, N. Cheng, N. Zhang, P. Yang, W. Zhuang, and X. Shen, "Fast mmwave beam alignment via correlated bandit learning," *IEEE Transactions on Wireless Communications*, pp. 1–1, 2019.

[12] I. F. Akyildiz, J. M. Jornet, and C. Han, "Terahertz band: Next frontier for wireless communications," *Physical Communication*, vol. 12, pp. 16–32, 2014.

[13] B. A. Bash, S. Guha, D. Goeckel, and D. Towsley, "Quantum noise limited optical communication with low probability of detection," in *IEEE ISIT 2013*, 2013, pp. 1715–1719.

[14] B. A. Bash, D. Goeckel, and D. Towsley, "Covert communication gains from adversarys ignorance of transmission time," *IEEE Transactions on Wireless Communications*, vol. 15, no. 12, pp. 8394–8405, 2016.

[15] S. Lee, R. J. Baxley, M. A. Weitnauer, and B. Walkenhorst, "Achieving undetectable communication," *IEEE Journal of Selected Topics in Signal Processing*, vol. 9, no. 7, pp. 1195–1205, October 2015.
[16] B. He, S. Yan, X. Zhou, and V. K. N. Lau, "On covert communication with noise uncertainty," *IEEE Communications Letters*, vol. 21, no. 4, pp. 941–944, April 2017.
[17] Z. Liu, J. Liu, Y. Zeng, J. Ma, and Q. Huang, "On covert communication with interference uncertainty," in *IEEE ICC*, Kansas City, MO, USA, May 2018.
[18] S. Gollakota, H. Hassanieh, B. Ransford, D. Katabi, and K. Fu, "They can hear your heartbeats: Non-invasive security for implantable medical devices," in *ACM SIGCOMM*, New York, NY, USA, 2011, pp. 2–13.
[19] X. Fang, N. Zhang, S. Zhang, D. Chen, X. Sha, and X. Shen, "On physical layer security: Weighted fractional fourier transform based user cooperation," *IEEE Transactions on Wireless Communications*, vol. 16, no. 8, pp. 5498–5510, August 2017.
[20] T. V. Sobers, B. A. Bash, S. Guha, D. Towsley, and D. Goeckel, "Covert communication in the presence of an uninformed jammer," *IEEE Transactions on Wireless Communications*, vol. 16, no. 9, pp. 6193–6206, 2017.
[21] R. Soltani, D. Goeckel, D. Towsley, B. A. Bash, and S. Guha, "Covert wireless communication with artificial noise generation," *IEEE Transactions on Wireless Communications*, vol. 17, no. 11, pp. 7252–7267, November 2018.
[22] B. He, S. Yan, X. Zhou, and H. Jafarkhani, "Covert wireless communication with a poisson field of interferers," *IEEE Transactions on Wireless Communications*, vol. 17, no. 9, pp. 6005–6017, 2018.
[23] V. Petrov, M. Komarov, D. Moltchanov, J. M. Jornet, and Y. Koucheryavy, "Interference and sinr in millimeter wave and terahertz communication systems with blocking and directional antennas," *IEEE Transactions on Wireless Communications*, vol. 16, no. 3, pp. 1791–1808, March 2017.
[24] P. Beckmann and A. Spizzichino, *The Scattering of Electromagnetic Waves From Rough Surfaces*. Reading, MA: Artech House, 1987.
[25] J. Ma, R. Shrestha, J. Adelberg, C.-Y. Yeh, Z. Hossain, E. Knightly, J. M. Jornet, and D. M. Mittleman, "Security and eavesdropping in terahertz wireless links," *Nature*, vol. 563, pp. 89–93, November 2018.
[26] M. Haenggi and R. K. Ganti, "Interference in large wireless networks," *Foundations and Trends®in Networking*, vol. 3, no. 2, pp. 127–248, 2008.
[27] S. Weber, J. G. Andrews, and N. Jindal, "The effect of fading, channel inversion, and threshold scheduling on ad hoc networks," *IEEE Transactions on Information Theory*, vol. 53, no. 11, pp. 4127–4149, 2007.
[28] C. Tepedelenlioğlu, A. Rajan, and Y. Zhang, "Applications of stochastic ordering to wireless communications," *IEEE Transactions on Wireless Communications*, vol. 10, no. 12, pp. 4249–4257, December 2011.
[29] J. Kokkoniemi, V. Petrov, D. Moltchanov, J. Lehtomaeki, Y. Koucheryavy, and M. Juntti, "Wideband terahertz band reflection and diffuse scattering measurements for beyond 5g indoor wireless networks," in *European Wireless 2016; 22th European Wireless Conference*, May 2016, pp. 1–6.
[30] C. Jansen, S. Priebe, C. Moller, M. Jacob, H. Dierke, M. Koch, and T. Kurner, "Diffuse scattering from rough surfaces in thz communication channels," *IEEE Transactions on Terahertz Science and Technology*, vol. 1, no. 2, pp. 462–472, November 2011.

Zhihong Liu received his Ph.D. degree in cryptography from Xidian University in 2009. He is currently an associate professor with the School of Cyber Engineering, Xidian University, China. His research interests cover a wide range of areas including cryptography, distributed computing, and wireless physical layer security.

Jiajia Liu [S'11, M'12, SM'15] is currently a full professor at the School of Cybersecurity, Northwestern Polytechnical University, China. His research interests cover wireless mobile communications, FiWi, IoT, and more. He has published more than 90 peer-reviewed papers in many prestigious IEEE journals and conferences, and currently serves as an Associate Editor for IEEE Transactions on Communications and IEEE Transactions on Vehicular Technology, an Editor for IEEE Network, and a Guest Editor of IEEE TETC and the IEEE Internet of Things Journal. He is a Distinguished Lecturer of IEEE ComSoc.

Yong Zeng is currently an associate professor with the School of Cyber Engineering, Xidian University, China. His research interests cover a wide range of areas including physical layer security, wireless mobile ad hoc network security, and cryptography.

Jianfeng Ma received his M.E. and Ph.D. degrees in computer software and communications engineering from Xidian University in 1988 and 1995, respectively. From 1999 to 2001, he was with Nanyang Technological University of Singapore as a research fellow. He is a senior member of Chinese Institute of Electronics and Changjiang Scholars Distinguished Professor of China. Now he is currently a full Professor in the School of Cyber Engineering, Xidian University, advisor of Ph.D candidates of computer system architecture and cryptology. His research interests include distributed systems, wireless and mobile computing systems, computer networks, and information and network security. He has published over 150 refereed articles in these areas and coauthored over ten books.