Hindawi
Wireless Communications and Mobile Computing
Volume 2022, Article ID 5445676, 10 pages
https://doi.org/10.1155/2022/5445676

Research Article

Physical Layer Security of Two-Way Ambient Backscatter Communication Systems

Hao Wang[1], **Junjie Jiang**[1], **Gaojian Huang**[1], **Wenbin Wang**[2], **Dan Deng**[3], **Basem M. Elhalawany**[4] and **Xingwang Li**[1]

[1]*School of Physics and Electronic Information Engineering, Henan Polytechnic University, Jiaozuo 454000, China*
[2]*Henan Chuitian Technology Co., Ltd., Hebi 458000, China*
[3]*School of Information Engineering, Guangzhou Panyu Polytechnic, Guangzhou 410630, China*
[4]*Benha University, Cairo 11672, Egypt*

Correspondence should be addressed to Gaojian Huang; g.huang@hpu.edu.cn

Received 25 December 2021; Revised 11 February 2022; Accepted 2 March 2022; Published 29 March 2022

Academic Editor: Yinghui Ye

Achieving high network traffic demand in limited spectrum resources is a technical challenge for the beyond 5G and 6G communication systems. To this end, ambient backscatter communication (AmBC) is proposed for Internet-of-Things (IoT), because the backscatter device (BD) can realize communication without occupying extra spectrum resources. Moreover, the spectral efficiency can be further improved by using two-way (TW) communication. However, secure communication is a great challenge for accessing massive IoT devices due to the broadcasting nature of wireless propagation environments. In light of this fact, this article proposed a two-way ambient backscatter communication (TW-AmBC) network with an eavesdropper. Specifically, the physical layer security (PLS) is studied through deriving the analytical/asymptotic expressions of the outage probability (OP) and intercept probability (IP). Moreover, the outage probabilities (OPs) in high signal-to-noise ratio (SNR) regions are studied for the asymptotic behavior and the intercept probabilities (IPs) in high main-to-eavesdropping ratio (MER) regions as well. Through analysis and evaluation of simulation performance, the results show that (i) when considering the target node, the OP of the BD decreases with increasing SNR, that is, enhancing the reliability; (ii) an optimal value of BD's reflection coefficient that maximize the reliability of backscatter link can be obtained; (iii) in high SNR regions, the OPs approach a constant; thus, the diversity orders are zero; (iv) when increasing the MER, the IP of target node decreases, suggesting the security enhances; (v) a trade-off exists between reliability and security which can be optimized by carefully designing the parameters.

1. Introduction

Due to faster network traffic demand and limited spectrum resources, the next-generation wireless communication techniques urgently need to improve the spectrum efficiency (SE) and reduce latency [1]. The ambient backscatter communication (AmBC) that could utilize the environmental wireless signals for both powering low-power devices and backscattering signals was used to address the problem of limited spectrum resources [2]. The main advantages of AmBC for Internet-of-Things (IoT) can be summarized as follows: (i) the SE can be improved since information is conveyed without consuming additional bandwidth [3]; (ii) the expensive and energy-consuming components such as oscillators, filters, and amplifiers are not required for the backscatter device (BD); thus, it enjoys low cost and low power [4]. As a new green paradigm, AmBC has aroused great research interest. However, due to the simplicity of the components, BD cannot separate interfering signals from received signals and is vulnerable to security attacks.

In particular, the performance of combining AmBC with other technologies was studied in much of the existing literature. For instance, in [5], the authors first studied the outage probability (OP) of symbiotic system incorporating the nonorthogonal multiple access (NOMA) and backscatter techniques. The authors in [6] acquired the analytical

expressions of the OP and studied the outage performance of AmBC system with considering in-phase and quadrature-phase imbalance (IQI). In [7], the backscatter technique was studied with intelligent reflecting surface (IRS) which is known as another low-power technique; the proposed scheme can achieve a balance between the average throughput and coverage probability according to practical condition. In [8], the multiantenna backscatter tag AmBC system was proposed, wherein the multiantenna technique was used to enhance the reliability. In [9], an adaptive reflection coefficient scheme was proposed to minimize the OP of backscatter link, which provided a guideline to design the optimal reflection coefficient for practical AmBC systems.

Meanwhile, in AmBC system, the power of BD is limited which is in contrast to the traditional key mechanism requiring high computing power; thus, some researchers focused on the security problems. Without consuming high computing power, the physical layer security (PLS) can be achieved by using the inherent randomness of physical media and the difference between legal channels and eavesdropping channels. Thus, it has attracted much attention in academia and industry and was studied in different scenarios [10–12]. For instance, in [13], the secrecy performance of AmBC systems considering IQI was investigated by deriving the analytical expressions of the OP and intercept probability (IP). In [14], the secrecy outage probability (SOP) of the multitag backscatter systems over the Rayleigh fading channels was given, where the channel correlation between the forward and backscatter links may exist. In [15], the authors studied the PLS for the relay selection schemes of NOMA systems, indicating that better security performance can be achieved when increasing the number of relays.

On the other hand, due to the network congestion caused by information explosion, it is imperative to study the techniques increasing the throughput which is defined as the amount of data successfully transferred per unit time of a communication channel. The two-way (TW) communication method enables the capability of improving throughput and SE since the relay in the TW communication system can receive information from both nodes in a single time slot. The TW communication system therefore has been extensively studied specifically on the PLS aspect. For example, in [16], the OP of a TW relay system can be minimized by an improved dynamic scheme, which both the power-splitting ratios and the power allocation ratio can be dynamically adjusted. In [17], the OP of TW full-duplex relay system considering self-interference was evaluated, and asymptotic OP was presented for more insight. Different from the above works, reconfigurable intelligent surface (RIS) technique with great channel capacity advantage was employed in wireless communication systems to improve the performance [18]. Similarly, in [19], the performance of the RIS-assisted TW communication systems was studied wherein the channels can either be reciprocal or nonreciprocal, and the closed-form expressions of OP were derived for single-element RIS. Moreover, in [20], an artificial noise-assisted opportunistic relay selection scheme was proposed to enhance the security of underlay cognitive TW relay network.

1.1. Motivation and Contributions. In the existing works, in [21], an optimization algorithm was proposed to maximize throughput of relaying system where an unmanned aerial vehicle (UAV) enabled TW relay assist communication. In [22], the secrecy of TW relay NOMA systems was evaluated in terms of the ergodic secrecy sum rate, which degraded when the distance between the eavesdropper and either user becomes closer. In [23], the outage performance of a TW model wherein BD is embedded in the relay for backscattering was investigated. In [24], a BD cooperative relay communication network was proposed and the system reliability performance was studied. It is noted that all the reported works established models with relays and for the case of without relay was neglected. In this article, we first consider a two-way ambient backscatter communication (TW-AmBC) system without relay and study the reliability and security of the proposed system, where sources communicate with each other and also via BD with an eavesdropper. The main contributions of the article can be listed as follows:

(i) We propose a novel TW-AmBC model without relay and study the PLS of target node, wherein BD and nodes transmit signals in the presence of an eavesdropper

(ii) We derive the analytical expressions of the outage probabilities (OPs) for the target node and BD and the analytical expressions of the intercept probabilities (IPs) for eavesdropper. It is found that the reflection coefficient and transmitted power have the opposite effect on OPs and IPs. The trade-off between security and reliability can be flexibly adjusted

(iii) We evaluate the performance of OPs and IPs in high signal-to-noise ratio (SNR) and main-to-eavesdropping ratio (MER) regions. Furthermore, we discuss the diversity orders of the target node and BD in high SNR regions. The diversity orders are zero owing to the OPs approach a constant, proving that the joint error-floor exists

(iv) We analyze the comprehensive influence factor on performance of both the reflection coefficient and transmitted power in the TW-AmBC network. When transmitted power is high, the system performance enjoys little fluctuation, and when the reflection coefficient increases, the security of the target node can be increased

1.2. Organization and Notations. The remainder of the article is composed as follows. In Section 2, the TW-AmBC system without relay is first constructed, followed by the elaboration of deriving expressions of OPs and IPs in Section 3. In Section 4, the correctness of the theoretical analysis is validated via numerical results. Finally, conclusions are given in Section 5.

$E(\bullet)$ is deemed as the expectation operation. $\Pr(\bullet)$ denotes the probability and $K_v(\bullet)$ denotes the v-th order

modified Bessel function of the second kind. $\mathcal{CN}(\mu, \sigma^2)$ denotes the complex Gaussian random variable with mean μ and variance σ^2. Besides, $Ei(\bullet)$ is the exponential integral function and $W_{u,v}(\bullet)$ is the Whittaker function. n denotes the natural number, and $n!$ denotes the factorial operation. The cumulative distribution function (CDF) is expressed as $F(\bullet)$, and the probability dense function (PDF) is expressed as $f(\bullet)$.

2. System Model

As illustrated in Figure 1, we consider a TW-AmBC system which is composed of two source nodes (A and B), a BD, and an eavesdropper (E), wherein h_n, h_0, and h_e, respectively, denote the channel responses from A to BD, B, and E. g_n and f_e represent the channel responses from BD to B and E, respectively. In different time slots, B and A can directively transmit signals to each other, also via a BD. The eavesdropper can intercept signals from nodes and BD. We assume that (i) all nodes are equipped with a single antenna; (ii) all channel parameters are subjected to the independent Rayleigh fading. We have $h_0 \sim \mathcal{CN}(0, \lambda_{h0})$, $h_n \sim \mathcal{CN}(0, \lambda_{hn})$, $h_e \sim \mathcal{CN}(0, \lambda_{he})$, $g_n \sim \mathcal{CN}(0, \lambda_{gn})$, $g_e \sim \mathcal{CN}(0, \lambda_{ge})$, and $f_e \sim \mathcal{CN}(0, \lambda_{fe})$.

2.1. Received Signals at B. The received signals at B include signals from A and the backscattered signals from BD. The BD adds its own message $c(t)$ to signals from A or B and then backscatters, where $E(|c(t)|^2) = 1$. Thus, the received signals y_B at B can be expressed as

$$y_B = h_0\sqrt{P_s}x_A(t) + \beta h_n g_n \sqrt{P_s}x_A(t)c(t) + n_1(t), \quad (1)$$

where β is the complex reflection coefficient used to normalize $c(t)$ and $n_1 \sim \mathcal{CN}(0, \sigma^2)$ is the complex Gaussian noise with zero mean. $x_A(t)$ is the transmitted signal of A. P_s denotes the transmitted power. Furthermore, in order to extract the real-information from the scrambled signals, successive interference cancellation (SIC) technique is adopted at the receiver end [25]. Therefore, the received signal-to-interference-plus-noise ratio (SINR) extracting $x_A(t)$ at B can be written as

$$\gamma_B = \frac{\gamma|h_0|^2}{\gamma|\beta|^2|h_n|^2|g_n|^2 + 1}, \quad (2)$$

where $\gamma = P_s/\sigma^2$ is the transmit SNR. By eliminating the interference from A, the SNR at B can be written as

$$\gamma_{\mathrm{BD}} = \gamma|\beta|^2|h_n|^2|g_n|^2. \quad (3)$$

2.2. Wiretapped Signals. In the 1st time slot, the received signals at E can be expressed as

$$y_e(t) = g_e\sqrt{P_s}x_B(t) + \beta g_n f_e \sqrt{P_s}x_B(t)c(\mathrm{t}) + n_2(t), \quad (4)$$

where $n_2(t)$ is the complex Gaussian noise at E and follows $n_2 \sim \mathcal{CN}(0, \sigma^2)$. $x_B(t)$ is the transmitted signal of B. When only direct link signals are decoded at E, the SINR can be given by

$$\gamma_{e,B} = \frac{\gamma|g_e|^2}{\gamma|\beta|^2|g_n|^2|f_e|^2 + 1}. \quad (5)$$

It is noted that E can eliminate direct link signals and extract the signals from BD with aid of SIC technique. In this case, the SNR can be expressed as

$$\gamma_{e,\mathrm{BD}} = \gamma|\beta|^2|g_n|^2|f_e|^2. \quad (6)$$

3. Performance Analysis

In this section, we derive the analytical expressions of OPs and IPs to investigate the security and reliability of the TW-AmBC system. Furthermore, the asymptotic behaviors of OPs and IPs are studied by asymptotic expressions, and the diversity orders are derived in high SNR regions.

3.1. Outage Performance Analysis

3.1.1. Outage Probability Expressions for B. Considering the direct link only, the outage event would occur when signal $x_A(t)$ is unsuccessfully decoded at B. Thus, the OP at B can be given by

$$P_{\mathrm{out}}^B = 1 - \Pr\left(\gamma_B > \gamma_{\mathrm{th}}^B\right), \quad (7)$$

where γ_{th}^B is the SNR threshold at B.

Theorem 1. *For the direct link, we can get the OP analytical expression, which can be expressed as*

$$P_{out}^B = 1 + Q_1 e^{Q_1 - \gamma_{th}^B/\gamma\lambda_{h0}} Ei(-Q_1), \quad (8)$$

where $Q_1 = \lambda_{h0}/\gamma_{th}^B|\beta|^2\lambda_{hn}\lambda_{gn}$, $Ei(x)$ represents the exponential integral function and $Ei(x) = \int_{-\infty}^{x}(e^t/t)dt$, where t denotes the variable. $Ei(x)$ can be expanded to a series form which is given by

$$Ei(x) = \nu + \ln x + \sum_{n=1}^{\infty}\frac{x^n}{n \cdot n!}, \quad (9)$$

where ν is the Euler constant, $\nu \approx 0577$. n denotes the natural number, and $n!$ denotes the factorial operation for n.

Proof. See Appendix A. □

Corollary 1. *Under high signal-to-noise ratio (SNR) case, the OP asymptotic expression of direct link can be given as*

$$P_{out,\infty}^B = 1 + Q_1 e^{Q_1}\left(1 - \frac{\gamma_{th}^B}{\gamma\lambda_{h0}}\right)Ei(-Q_1). \quad (10)$$

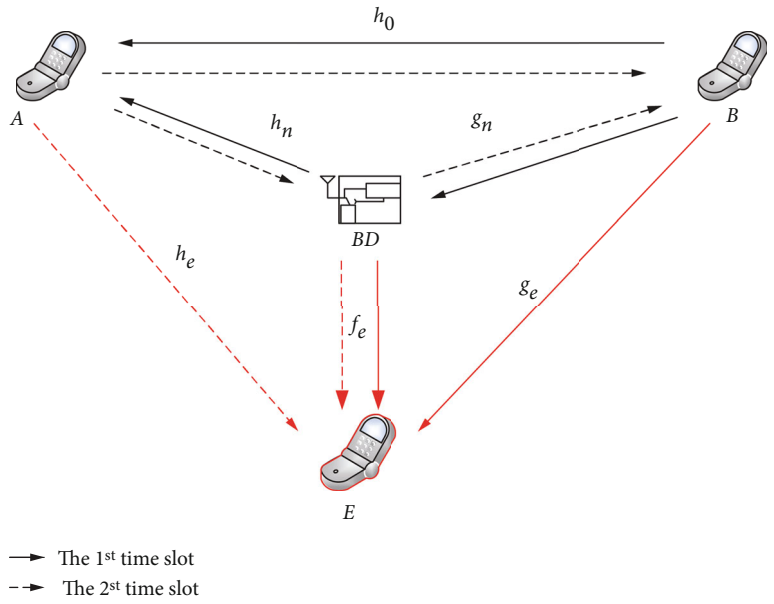

Figure 1: Two-way ambient backscatter communication system model.

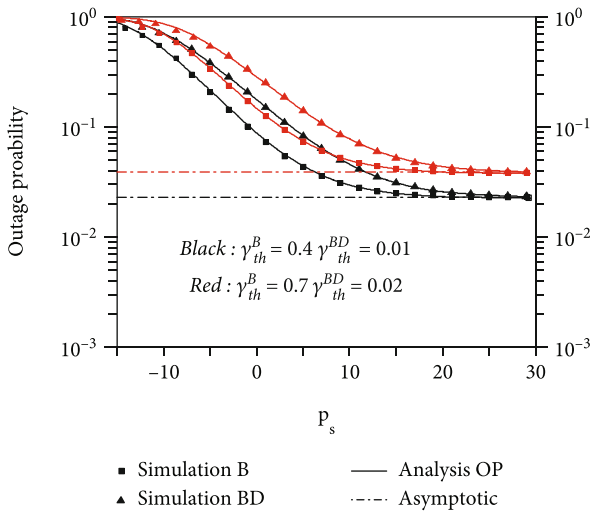

Figure 2: OPs versus P_s for different SNR threshold values.

Proof. According to asymptotic principle, Equation (10) can be derived from Equation (8) by using approximate equation $e^{-x} \approx 1 - x$ when $\gamma \longrightarrow \infty$. □

3.1.2. Outage Probability Expressions for BD. For the backscatter link, the outage event occurs when direct link signals are successfully decoded but failing with backscattered signals. Therefore, the OP of backscattered signals can be expressed as

$$P_{\text{out}}^{\text{BD}} = 1 - \Pr\left(\gamma_B > \gamma_{\text{th}}^B, \gamma_B > \gamma_{\text{th}}^{\text{BD}}\right), \tag{11}$$

where $\gamma_{\text{th}}^{\text{BD}}$ is the SNR threshold for backscattered signals.

Theorem 2. *For the backscatter link, we can obtain the OP analytical expression, which can be expressed as*

$$P_{out}^{BD} = 1 + Q_1 e^{Q_1 - \gamma_{th}^B/\gamma\lambda_{h0}} Ei(-Q_1) + \frac{\pi\Delta_2}{N}\sum_{i=1}^{N} e^{-\Delta_1} K_0\left(\sqrt{2\Delta_2(\delta_i + 1)}\right)\sqrt{1-\delta_i^2}, \tag{12}$$

where $\Delta_1 = (\gamma_{th}^B\gamma_{th}^{BD}(\delta_i + 1) + 2\gamma_{th}^B)/2\gamma\lambda_{h0}$, $\Delta_2 = \gamma_{th}^{BD}/\gamma|\beta|^2\lambda_{hn}$ λ_{gn}, $\delta_i = \cos\left(((2i-1)/2N)\pi\right)$, N *is a trade-off parameter between accuracy and complexity, and* $K_0(\bullet)$ *is the 0th order modified Bessel function of the second kind.*

Proof. See Appendix B. □

Corollary 2. *Under high SNRs case, the OP asymptotic expression for backscatter link in the proposed system can be given as*

$$P_{out,\infty}^{BD} = 1 + Q_1 e^{Q_1}\left(1 - \frac{\gamma_{th}^B}{\gamma\lambda_{h0}}\right)Ei(-Q_1) - \frac{\pi\Delta_2}{N}\sum_{i=1}^{N}(1-\Delta_1)\ln \cdot \left(\sqrt{\frac{\Delta_2(\delta_i+1)}{2}}\right)\sqrt{1-\delta_i^2}. \tag{13}$$

Proof. According to the asymptotic principle, through using two approximate equations, i.e., $K_0(x) \approx -\ln(x/2)$ and $e^x = 1 + x$, Equation (13) can be obtained.

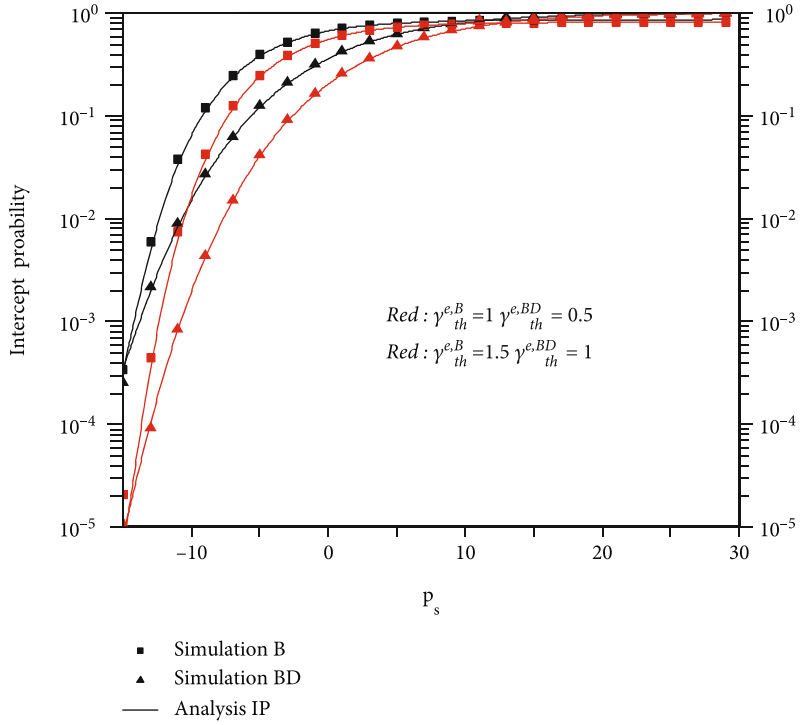

FIGURE 3: IPs versus P_s for different secrecy SNR threshold values.

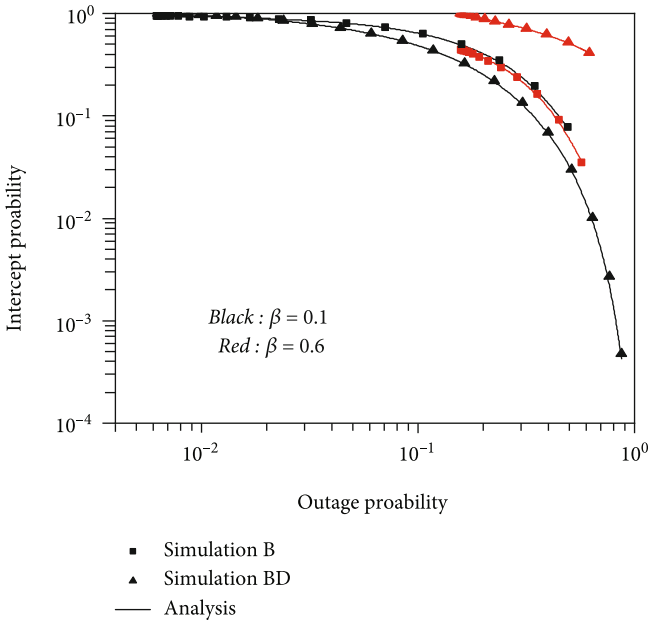

FIGURE 4: IPs versus OPs for different β values.

For further insights on the backscatter link and direct link, we also study the diversity order d_ψ, $\psi \in \{B, \mathrm{BD}\}$. The diversity order is given [26]:

$$d_\psi = -\lim_{\gamma \longrightarrow \infty} \frac{\log\left(P^{\psi}_{\mathrm{out},\infty}\right)}{\log \gamma}. \tag{14}$$

□

Corollary 3. *The diversity orders of the two links can be calculated as*

$$d_B = d_{BD} = 0. \tag{15}$$

Remark 1. From Corollaries 1–3 and Theorems 1 and 2, we can know that (1) when increasing P_s, the OPs decrease, enhancing the reliability of the system; (2) when increasing β, the OP of direct link increases; (3) when γ is large, the latter of Equation (12) is almost zero; thus, when $\gamma \longrightarrow \infty$, $P^{\mathrm{BD}}_{\mathrm{out},\infty}$ approximates $P^{B}_{\mathrm{out},\infty}$; (4) when $\gamma \longrightarrow \infty$, asymptotic OPs exist the joint error-floor, causing that the diversity orders are zero.

3.2. Security Performance Analysis. When the SINR or SNR at E surpasses the secrecy SNR threshold, direct link signals or backscattered signals would be intercepted. In further detail below, the expressions of IPs are derived to investigate the system security.

3.2.1. Intercept Probability Expressions for B. The IP expression of direct link signals can be written as

$$P^{B}_{\mathrm{int}} = \Pr\left(\gamma_{e,B} > \gamma^{e,B}_{\mathrm{th}}\right), \tag{16}$$

where $\gamma^{e,B}_{\mathrm{th}}$ is the secrecy SNR threshold for B.

Theorem 3. *For the direct link, we can get the IP analytical expression, which can be expressed as*

$$P^{B}_{\mathrm{int}} = -e^{-\gamma^{e,B}_{th}/\gamma\lambda_{ge}} Q_2 e^{Q_2} Ei(-Q_2), \tag{17}$$

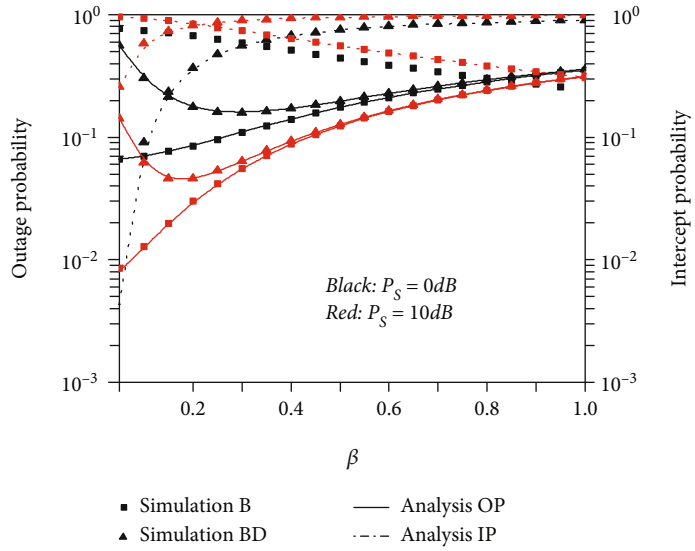

Figure 5: OPs and IPs versus β for different P_s values.

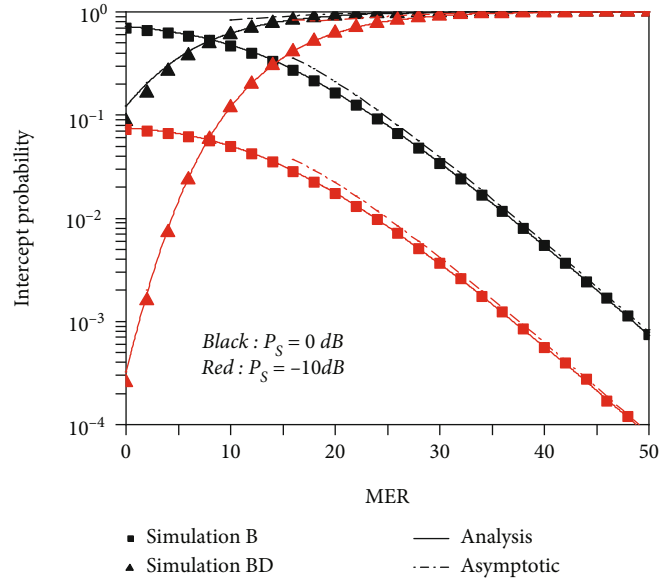

Figure 6: IPs versus MER for different P_s values.

where $Q_2 = \lambda_{ge}/\gamma_{th}^{e,B}|\beta|^2\lambda_{gn}\lambda_{fe}$.

Proof. Substituting Equation (5) into Equation (16), the IP of direct link signals can be expressed as

$$P_{\text{int}}^{B} = e^{-\gamma_{\text{th}}^{e,B}/\gamma\lambda_{ge}} \int_0^{\infty} e^{-\gamma_{\text{th}}^{e,B}|\beta|^2 y/\lambda_{ge}} f_{|gn|^2|fe|^2}(y)dy, \quad (18)$$

where $f_{|gn|^2|fe|^2}(y) = (2/\lambda_{gn}\lambda_{fe})K_0(2\sqrt{y/\lambda_{gn}\lambda_{fe}})$. The integral can be resolved by Appendix A, and Equation (17) can be derived. □

Here, we use the MER metric to study the asymptotic behavior of IPs, which depends on the ratio of the main link to eavesdropping link [27]. The main link and eavesdropping link are B to BD and BD to E, respectively. The MER can be expressed as $\lambda_{me} = \lambda_{gn}/\lambda_{fe}$. In the next corollary, the asymptotic analysis for IPs in high MER regions is derived.

Corollary 4. *Under high main-to-eavesdropping ratio (MER) case, the IP asymptotic expression can be given by*

$$P_{\text{int},\infty}^{B} = -e^{-\gamma_{th}^{e,B}/\gamma\lambda_{ge}} Q_2^*(1 + Q_2^*) \ln(-Q_2^*), \quad (19)$$

where $Q_2^* = \lambda_{ge}/\gamma_{th}^{e,B}|\beta|^2\lambda_{me}\lambda_{fe}^2$.

Proof. According to the asymptotic principle, Equation (19) can be obtained by substituting $e^x \approx 1 + x$ and $Ei(x) \approx \ln x + C$ into Equation (17), where C is a constant. □

3.2.2. Intercept Probability Expressions for BD. The IP expression of backscattered signals can be written as

$$P_{\text{int}}^{\text{BD}} = \Pr\left(\gamma_{e,\text{BD}} > \gamma_{\text{th}}^{e,\text{BD}}\right), \tag{20}$$

where $\gamma_{\text{th}}^{e,\text{BD}}$ is the secrecy SNR threshold of BD.

Theorem 4. *For the backscatter link, we can get the IP analytical expression, which can be expressed as*

$$P_{\text{int}}^{BD} = 2\sqrt{Q_3}K_1\left(2\sqrt{Q_3}\right), \tag{21}$$

where $Q_3 = \gamma_{th}^{e,BD}/\gamma|\beta|^2\lambda_{gn}\lambda_{fe}$ *and* $K_1(\bullet)$ *is the 1st order modified Bessel function of the second kind.*

Proof. Substituting Equation (6) into Equation (20), $P_{\text{int}}^{\text{BD}}$ can be expressed as

$$P_{\text{int}}^{\text{BD}} = \frac{1}{\lambda_{fe}}\int_0^{\infty} e^{-\gamma_{\text{th}}^{e,\text{BD}}/\gamma|\beta|^2\lambda_{gn}y - y/\lambda_{fe}}dy, \tag{22}$$

where the integral can be calculated by Equation (3.324.1) [28]. □

Corollary 5. *Under high MER case, the IP asymptotic expression for backscatter link can be written as*

$$P_{\text{int},\infty}^{BD} = 1 + 2Q_3^* \ln\left(\sqrt{Q_3^*}\right), \tag{23}$$

where $Q_3^* = \gamma_{th}^{e,BD}/\gamma|\beta|^2\lambda_{me}\lambda_{fe}^2$.

Proof. By using approximate equation $K_1(x) \approx (1/x) + (x/2)\ln(x/2)$, we can get Equation (23). □

Remark 2. From Theorems 3 and 4 and Corollaries 4 and 5, we can know that (1) with increasing reflection coefficient β, the security of B gets enhanced owing to P_{int}^{B} decreases; (2) the security of B and BD decrease when P_s increases; (3) when λ_{me} increases, the security of B is enhanced; (4) when $\lambda_{me} \longrightarrow \infty$, $P_{\text{int},\infty}^{\text{BD}}$ is close to 1, suggesting λ_{me} takes small value to ensure BD security.

4. Numerical Results

In this section, the correctness of previous analysis is validated via numerical simulation results. In these simulation examples, we consider 10^5 Monte Carlo trials. It is assumed that $\lambda_{h0} = 6$, $\lambda_{hn} = 4$, $\lambda_{gn} = 5$, $\lambda_{fe} = 6$, $\lambda_{ge} = 4$, $\beta = 0.2$, and $\sigma^2 = 1$.

The simulation results of OPs versus P_s for B and BD are plotted in Figure 2. It can be seen that in high P_s regions, the OPs are getting close to constant with increasing P_s, resulting in 0 diversity orders. From Remark 1, we can know that the value of the joint error-floor depends on the SNR threshold at B. Furthermore, it can be seen that the OPs increase when the SNR thresholds, i.e., γ_{th}^{B} and $\gamma_{\text{th}}^{\text{BD}}$, increase.

The IPs versus P_s for B and BD are plotted in Figure 3. The IPs decrease as the secrecy SNR thresholds increase. In low P_s regions, it is shown that the IP decreases significantly, indicating that the TW-AmBC system has higher security performance. In high P_s regions, the IPs are close to 1; thus, the security is impaired. Meanwhile, from Figures 2 and 3, it can be observed that when P_s increases, the OPs decrease but the IPs increase. Thus, it can be inferred that a trade-off between reliability and security exists in this system.

Figure 4 illustrates the IPs versus OPs for different β values. It can be observed that the system outage performance gets impaired when β changes from 0.1 to 0.6. This is because the backscattered signals make the interference stronger when B decodes signals. In addition, it can be observed that the secrecy performance of direct link is enhanced when β increases. It can be explained that the backscattered signals increase with increasing β; thus, it can project more interference when E decodes the signals from B. Meanwhile, when increasing β, the scopes of OP and IP are obviously reduced, which indicates that the trade-off between security and reliability degrades. In summary, high reliability and high security cannot be achieved simultaneously, which indicates that the reliability is compromised to get better security and vice versa.

The OPs and IPs versus β for different P_s values are plotted in Figure 5. In low β regions, the IP of BD decreases significantly, which greatly improves the system security performance. Thus, when β is small, the eavesdropper can easily intercept the messages from B, but it is difficult to decode the messages from BD. The IP trend curves of BD and B are opposite, indicating that high security of one link can be achieved with compromised security performance of the other link. Thus, a trade-off of security exists between the two links. Meanwhile, the curve of BD's OP firstly decreases and then increases, suggesting that we can get an optimal value β to minimize OP.

Figure 6 reveals the variations of IPs versus MER in conditions of different P_s values, with $\beta = 0.1$. We consider 10^6 Monte Carlo trials to reduce the impact of randomness on experimental accuracy. It can be observed that when MER increases, the IP of B decreases and that of BD increases, and in high MER regions, the IP of BD is close to 1, suggesting that the security of backscatter link can only be achieved when MER is low. When P_s decreases, the IPs decrease, indicating that the security gets enhanced. Beyond that, there is the strict approximation relationship between the theoretical value and the asymptotic value.

5. Conclusions

In this article, a novel TW-AmBC network structure was proposed, which integrated the benefits of both TW communication and AmBC. Through analyzing the PLS performance of the proposed TW-AmBC, it is found that the parameters can be designed to achieve an optimal trade-off between reliability and security, such as reflection coefficient β and the transmitted power P_s. Specifically, the secrecy performance of B can be enhanced when reflection coefficient β increases. When the transmitted power P_s is

high, the asymptotic OPs approach a joint error-floor, indicating that the reliability of two links is similar. These findings would be useful in instructing to apply BD in limited spectrum resource application scenarios.

Appendix

A. Proof of Theorem 1

Substituting Equation (2) into Equation (7), the OP of B can be given as

$$P_{\text{out}}^{B} = 1 - \underbrace{\Pr\left(\frac{\gamma|h_0|^2}{\gamma|\beta|^2|h_n|^2|g_n|^2+1} > \gamma_{\text{th}}^{B}\right)}_{I_1}, \tag{A.1}$$

where I_1 can be calculated as follows:

$$I_1 = \int_0^{\infty}\int_{\gamma_{\text{th}}^{B}|\beta|^2 y+\gamma_{\text{th}}^{B}/\gamma}^{\infty} \frac{1}{\lambda_{h0}} e^{-x/\lambda_{h0}} f_{|hn|^2|gn|^2}(y)dxdy, \tag{A.2}$$

where $f_{|hn|^2|gn|^2}(y)$ is the joint probability density function. The probability density functions of hn and gn are $f_{|hn|^2}(x) = (1/\lambda_{hn})e^{-x/\lambda_{hn}}$ and $f_{|gn|^2}(y) = (1/\lambda_{gn})e^{-y/\lambda_{gn}}$, respectively. We make $Z = X \bullet Y$; the joint probability density function $f_{|hn|^2|gn|^2}(z)$ can be expressed as

$$\begin{aligned} f_{|hn|^2|gn|^2}(z) &= \int_0^{\infty} \frac{1}{u} f_{|hn|^2}\left(\frac{z}{u}\right) f_{|gn|^2}(u)du \\ &= \frac{1}{\lambda_{hn}\lambda_{gn}} \int_0^{\infty} \frac{1}{u} e^{-z/u\lambda_{hn}-u/\lambda_{gn}} du \\ &= \frac{2}{\lambda_{hn}\lambda_{gn}} K_0\left(2\sqrt{\frac{z}{\lambda_{hn}\lambda_{gn}}}\right), \end{aligned} \tag{A.3}$$

where the integral can be derived by Equation (3.324.1) [28] and $K_0(\bullet)$ is the 0th modified Bessel function of the second kind. Substituting Equation (A.3) into Equation (A.2), I_1 can be expressed as

$$I_1 = \frac{2e^{-\gamma_{\text{th}}^{B}/\gamma\lambda_{h0}}}{\lambda_{hn}\lambda_{gn}} \int_0^{\infty} e^{-\gamma_{\text{th}}^{B}|\beta|^2 y/\lambda_{h0}} K_0\left(2\sqrt{\frac{y}{\lambda_{hn}\lambda_{gn}}}\right) dy, \tag{A.4}$$

where the integral can be resolved by Equation (6.643.3) [28], we have

$$\int_0^{\infty} e^{-\alpha x} K_0\left(2\theta\sqrt{x}\right) dx = \frac{e^{\theta^2/2\alpha}}{2\theta\sqrt{\alpha}} W_{-1/2,0}\left(\frac{\theta^2}{\alpha}\right), \tag{A.5}$$

where $\alpha = \gamma_{th}^{B}|\beta|^2/\lambda_{h0}$, $\theta = \sqrt{1/\lambda_{hn}\lambda_{gn}}$, and $W_{-1/2,0}(\theta^2/\alpha)$ is the Whittaker function, which can be substituted with the exponential function by Equation (9.222.1) [28], we have

$$W_{-1/2,0}\left(\frac{\theta^2}{\alpha}\right) = \left(\frac{\theta^2}{\alpha}\right)^{1/2} e^{-\theta^2/2\alpha} \int_0^{\infty} \frac{e^{-\left(\theta^2/\alpha\right)t}}{1+t} dt, \tag{A.6}$$

where the integral can be resolved by Equation (3.352.4) [28], and thus, $W_{-1/2,0}(\theta^2/\alpha) = -\sqrt{(\theta^2/\alpha)}e^{\theta^2/2\alpha}Ei(-\theta^2/\alpha)$. I_1 can be expressed as

$$I_1 = -Q_1 e^{Q_1 - \gamma_{\text{th}}^{B}/\gamma\lambda_{h0}} Ei(-Q_1), \tag{A.7}$$

where $Q_1 = \lambda_{h0}/\gamma_{\text{th}}^{B}|\beta|^2\lambda_{gn}\lambda_{hn}$.

Thus, Equation (8) can be given by substituting Equation (A.7) into Equation (A.1).

B. Proof of Theorem 2

The OP of BD can be denoted as

$$P_{\text{out}}^{\text{BD}} = 1 - \underbrace{\Pr\left(\gamma_B > \gamma_{\text{th}}^{B}, \gamma_{\text{BD}} > \gamma_{\text{th}}^{\text{BD}}\right)}_{I_2}, \tag{B.1}$$

where

$$I_2 = \int_{\gamma_{\text{th}}^{\text{BD}}/\gamma|\beta|^2}^{\infty}\int_{\gamma_{\text{th}}^{B}|\beta|^2 y+\gamma_{\text{th}}^{B}/\gamma}^{\infty} \frac{1}{\lambda_{h0}} e^{-x/\lambda_{h0}} f_{|hn|^2|gn|^2}(y)dxdy. \tag{B.2}$$

We can see from Equations (A.2) and (B.2) that there exists a difference between I_1 and I_2 on the lower limit of integration for x. Thus, we have

$$I_1 - I_2 = \int_0^{\gamma_{\text{th}}^{\text{BD}}/\gamma|\beta|^2}\int_{\gamma_{\text{th}}^{B}|\beta|^2 y+\gamma_{\text{th}}^{B}/\gamma}^{\infty} \frac{1}{\lambda_{h0}} e^{-x/\lambda_{h0}} f_{|hn|^2|gn|^2}(y)dxdy. \tag{B.3}$$

Meanwhile, it is challenging to calculate the integral I_2, thus changing I_2 into the following form.

$$I_2 = I_1 - \underbrace{\frac{2e^{-\gamma_{\text{th}}^{B}/\gamma\lambda_{h0}}}{\lambda_{hn}\lambda_{gn}} \int_0^{\gamma_{\text{th}}^{\text{BD}}/\gamma|\beta|^2} e^{-\gamma_{\text{th}}^{B}|\beta|^2 y/\lambda_{h0}} K_0\left(2\sqrt{\frac{y}{\lambda_{hn}\lambda_{gn}}}\right) dy}_{I_3}, \tag{B.4}$$

where can be given as Equation (B.5) by the Gaussian Chebyshev approximation Equation (20) [29].

$$I_3 = \frac{\pi\gamma_{\text{th}}^{\text{BD}}}{N\gamma|\beta|^2\lambda_{hn}\lambda_{gn}} \sum_{i=1}^{N} e^{-\gamma_{\text{th}}^{B}\gamma_{\text{th}}^{\text{BD}}(\delta_i+1)+2\gamma_{\text{th}}^{B}/2\gamma\lambda_{h0}} K_0\left(\sqrt{\frac{2\gamma_{\text{th}}^{\text{BD}}(\delta_i+1)}{\gamma|\beta|^2\lambda_{hn}\lambda_{gn}}}\right)\sqrt{1-\delta_i^2}. \tag{B.5}$$

Finally, Equation (12) can be obtained by substituting Equations (A.7), (B.4) and (B.5) into Equation (B.1).

Data Availability

The data is available from the corresponding author upon request.

Conflicts of Interest

The authors declare that there is no conflict of interest regarding the publication of this paper.

Acknowledgments

This work was supported in part by the Programs of Henan Polytechnic University (No. B2017-57 and B2022-2), in part by the Fundamental Research Funds for the Universities of Henan Province (No. NSFRF200335), in part by the Natural Science Foundation of Guangdong Province with grant number 2022A030313736, in part by the Scientific Research Project of Education Department of Guangdong with grant number 2021KCXTD061, in part by the Science and Technology Program of Guangzhou with grant number 202207010389, Yangcheng Scholar, in part by the Scientific Research Project of Guangzhou Education Bureau with grant number 202032761, and in part by the Application Technology Collaborative Innovation Center of GZPYP with grant number 2020ZX01.

References

[1] X. Yue and Y. Liu, "Performance analysis of intelligent reflecting surface assisted NOMA networks," *IEEE Transactions on Wireless Communications*, pp. 1–1, 2021.

[2] W. Zhang, Y. Qin, W. Zhao et al., "A green paradigm for Internet of things: ambient backscatter communications," *China Communications*, vol. 16, no. 7, pp. 109–119, 2019.

[3] N. Van Huynh, D. T. Hoang, X. Lu, D. Niyato, P. Wang, and D. I. Kim, "Ambient backscatter communications: a contemporary survey," *IEEE Communications Surveys Tutorials*, vol. 20, no. 4, pp. 2889–2922, 2018.

[4] Y. Ye, L. Shi, R. Qingyang Hu, and G. Lu, "Energy efficient resource allocation for wirelessly powered backscatter communications," *IEEE Communications Letters*, vol. 23, no. 8, pp. 1418–1422, 2019.

[5] Q. Zhang, L. Zhang, Y.-C. Liang, and P.-Y. Kam, "Backscatter-NOMA: a symbiotic system of cellular and Internet-of-Things networks," *IEEE Access*, vol. 7, pp. 20000–20013, 2019.

[6] X. Li, Y. Zheng, M. D. Alshehri et al., "Cognitive AmBC-NOMA IoV-MTS networks with IQI: reliability and security analysis," *IEEE Transactions on Intelligent Transportation Systems*, pp. 1–12, 2021.

[7] Z. Yang, L. Feng, F. Zhou, X. Qiu, and W. Li, "Analytical performance analysis of intelligent reflecting surface aided ambient backscatter communication network," *IEEE Wireless Communications Letters*, vol. 10, no. 12, pp. 2732–2736, 2021.

[8] Z. Niu, W. Ma, W. Wang, and T. Jiang, "Spatial modulation-based ambient backscatter: bringing energy self-sustainability to massive internet of everything in 6G," *China Communications*, vol. 17, no. 12, pp. 52–65, 2020.

[9] Y. Ye, L. Shi, X. Chu, and G. Lu, "On the outage performance of ambient backscatter communications," *IEEE Internet of Things Journal*, vol. 7, no. 8, pp. 7265–7278, 2020.

[10] H. Yang, Y. Ye, X. Chu, and S. Sun, "Energy efficiency maximization for UAV-enabled hybrid backscatter-harvest-then-transmit communications," *IEEE Transactions on Wireless Communications*, pp. 1–1, 2021.

[11] X. Li, M. Zhao, M. Zeng et al., "Hardware impaired ambient backscatter NOMA systems: reliability and security," *IEEE Transactions on Communications*, vol. 69, no. 4, pp. 2723–2736, 2021.

[12] X. Li, Y. Zheng, W. U. Khan et al., "Physical layer security of cognitive ambient backscatter communications for green Internet-of-Things," *IEEE Transactions on Green Communications and Networking*, vol. 5, no. 3, pp. 1066–1076, 2021.

[13] X. Li, M. Zhao, Y. Liu, L. Li, Z. Ding, and A. Nallanathan, "Secrecy analysis of ambient backscatter NOMA systems under I/Q imbalance," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 10, pp. 12286–12290, 2020.

[14] Y. Zhang, F. Gao, L. Fan, X. Lei, and G. K. Karagiannidis, "Secure communications for multi-tag backscatter systems," *IEEE Wireless Communications Letters*, vol. 8, no. 4, pp. 1146–1149, 2019.

[15] Z. Wang and Z. Peng, "Secrecy performance analysis of relay selection in cooperative NOMA systems," *IEEE Access*, vol. 7, pp. 86274–86287, 2019.

[16] L. Shi, Y. Ye, R. Q. Hu, and H. Zhang, "System outage performance for three-step two-way energy harvesting DF relaying," *IEEE Transactions on Vehicular Technology*, vol. 68, no. 4, pp. 3600–3612, 2019.

[17] Z. Wang, W. Shi, W. Liu, Y. Zhao, and K. Kang, "Performance analysis of two-way full-duplex relay mixed RF/FSO system with self-interference," *IEEE Communications Letters*, vol. 25, no. 1, pp. 209–213, 2021.

[18] G. Li, H. Liu, G. Huang, X. Li, B. Raj, and F. Kara, "Effective capacity analysis of reconfigurable intelligent surfaces aided NOMA network," *EURASIP Journal on Wireless Communications and Networking*, vol. 2021, pp. 1–16, 2021.

[19] S. Atapattu, R. Fan, P. Dharmawansa, G. Wang, J. Evans, and T. A. Tsiftsis, "Reconfigurable intelligent surface assisted two-way communications: performance analysis and optimization," *IEEE Transactions on Communications*, vol. 68, no. 10, pp. 6552–6567, 2020.

[20] Z. Cao, X. Ji, J. Wang, S. Zhang, Y. Ji, and J. Wang, "Security-reliability tradeoff analysis for underlay cognitive two-way relay networks," *IEEE Transactions on Wireless Communications*, vol. 18, no. 12, pp. 6030–6042, 2019.

[21] X. Guo, B. Li, J. Cong, and R. Zhang, "Throughput maximization in a UAV-enabled two-way relaying system with multi-pair users," *IEEE Communications Letters*, vol. 25, no. 8, pp. 2693–2697, 2021.

[22] M. K. Shukla and H. H. Nguyen, "Ergodic secrecy sum rate analysis of a two-way relay NOMA system," *IEEE Systems Journal*, vol. 15, no. 2, pp. 2222–2225, 2021.

[23] Y. Liu, Y. Ye, G. Yan, and Y. Zhao, "Outage performance analysis for an opportunistic source selection based two-way cooperative ambient backscatter communication system," *IEEE Communications Letters*, vol. 25, no. 2, pp. 437–441, 2021.

[24] S. T. Shah, K. W. Choi, T.-J. Lee, and M. Y. Chung, "Outage probability and throughput analysis of SWIPT enabled

cognitive relay network with ambient backscatter," *IEEE Internet of Things Journal*, vol. 5, no. 4, pp. 3198–3208, 2018.

[25] Z. Yang, Z. Ding, P. Fan, and N. Al-Dhahir, "A general power allocation scheme to guarantee quality of service in downlink and uplink NOMA systems," *IEEE Transactions on Wireless Communications*, vol. 15, no. 11, pp. 7244–7257, 2016.

[26] E. Biglieri, R. Calderbank, A. Constantinides, A. Goldsmith, A. Paulraj, and H. V. Poor, *MIMO Wireless Communications*, Cambridge university Press, 2007.

[27] S. Jacob, V. G. Menon, K. S. Fathima Shemim, B. Mahapatra, and M. Mukherjee, "Intelligent vehicle collision avoidance system using 5G-enabled drone swarms," in *In Proceedings of the 2nd ACM MobiCom Workshop on Drone Assisted Wireless Communications for 5G and Beyond*, pp. 91–96, New York, NY, USA, 2020.

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