micromachines

MDPI

Article

Secure Transmission of Terahertz Signals with Multiple Eavesdroppers

Yuqian He [1], Lu Zhang [1], Shanyun Liu [2], Hongqi Zhang [1] and Xianbin Yu [1,2,*]

[1] College of Information Science and Electronic Engineering, Zhejiang University, Hangzhou 310027, China
[2] Zhejiang Lab, Hangzhou 310000, China
* Correspondence: xyu@zju.edu.cn

Abstract: The terahertz (THz) band is expected to become a key technology to meet the ever-increasing traffic demand for future 6G wireless communications, and a lot of efforts have been paid to develop its capacity. However, few studies have been concerned with the transmission security of such ultra-high-speed THz wireless links. In this paper, we comprehensively investigate the physical layer security (PLS) of a THz communication system in the presence of multiple eavesdroppers and beam scattering. The method of moments (MoM) was adopted so that the eavesdroppers' channel influenced by the PEC can be characterized. To establish a secure link, the traditional beamforming and artificial noise (AN) beamforming were considered as transmission schemes for comparison. For both schemes, we analyzed their secrecy transmission probability (STP) and ergodic secrecy capacity (ESC) in non-colluding and colluding cases, respectively. Numerical results show that eavesdroppers can indeed degrade the secrecy performance by changing the size or the location of the PEC, while the AN beamforming technique can be an effective candidate to counterbalance this adverse effect.

Keywords: THz communications; physical layer security; multiple eavesdroppers; beam scattering; artificial noise

Citation: He, Y.; Zhang, L.; Liu, S.; Zhang, H.; Yu, X. Secure Transmission of Terahertz Signals with Multiple Eavesdroppers. *Micromachines* **2022**, *13*, 1300. https://doi.org/10.3390/mi13081300

Academic Editors: Dmitri V. Lioubtchenko and Jeonghyun Kim

Received: 4 July 2022
Accepted: 9 August 2022
Published: 12 August 2022

1. Introduction

Wireless traffic volume has exponentially grown in recent years and wireless data rates exceeding 100 Gbit/s will be required in the coming decades [1]. As a result, new frequency spectra are demanded to fulfill the broad bandwidth requirements for future communication. Among others, the THz band (0.06–10 THz) is regarded as a promising candidate to enable ultra-fast and ultra-broadband data transmission [2–5]. Recently, THz wireless communication systems are under rapid development and many wireless transmissions exceeding 100 Gbit/s have already been demonstrated in laboratories and in field environments [6–11], which bring THz communication closer to reality. However, ultra-high-speed THz communications also pose major challenges to information security [12,13]. Once a malicious eavesdropper tries to intercept the signals, a vast amount of information will be leaked in the blink of an eye which is absolutely unacceptable, particularly in some sensitive fields such as the military and financial industry.

Security mechanisms exist at every layer of a network. Compared to the conventional upper-layer methods [14,15], physical-layer security (PLS) approaches [16–20] do not rely on the assumption that eavesdroppers have limited computational abilities and avoid distributing and managing secret keys [21–24]. In contrast to the broadcast nature of the microwave communication, highly directive THz waves are more prone to the blockage problem caused by the malicious eavesdropper [25,26]. Recently, researchers have comprehensively investigated the blocking effects of an illegal recipient and proposed a hybrid beamforming and reflecting scheme to eliminate the adverse effects [27,28]. In this environment, any eavesdropper intending to hide itself should control its size, otherwise, it may cast a detectable shadow and raise an alarm. Therefore, the performance of eavesdropping is restricted by the size of the illegal receiver. Alternatively, recent works have pointed

out that an eavesdropper may put a tiny passive object instead of itself, like a metal cup or a mobile phone, inside the narrow beam to scatter THz electromagnetic waves [29,30]. By this mean, the bulky illegal receiver placed outside the THz beam can capture the information signal without raising an alarm, as a consequence. We note that the feasibility of this scheme has already been demonstrated in experiments in which the eavesdropper can even intercept a signal strength as good as that of the intended receiver. Nevertheless, all the aforementioned work using scatter (tiny passive object) only consider a single-eavesdropper scenario while a case with multiple eavesdroppers has not been investigated. The reflector in the narrow beam scattering THz waves to multiple eavesdroppers may bring a greater security threat to the THz communication system.

Compared to the single eavesdropper, multiple eavesdroppers can increase the occurrence of stronger attackers that are closer to the legitimate transmitter due to the random spatial distribution [31,32]. Additionally, multiple eavesdroppers may also combine their own observations and jointly process their received message, which will considerably degrade the secrecy performance [33–35]. From a practical point of view, multi-eavesdropper scenes will be widespread phenomenon in our future, since potential eavesdroppers in the ubiquitous Internet of Things (IoT) may be some curious legitimate devices belonging to different subsystems [36]. However, secrecy performance and secure transmission schemes in highly directive THz communication systems have not been yet analyzed in the presence of multiple eavesdroppers. Moreover, how to safeguard this point-to-point THz system against randomly located eavesdroppers is still unknown.

In this paper, we comprehensively investigated the secrecy performance of a highly directive THz communication link with multiple eavesdroppers. We established the received signal models with two different multi-antenna techniques, namely traditional beamforming and AN beamforming, as transmission schemes for comparison. We note that the received signal mode is affected by the fading channel, where both the large-scale and small-scale effects matter. We emulate the effect of perfect electric conductor (PEC) parameters on the received signal-to-noise ratio (SNR) of Eve in a multiple-eavesdropper environment. We derive the mathematical framework of the STP and ESC in both non-colluding and colluding cases, so that the secrecy performance of the THz wireless link can be characterized. The results show that Eves can successfully intercept a huge amount of information by changing some parameters, such as the density, size, and distance. As a countermeasure, Alice could consider the deployment of the AN beamforming technique to counterbalance the adverse effect of multiple eavesdroppers.

The rest of the paper is organized as follows. In Section 2, we introduce the system model in the presence of multiple eavesdroppers. In Section 3, we analyze the STP and ESC in non-colluding and colluding cases, respectively. In Section 4, we conduct simulation experiments and demonstrate the factors affecting the secrecy performance. In Section 5, we discuss how one may find the attackers. Finally, we give a brief conclusion in Section 6. Additionally, the important notations in this paper are listed in Table 1 to make this paper clearer.

Table 1. Parameter settings.

Side	Symbol	Parameter Setting	Value
Alice	P	Transmitting power	−10 dBm
	G_t	Antenna gain	25/27 dBi
	N	Antenna number	Independent variable
	η	Power allocation ratio	Independent variable

Table 1. *Cont.*

Side	Symbol	Parameter Setting	Value
Channel	R_S	Covering radius	10/15 m
	λ_p	Density of eavesdroppers	Independent variable
	N_E	Number of eavesdroppers	Independent variable
	a	Radius of cylinder	Independent variable
	d_2	Distance between Eve and PEC	Independent variable
	d_3	Distance between Alice and PEC	Independent variable
	m	Nakagami fading parameters	2
Bob	d_1	Distance between Alice and Bob	Independent variable
	G_r	Antenna gain	25/27 dBi
Other	c	Speed of light	3×10^8 m/s
	f	Frequency	Independent variable
	P_N	Noise power	−75 dBm
	W	Bandwidth	50 GHz
	N-C	Non-colluding case	-
	C	Colluding case	-

2. System Model

In this section, we first propose a security model for the THz system, in which two transmission schemes, namely traditional beamforming and AN beamforming, are adopted to prevent being overheard by multiple eavesdroppers. Then, the details of the highly directive channel of Bob $\boldsymbol{h_B}$ and the scatter channel of Eve $\boldsymbol{h_E}$ are investigated, respectively.

2.1. Signal Model

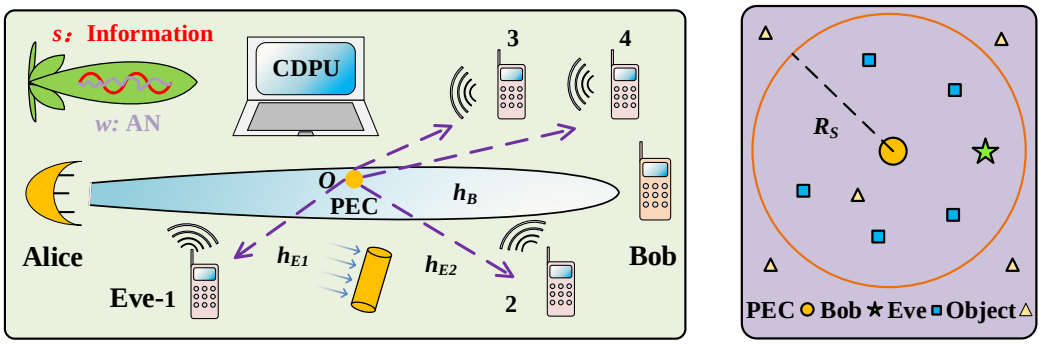
As shown in Figure 1a, a transmitter (Alice) sends a highly directive THz wave to the receiver (Bob) in the presence of multiple eavesdroppers (Eves). A PEC on the origin O is put inside this narrow beam between Alice and Bob. When there is an incident beam, PEC will scatter the THz signal to Eves in all directions (see Appendix A). We note that the PEC is located at the very edge of the THz beam with only a sliver of THz wave so it will not cast a detectable shadow in the receiver Bob. Additionally, the PEC is a cylinder which has the advantage of being able to scatter light in all directions, giving an attacker more flexibility. We model the locations of multiple eavesdroppers by the homogeneous Poisson point process (PPP) Φ in a circle region of radius R_S with a density λ_p, as shown in Figure 1b. The total number of Eves N_E in PPP is a random variable but the average number can be determined by $\overline{N_E} = \pi R_S^2 \lambda_p$. Due to the short transmission distance ($R_S < 15$ m) in an indoor environment, all receivers are supposed to be in a high SNR regime. Alice has N antennas while Bob and all the Eves use only one antenna each for reception.

When traditional beamforming is adopted, the received symbols at Bob and i-th Eve are, respectively, given by:

$$\boldsymbol{y_B} = \boldsymbol{h_B x} + n_B, \tag{1}$$

$$\boldsymbol{y_{E_i}} = \boldsymbol{h_{E_i} x} + n_E, \; i = 1, 2, \cdots, N_E, \tag{2}$$

where $\boldsymbol{h_B}$ and $\boldsymbol{h_{E_i}}$ are both $1 \times N$ vectors denoting the channel between Alice and Bob and between Alice and the i-th Eve, respectively; N_E is the total number of eavesdroppers; $\boldsymbol{x} = \boldsymbol{p} u_x$ is the transmitted signal containing the beamforming vector $\boldsymbol{p}$ and signal u_x with useful information; n_B and n_E are i.i.d. additive white Gaussian noise with $n \sim \mathcal{CN}(0, \sigma_n^2)$. We assume that both Alice and Bob only know the CSI of $\boldsymbol{h_B}$, while Eve knows both $\boldsymbol{h_B}$ and $\boldsymbol{h_{E_i}}$ perfectly, which is a more rigorous scenario for the security issue [37–39].



(**a**) (**b**)

Figure 1. System model. (**a**) Alice transmits a highly directive THz signal $\boldsymbol{x}$ to Bob with or without AN $\boldsymbol{w}$. A PEC (orange cylinder) located at the edge of beam can scatter the incident THz wave to Eves in all directions. (**b**) The spatial distribution of Eves is modeled as PPP in a circle region. The objects in this indoor scene can scatter THz signals.

With the introduction of AN beamforming, the transmitted THz signal $\boldsymbol{x}$ can be carefully designed as: $\boldsymbol{x} = \boldsymbol{s} + \boldsymbol{w}$. The information signal $\boldsymbol{s} = \boldsymbol{p}u_s$, where the $N \times 1$ beamforming vector $\boldsymbol{p} = \boldsymbol{h_B^\dagger}/||\boldsymbol{h_B}||$ and signal u_s with a variance of $\sigma_{u_s}^2$. The AN $\boldsymbol{w} = \boldsymbol{Z}\boldsymbol{v}$, where the $N \times (N-1)$ matrix $\boldsymbol{Z}$ is the null space of vector $\boldsymbol{h_B}$ so that $\boldsymbol{h_B Z} = 0$ while $\boldsymbol{h_E Z} \neq 0$ and noise vector $\boldsymbol{v}$ contains $(N-1)$ random noise elements with a variance of σ_v^2. Consequently, the received signals of Bob and i-th Eve are, respectively, given by:

$$\boldsymbol{y_B} = \boldsymbol{h_B}(\boldsymbol{s} + \boldsymbol{w}) + n_B = \boldsymbol{h_B p} u_s + n_B, \tag{3}$$

$$\boldsymbol{y_{E_i}} = \boldsymbol{h_{E_i}}(\boldsymbol{s} + \boldsymbol{w}) + n_E = \boldsymbol{h_{E_i} p} u_s + \boldsymbol{h_{E_i} Z v} + n_E. \tag{4}$$

The AN $\boldsymbol{w}$ passes through the channel $\boldsymbol{h_{E_i}}$ and finally develops into the additional noise $\boldsymbol{h_{E_i} w}$. We stress that, despite the AN, the $\boldsymbol{w}$ on Alice's side is sent to both the i-th Eve and Bob, whereas on the receiving side, the AN only deteriorates the i-th Eve without impacting Bob. As we can see, there is additional noise $\boldsymbol{h_{E_i} Z v}$ on Equation (4) while there is no extra term on Equation (3).

The total transmitter power $P = E[\boldsymbol{x}^\dagger \boldsymbol{x}] = \sigma_{u_s}^2 + (N-1)\sigma_v^2$, where $(\cdot)^\dagger$ denotes the conjugate transpose. We define η as the fraction of $\sigma_{u_s}^2$ to the total transmit power P. When $\eta = 1$, the AN beamforming is equivalent to traditional beamforming as the information signal is transmitted with the full power P. We note that η is an important design parameter that can optimize the secrecy performance.

2.2. Highly Directive Channel

The channel model of Bob $\boldsymbol{h_B}$ can be obtained as:

$$\boldsymbol{h_B} = l_B \boldsymbol{s_B}, \tag{5}$$

where l_B is the large-scale factor denoting the fixed pass loss and $\boldsymbol{s_B}$ is the small-scale random vector containing N elements. The l_B influenced by the free space pass loss (FSPL) and highly directive antennas is given by:

$$l_B = \frac{\lambda \sqrt{G_t G_r}}{4\pi d_1}, \tag{6}$$

where G_t and G_r, respectively, represent the antenna gains of Alice and Bob, and λ stands for the wavelength, and d_1 is the distance between Alice and Bob.

Unlike the conventional channel on the microwave band where the small-scale fading follows normal distribution, $\boldsymbol{s_B}$ on the THz band is usually represented by Nakagami-m distribution with the i-th element $s_{B_i} \sim Nakagami(m, 1)$, which has recently been proven

by experiments [40,41]. Finally, according to Equation (3), the signal-to-noise ratio (SNR) of Bob is given by:

$$\mathrm{SNR}_B = S_B \frac{L_B P \eta}{\sigma_n^2}, \tag{7}$$

where $S_B \sim Gamma(mN, m)$ and $L_B = l_B^2$ are given by Equation (6).

2.3. Scatter Channel

The scatter channel of Eve $\boldsymbol{h_E}$ is given by:

$$\boldsymbol{h_{E_i}} = l_{E_i} \boldsymbol{s_{E_i}}, \tag{8}$$

where l_i and $\boldsymbol{s_{E_i}}$ are, respectively, the large-scale factor and small-scale random vector of i-th Eve. The l_E and $\boldsymbol{s_E}$ are totally different from l_B and $\boldsymbol{s_B}$ owing to the PEC between Alice and Bob. The PEC between Alice and Bob is a kind of material with infinite conductivity and zero electric field inside. When the incident field E_i strikes the surface of PEC, it provokes a surface current J_Z that generates a scattered field E_s and total reflection occurs. By adopting the method of moments (MoM) [42], the scatter field E_s around the PEC at i-th Eve is given by (see Appendix A):

$$E_s = \frac{-k\eta_0}{4\pi} \sqrt{\frac{\eta_0 P G_t}{k d_{2_i}}} exp\{-j(k d_{2_i} - \frac{\pi}{4})\} \mathbf{C}^T \mathbf{A}^{-1} \mathbf{D}, \tag{9}$$

where k is the wave number, $\eta_0 \simeq 377\,\Omega$ is the intrinsic impedance of free space, d_{2_i} is the distance between the PEC and i-th Eve and the matrices $\mathbf{C}, \mathbf{A}, \mathbf{D}$ are determined by the shape, size, and location of the PEC. Here, we assume that the PEC is a cylinder with sufficient height. As such, we can denote the scattering coefficient $K(a, d_3) = \mathbf{C}^T \mathbf{A}^{-1} \mathbf{D}$, where a is the radius of PEC and d_3 is the distance between Alice and PEC. Therefore, the l_{E_i} can be derived as:

$$l_{E_i} = \sqrt{\frac{|E_s|^2}{2\eta_0} \frac{G_r \lambda^2}{4\pi P}} = \frac{\eta_0 \lambda K(a, d_3)}{8\pi} \sqrt{\frac{k G_t G_r}{2\pi d_{2_i}}}, \tag{10}$$

where we assume that Bob and all Eves have the same antenna gain G_r.

The scattering coefficient K is influenced by a and d_3. As shown in Figure 2, the THz wave nearly scatters uniformly around the PEC center ($d_2 \gg \lambda$, [42]) and the scattered field gradually fades along as it becomes farther away from the center. The scattering coefficient K increases with radius a and decreases with d_3, as we can see since the color in Figure 2b is deeper than that in Figure 2a.

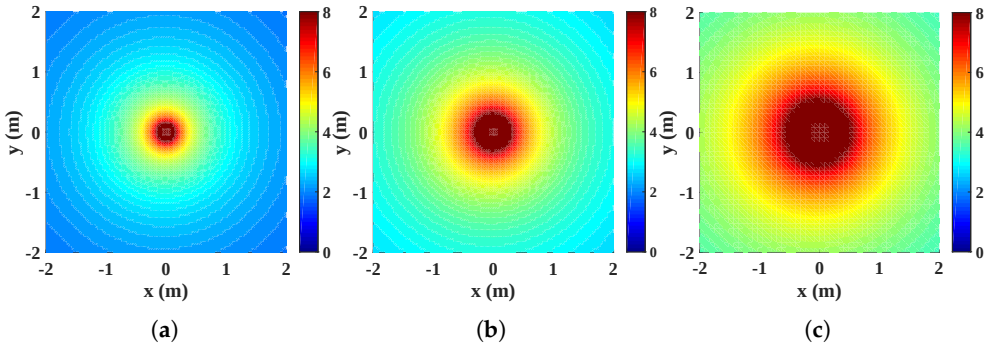


Figure 2. The scattered fields of PEC for (**a**) a = 20 mm, d_3 = 2 m (**b**) a = 40 mm, d_3 = 2 m (**c**) a = 40 mm, d_3 = 1.5 m. The maximum values were cut off at 8 since only a few values exceed it.

Unlike the main channel wherein a direct line-of-sight (LOS) link exists between Alice and Bob, Eve indirectly receives the signal information from non-line-of-sight (NLOS)

transmission. Many rays will scatter from PEC and finally converge on Eve's side as each point on the surface of PEC can generate an electromagnetic field. As such, a tiny move of PEC or Eve may tremendously change the received signal strength. Therefore, we assume $s_{E_i} \sim Nakagami(1,1)$, which is also a *Rayleigh* distribution. Based on Equation (4), the SNR of i-th Eve is given by:

$$\mathrm{SNR}_{E_i} = \frac{S_{E_i} L_{E_i} P\eta}{\frac{AL_{E_i} P(1-\eta)}{N_A - 1} + \sigma_n^2} \overset{(a)}{\leq} \phi S_{equal_i}, \tag{11}$$

where $A \sim Gamma(N-1)$, $S_{E_i} \sim Exp(1)$, $L_{E_i} = l_{E_i}^2$, the PDF of random variable S_{equal_i} is given by $f_{S_{equal}}(x) = \frac{N-1}{(1+x)^N}$ and $\phi = \frac{\eta(N-1)}{1-\eta}$, (a) holds for considering the worst-case situation where the normalized noise σ_n are arbitrarily small. Note that this approach was also taken in [16,35,37].

3. Secrecy Performance

In this section, we introduce STP and ECS which are both secrecy performance metrics. Then, we analyze the secrecy performance with and without AN in both non-colluding and colluding cases.

3.1. Performance Metrics

In the non-colluding case, the eavesdropper individually overhears the communication between Alice and Bob without any centralized processing. Therefore, the SNR of multiple eavesdroppers is given by $\mathrm{SNR}_E = \max(\mathrm{SNR}_{E_i})$, where SNR_{E_i} is defined in Equation (11). Whereas, in the colluding case, N_E Eves are capable of sending the information to a central data processing unit (CDPU) and jointly process their received information as shown in Figure 1a. Thus, the SNR of multiple eavesdroppers is given by $\mathrm{SNR}_E = \sum_{i=1}^{N_E} \mathrm{SNR}_{E_i}$. We adopt the following metrics to evaluate the secrecy performance of the proposed system.

Secure transmission probability (STP): STP is defined as a complementary element of secrecy outage probability (SOP) [31]. A supremum of the secrecy transmission rate R is determined by the difference of the main channel capacity $C_B = log(1 + \mathrm{SNR}_B)$ and the wiretap channel capacity $C_E = log(1 + \mathrm{SNR}_E)$. If secrecy transmission rates R are less than this supremum $C_S = C_B - C_E$, a secure transmission can be realized, otherwise, a secrecy outage occurs. The STP in non-colluding and colluding cases are, respectively, defined as:

$$P(C_S > R) = \prod_{E_i \in \Phi} P\left(\frac{1 + \mathrm{SNR}_B}{1 + \mathrm{SNR}_{E_i}} > 2^R\right), \tag{12}$$

$$P(C_S > R) = P\left(\frac{1 + \mathrm{SNR}_B}{1 + \sum \mathrm{SNR}_{E_i}} > 2^R\right). \tag{13}$$

Ergodic secrecy capacity (ESC): ESC is defined as the average transmission rate of the confidential message, which is formulated as:

$$\overline{C}_S = E[C_S] = \int_0^\infty P(C_S > R) dR. \tag{14}$$

In practice, ECS is used to describe the fast fading channel while STP for a slow fading channel. However, the numerical value of ECS is still determined by the STP. As long as we obtain the STP, the ESC can be simply calculated by its integration.

3.2. Non-Colluding Eavesdroppers

In a non-colluding eavesdroppers scenario, we investigated the STP for traditional beamforming ($\eta = 1$) and AN beamforming ($\eta \neq 1$). When traditional beamforming is adopted, we derived the exact value of STP, whereas AN is introduced, and we calculated the lower bound of STP which is a rigorous assumption and common practice [16,37].

We denote the STP for traditional beamforming as P_1 and for AN beamforming as P_2, respectively. Based on Equation (12), P_1 is given by:

$$P_1 = \prod_{E_i \in \Phi} P(\frac{1+\mathrm{SNR}_B}{1+\mathrm{SNR}_{E_i}} > 2^R) \overset{(b)}{=} E_{S_B}\{exp(-2\pi\lambda_p \int_0^{R_S} P(S_E > \frac{S_B L_B}{2^R L_E})\rho d\rho)\}, \tag{15}$$

where (b) holds for $\mathrm{SNR_B} \gg 1$, $\mathrm{SNR_E} \gg 1$ and the *probability generating functional lemma* (PGFL, ref. [43]) over PPP.

By denoting $u = kG_tG_r(\eta_0 K\lambda)^2/128\pi^3$, we have $L_E = u\frac{1}{d_2}$. As $S_E \sim E(1)$, the Equation (15) can finally be derived as:

$$P_1 = E_{S_B}\{exp(2\pi\lambda_p((vR_S + v^2)e^{-\frac{R_S}{v}} - v^2))\}, \tag{16}$$

where $v = u2^R/S_B L_B$.

Similarly to the calculation of P_1 and by denoting $\beta = \frac{2^R\sigma_n^2}{PL_B}$, $P_2(C_S > R)$ is given by:

$$P_2 = \prod_{E_i \in \Phi} P(\frac{1+\mathrm{SNR}_B}{1+\mathrm{SNR}_{E_i}} > 2^R) \overset{(c)}{=} E_{S_B}\{exp(\frac{-\pi R_S^2 \lambda_p}{(1+\frac{S_B\eta-\beta}{\beta\phi})^{N-1}})\}, \tag{17}$$

where (c) holds for $\mathrm{SNR_B} \gg 1$ and the PGFL over PPP.

3.3. Colluding Eavesdroppers

In colluding case, we denote the STP without AN as P_3 and with AN as P_4, respectively. The STP $P_3(C_S > R)$ is given by:

$$P_3 = P(\frac{1+\mathrm{SNR}_B}{1+\sum \mathrm{SNR}_{E_i}} > 2^R) = P(S_B > \frac{2^R \sum_{E_i \in \Phi} S_{E_i} L_{E_i}}{L_B}). \tag{18}$$

We let $I_1 = \sum_{E_i \in \Phi} S_{E_i} L_{E_i}$ and thus P_3 can be modified as:

$$P_3 = \int_0^\infty P(S_B > p_1 i) f_{I_1}(i) di \overset{(d)}{=} \sum_{b=0}^{mN-1} m_b p_1^b (-1)^b \mathcal{L}^{(b)}\{f_{I_1}(i)\}(mp_1), \tag{19}$$

where $f_{I_1}(i)$ is the probability density function (PDF) of I_1 and $p_1 = 2^R/L_B$, (d) holds for $S_B \sim Gamma(mN, m)$ and the complementary cumulative distribution function (CCDF) of S_B is given by $F_{S_B}^c = e^{-mx}\sum_{b \in B} m_b x^b$, where $m_b = \frac{m^b}{b!}$ and $b \sim (0, mN-1)$. The Laplace transformation $\mathcal{L}\{f_{I_1}(i)\}(mp_1)$ of function $f_{I_1}(i)$ is given by:

$$\mathcal{L}\{f_I\}(p_1) = exp\{-2\pi\lambda_p p_1 u R_S\}(1 + \frac{R_S}{p_1 u})^{2\pi\lambda p_1^2 u^2}. \tag{20}$$

By adopting *Bruno's formula* [44], we can obtain the n-degree derivation of $\mathcal{L}\{f_{I_1}(i)\}(p_1)$ as:

$$\mathcal{L}^{(n)}\{f_{I_1}\}(p_1) = \sum \frac{n!}{b_1! \cdot \cdot b_n!} e^{f(p_1)} \prod_{j=1}^{n} (\frac{f^{(j)}(p_1)}{j!})^{b_j}, \tag{21}$$

where the sum is over all the solutions $b_1, \cdots, b_n \geq 0$ to $b_1 + 2b_2 + \cdots + nb_n = n$. By denoting $w = R_S/u, c_1 = 2\pi\lambda_p, c_2 = 1 + \frac{w}{p_1}, c_3 = \frac{1}{p_1+w} - \frac{1}{p_1}, c_4 = \frac{1}{p_1^2} - \frac{1}{(p_1+w)^2}$, $f(p_1)$ and $f^{(j)}(p_1)$ are given by:

$$f(p_1) = c_1(p_1^2 u^2 lnc_2 - p_1 u R_S), \tag{22a}$$

$$f^{(1)}(p_1) = c_1(2p_1u^2lnc_2 + p_1^2u^2c_3 - uR_S), \tag{22b}$$

$$f^{(2)}(p_1) = c_1(2u^2lnc_2 + 4p_1u^2c_3 + p_1^2u^2c_4), \tag{22c}$$

$$f^{(j>2)}(p_1) = c_1u^2\sum_{kk=0}^{2} C_2^{kk}(-1)^{j-kk}\frac{j!}{(j-kk)}p_1^{2-kk}(\frac{1}{p_1^{j-kk}} - \frac{1}{(p_1+w)^{j-kk}}). \tag{22d}$$

When AN beamforming is introduced, $P_4(C_S > R)$ is given by:

$$P_4 = \int_0^\infty P(S_B > p_2 i)f_{I_2}(i)di = P(S_B > \frac{\beta(1+\sum_{E_i\in\Phi}\phi S_{equal_i})}{\eta}). \tag{23}$$

We let $I_2 = 1 + \sum_{E_i\in\Phi}\phi S_{equal_i}$ and thus P_4 can be rewritten as:

$$P_4 = \int_0^\infty P(S_B > p_2 i)f_{I_2}(i)di = \sum_{b=0}^{mN-1} m_b p_2^b(-1)^b\mathcal{L}^{(b)}\{f_{I_2}(i)\}(mp_2), \tag{24}$$

where $f_{I_2}(i)$ is the PDF of I_2 and $p_2 = \frac{\beta}{\eta}$. As long as we obtain $\mathcal{L}\{f_{I_2}(i)\}(mp_2)$, P_4 can be calculated. The Laplace transformation $\mathcal{L}\{f_{I_2}(i)\}(p_2)$ is given by:

$$\mathcal{L}\{f_{I_2}\}(p_2) = exp\{-p_2 - N_E + q_1q_2\}, \tag{25}$$

where $q_1 = exp(p_2\phi)E_N(p_2\phi)$, $E_N(x) = \int_1^\infty \frac{e^{-xt}}{t^N}dt$ is the N-degree exponential integral and $q_2 = N_E(N-1)$. As such, the n-degree of $\mathcal{L}\{f_{I_2}(i)\}(p_2)$ is given by:

$$\mathcal{L}^{(n)}\{f_{I_2}\}(p_2) = \sum\frac{n!}{b_1!\cdot\cdot b_n!}e^{g(p_2)}\prod_{j=1}^{n}(\frac{g^{(j)}(p_2)}{j!})^{b_j}, \tag{26}$$

where $g(p_2)$ and $g^{(j)}(p_2)$ are given by:

$$g(p_2) = -p_2 - N_E + q_1q_2, \tag{27a}$$

$$g^{(1)}(p_2) = -1 + q_2\phi e^{k\phi}(E_N - E_{N-1}), \tag{27b}$$

$$g^{(j\geq 2)}(p_2) = q_2\phi^j e^{k\phi}\sum_{jj=0}^{j} C_j^{jj}(-1)^{jj}E_{N-jj}. \tag{27c}$$

4. Security Analysis

In what follows, we describe Eve's strategies to degrade the secrecy performance with a PEC, and then we show the function of AN as a countermeasure to resist the multiple eavesdroppers. Meanwhile, power allocation as a significant parameter of AN beamforming is also analyzed. Table 1 shows the parameter settings.

4.1. Eve's Attack

The intensity of Eves' attack is affected by the spatial distribution. In Figure 3a, when we compare the blue line with the red and yellow line, respectively, we find that the covering radius R_S has little effect on STP while density λ_p significantly reduces the STP. However, in Figure 3b, both the value of R_S and λ_p have significant impacts on the STP. The reason is that the SNR of multiple eavesdroppers in the non-colluding case depends on the 'nearest' Eve which has the best channel quality while the SNR in the colluding case only depends on the total number. The parameter R_S can barely increase the chance of the 'nearest' Eve as the THz transmit power quickly attenuates with the distance but indeed increases the total number of them. Therefore, from Eves' perspective, they have to focus on 'a better channel' or 'a better location' rather than the total number in a non-colluding

case, as we can see the STP of the case when $\overline{N_E}$ = 17 performs even better than the STP when $\overline{N_E}$ = 7 in Figure 3a.

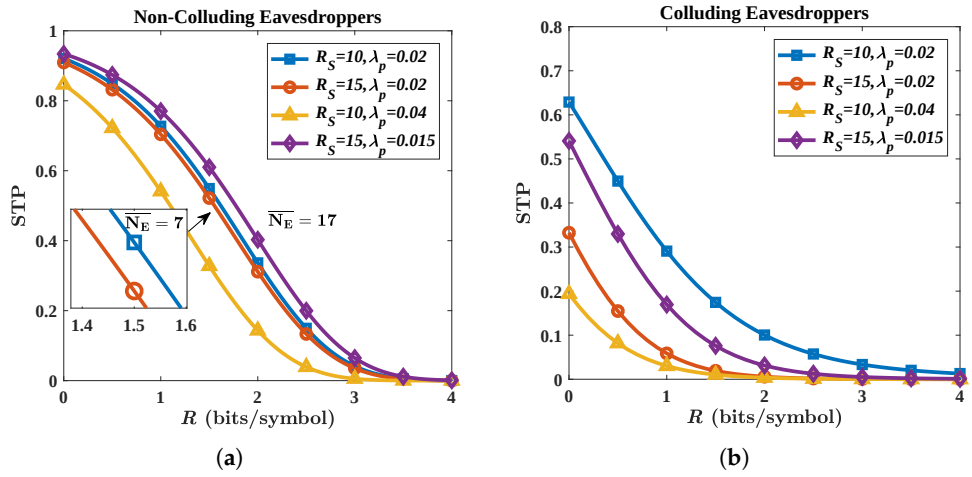


Figure 3. Secure transmission probability (STP) under different R_S and λ_p for (**a**) non-colluding case and (**b**) colluding case. Parameters are given by: G = 25 dBi; N = 5; f = 300 GHz; and P = −10 dBm.

In Figure 4, we use normalized secrecy capacity [30] to show the extent to which Eves reduce the secrecy capacity in non-colluding and colluding cases, respectively. It is shown that for d_2 = 20, the existence of Eves reduces the original capacity by 20% in non-colluding case and by nearly 40% in colluding case.

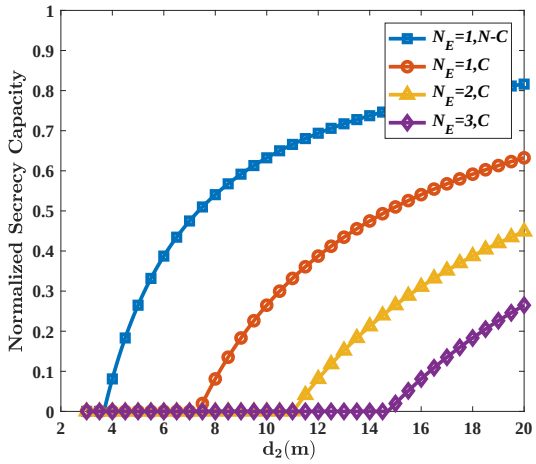


Figure 4. The normalized secrecy capacity as a function of d_2 in the non-colluding and colluding cases. Here, all the eavesdroppers have the same distance d_2 to the PEC and the channel fading is ignored. Other parameters are given by: G = 25 dBi; f = 300 GHz; P = −10 dBm; R_S = 15 m; and d_3 = 1 m.

Eve can move the PEC closer to Alice to strengthen the attack. In Figure 5, we find that the ESC monotonically increases with d_3 (PEC) while decreasing with the d_1 (Bob). In addition, the parameters d_1 and d_3 may have interacted with each other. For example, for d_1 = 3, a unit increase in d_3 will give birth to the improved ESC by ΔESC = 1.45. For d_1 = 5, ΔESC becomes 1.95. That is to say, $d_3(d_1)$ may exhibit a different effect when the other factor changes. Furthermore, if PEC is located in the midpoint between Alice and Bob, the ESC will not change significantly with the increase in d_1, as we can see that the white line in Figure 5 nearly remains unchanged at ESC = 4.85.

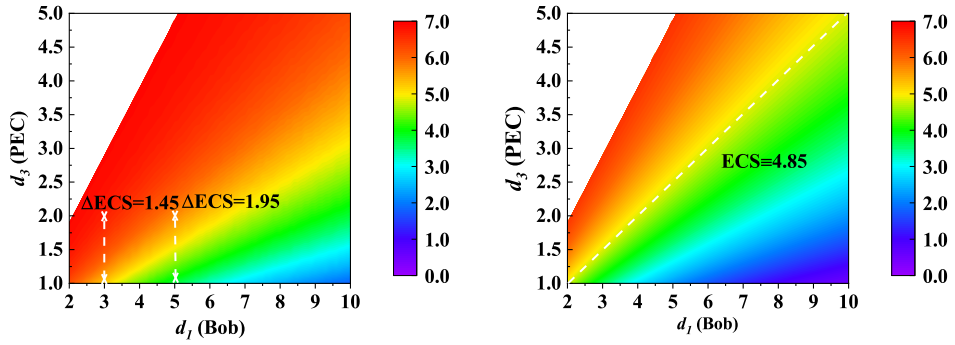


Figure 5. Ergodic secrecy capacity (ESC) as a function of d_1 (Alice–Bob) and d_3 (Alice–PEC) for (**a**) non-colluding eavesdroppers and (**b**) colluding eavesdroppers. Other parameters are given by: $G = 25$ dBi; $N = 3$; $f = 300$ GHz; $P = -10$ dBm; $R_S = 15$ m; and $\lambda_p = 0.015$.

Eve can increase the size of PEC to strengthen the attack. In Figure 6a, we find that the STP will decrease when the radius a rises from 20 mm to 40 mm, regardless of whether it is in the non-colluding case or in the colluding case. As shown in Figure 2, as a grows from 20 mm to 40 mm, the electromagnetic field around the PEC will be augmented and hence Eves obtains better signal quality. Additionally, we find that Eves benefit from increasing a to various degrees when the location of PEC d_3 changes. For $d_3 = 5$ m, as shown in Figure 6b, reducing a from 10 mm to 50 mm will lead to an ESC decrease of 36%. For $d_3 = 1$ m, however, reducing a from 10 to 50 decreases the ESC by 87% to nearly 0 which means that Eves can almost intercept all the information. Since being too near to Alice will increases the risk of being detected, Eve's strategy is to select a proper size and optimal location in such a way she can obtain as good a signal strength as possible and hide herself simultaneously.

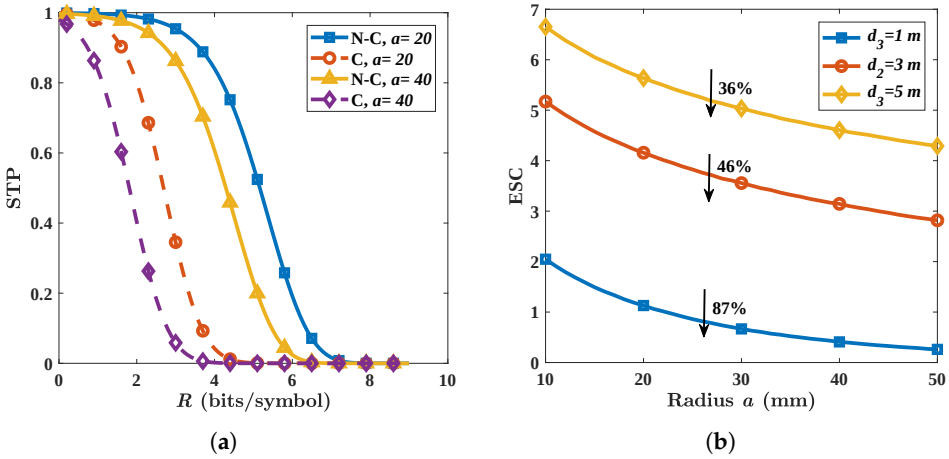


Figure 6. (**a**) Influence of radius a on STP. (**b**) ESC versus radius a under different PEC location d_3. The solid line describes the non-colluding case while the dashed line describes the colluding case. Other parameters are given by: $G = 25$ dBi; $N = 3$; $f = 300$ GHz; $P = -10$ dBm; $R_S = 15$ m; and $\lambda_p = 0.04$.

4.2. AN as a Countermeasure

We find that the AN beamforming can compensate for the detriment of multiple eavesdroppers. As shown in Figure 7, the increase in λ_p causes an STP ($P(C_S \geq 0)$) reduction from 0.85 to 0.75 and 0.5 to 0.1, respectively. However, with the introduction of AN in the non-colluding case, the STP ($P(C_S \geq 0)$) rises to 0.95, leading to an improvement

of nearly 27%. In the colluding case, the STP rises to 0.7, corresponding to an improvement of 600%. It is noteworthy that the detriment of multiple eavesdroppers in the colluding case is more than that in the non-colluding case. In the non-colluding case, for $R > 2$, the STP with AN beamforming ($\lambda_p = 0.02$) is higher than that with traditional beamforming ($\lambda_p = 0.01$). However, in the colluding case, the situation is reversed for $R > 2$ which means that colluding eavesdroppers cause greater damage to transmission security.

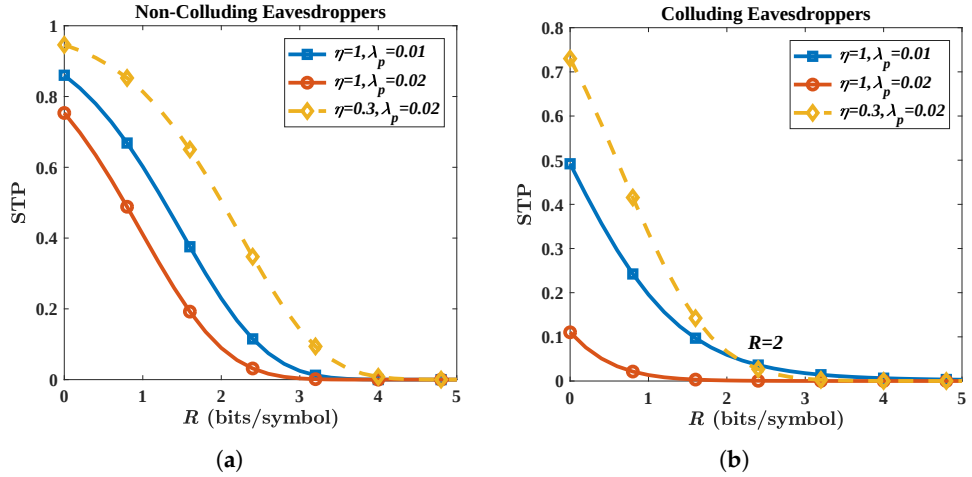


Figure 7. The benefit of AN on STP for (**a**) a non-colluding case; and a (**b**) colluding case. Other parameters are given by: G = 25 dBi, N = 3, f = 300 GHz, P = −10 dBm, R_S = 15 m, η = 0.3.

In Figure 8, we find that the optimal η depends on both density λ_p and the number of antennas N. For $\lambda_p = 0.01$ (blue and yellow line), the optimal η in the non-colluding and colluding cases is 0.28 and 0.22, respectively, which are larger than 0.21 and 0.15 for $\lambda_p = 0.02$. More Eves around PEC signify stronger information attacks. Therefore, Alice must allocate more transmission power to AN to resist the adverse effect of the added Eves. Additionally, the optimal value of η increases with N. As shown in the inset, the optimal η are 0.34 and 0.27 for $N = 6$ while 0.28 and 0.22 for $N = 2$. We stress that only Bob benefits from the increase in antennas since the transmitter maximizes the signal strength to Bob and the signal power at Eves' side remains unchanged.

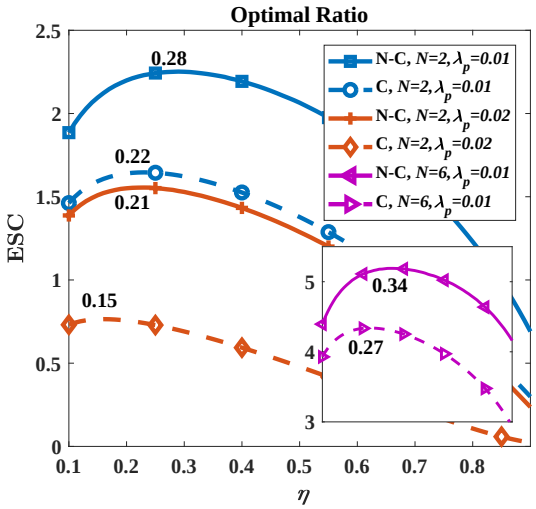
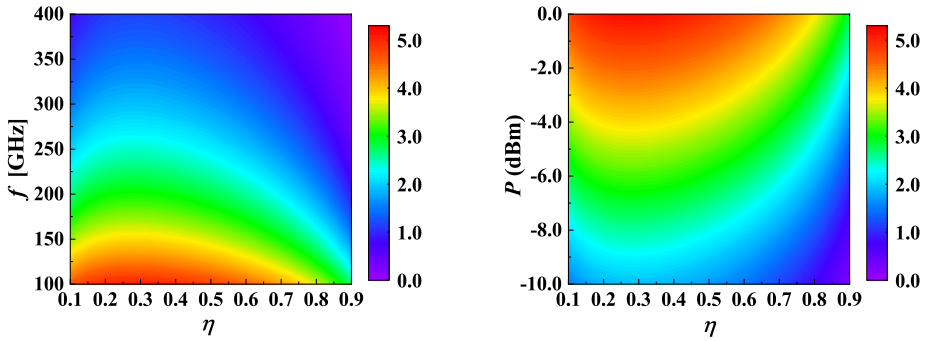


Figure 8. The optimal η under different λ_p and N. The solid line describes non-colluding cases while the dashed line describes colluding cases. The main figure for N = 2 while the inset for N = 6. Other parameters are given by: G = 27 dBi; f = 300 GHz; P = −10 dBm; and R_S = 15 m.

In Figure 9, we find that the ESC decreases with the f while increasing with the P when $\eta \neq 1$. For a system without AN, the ESC will not be influenced by P since $\mathrm{SNR_B}$ and $\mathrm{SNR_E}$ benefit from them to the same extent, as shown by Equations (7) and (11). However, with the introduction of AN, P can no longer influence the supremum of $\mathrm{SNR_E}$ but still impacts $\mathrm{SNR_B}$. Additionally, we also find P and f cannot significantly change the optimal η. In Figure 9a,b, the optimal η varies in the ranges of 0.27∼0.31 and 0.26∼0.3 with standard deviations (STD) of 1.13×10^{-2} and 1.14×10^{-2}, respectively, lending to a tiny change. We note that despite Figure 9 only showing a non-colluding case, the same rule can also be applied to the colluding scenario.



(**a**) (**b**)

Figure 9. Secrecy performance in a non-colluding case. (**a**) The ECS as a function of η and f with $P = -10$ dBm; (**b**) The ECS as a function of η and P with f = 300 GHz. Other parameters are given by: G = 25 dBi, N = 3, R_S = 15 m, λ_p = 0.02.

5. Discussion

In practice, the first step to guarantee transmission security is to determine whether attackers exist instead of determining how to resist attackers. Therefore, before using unique techniques (such as AN), we should adopt a specific measure to detect the existence of an attacker, otherwise, many resources will be wasted. Recent work in [30] can successfully distinguish the suspicious objects from the ordinary environment through measuring the incoming signal. Here, we consider the possibility of increasing the beam directivity or enlarging the aperture of the receiver to guarantee the security. In this paper, the diameter of the THz beam is larger than the aperture of the receiver. Thus, Eves can utilize the edge of the beam to realize an attack. However, if the receiver has the ability to capture all of the transmitted THz wave without any leakage, any eavesdroppers trying to put an object in the beam will cause an extensive power reduction on Bob' side. In this case, if Eves still wants to implement an attack, she needs to either utilize the misalignment effect between Alice and Bob which may also induce a leakage or pretend to be irrelevant moving objects. Nevertheless, either way, Eves' strategy to implement an attack would be significantly more complicated and harder to implement. Another purpose of increasing the directivity is to resist the interference. Transceivers on the same unlicensed bandwidth may have interacted with each other. Additionally, jammers can also take advantage of this large bandwidth in the THz band for interference [45]. Increasing their directivity gains can make irrelevant transceivers and jammers either less effective or need to increase their transmit power.

In some cases, Eves are not afraid of being found because they are intended to block the signal power of Bob (reduce the secrecy capacity at the same time). As a countermeasure, multiple IRS-assisted THz systems with opportunistic connectivity may be a choice since Alice can choose different ways to transmit the signal and design unique beamforming schemes to maximize the secrecy rate performance. Researchers have found that opportunistic connectivity [46] with well-designed beamforming schemes can significantly boost the secrecy rate performance and reduce blocking probability.

6. Conclusions

In this paper, we investigated the secure transmission of THz waves in the indoor environment against randomly distributed eavesdroppers. We established the PLS model for this THz communication system, where Bob's channel is featured by a highly directive beam while Eve's channel scatters THz waves. Particularly, we characterize both channels with stochastic small-scale fading in order to accommodate the random variation in practice such as scattering on aerosols or the movement of objects. The security performance of traditional beamforming and AN beamforming in both non-colluding and colluding cases are analyzed by deriving the STP and ESC. Based on our analysis, we reveal that Eves can indeed take different strategies to degrade the secrecy performance, for instance, by changing the size or the distance of the scatter and increasing the density. To deal with this issue, an AN beamforming technique with a well-designed power allocation can be an effective candidate to counterbalance this adverse effect. Our study can not only serve as an inspiration for eavesdropping scenes but also for a widespread network scenario. Future work may extend this point-to-point communication scene to an indoor THz wireless local area networks (WLANs) which seem more appealing.

Author Contributions: Design, fabrication, and data analysis, Y.H. and X.Y.; software, Y.H. and L.Z., writing—original draft preparation, Y.H.; writing—review and editing, S.L. and H.Z.; supervision, X.Y. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported by the National Key Research and Development Program of China (2020YFB1805700), in part by the Natural National Science Foundation of China under Grant 62101483, in part by the Natural Science Foundation of Zhejiang Province under Grant LQ21F010015, the Fundamental Research Funds for the Zhejiang Lab (no. 2020LC0AD01), the State Key Laboratory of Advanced Optical Communication Systems and Networks of Shanghai Jiao Tong University and in part by Zhejiang Lab (NO. 2020LC0AA03).

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

Appendix A

When the incident field E_i strikes the surface of PEC, it provokes surface current J_Z on PEC, which in turn generates a scattered field E_s which is given by:

$$E_s(\rho) = -\frac{k\eta_0}{4}\int_C J_Z(\rho')H_0^{(2)}(k|\rho-\rho'|)dS', \tag{A1}$$

where ρ is the field point on the plane, ρ' is the source point on the surface and $H_0^{(2)}$ is the Hankel function of the second kind of zero order. The integral in Equation (A1) is along the surface C which is divided into N_C segments. According to the property of PEC, the incident field of segment n $E_i({\rho'}_n)$ is given by:

$$E_i({\rho'}_n) = -\frac{k\eta_0}{4}\Sigma_{m=1}^{N} J_Z({\rho_m}')H_0^{(2)}(k|{\rho'}_n-{\rho_m}'|)\Delta C_m, \tag{A2}$$

where ${\rho'}_n$, ${\rho'}_m$ is, respectively, the midpoint of segment n and m and ΔC_m is the length of segment m. By applying Equation (A2) to all the segments, there are totally N_C equations and all the equations can be cast in matrix form as:

$$\begin{bmatrix} E_i({\rho'}_1) \\ \cdots \\ E_i({\rho'}_{N_C}) \end{bmatrix} = \begin{bmatrix} A_{11} & \cdots & A_{1N_C} \\ \cdots & \cdots & \cdots \\ A_{N_C1} & \cdots & A_{N_CN_C} \end{bmatrix} \begin{bmatrix} J({\rho'}_1) \\ \cdots \\ J({\rho'}_{N_C}) \end{bmatrix}, \tag{A3}$$

where the elements of impedance matrix **A** are influenced by the PEC itself and the incident field of segment n $E_i({\rho'}_n)$ is also given by $E_i({\rho'}_n) = \sqrt{2\eta_0 PG_t/4\pi D_n^2}$, where $D_n = d_3 +$

$acos\theta_n$ is the distance between Alice and the segment n. Finally, we can calculate the scatter field E_s by substituting $E_i(\rho'_n)$ and Equation (A3) into Equation (A2):

$$\begin{aligned} E_s(\rho) &= \frac{-k\eta_0}{4}\begin{bmatrix} H_0^{(2)}(k|\rho-\rho'_1|)\Delta C_1 \\ \cdots \\ H_0^{(2)}(k|\rho-\rho'_{N_C}|)\Delta C_{N_C} \end{bmatrix}^T \mathbf{A}^{-1}\begin{bmatrix} E_i(\rho'_1) \\ \cdots \\ E_i(\rho'_{N_C}). \end{bmatrix} \\ &\overset{(e)}{=} \frac{-k\eta_0}{4\pi}\sqrt{\frac{\eta_0 P G_t}{kd_2}}exp\{-j(kd_2-\frac{\pi}{4})\}\mathbf{C}^T\mathbf{A}^{-1}\mathbf{D}, \end{aligned} \tag{A4}$$

where $\mathbf{C} = [\Delta C_1 \cdots \Delta C_{N_C}]$, $\mathbf{D} = [1/D_1 \cdots \Delta 1/D_{N_C}]^T$, (e) holds for $kd_2 \gg 1$ in the THz band so that approximations can be made with $|\rho - \rho'| \approx d_2$.

References

1. Nagatsuma, T.; Ducournau, G.; Renaud, C.C. Advances in terahertz communications accelerated by photonics. *Nat. Photonics* **2016**, *10*, 371–379. [CrossRef]
2. Chen, S.; Liang, Y.C.; Sun, S.; Kang, S.; Cheng, W.; Peng, M. Vision, requirements, and technology trend of 6G: How to tackle the challenges of system coverage, capacity, user data-rate and movement speed. *IEEE Wirel. Commun.* **2020**, *27*, 218–228. [CrossRef]
3. Huq, K.M.; Kazi, M.S.; Busari, S.A.; Rodriguez, J.; Frascolla, V.; Bazzi, W.; Sicker, D.C. Terahertz-enabled wireless system for beyond-5G ultra-fast networks: A brief survey. *IEEE Netw.* **2019**, *33*, 89–95. [CrossRef]
4. Zhang, Z.; Xiao, Y.; Ma, Z.; Xiao, M.; Ding, Z.; Lei, X.; Karagiannidis, G.K.; Fan, P. 6G wireless networks: Vision, requirements, architecture, and key technologies. *IEEE Veh. Technol. Mag.* **2019**, *14*, 28–41. [CrossRef]
5. Han, C.; Bicen, A.O.; Akyildiz, I.F. Multi-ray channel modeling and wideband characterization for wireless communications in the terahertz band. *IEEE Trans. Wirel. Commun.* **2015**, *14*, 2402–2412. [CrossRef]
6. Yu, X.; Jia, S.; Hu, H.; Galil, M.; Morioka, T.; Jepsen, P.U.; Oxenløwe, L.K. 160 Gbit/s photonics wireless transmission in the 300–500 GHz band. *Apl Photonics* **2016**, *1*, 081301. [CrossRef]
7. Jia, S.; Pang, X.; Ozolins, O.; Yu, X.; Hu, H.; Yu, J.; Guan, P.; Ros, F.D.; Po, S.; Jacobsen, G.; et al. 0.4 THz photonic-wireless link with 106 Gb/s single channel bitrate. *J. Lightw. Technol.* **2018**, *36*, 610–616. [CrossRef]
8. Zhang, H.; Zhang, L.; Wang, S.; Lu, Z.; Yang, Z.; Liu, S.; Qiao, M.; He, Y.; Pang, X.; Zhang, X.; et al. Tbit/s multi-dimensional multiplexing THz-over-fiber for 6G wireless communication. *J. Lightw. Technol.* **2021**, *39*, 5783–5790. [CrossRef]
9. Wang, S.; Lu, Z.; Li, W.; Jia, S.; Zhang, L.; Qiao, M.; Pang, X.; Idrees, N.; Saqlain, M.; Gao, X.; et al. 26.8-m THz wireless transmission of probabilistic shaping 16-QAM-OFDM signals. *APL Photonics* **2020**, *5*, 056105. [CrossRef]
10. Harter, T.; Füllner, C.; Kemal, J.N.; Ummethala, S.; Steinmann, J.L.; Brosi, M.; Hesler, J.L.; Bründermann, E.; Müller, A.-S.; Freude, W.; et al. Generalized Kramers–Kronig receiver for coherent terahertz communications. *Nat. Photonics* **2020**, *14*, 601–606. [CrossRef]
11. Idrees, N.M.; Lu, Z.; Saqlain, M.; Zhang, H.; Wang, S.; Zhang, L.; Yu, X. A W-Band Communication and Sensing Convergence System Enabled by Single OFDM Waveform. *Micromachines* **2022**, *13*, 312. [CrossRef]
12. Yang, P.; Xiao, Y.; Xiao, M.; Li, S. 6G wireless communications: Vision and potential techniques. *IEEE Netw.* **2019**, *33*, 70–75. [CrossRef]
13. Tariq, F.; Khandaker, M.R.; Wong, K.K.; Imran, M.A.; Bennis, M.; Debbah, M. A speculative study on 6G. *IEEE Wirel. Commun.* **2020**, *27*, 118–125. [CrossRef]
14. Zou, Y.; Zhu, J.; Wang, X.; Hanzo, L. A survey on wireless security: Technical challenges, recent advances, and future trends. *Proc. IEEE* **2016**, *104*, 1727–1765. [CrossRef]
15. Yang, N.; Wang, L.; Geraci, G.; Elkashlan, M.; Yuan, J.; Renzo, M.D. Safeguarding 5G wireless communication networks using physical layer security. *Nat. Photonics* **2015**, *53*, 20–27. [CrossRef]
16. Goel, S.; Negi, R. Guaranteeing secrecy using artificial noise. *IEEE Trans. Wirel. Commun.* **2008**, *7*, 2180–2189. [CrossRef]
17. Li, B.; Zhang, M.; Rong, Y.; Han, Z. Artificial Noise-Aided Secure Relay Communication With Unknown Channel Knowledge of Eavesdropper. *IEEE Trans. Wirel. Commun.* **2021**, *20*, 3168–3179. [CrossRef]
18. Yang, F.; Zhang, K.; Zhai, Y.; Quan, J.; Dong, Y. Artificial Noise Design in Time Domain for Indoor SISO DCO-OFDM VLC Wiretap Systems. *J. Lightw. Technol.* **2021**, *39*, 6450–6458. [CrossRef]
19. Xu, W.; Li, B.; Tao, L.; Xiang, W. Artificial Noise Assisted Secure Transmission for Uplink of Massive MIMO Systems. *IEEE Trans. Veh. Technol.* **2021**, *70*, 6750–6762. [CrossRef]
20. Ding, X.; Song, T.; Zou, Y.; Chen, X.; Hanzo, L. Security-reliability tradeoff analysis of artificial noise aided two-way opportunistic relay selection. *IEEE Trans. Veh. Technol.* **2017**, *66*, 3930–3941. [CrossRef]
21. Wyner, A.D. The wire-tap channel. *Bell Syst. Tech. J.* **1975**, *54*, 1355–1387. [CrossRef]
22. Gopala, P.K.; Lai, L.; Gamal, H.E. On the secrecy capacity of fading channels. *IEEE Trans. Inf. Theory* **2008**, *10*, 4687–4698. [CrossRef]

23. Shafiee, S.; Liu, N.; Ulukus, S. Towards the secrecy capacity of the Gaussian MIMO wire-tap channel: The 2-2-1 channel. *IEEE Trans. Inf. Theory* **2009**, *55*, 4033–4039. [CrossRef]
24. Helena, R.P.; Jordi, H.J. Computational and energy costs of cryptographic algorithms on handheld devices. *Future Internet* **2011**, *3*, 31–48.
25. Jia, S.; Lo, M.-C.; Zhang, L.; Ozolins, O.; Udalcovs, A.; Kong, D.; Pang, X.; Yu, X.; Xiao, S.; Popov, S.; et al. Integrated dual-DFB laser for 408 GHz carrier generation enabling 131 Gbit/s wireless transmission over 10.7 meters. In Proceedings of the Optical Fiber Communication Conference, San Diego, CA, USA, 7 March 2019.
26. Guerboukha, H.; Shrestha, R.; Neronha, J.; Ryan, O.; Hornbuckle, M.; Fang, Z.; Mittleman, D.M. Efficient leaky-wave antennas at terahertz frequencies generating highly directional beams. *Appl. Phys. Lett.* **2020**, *117*, 261103. [CrossRef]
27. Qiao, J.; Alouini, M. Secure Transmission for Intelligent Reflecting Surface-Assisted mmWave and Terahertz Systems. *IEEE Wirel. Commun. Lett.* **2020**, *9*, 1743–1747. [CrossRef]
28. Qiao, J.; Zhang, C.; Dong, A.; Bian, J.; Alouini, M. Securing Intelligent Reflecting Surface Assisted Terahertz Systems. *IEEE Trans. Veh. Technol.* 2022, *accepted*. [CrossRef]
29. Steinmetzer, D.; Chen, J.; Classen, J.; Knightly, E.; Hollick, M. Eavesdropping with periscopes: Experimental security analysis of highly directional millimeter waves. In Proceedings of the IEEE Conference on Communications and Network Security (CNS), Florence, Italy, 28–30 September 2015.
30. Ma, J.; Shrestha, R.; Adelberg, J.; Yeh, C.Y.; Hossain, Z.; Knightly, E.; Jornet, J.M.; Mittleman, D.M. Security and eavesdropping in terahertz wireless links. *Nature* **2018**, *563*, 89–93. [CrossRef]
31. Ju, Y.; Wang, H.W.; Zheng, T.X.; Yin, Q.; Lee, M.H. Safeguarding millimeter wave communications against randomly located eavesdroppers. *IEEE Trans. Wirel. Commun.* **2018**, *17*, 2675–2689. [CrossRef]
32. Wu, Y.; Kokkoniemi, J.; Han, C.; Juntti, M. Interference and coverage analysis for terahertz networks with indoor blockage effects and line-of-sight access point association. *IEEE Trans. Wirel. Commun.* **2020**, *20*, 1472–1486. [CrossRef]
33. Pinto, P.C.; Barros, J.; Win, M.Z. Wireless physical-layer security: The case of colluding eavesdroppers. In Proceedings of the IEEE International Symposium on Information Theory, Seoul, Korea, 28 June–3 July 2009.
34. Zhou, X.; Ganti, R.K.; Andrews, J.G. Secure wireless network connectivity with multi-antenna transmission. *IEEE Trans. Wirel. Commun.* **2011**, *10*, 425–430. [CrossRef]
35. Zhang, X.; Zhou, X.; McKay, M.R. Enhancing secrecy with multi-antenna transmission in wireless ad hoc networks. *IEEE Trans. Inf. Forensics Secur.* **2013**, *11*, 1802–1814. [CrossRef]
36. Xu, Q.; Ren, P.; Song, H.; Du, Q. Security enhancement for IoT communications exposed to eavesdroppers with uncertain locations. *IEEE Access* **2016**, *4*, 2840–2853. [CrossRef]
37. Zhou, X.; McKay, M.R. Secure transmission with artificial noise over fading channels: Achievable rate and optimal power allocation. *IEEE Trans. Veh. Technol.* **2010**, *59*, 3831–3842. [CrossRef]
38. Wang, H.M.; Zheng, T.; Xia, X.G. Secure MISO wiretap channels with multiantenna passive eavesdropper: Artificial noise vs. artificial fast fading. *IEEE Trans. Wirel. Commun.* **2015**, *14*, 94–106. [CrossRef]
39. Zhang, X.; McKay, M.R.; Zhou, X.; Heath, R.W. Artificial-noise-aided secure multi-antenna transmission with limited feedback. *IEEE Trans. Wirel. Commun.* **2015**, *14*, 2742–2754. [CrossRef]
40. Papasotiriou, E.N.; Boulogeorgos, A.A.A.; Alexiou, A. Performance analysis of THz wireless systems in the presence of antenna misalignment and phase noise. *IEEE Commun. Lett.* **2020**, *24*, 1211–1215. [CrossRef]
41. Ekti, A.R.; Boyaci, A.; Alparslan, A.; Ünal, İ.; Yarkan, S.; Görçin, A.; Arslan, H.; Uysal, M. Statistical modeling of propagation channels for terahertz band. In Proceedings of the IEEE Conference on Standards for Communications and Networking (CSCN), Helsinki, Finland, 18–20 September 2017.
42. Sadiku, M.N. *Numerical Techniques in Electromagnetics*, 2nd ed.; CRC Press: Boca Raton, FL, USA, 2000.
43. Stoyan, D.; Kendall, W.; Mecke, J. *Stochastic Geometry and Its Applications*, 2nd ed.; John Wiley and Sons: Hoboken, NJ, USA, 1996.
44. Johnson, W. The curious history of Faà di Bruno's formula. *Am. Math. Mon.* **2002**, *109*, 217–234.
45. Shrestha, R.; Guerboukha, H.; Fang, Z.; Knightly, E.; Mittleman, D.M. Jamming a terahertz wireless link. *Nat. Commun.* **2022**, *13*, 3045. [CrossRef]
46. Boulogeorgos, A.A.A.; Jornet, J.; Alexiou, A. Directional terahertz communication systems for 6G: Fact check: A quantitative look. *IEEE Veh. Technol. Mag.* **2021**, *16*, 68–77. [CrossRef]