# Covert Backscatter Communication in the Presence of Multi-Antenna Eavesdropper

Yifan Zhang, *Graduate Student Member, IEEE*, Roberto Di Candia, Hüseyin Yiğitler,
Riku Jäntti, *Senior Member, IEEE*, and Zheng Yan, *Fellow, IEEE*

***Abstract*— Covert communication promises a secure transmission mechanism for Backscatter Communication (BC) by hiding the transmission behavior of backscatter devices from potential eavesdroppers. This letter investigates the upper limit of the covert rate in a scenario where a multi-antenna eavesdropper is present in BC setup, considering the inherent structural reflection of a backscatter tag. Specifically, the transceiver can employ a Gaussian signal to illuminate the tag, with special considering two distinct signals: a modulated signal and an additional reflected signal from the tag's antenna structure. This letter considers a powerful eavesdropper who is equipped with a massive antenna to enhance its ability to detect the tag's transmission activities. The results reveal the presence of the square root law ($\Theta(\sqrt{n})$ covert bits in $n$ channel uses) across various scenarios. Theoretical analysis demonstrates the inhibitory effects of both the tag's antenna structural reflection and the variance of the transceiver's Gaussian signal on the eavesdropper's detection capabilities. Furthermore, numerical results illustrate the impact of different parameters on the covertness of the system.**

***Index Terms*— Covert communication, backscatter communication, tag's structural reflection.**

## I. Introduction

The rapid development of the Internet of Things (IoT) has led to an increasing demand for wireless sensing devices. With considerations on both quantity and power consumption, Backscatter Communication (BC) enables passive tags to communicate by reflecting surrounding wireless signals without a battery, making it a promising technology for a wide array of IoT applications [1]. However, due to the broadcast nature of wireless communication, these tags are vulnerable to eavesdropping, which poses substantial security and privacy concerns [2]. Meanwhile, simple-designed backscatter tags present challenges for implementing conventional cryptography methods that depend on complex key variations [1]. Fortunately, covert communication offers a low-cost and effective solution, capable of hiding the transmission behavior from potential eavesdroppers by introducing uncertainty, such as noise or power fluctuations, into wireless channels [2]. Thus, it has been integrated into the BC system to enhance its security.

Covert BC have been extensively studied in [2], [3], [4], [5], [6], and [7]. In [2] and [3], the adjustment of the transmitted signal's power was explored to maximize the eavesdropper's detection error probability for legitimate channels. Similarly, the author in [4] proposed an energy-efficient covert communication scheme to minimize tags' power consumption by adjusting their backscattering coefficient. Additionally, the Square Root Law (SRL) was proven within a BC system in [5], which states that at most $\Theta(\sqrt{n})$ bits can be transmitted reliably and covertly over $n$ channel uses, assuming Alice and Bob share a sufficiently large codebook designed to encrypt each of Alice's transmitting symbols. The square root law also applies when attackers perform quantum eavesdropping [6]. Moreover, utilizing multi-antenna tags and beamforming techniques, the enhancement of the covert rate performance in BC systems was addressed by the author in [7]. These studies have wide-ranging implications for the development of an efficient covert BC system.

Those covert BC studies lack research on the practicality of achieving covert communications using the tags' inherent antenna reflection against eavesdroppers with massive antenna arrays. In practice, multi-antenna technology allows eavesdroppers to track and compensate received signals from various directions, providing significant array gains for signal detection in the tag's transmission activities [8]. Although technologies such as artificial noise [3] and multi-antenna tags [7] have demonstrated effectiveness in covert communication, their implementation requires power consumption and complex design, which are impractical for resource-constrained tags. In this letter, a BC system is explored as shown in Fig.1, where a transceiver named Bob illuminates a tag labeled Alice using Gaussian signals. Specifically, Alice harvests energy and modulates information on the incident signal, aiming to secure communication with Bob in the presence of an eavesdropper named Willie equipped with massive antennas. The main contributions of this work are as follows:

1) This study examines the covert rate limit in BC with a multi-antenna eavesdropper, focusing on Willie's detection probability with a large antenna array.
2) The confirmation of the square root law in covert BC illustrates how a tag's inherent reflection in its 'off' state adds noise for the eavesdropper, thus facilitating covert communication studies.
3) A numerical analysis assesses covertness across different scenarios, examining parameters to understand their impact on the system's covertness.

Notations: $(.)^{-1}$, $(.)^{T}$, $(.)^{H}$, and $|.|$ denote the inverse, transpose, conjugate, and determinant operations of a matrix.

Manuscript received 27 March 2024; revised 6 May 2024 and 4 June 2024; accepted 6 June 2024. Date of publication 11 June 2024; date of current version 14 August 2024. This work is supported in part by the National Natural Science Foundation of China under Grant U23A20300 and 62072351; in part by the Key Research Project of Shaanxi Natural Science Foundation under Grant 2023-JC-ZD-35; in part by the Academy of Finland under Grant 345072 and Grant 350464. The associate editor coordinating the review of this letter and approving it for publication was V. Jamali. *(Corresponding author: Yifan Zhang.)*

Yifan Zhang, Roberto Di Candia, Hüseyin Yiğitler, and Riku Jäntti are with the Department of Information and Communications Engineering, Aalto University, 02150 Espoo, Finland (e-mail: yifan.1.zhang@aalto.fi; roberto.dicandia@aalto.fi; huseyin.yigitler@aalto.fi; riku.jantti@aalto.fi).

Zheng Yan is with the School of Cyber Engineering, Xidian University, Xi'an, Shaanxi 710026, China (e-mail: zyan@xidian.edu.cn).

Digital Object Identifier 10.1109/LCOMM.2024.3412271

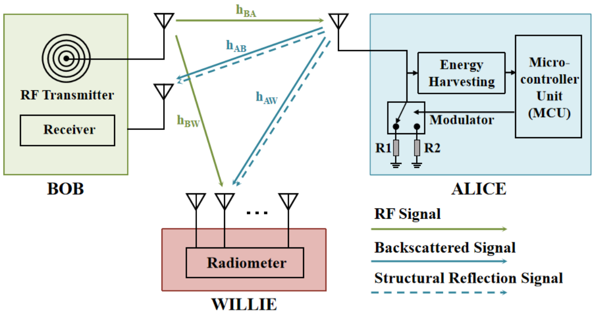

Fig. 1. System setup for covert monostatic backscatter communications. Alice performs binary phase shift keying by switching R1 and R2 to ‘open’ or ‘closed’. Willie uses a massive antenna array to track Bob’s illuminated and Alice’s modulated signals.

The absolute value and the conjugate operator for a complex number $z$ are denoted by $|z|$ and $z^*$. $\mathbb{E}\{\cdot\}$ stands for the statistical expectation of a random variable, while $\Re\{\cdot\}$ represents the real part of a complex number. $||\cdot||_{l1}$ and $||\cdot||$ are 1-norm and Euclidean norm, respectively. $f(x) \simeq g(x)$ denotes that $\lim_{x\to c}\frac{f(x)}{g(x)} = 1$, indicating asymptotic equality. $\boldsymbol{Q}(zt) = \int_{-\infty}^{z} e^{-\frac{1}{2}t^2}dt$ represents the Q-function. $\mathcal{D}_{\mathrm{KL}}(p||q)$ measures Kullback-Leibler (KL) divergence for possibility distribution $q$ and $p$, where $\mathcal{D}_{\mathrm{KL}}(p||q) = \sum_i p(i)\log\frac{p(i)}{q(i)}$.

## II. System Model

Fig. 1 illustrates a monostatic backscatter system, including Alice’s backscatter transponder and Bob’s full-duplex transceiver [1]. Initially, Bob transmits a Gaussian waveform $b$ to Alice’s antenna. The waveform $b$ is independent and follows a complex Gaussian distribution $\mathcal{CN}(0, P_b)$, where $P_b$ represents Bob’s average transmitting power, defined as $\mathbb{E}|b|^2$. Subsequently, Alice harvests energy from $b$ and proceeds to encode her message through load modulation on the incident wave. Specifically, let $a$ denote Alice’s information symbol, which is modeled with Binary Phase Shift Keying (BPSK). Alice sets $a = \pm 1$ when she is active and $a = 0$ when she is inactive. As Bob possesses knowledge of $b$, the modulation effect of Alice’s message $a$ on $b$ can be compared to subjecting each symbol $b$ to a known fast-fading channel, with the instantaneous coefficient $a$ considered from Bob’s perspective. Therefore, unlike the approach proposed in [5], Alice and Bob do not require a pre-shared codebook in the data transmission stage. Meanwhile, armed with massive antennas, Willie passively listens and intercepts Bob’s and Alice’s signals to determine whether Alice is transmitting messages to Bob. Given Willie’s observation of the signals from Bob and Alice, the signal received by Willie can be written as

$$\boldsymbol{y}_W = \boldsymbol{h}_{AW}(xa + \eta)b + \boldsymbol{h}_{BW}b + z, \tag{1}$$

where $\boldsymbol{h}_{AW} = \frac{g_{BA}g_{AW}}{\sigma_{WA}}\sqrt{P}$ presents the attenuation from Bob to Alice to Willie, and $\boldsymbol{h}_{BW} = \frac{g_{BW}}{\sigma_{BW}}\sqrt{P}$ is the attenuation from Bob to Willie. We assume a block fading channel model where the channel gains, denoted as $g_{KL}$ for $KL \in \{BA, AB, BW, AW\}$, are independently and identically distributed, while maintaining constant non-zero values within a detection cycle. Though the theoretical distribution could potentially include zero, the likelihood of a zero gain during any detection cycle under practical conditions is negligible. $\sigma_{AW}$ and $\sigma_{BW}$ are the standard deviation of the receiver noise at Alice-to-Willie and Bob-to-Willie channels. $x$ denotes Alice’s backscatter device’s attenuation factor, $0 < x < 1$. The factor $\eta$ stands for the reflection losses induced by the inherent structure of Alice. Even when Alice is inactive, power is still reflected due to the structural characteristics of the antenna chip. The experimental results from [9] suggest that the feasible range of the parameter $\eta$ includes values from 1 to 0.1. $z$ represents the Gaussian receiver noise at Willie, following the distribution $\mathcal{CN}(0, 1)$.

To improve the Signal-to-Noise Ratio(SNR), Willie can employ a matched filter to project the received high-dimensional signal $y_W$ onto two subspaces: one containing Bob’s illumination signal and another containing Alice’s signal. Subsequently, the Gram-Schmidt procedure is utilized to transform Willie’s received signal into two orthogonal bases [10]:

$$\boldsymbol{s}_{AW} = \frac{\boldsymbol{h}_{AW}}{||\boldsymbol{h}_{AW}||}, \quad \boldsymbol{s}_{BW} = \frac{\boldsymbol{h}_{BW} - \rho\boldsymbol{s}_{AW}}{||\boldsymbol{h}_{BW} - \rho\boldsymbol{s}_{AW}||}, \tag{2}$$

where $\rho = \frac{\boldsymbol{h}_{AW}\boldsymbol{h}_{BW}}{||\boldsymbol{h}_{AW}||||\boldsymbol{h}_{BW}||}$ shows the correlation between the two channel vectors, $0 \leq \rho \leq 1$. $\boldsymbol{h}_{BW}$ is represented as:

$$\boldsymbol{h}_{BW} = ||\boldsymbol{h}_{BW}||(\rho\boldsymbol{s}_{AW} + \sqrt{1 - |\rho|^2}\boldsymbol{s}_{BW}). \tag{3}$$

Thus, $y_W$ is mapped as two orthogonal signals $y_1$ and $y_2$.

$$\begin{aligned} y_1 = \Re\{\boldsymbol{g}_{AW}^H\boldsymbol{y}_W\} = (||\boldsymbol{h}_{AW}||\eta + ||\boldsymbol{h}_{BW}||\Re\{\rho\} \\ + ||\boldsymbol{h}_{AW}||xa)b + z_1, \end{aligned} \tag{4}$$

$$y_2 = \Re\{\boldsymbol{g}_{BW}^H\boldsymbol{y}_W\} = ||\boldsymbol{h}_{BW}||\sqrt{1 - |\rho|^2}b + z_2. \tag{5}$$

Denoting Willie’s received signal in vector form as $\boldsymbol{y} = (y_1, y_2)^T$, the channel covariance matrix observed by Willie, conditioned on $a$, is given by:

$$\boldsymbol{R}(ax) \triangleq \mathbb{E}\{\boldsymbol{y}\boldsymbol{y}^T|a\}. \tag{6}$$

When $a = 0$, Willie can determine the channel covariance as only Bob’s signal is present. According to [11], Willie can enhance the SNR and channel capacity by applying a whitening filter to the measured signal.

$$\boldsymbol{u} = \boldsymbol{R}^{\frac{1}{2}}(0)\boldsymbol{y}, \tag{7}$$

where $\boldsymbol{u} \in \mathbb{C}^{2\times 1}$ and each element in $\boldsymbol{u}$ contains $n$ samples captured by Willie. The Probability Density Function (PDF) of $u$ is [12].

$$\begin{aligned} & p_W(\boldsymbol{u}|a = 0) \\ & = \frac{1}{2\pi}\exp\left(-\frac{1}{2}||\boldsymbol{u}||^2\right) \end{aligned} \tag{8}$$

$$\begin{aligned} & p_W(\boldsymbol{u}|a \neq 0) \\ & = \sum_{a\in\pm 1}\frac{1}{4\pi|\boldsymbol{Q}(ax)|^{\frac{1}{2}}}\exp\left(-\frac{1}{2}\boldsymbol{u}^T\boldsymbol{Q}^{-1}(ax)\boldsymbol{u}\right), \end{aligned} \tag{9}$$

where $\boldsymbol{Q}(ax) = \boldsymbol{R}^{\frac{1}{2}}(0)\boldsymbol{R}(ax)\boldsymbol{R}^{\frac{1}{2}}(0)$. $p_W(\boldsymbol{u}|a = 0)$ is derived from the standard model of a circularly symmetric complex Gaussian random vector with zero mean and unit variance, commonly associated with noise-only conditions in signal processing. Conversely, when $a \neq 0$, $\boldsymbol{u}$ represents states where a signal is present. In these cases, the PDF is derived using a typical mixture model across the possible non-zero states of $a$.

Bob receiving signals from Alice are:

$$y_B = \boldsymbol{h}_{AB}(\eta + ax)b + z_{BA}, \tag{10}$$

where $\boldsymbol{h}_{AB} = \frac{g_{BA}g_{AB}}{\sigma_{BA}}\sqrt{P}$ is the attenuation from Alice to Bob. Alice and Bob can use a shared secret to encrypt their training sequence with a one-time pad to avoid Willie detecting $\boldsymbol{h}_{AB}$. To enable efficient signal detection, Bob adopts a matched filter that uses the knowledge of signal $b$ to optimize SNR [13].

$$v = \boldsymbol{h}_{AB}(\eta + ax) + \frac{b^*}{|b|}z_{BA}, \tag{11}$$

where $\eta$ does not influence the phase of the received signals because Bob is able to estimate channel information. Therefore, the SNR at Bob's receiver is $|b|^2||\boldsymbol{h}_{AB}||^2x^2$.

## III. Performance Analysis

### A. Willie's Detection Probability

We assume that Alice transmits $K$ symbols and Willie gets $L$ samples for each symbol Alice transmits. Let $\boldsymbol{u}^{(k,l)}$ denote $l^{\text{th}}$ sample related to Alice's $k^{\text{th}}$ symbol. Hence the total number of samples collected by Willie is $n = KL$, where $n$ represents limited channel use. Willie seeks to decide between two hypotheses $\mathcal{H}_0$, corresponding to communication off ($a^{(i)} = 0$), and $\mathcal{H}_1$ ($a^{(i)} = \pm 1$), corresponding to communication on. The respective probability distributions at Willie are

$$\mathcal{H}_0 : \boldsymbol{U} \sim \prod_{k=1}^{K}\prod_{l=1}^{L} p_W(\boldsymbol{u}^{(k,l)}|a^{(k)} = 0) \triangleq p(\boldsymbol{u}|\mathcal{H}_0) \tag{12}$$

$$\mathcal{H}_1 : \boldsymbol{U} \sim \prod_{k=1}^{K}\prod_{l=1}^{L} p_W(\boldsymbol{u}^{(k,l)}|a^{(k)} \neq 0) \triangleq p(\boldsymbol{u}|\mathcal{H}_1), \tag{13}$$

where $\boldsymbol{U} \in \mathbb{C}^{K\times L}$ is a matrix containing Willie's detection samples.

Assuming equal a priori probabilities for $\mathcal{H}_0$ and $\mathcal{H}_1$, Willie's detection error probability is [14].

$$\mathbb{P}_e^{(W)} = 1 - \frac{1}{2}\left\|p_W^{(n)}(\boldsymbol{u}|\mathcal{H}_0) - p_W^{(n)}(\boldsymbol{u}|\mathcal{H}_1)\right\|_{l_1}, \tag{14}$$

As provided in [15], the Pinsker's inequality can be used to bound (14) as a function of the KL divergence $\mathcal{D}_{\text{KL}}\left(p(\mathbf{z})||q(\mathbf{z})\right)$ as follows:

$$\mathbb{P}_e^{(W)} \geq 1 - \sqrt{\frac{n}{2}\mathcal{D}_{\text{KL}}\left(p_W(\boldsymbol{u}|\mathcal{H}_0)\|\ p_W(\boldsymbol{u}|\mathcal{H}_1)\right)}, \tag{15}$$

where the term $n$ in Eq. (14) becomes the multiplier term in Eq. (15), due to the independent distribution and additivity property of the KL divergence. To simplify the notation, we set $||\boldsymbol{h}_{AW}||\eta + ||\boldsymbol{h}_{BW}||\Re\{\rho\} = \mathrm{A}$, $||\boldsymbol{h}_{BW}||\sqrt{1-|\rho|^2} = \mathrm{B}$. Now the KL divergence is bound as follows:

$$\mathcal{D}_{\text{KL}}\left(p_W(\boldsymbol{u}|\mathcal{H}_0)||p_W(\boldsymbol{u}|\mathcal{H}_1)\right) \leq \kappa(A,B)||\boldsymbol{h}_{AW}||^4x^4, \tag{16}$$

where

$$\begin{aligned}\kappa(A,B) = \frac{1}{4\left(A^2+B^2+1\right)^4}&\big(3A^4B^4 + 14A^4B^2 + 13A^4 \\ &+ 6A^2B^6 + 22A^2B^4 + 18A^2B^2 + 2A^2 + 3B^8 \\ &+ 8B^6 + 8B^4 + 4B^2 + 1\big).\end{aligned} \tag{17}$$

The bound is derived by expanding the Taylor series of the KL divergence and noting that the lower-order terms vanish, as specified in [14]. Furthermore, by applying the Taylor Reminder Theorem, it can be shown that this truncation of the series is an upper bound. Alice can thus bound Willie's sum detection probability as:

$$\mathbb{P}_e^{(W)} \geq 1 - ||\boldsymbol{h}_{AW}||^2x^2\sqrt{\frac{n}{2}\kappa(A,B)} = 1 - \varepsilon, \tag{18}$$

by controlling its attenuation factor $x^2$ as follows:

$$x^2 \leq \frac{\sqrt{2}\varepsilon}{\sqrt{\kappa(A,B)}}\frac{1}{||\boldsymbol{h}_{AW}||^2}\frac{1}{\sqrt{n}}, \tag{19}$$

where $\varepsilon$ is maintained as a constant throughout different values of $n$, which is a standard definition in covertness literature representing a target covertness level [14].

### B. Performance of the Link Between Alice and Bob

The expected SNR at Bob is $\mathsf{SNR}_{BA} = \mathbb{E}\{|b|^2||\boldsymbol{h}_{AB}||^2x^2\} = ||\boldsymbol{h}_{AB}||^2x^2$. In the case of BPSK and Additive White Gaussian Noise (AWGN) channel, Bob's bit error probability conditions on his received signal amplitude: $p_b = Q(\sqrt{\mathsf{SNR}_{BA}|b|^2})$ For a small $z$, $Q(z) \simeq \frac{1}{2} - \frac{z}{\sqrt{2\pi}}$ using Taylor expanding and taking the first-order term. Thus, for a very small SNR on the Alice-to-Bob link, the bit error probability can be approximated as:

$$p_b \simeq \frac{1}{2} - \sqrt{\frac{\mathsf{SNR}_{BA}|b|^2}{2\pi}} = \frac{1}{2} - \sqrt{\frac{||\boldsymbol{h}_{AB}||^2|b|^2x^2}{2\pi}}. \tag{20}$$

Both soft and hard decisions can be made in the decoding procedure of the BC system. Since soft-decision decoding produces optimum results [16], the worst-case is considered that Bob uses hard-decision decoding, i.e., $y_B^{(i)} > 0$ for bit 1 and $y_B^{(i)} \leq 0$ for bit 0. The capacity of a Binary Symmetric Channel (BSC) is used to evaluate the link capacity (in bits per channel use) between Alice and Bob. The equation can be simplified and expressed as follows:

$$\mathsf{c} = 1 - H_2(p_b) \simeq \frac{1}{2\ln(2)}\left(p_b - \frac{1}{2}\right)^2 + O\left(\left(p_b - \frac{1}{2}\right)^4\right), \tag{21}$$

where $H_2(p_b) = p_b\log_2(p_b) + (1-p_b)\log_2(1-p_b)$ is the binary entropy function. The approximation for $\mathsf{c}$ comes from a Taylor series expansion of $1 - H_2(p_b)$ around $p_b = \frac{1}{2}$, which is the point of maximum entropy, suggesting the bad channel and bit errors are highly probable. The notion $O\left(\left(p_b - \frac{1}{2}\right)^4\right)$ signifies that the contributions of the fourth order and higher terms are asymptotically negligible compared to the second order term. According to [17], $\mathsf{c}$ can be further simplified as

$$\mathsf{c} \simeq \frac{||\boldsymbol{h}_{AB}||^2|b|^2x^2}{2\pi}. \tag{22}$$

Since Bob's signal amplitude is randomly changing, the covert rate resembles that of the fading channel:

$$\bar{\mathsf{c}} = \mathbb{E}_h\{\mathsf{c}\} \simeq \frac{||\boldsymbol{h}_{AB}||^2x^2}{2\pi} = \frac{\mathsf{SNR}_{BA}}{2\pi}. \tag{23}$$

Considering repetition coding, let $R = \frac{m}{n}$ denote the data rate used by Alice. The error probability for detecting these messages in this situation is bounded by typical Gallager's random coding bound [18] as:

$$\mathbb{P}_e^{(B)} \le e^{-nE_r(R)}, \tag{24}$$

where $E_r(R)$ is Gallagher's random coding error exponent, and $n$ is defined in Eq. (12). This bound demonstrates the reliability of communication systems, i.e., the exponential decrease of the error probability with increasing block length. As specified in [17], in the limit of small SNR, Gallagher's random coding error can be expressed as:

$$E_r(R) \simeq \begin{cases} \bar{\mathsf{c}}/2 - R & 0 \le \frac{R}{\bar{\mathsf{c}}} \le \frac{1}{4} \\ \left(\sqrt{\bar{\mathsf{c}}} - \sqrt{R}\right)^2 & \frac{1}{4} \le \frac{R}{\bar{\mathsf{c}}} \le 1. \end{cases} \tag{25}$$

## IV. Numerical Results and Discussion

This section evaluates Willie's detection capabilities for Alice's transmissions under various scenarios and parameters. SRL is proven in multiple specific cases, and simulation results illustrate how channel correlation and Alice's antenna reflection factor affect covertness. The path loss exponent is set as $\gamma = 2$, and the typical distances between two nodes are set as $d_k = 1\ m, k \in \{AW, BW, AB\}$.

**Case I: Willie knows Bob's signals.** Willie can boost the SNR of the Bob-to-Willie channel if he is equipped with infinite antennas and steers most of his antennas to Bob, i.e., $||\boldsymbol{h}_{BW}|| \to \infty$. According to Eq.(17), the bound of $\kappa(A, B)$ can be found as:

$$\lim_{||\boldsymbol{h}_{BW}|| \to \infty} \kappa(A, B) = \frac{3(|\rho|^2 - 1)^2}{4}. \tag{26}$$

The SNR of the Alice to Bob link now becomes:

$$\mathsf{SNR}_{BA}^{(1)} = 4\sqrt{\frac{2}{3}} \frac{1}{1 - |\rho|^2} \frac{||\boldsymbol{h}_{AB}||^2}{||\boldsymbol{h}_{AW}||^2} \frac{\varepsilon}{\sqrt{n}}. \tag{27}$$

From Eq. (27), it can be found that Alice's structural reflection factor $\eta$ cannot affect $\mathsf{SNR}_{BA}^{(1)}$ in this case. The reason is Willie can identify and filter out Alice's structural reflection signals, as they are distinct from the correlated signals of Alice and Bob. In what follows, two cases are analyzed based on the value of the channel correlation $\rho$.

*1) 0≤ρ<1:* From Eq. (27), it can be found that increasing $\rho$ and the distance between Alice and Willie enhance $\mathsf{SNR}_{BA}^{(1)}$, since the reduced channel gain $||\boldsymbol{h}_{AW}||$ and the strong correlation between Alice's and Bob's signals make it hard for Willie to extract Alice's signals from Alice's and Bob's correlated signals under a targeted covertness level $\varepsilon$. From Fig. 2 and Eq. (27), it can be found that a higher $\varepsilon$ means that Alice can transmit more power without being detected by Willie. This results in a higher $\mathsf{SNR}_{BA}^{(1)}$ and the error exponent $nE_r(R)$, enhancing the communication quality between Alice and Bob. Similar results also exist in other cases. Besides, Fig. 2 illustrates that the error exponent $nE_r(R)$ scales with channel use $n$, leading to exponential decay in decoding error probability, supporting the SRL observed in [5].

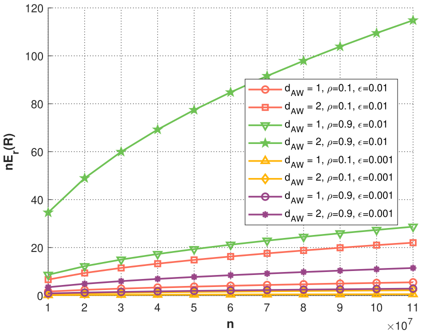

Fig. 2. Willie has Bob's signal.

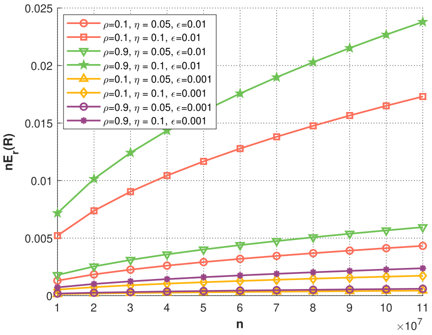

Fig. 3. Willie has Bob's signal with bounded SNR.

*2) $\rho = 1$:* This case corresponds to very short distances between Alice and Bob. It is challenging for Willie to distinguish Alice's and Bob's signals due to their strong correlation. For large $n$, the error exponent scales directly proportional to $n$ by scale $||h_{AB}||$ proportional to $\sqrt{n}$.

**Case II: Willie knows Bob's signal with bounded SNR.** Bounding $||\boldsymbol{h}_{BW}||$ would imply that Bob employs an extra noise transmitter with a directed antenna pointed towards Willie's antenna and uses jamming power $J \propto P$. Bob can also limit Willie's SNR by using a highly directive antenna pointed towards Alice, assuming that Willie is located in a different direction from Alice. Taking the worst case that Willie can boost the SNR of the Alice-to-Willie channel, i.e., $||\boldsymbol{h}_{AW}|| \to \infty$, now we have

$$\lim_{\|\boldsymbol{h}_{AW}\| \to \infty} \kappa(A, B)\|\boldsymbol{h}_{AW}\|^4 = \frac{13 + 3\|\boldsymbol{h}_{BW}\|^4(|\rho|^2 - 1)^2 + 14\|\boldsymbol{h}_{BW}\|^2(|\rho|^2 - 1)}{4\eta^4} \tag{28}$$

$$\mathsf{SNR}_{BA}^{(2)} = 4\sqrt{2}\eta^2 \frac{\boldsymbol{h}_{AB}^2}{\|\boldsymbol{h}_{BW}\|^2} \times \frac{\varepsilon}{\sqrt{3(|\rho|^2 - 1)^2 + \frac{14(|\rho|^2 - 1)}{\|\boldsymbol{h}_{BW}\|^2} + \frac{13}{\|\boldsymbol{h}_{BW}\|^4}}} \times \frac{1}{\sqrt{n}}. \tag{29}$$

Similar to Case I, SRL is revealed from Fig. 3 that the error exponent $nE_r(R)$ exhibits square root growth with the channel use $n$, and thus decoding error probability decays exponentially to zero as n increases. Fig. 3 and Eq. (29) show that increasing Alice's structural reflection factor $\eta$ and channel correlation $\rho$ improves the error component and the SNR of Alice to Bob link. This is because the additional structural reflection and strong channel correlation confuse Willie about Alice's transmission activity and provide SNR gain for Alice

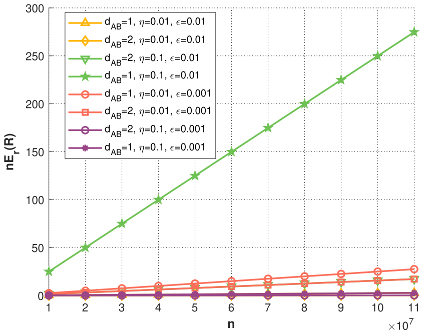

Fig. 4. Willie doesn't have the signal from Bob.

to Bob link under a target $\varepsilon$. Besides, $SNR_{BA}^{(2)}$ decreases as $||\boldsymbol{h}_{BW}||$ increases since Bob has to reduce transmitting power to keep a constant $\varepsilon$. It is notable that Case I and Case II cannot be directly compared as they are derived in different limitations.

**Case III: Willie cannot detect the signal from Bob.** This could happen when Bob is equipped with multiple antennas that are steered toward Willie's null space by beamforming or the Bob to Willie channel is physically blocked. Now $\kappa(A,B)$ becomes:

$$\lim_{||\boldsymbol{h}_{BW}||\to 0} \kappa(A,B) = \frac{13||\boldsymbol{h}_{AW}||^4\eta^4 + 2||\boldsymbol{h}_{AW}||^2\eta^2 + 1}{4(||\boldsymbol{h}_{AW}||^2\eta^2 + 1)^4}. \tag{30}$$

Taking the limit as $||\boldsymbol{h}_{AW}|| \to \infty$ yields

$$\lim_{||\boldsymbol{h}_{AW}||\to\infty} \mathbb{P}_e^{(W)} \geq 1 - x^2\sqrt{\frac{13n\eta^4}{4}}. \tag{31}$$

$$\lim_{||\boldsymbol{h}_{AW}||\to\infty} \mathsf{SNR}_{BA}^{(3)} = 4\eta^2||\boldsymbol{h}_{AB}||^2\sqrt{\frac{2}{13}}\frac{\varepsilon}{\sqrt{n}}, \tag{32}$$

Eq. (31) and (32) show that Bob can increase its power $P$ while constraining Willie's detection probability. That is, given SNR can be maintained at Bob's receiver while limiting Willie's detection probability to be arbitrarily small. If we set $||h_{AB}||^2 = ||h_{AB}||^2\sqrt{n} \to \infty$, the error exponent $nE_r(R)$ scales directly proportional to $n$, which means the SRL of covert communication can be circumvented by denying Willie access to Bob's signals. Nevertheless, when Bob's transmitting signals are limited to a maximum power constraint, the square root law still holds since $H_{AB}^2$ is a constant in this case. Fig. 4 shows that increasing Alice's structural antenna reflection coefficient impairs Willie's detection ability, since the added structural reflections by Alice contribute additional noise, complicating Willie's detection efforts.

## V. Discussion and Conclusion

This letter assumes Alice and Bob share a secret to evade Willie's detection during channel training, requiring substantial resources from Alice. Alternatively, Alice could use differential BPSK, eliminating the training stage but causing a 3dB SNR reduction in the Alice-Bob link [19]. Essentially, this adjustment introduces a constant term to the original scheme, maintaining the square root law's integrity. Besides, some training sequences could still be needed for Bob to obtain frame synchronization with Alice. This can be avoided if Alice and Bob share a clock and Alice follows a fixed transmission schedule. As for modulation methods' influence on covertness, this letter assumes Alice's adopting BPSK. Moreover, Quadrature Phase Shift Keying (QPSK) and Quadrature Amplitude Modulation (QAM) are alternative options for enhancing the security of BC systems in scenarios requiring covert operation, increased data rates, and improved bit error rates [16].

In conclusion, this letter examines the limited covertness of the BC system under a multi-antenna eavesdropper. The eavesdropper's detection capabilities are assessed, and the square root law is verified by exploiting Alice's structural reflection. Through numerical simulations, the communication performance and the impact of key factors are demonstrated. Furthermore, the potential to circumvent the square root law by blocking the Bob-to-Willie channel is illustrated.

## References

[1] P. Wang, Z. Yan, and K. Zeng, "BCAuth: Physical layer enhanced authentication and attack tracing for backscatter communications," *IEEE Trans. Inf. Forensics Security*, vol. 17, pp. 2818–2834, 2022.

[2] J. Liu, J. Yu, X. Chen, R. Zhang, S. Wang, and J. An, "Covert communication in ambient backscatter systems with uncontrollable RF source," *IEEE Trans. Commun.*, vol. 70, no. 3, pp. 1971–1983, Mar. 2022.

[3] K. Shahzad and X. Zhou, "Covert communication in backscatter radio," in *Proc. IEEE Int. Conf. Commun. (ICC)*, May 2019, pp. 1–6.

[4] Y. Wang, S. Yan, W. Yang, Y. Huang, and C. Liu, "Energy-efficient covert communications for bistatic backscatter systems," *IEEE Trans. Veh. Technol.*, vol. 70, no. 3, pp. 2906–2911, Mar. 2021.

[5] W. Chen, H. Ding, S. Wang, and F. Gong, "On the limits of covert ambient backscatter communications," *IEEE Wireless Commun. Lett.*, vol. 11, no. 2, pp. 308–312, Feb. 2022.

[6] R. Di Candia, H. Yiğitler, G. S. Paraoanu, and R. Jäntti, "Two-way covert quantum communication in the microwave regime," *PRX Quantum*, vol. 2, no. 2, May 2021, Art. no. 020316.

[7] J. Liu, J. Yu, D. Niyato, R. Zhang, X. Gao, and J. An, "Covert ambient backscatter communications with multi-antenna tag," *IEEE Trans. Wireless Commun.*, vol. 22, no. 9, pp. 6199–6212, Feb. 2023.

[8] G. Liu, A. Liu, R. Zhang, and M. Zhao, "Angular-domain selective channel tracking and Doppler compensation for high-mobility mmWave massive MIMO," *IEEE Trans. Wireless Commun.*, vol. 20, no. 5, pp. 2902–2916, May 2021.

[9] J. Li, A. Li, D. Han, Y. Zhang, T. Li, and Y. Zhang, "RCID: Fingerprinting passive RFID tags via wideband backscatter," in *Proc. IEEE Conf. Comput. Commun.*, May 2022, pp. 700–709.

[10] P. D. Lax, *Linear Algebra and its Applications*, vol. 78. Hoboken, NJ, USA: Wiley, 2007.

[11] W. L. Melvin and G. A. Showman, "An approach to knowledge-aided covariance estimation," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 42, no. 3, pp. 1021–1042, Jul. 2006.

[12] A. Abdelaziz and C. E. Koksal, "Fundamental limits of covert communication over MIMO AWGN channel," in *Proc. IEEE Conf. Commun. Netw. Secur. (CNS)*, Oct. 2017, pp. 1–9.

[13] L. Xi and S. H. Cho, "A RFID decoder using a matched filter for compensation of the frequency variation," in *Proc. 5th Int. Conf. Wireless Commun.*, 2009, pp. 1–5.

[14] B. A. Bash, D. Goeckel, and D. Towsley, "Limits of reliable communication with low probability of detection on AWGN channels," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 9, pp. 1921–1930, Sep. 2013.

[15] T. M. Cover, *Elements of Information Theory*. Hoboken, NJ, USA: Wiley, 1999.

[16] F. Rezaei, D. Galappaththige, C. Tellambura, and S. Herath, "Coding techniques for backscatter communications—A contemporary survey," *IEEE Commun. Surveys Tuts.*, 2023.

[17] E. E. Majani, "A model for the study of very noisy channels, and applications," Ph.D. dissertation, California Inst. Technol., Pasadena, CA, USA, 1988.

[18] R. G. Gallager, *Information Theory and Reliable Communication*, vol. 2. Cham, Switzerland: Springer, 1968.

[19] C. Xu, X. Liu, and X. Wei, "Differential phase-shift keying for high spectral efficiency optical transmissions," *IEEE J. Sel. Topics Quantum Electron.*, vol. 10, no. 2, pp. 281–293, Mar. 2004.