Covert Communication in Backscatter Radio

Khurram Shahzad and Xiangyun Zhou
Research School of Engineering, The Australian National University, Canberra, ACT 2601, Australia
Email: {khurram.shahzad, xiangyun.zhou}@anu.edu.au

***Abstract*—Covert communication in backscatter radio systems is considered, where the transmitter controls its transmit power to keep the transponder's response hidden, while a warden tries to detect this covert communication. To achieve covertness, we propose a non-conventional transmission scheme where the transmitter emits noise-like signal with transmit power varying across different communication slots. Under the assumption of a radiometer as the detector at the warden, we first derive the optimal detection threshold for this detector. Next, building upon the detection performance of warden, we analyze the condition on the transmit power to achieve a target level of covertness. Our numerical results illustrate the price a backscatter system has to pay, in terms of bit error rate, for achieving covert communication.**

I. Introduction

The Internet of Things (IoT) foresees integration of every object for interaction via embedded systems. This will lead to a highly distributed network of devices communicating with human beings as well as other devices. The IoT devices are expected to be equipped with millions of sensors and communication capabilities, making them an intrinsic part of the existing communication systems. It can be an arduous task to keep these energy-hungry sensors alive, since majority of these sensors are not easily accessible, due to their deployment in toxic and unsafe environments, or at places hard to reach. Backscatter communication [1, 2] offers unique advantages, eliminating the need of any active radio frequency (RF) components, resulting in a prolonged life-span of the wireless devices and continued network functionality. These wireless devices can not only harvest energy from the transmitter's signal, but can also modulate the same signal to convey information. Although backscatter communication has been largely deployed in radio frequency identification (RFID) systems for consumer-based applications e.g., supply-chain management, RFID cards have also made their way into more sensitive arenas, e.g., access control, payment systems and asset tracking. However, the application of backscatter systems in such sensitive scenarios is limited, owing to their broadcast nature and the ease of snooping information through eavesdropping. One option to alleviate this issue may be to use stronger encryption protocols, but the size, cost and power constraints of most backscatter transponders do not warrant such luxuries [3].

Physical layer security techniques offer compelling alternatives to encryption, by exploiting the varying physical characteristics of the wireless channel [4]. These techniques can also be used in conjunction with encryption to strengthen the existing layer of defense. However, situations exist where apart from protecting the content of communication, it is imperative to hide the transmission, making it undetectable. Such circumstances arise in sensitive communication scenarios or situations where an organization is interested in keeping its activities hidden over the air. The aforementioned activities require covert communication that is undetectable by a third party [5]. The fundamental limits of covert communication has been explored in [6], providing a square root law on the limit of covertly transmitted information. Further research efforts in this regard have demonstrated a positive communication rate under the exploitation of channel and noise uncertainty at the eavesdropper [7–10], presence of friendly jammers [11, 12] and using a full-duplex receiver generating artificial noise [13] to facilitate covert transmissions.

Security of backscatter systems and specifically RFIDs has been considered widely in the recent literature. The physical layer security of backscatter systems has been considered in detail in [14–16], and references therein. In [17], a frequency hopping RFID system in the presence of an adversarial reader is considered and a theoretical analysis of decoding error probability is provided. Despite a plethora of research in the security and privacy of backscatter systems, to the best of our knowledge, covert communication in backscatter communication has not been studied before. In this work, we present a study on a backscatter system where the reader (i.e., the transmitter) tries to obtain information from a tag (i.e., the transponder) in such a way that the transmission from the tag remains covert from a warden, Willie, who is looking to detect the tag's transmission to the reader.[1] In our considered system, the reader's transmitted signal is not intended to be hidden, rather the reader looks to manipulate its signal such that Willie remains unaware of tag's response state.

The main contributions of this work are as follows:

- To achieve covert backscatter communication, we propose to use a noise-like signal with variable power at the reader when sending its transmitted signal. This transmission scheme achieves a desired level of covertness by controlling the variation in reader's transmit power.
- Under the proposed scheme, we derive a closed-form expression for the optimal detection threshold for a radiometer at Willie.
- We analytically characterize the condition on the reader's transmit power to achieve a target level of covertness and

[1] We adopt the terms "reader" and "tag" as is commonly used in RFID literature, although the analysis is applicable to a variety of systems employing backscatter communication.

numerically investigate the bit error rate (BER) performance of the backscatter communication. The tradeoff between covertness against Willie's detection and BER performance at the reader is presented.

II. System Model

A backscatter communication system with a passive tag is considered, as shown in Fig. 1, where the tag possesses sensitive information that needs to be sent to the reader. Being passive, the tag has no power supply, thus it cannot initiate communication on its own and fully relies on the reader's signal for its operation. A monostatic reader is considered, whose transmitted signal is not only used by the tag to harvest energy, but is also modulated by the tag to send information to the reader. The tag utilizes Binary Phase Shift Keying (BPSK) [1] to send information to the reader, thus the intentional reflection from the tag has two possible states in each symbol, depending on the data the tag has to transmit. We define a communication slot as a block of time over which the transmission of a message from the tag to the reader is complete. Each slot contains n symbol periods and we assume that n is large enough, i.e., $n \to \infty$. Under this setting, a warden Willie is also present as a silent observer, trying to detect whether or not the tag transmits to the reader in a given slot. We use the subscripts r, t and w to represent the terms associated with reader, tag and Willie, respectively. The distances from reader-tag, tag-Willie and reader-Willie are represented by d_{rt}, d_{tw} and d_{rw}, respectively. For simplicity, we consider the time delay among the signals arriving at a node to be negligible. The channel coefficient between any two users a and b is denoted by h_{ab}, and is dependent upon the combined antenna gain and distance between the two users. The additive Gaussian noise at the reader's receiver and Willie is denoted by $n_r \sim \mathcal{N}(0, \sigma_r^2)$ and $n_w \sim \mathcal{N}(0, \sigma_w^2)$, respectively.

A. Proposed Reader Transmission Scheme

In conventional backscatter communication, the reader transmits a continuous wave (CW) with a constant amplitude. This approach does not lend itself well to covert communication, since under the assumption of Willie knowing the reader's constant transmit power, it is straightforward for Willie to raise an alarm when an additional reflection from the tag is received at Willie alongside the reader's signal.

To achieve covertness, we propose the following transmission scheme: Instead of transmitting a simple unmodulated CW, the reader transmits a noise-like signal following Gaussian distribution. This creates confusion at Willie and makes it impossible for Willie to cancel such a signal. More importantly, the transmit power of the noise-like signal is randomized such that the reader's transmit power in each slot, P_R, is a random variable, following a uniform distribution, i.e., $P_R \sim \mathcal{U}(P_{\min}, P_{\max})$. The introduction of randomness in the reader's transmit power creates uncertainty in Willie's received power, effectively creating an artificial fading [18], such that Willie is unsure whether an increase in the received power is due to the tag's backscatter or simply a variation in the power of the reader's transmitted signal. Note that we consider the uniform distribution as a first example; other distributions will be investigated in future work.

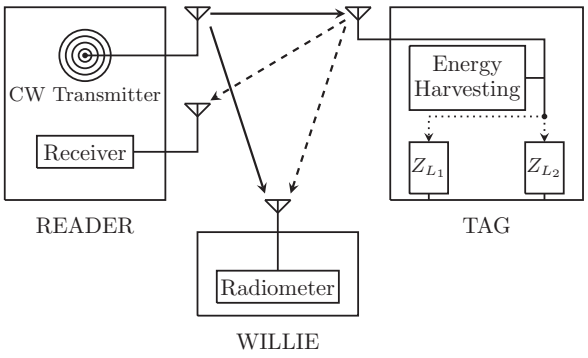

Fig. 1. System model for covert communication in a backscatter system.

B. Tag's Operation

If the tag has information to send in a slot, it modulates the incident signal by changing its load impedance. It reflects back a certain portion of the power contained in the signal and absorbs the rest of the power for utilization, including energy consumption by the tag's chip, modulation circuitry and antenna. Assuming complex impedances, the wave reflection coefficient at the tag is given by [1]

$$\Gamma = \frac{Z_L - Z_A^*}{Z_L + Z_A^*}, \tag{1}$$

where Z_L and Z_A represent the tag's load and antenna impedance, respectively, and $(\cdot)^*$ denotes the conjugate operation. To convey any information to the reader, the tag chooses an appropriate load impedance,

$$Z_L = \frac{Z_A^* + \Gamma_x Z_A^*}{1 - \Gamma_x}, \tag{2}$$

where, under BPSK, Γ_x can be Γ_{-1} or Γ_{+1}, depending upon the information symbol $x \in \{-1, +1\}$. In this work, we assume that $|\Gamma_{-1}| = |\Gamma_{+1}| = |\Gamma|$.

C. Requirement for Covertness

Based on the signals received in a slot, Willie has to decide whether the tag transmitted any information by modulating the reader's signal. Here, Willie faces a binary hypothesis testing problem. The null hypothesis, H_0, says that the tag did not send any information to the reader, while the alternative hypothesis, H_1, says that the tag did modulate the reader's signal, hence sending information to the reader. It is assumed that Willie is unaware of the exact transmit power used by the reader in each slot, although the transmission model and distribution of reader's transmit power is known to Willie. Also, Willie has full knowledge of the associated antenna gains, reflection coefficients utilized by the tag under BPSK and his receiver's noise variance.

Willie has to make a decision at the end of each slot regarding the tag's actions in that slot. We define the probability of false alarm (or Type I error) as the probability that Willie makes a decision in favour of H_1 while H_0 is true, and denote it by $\mathbb{P}_{FA}$. Similarly, the probability of missed detection (or Type II error) is defined as the probability of Willie making a decision in favour of H_0 while H_1 is true, and is denoted by $\mathbb{P}_{MD}$. Under the assumption of both hypotheses being presented with an equal *a priori* probability [6, 10], we consider the reader achieving covert communication if, for a target $\epsilon > 0$, a communication scheme exists such that $\mathbb{P}_{FA} + \mathbb{P}_{MD} \geq 1 - \epsilon$, as $n \to \infty$. Here ϵ signifies the covert requirement, since a sufficiently small ϵ renders any detector employed at Willie to be ineffective [6].

III. Detection Scheme at Willie

Due to the independent and identically distributed (i.i.d.) nature of Willie's observation vector $\boldsymbol{y}_w = [y_w(1), y_w(2), \ldots, y_w(n)]$, the optimal approach for Willie to minimize his detection error, according to Neyman-Pearson criterion, is to use the *likelihood ratio test* [19],

$$\Lambda(\boldsymbol{y}_w) = \frac{f_{\boldsymbol{y}_w|H_1}(\boldsymbol{y}_w|H_1)}{f_{\boldsymbol{y}_w|H_0}(\boldsymbol{y}_w|H_0)} \underset{D_0}{\overset{D_1}{\gtrless}} \Upsilon, \tag{3}$$

where $\Upsilon = 1$ due to the assumption of equal *a priori* probabilities of each hypothesis. Here, D_1 and D_0 correspond to a decision in favor of hypothesis H_1 and H_0, and $f_{\boldsymbol{y}_w|H_1}(\boldsymbol{y}_w|H_1)$ and $f_{\boldsymbol{y}_w|H_0}(\boldsymbol{y}_w|H_0)$ are the likelihood functions of Willie's observation vectors for the considered slot, under hypothesis H_1 and H_0, respectively. Under H_0, the tag chooses a load impedance that is conjugate matched to the antenna impedance, resulting in a reflection bearing no information. The baseband signal received by Willie under H_0 is given by

$$y_w(i, H_0) = h_{rw}c(i) + S_w(i) + n_w(i), \tag{4}$$

where $i = 1, \ldots, n$ represents the symbol index. Here, $c(i)$ is the i^{th} symbol transmitted by the reader, $S_w(i) = h_{rt}h_{tw}c(i)$ represents the structural mode scattering component [20, 21] of the tag's reflection received at Willie[2], and $n_w(i)$ is Willie's receiver noise component.

Under H_1, the tag modulates the reader's signal by intentionally mismatching its load impedance to the antenna impedance, causing a deliberate reflection of the received signal back to the reader. In this case, the baseband signal received at Willie is

$$y_w(i, H_1) = h_{rw}c(i) + S_w(i) + A_w(i) + n_w(i), \tag{5}$$

where $A_w(i)$ represents the antenna mode scattering component of the tag's reflection received at Willie. The antenna mode component depends on the load chosen by the tag via (1) and (2), and is given by $A_w(i) = h_{rt}h_{tw}|\Gamma|c(i)x(i)$. Owing to its low complexity and ease of implementation, we assume in this work that Willie uses a radiometer [11, 13] for the detection of any covert response from the tag. Under this assumption, the average power received at Willie becomes a crucial quantity. Based on Frii's equation [22, 23], we have $h_{ab}^2 = \frac{G_{ab}K^2}{d_{ab}^2}$, where G_{ab} represents the combined transmitter-receiver antenna gain between users a and b, and $K = \frac{\lambda}{4\pi}$ is a constant dependent upon the carrier wavelength. Using (4), the average received power at Willie in a slot under H_0 can be calculated as

$$\begin{aligned} P_w(H_0) &= \lim_{n\to\infty} \frac{1}{n} \sum_{i=1}^{n} \left[\Big(y_w(i, H_0) \Big)^2 \right] \\ &= \lim_{n\to\infty} \frac{1}{n} \sum_{i=1}^{n} \left[\Big(h_{rw}c(i) + S_w(i) + n_w(i) \Big)^2 \right] \\ &= \alpha P_R + \sigma_w^2, \end{aligned} \tag{6}$$

where

$$\alpha = \frac{G_{rw}K^2}{d_{rw}^2} + \frac{G_{rt}G_{tw}K^4}{d_{rt}^2 d_{tw}^2}, \tag{7}$$

and in deriving (6), we have used the fact that $\sum_{i=1}^{n} c^2(i)$ corresponds to the sum of n independent and squared Gaussians, each with variance P_R, and this sum of squared Gaussians results in a Chi-squared random variable. In (7), the first term corresponds to the reader's signal received directly by Willie and the second term corresponds to the structural mode component of tag's antenna scattering as received by Willie.

Under H_1, the power received at Willie includes an additional term, due to the information-bearing reflection from the tag. Following steps similar to the analysis of H_0, the average power received at Willie in a slot under H_1 is given by

$$P_w(H_1) = \beta P_R + \sigma_w^2, \tag{8}$$

where

$$\beta = \frac{G_{rw}K^2}{d_{rw}^2} + \frac{G_{rt}G_{tw}K^4}{d_{rt}^2 d_{tw}^2} + \frac{G_{rt}G_{tw}K^4|\Gamma|^2}{d_{rt}^2 d_{tw}^2}. \tag{9}$$

In the following, we derive the optimal threshold of Willie's radiometer that minimizes the detection error probability.

Proposition 1. *Under the assumption of a radiometer, the optimal value of threshold for Willie's detector is*

$$\begin{cases} \gamma^* \in (\alpha P_{max} + \sigma_w^2, \beta P_{min} + \sigma_w^2), & \text{if} \quad \alpha P_{max} < \beta P_{min} \\ \gamma^* = \alpha P_{max} + \sigma_w^2, & \text{otherwise}, \end{cases} \tag{10}$$

where α and β are as defined in (7) and (9), respectively.

Proof. Willie compares the average received power to a threshold, γ, and decides on either of the hypothesis, H_0 or H_1, being true. In order to minimize his detection error, Willie considers the following optimization problem

$$\min_{\gamma} \quad \mathbb{P}_{FA} + \mathbb{P}_{MD}. \tag{11}$$

[2]Note that the tag gives a constant (structural mode) reflection even when no information is sent. In the majority of backscatter literature, the term originating from the structural mode is generally ignored in the analysis, as it has no impact on the reader's error probability [1].

Here, we have

$$\mathbb{P}_{FA} = \mathbb{P}\left[D_1|H_0\right] = \mathbb{P}\left[P_w > \gamma|H_0\right] = \mathbb{P}\left[\alpha P_R + \sigma_w^2 > \gamma\right] = \mathbb{P}\left[P_R > \frac{\gamma - \sigma_w^2}{\alpha}\right]. \quad (12)$$

Since $P_R \sim \mathcal{U}(P_{\min}, P_{\max})$,

$$\mathbb{P}_{FA} = \begin{cases} 1, & \text{if} \quad \frac{\gamma-\sigma_w^2}{\alpha} \leq P_{min} \\ \frac{P_{\max} - \left(\frac{\gamma-\sigma_w^2}{\alpha}\right)}{P_{\max}-P_{\min}}, & \text{if} \quad P_{\min} < \frac{\gamma-\sigma_w^2}{\alpha} \leq P_{\max} \\ 0, & \text{if} \quad \frac{\gamma-\sigma_w^2}{\alpha} > P_{\max}. \end{cases} \quad (13)$$

Similarly,

$$\mathbb{P}_{MD} = \mathbb{P}\left[D_0|H_1\right] = \mathbb{P}\left[P_w < \gamma|H_1\right] = \mathbb{P}\left[\beta P_R + \sigma_w^2 < \gamma\right] = \mathbb{P}\left[P_R < \frac{\gamma - \sigma_w^2}{\beta}\right]$$

$$= \begin{cases} 0, & \text{if} \quad \frac{\gamma-\sigma_w^2}{\beta} \leq P_{\min} \\ \frac{\left(\frac{\gamma-\sigma_w^2}{\beta}\right) - P_{\min}}{P_{\max}-P_{\min}}, & \text{if} \quad P_{\min} < \frac{\gamma-\sigma_w^2}{\beta} \leq P_{\max} \\ 1, & \text{if} \quad \frac{\gamma-\sigma_w^2}{\beta} > P_{\max}. \end{cases} \quad (14)$$

Willie has to choose his threshold, γ, such that $\mathbb{P}_{FA} + \mathbb{P}_{MD}$ is minimized. Using (13) and (14), the crucial values on the γ axis are $\alpha P_{\min} + \sigma_w^2$, $\alpha P_{\max} + \sigma_w^2$, $\beta P_{\min} + \sigma_w^2$ and $\beta P_{\max} + \sigma_w^2$. From (13) and (14), it can also be seen that choosing $\gamma \leq \alpha P_{\min} + \sigma_w^2$ or $\gamma > \beta P_{\max} + \sigma_w^2$ results in $\mathbb{P}_{FA} + \mathbb{P}_{MD} = 1$. Thus the best choice of γ for Willie lies in the interval $\alpha P_{\min} + \sigma_w^2 < \gamma \leq \beta P_{\max} + \sigma_w^2$. From the system model, we know that $\beta > \alpha$ and $P_{\max} > P_{\min}$, resulting in $\beta P_{\max} + \sigma_w^2 > \alpha P_{\min} + \sigma_w^2$, but the relation between $\alpha P_{\max} + \sigma_w^2$ and $\beta P_{\min} + \sigma_w^2$ can not be determined. To resolve this discrepancy in order to determine the best choice of γ for Willie, we consider these two options in further detail.

Case - I : $\alpha P_{max} < \beta P_{min}$

We have three different intervals for the choice of γ here, which are considered in the following:

(1) $\alpha P_{min} + \sigma_w^2 \leq \gamma \leq \alpha P_{max} + \sigma_w^2$*:* In this case,

$$\mathbb{P}_{FA} + \mathbb{P}_{MD} = \frac{\alpha P_{\max} - \gamma + \sigma_w^2}{\alpha(P_{\max} - P_{\min})}, \quad (15)$$

and $\frac{\partial(\mathbb{P}_{FA}+\mathbb{P}_{MD})}{\partial\gamma} = \frac{-1}{\alpha(P_{\max}-P_{\min})} < 0$, dictating that $\gamma > \alpha P_{\max} + \sigma_w^2$ should be chosen.

(2) $\beta P_{min} + \sigma_w^2 \leq \gamma \leq \beta P_{max} + \sigma_w^2$*:* In this case,

$$\mathbb{P}_{FA} + \mathbb{P}_{MD} = \frac{\gamma - \sigma_w^2 - \beta P_{\min}}{\beta(P_{\max} - P_{\min})}, \quad (16)$$

and $\frac{\partial(\mathbb{P}_{FA}+\mathbb{P}_{MD})}{\partial\gamma} = \frac{1}{\beta(P_{\max}-P_{\min})} > 0$, and resultantly, $\gamma < \beta P_{\min} + \sigma_w^2$ should be chosen.

(3) $\alpha P_{max} + \sigma_w^2 < \gamma < \beta P_{min} + \sigma_w^2$*:* In this case, $\mathbb{P}_{FA} + \mathbb{P}_{MD} = 0$, which means that a choice of γ in this interval will have no detection errors at Willie.

Case - II : $\alpha P_{max} \geq \beta P_{min}$

Again, we have three different intervals for the choice of γ, as considered in the following:

(1) $\alpha P_{min} + \sigma_w^2 \leq \gamma \leq \beta P_{min} + \sigma_w^2$*:* In this case,

$$\mathbb{P}_{FA} + \mathbb{P}_{MD} = \frac{\alpha P_{\max} - \gamma + \sigma_w^2}{\alpha(P_{\max} - P_{\min})}, \quad (17)$$

and $\frac{\partial(\mathbb{P}_{FA}+\mathbb{P}_{MD})}{\partial\gamma} = \frac{-1}{\alpha(P_{\max}-P_{\min})} < 0$, which dictates that $\gamma > \beta P_{\min} + \sigma_w^2$ should be chosen.

(2) $\beta P_{min} + \sigma_w^2 < \gamma \leq \alpha P_{max} + \sigma_w^2$*:* In this case,

$$\mathbb{P}_{FA} + \mathbb{P}_{MD} = \frac{\alpha P_{\max} - \gamma + \sigma_w^2}{\alpha(P_{\max} - P_{\min})} + \frac{\gamma - \sigma_w^2 - \beta P_{\min}}{\beta(P_{\max} - P_{\min})}, \quad (18)$$

and $\frac{\partial(\mathbb{P}_{FA}+\mathbb{P}_{MD})}{\partial\gamma} = \frac{-1}{\alpha(P_{\max}-P_{\min})} + \frac{1}{\beta(P_{\max}-P_{\min})} < 0$, and resultantly, $\gamma \geq \alpha P_{\max} + \sigma_w^2$ should be chosen.

(3) $\alpha P_{max} + \sigma_w^2 < \gamma < \beta P_{max} + \sigma_w^2$*:* In this case,

$$\mathbb{P}_{FA} + \mathbb{P}_{MD} = \frac{\gamma - \sigma_w^2 - \beta P_{\min}}{\beta(P_{\max} - P_{\min})}, \quad (19)$$

and $\frac{\partial(\mathbb{P}_{FA}+\mathbb{P}_{MD})}{\partial\gamma} = \frac{1}{\beta(P_{\max}-P_{\min})} > 0$, which dictates that $\gamma \leq \alpha P_{\max} + \sigma_w^2$ should be chosen.

Since α and β are fixed quantities determined by the system parameters and fully known by Willie, the results of Case-I and Case-II complete the proof. ■

IV. Reader's Strategy for Covertness

Under the considered scheme, the reader looks to manipulate its transmit power for achieving covertness. We first establish a condition on the parameters of reader's transmit power distribution such that there are detection errors at Willie. Next we consider the condition on the reader's transmit power to achieve a target covertness level determined by ϵ.

Lemma 1. *To cause any detection errors at Willie, the reader has to choose the support of its transmit power i.e.,* P_{min} *and* P_{max}*, such that*

$$\frac{P_{max}}{P_{min}} \geq \frac{\beta}{\alpha}, \quad (20)$$

where α *and* β *are as defined in (7) and (9), respectively.*

Proof. The proof builds on the proof of Proposition 1, where the condition under which Willie makes detection errors is derived in Case-II. ■

After having derived the condition under which Willie is forced to make detection errors, we now present the condition for achieving a target level of covertness.

Proposition 2. *To achieve a covertness level of* ϵ*, the reader should choose the support of its transmit power i.e.,* P_{min} *and* P_{max}*, such that*

$$\frac{P_{max}}{P_{min}} \geq \frac{\epsilon\beta}{\epsilon\beta - (\beta - \alpha)}, \quad (21)$$

where α *and* β *are as defined in (7) and (9), respectively.*

Proof. Building on Proposition 1 and Lemma 1, Willie's optimal choice of threshold, γ, under the condition $\alpha P_{\max} \geq$

$\beta P_{\min}$, is to choose $\gamma = \alpha P_{\max} + \sigma_w^2$. For this value of threshold, $\mathbb{P}_{FA} = 0$, and we have

$$\mathbb{P}_{FA} + \mathbb{P}_{MD} = \mathbb{P}_{MD} = \frac{\alpha P_{\max} - \beta P_{\min}}{\beta(P_{\max} - P_{\min})}. \tag{22}$$

To achieve a target covertness of ϵ, we require

$$\mathbb{P}_{FA} + \mathbb{P}_{MD} = \frac{\alpha P_{\max} - \beta P_{\min}}{\beta(P_{\max} - P_{\min})} \geq 1 - \epsilon, \tag{23}$$

and a simple rearrangement gives the desired result. ■

Remark 1. *We note that condition (21) in Proposition 2 holds as long as $\epsilon > 1 - \frac{\alpha}{\beta}$, thus the achievable value of ϵ depends on the ratio $\frac{\alpha}{\beta}$. This condition manifests in such a way that for given system parameters, covertness beyond a certain ϵ in not achievable, regardless of the choice of $\frac{P_{max}}{P_{min}}$.*

V. Reader's BER Analysis

The reader can easily tell whether the tag has transmitted BPSK-modulated signal by looking at its received power because it completely knows its transmit power in any slot. The reader's receiver looks to decide about the tag's message symbol x being $+1$ or -1 from the received signal. The baseband signal received at the reader after being reflected from the tag is

$$y_r(i, H_1) = A_r(i) + S_r(i) + n_r(i), \tag{24}$$

where $S_r(i) = h_{rt}h_{tr}c(i)$ and $A_r(i) = h_{rt}h_{tr}|\Gamma|c(i)x(i)$ represent the structural and antenna mode reflections from the tag at the reader, respectively. Having complete knowledge of $c(i)$, h_{rt} and h_{tr}, the reader can perfectly cancel out the structural mode component from the received signal. Resultantly

$$\begin{aligned} \overline{y}_r(i, H_1) &= A_r(i) + n_r(i) \\ &= h_{rt}h_{tr}|\Gamma|c(i)x(i) + n_r(i), \end{aligned} \tag{25}$$

as the received signal. Rewriting (25), we get

$$\overline{\overline{y}}_r(i, H_1) = x(i) + \frac{n_r(i)}{h_{rt}h_{tr}|\Gamma|c(i)}, \tag{26}$$

where we recall that $n_r \sim \mathcal{N}(0, \sigma_r^2)$ and $c \sim \mathcal{N}(0, P_R)$. The second term in (26) results in a Cauchy distribution with a location parameter of $l_0 = 0$ [24]. Thus the maximum likelihood decision rule at the reader's receiver is

$$\begin{cases} \hat{x}(i) = +1, & \text{if} \quad \overline{\overline{y}}_r(i, H_1) > 0 \\ \hat{x}(i) = -1, & \text{else.} \end{cases} \tag{27}$$

Using the probability density function (pdf) of a Cauchy random variable, the BER for the reader, p_r^b, can be obtained as

$$p_r^b = \int_{-\infty}^{\infty} \left[\frac{1}{2} - \frac{1}{\pi} \arctan\left(\frac{1}{\sqrt{\frac{\sigma_r^2 d_{rt}^4}{|\Gamma|^2 G_{rt} G_{tr} K^4 z}}} \right) \right] f_{P_R}(z) \mathrm{d}z, \tag{28}$$

where the argument of $\arctan(\cdot)$ is the square-root reciprocal of the received signal-to-noise ratio (SNR) at the reader, and $f_{P_R}(\cdot)$ denotes the probability density function of $P_R \sim \mathcal{U}(P_{\min}, P_{\max})$.

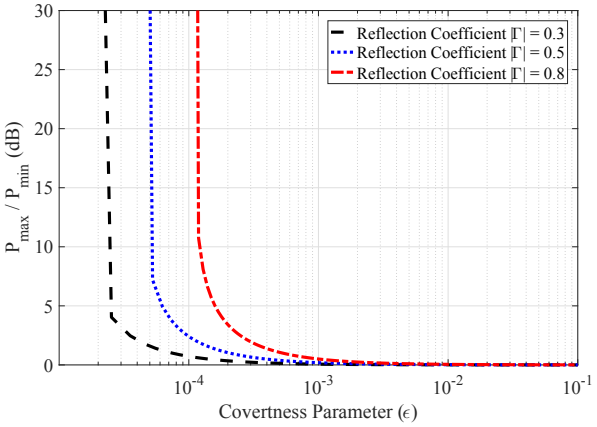

Fig. 2. Ratio of $P_{\max}$ and $P_{\min}$ required for a target covertness.

VI. Numerical Results and Discussion

In this section, we present numerical results to study the performance of our proposed covert communication scheme. A UHF system with a carrier frequency of 915 MHz is considered. The reader-tag, tag-Willie and reader-Willie distances are assumed to be 2 m, and all the users are assumed to have isotropic antennas. The noise variance at Willie and reader's receiver is -100dBm [15].

Fig. 2 shows the ratio of the support parameters of the reader's transmit power, $\frac{P_{\max}}{P_{\min}}$, plotted in dB against the covertness requirement, ϵ, for different values of the reflection coefficient, $|\Gamma|$. For a given value of the reflection coefficient, the required power ratio increases as the covertness requirement increases. Thus for a given $|\Gamma|$, the reader needs to have higher variations in its transmit power to achieve a better covert performance. However, as discussed in Remark 1, for a given combination of the reflection coefficient and system parameters (antenna gains, distances, carrier frequency), the achievable covertness does not increase beyond a certain value. Reducing the reflection coefficient $|\Gamma|$ helps to achieve a lower ϵ, hence better covertness. However, lowering $|\Gamma|$ reduces the received SNR at the receiver, hence degrading the BER performance of backscatter communication. We note here that the achievable covert performance depends on $P_{\min}$ and $P_{\max}$ only through the ratio $\frac{P_{\max}}{P_{\min}}$, not their individual values.

Fig. 3 plots the BER of a conventional non-covert communication, where the reader transmits a constant-amplitude CW signal, and the BER of the proposed covert communication with variable power at the reader. For the covert communication, we consider two covert requirements of $\epsilon = 0.1$ and $\epsilon = 1.1 \times 10^{-4}$. The tag's reflection coefficient is $|\Gamma| = 0.8$. Note that $\epsilon = 0.1$ represents a poor covert performance while $\epsilon = 1.1 \times 10^{-4}$ represents almost the best possible covert performance that can be achieved (see the curve for $|\Gamma| = 0.8$ in Fig. 2). The BER is plotted against the received SNR at the reader. For the covert communication with variable power, the distribution of transmit power (i.e., the values of $P_{\max}$ and $P_{\min}$) is set such that the average received SNR is the

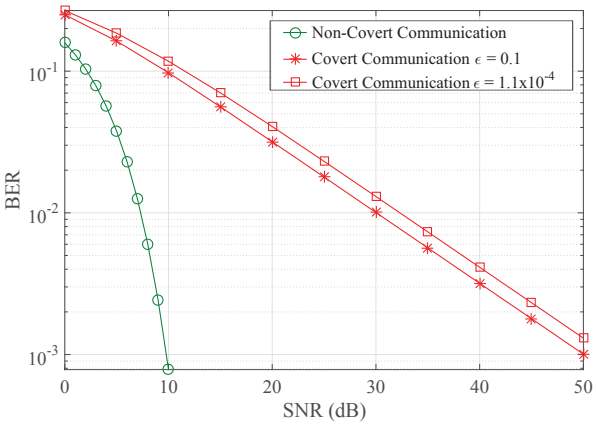

Fig. 3. BER Comparison of non-covert and covert communication schemes. The tag's reflection coefficient $|\Gamma| = 0.8$.

same as the received SNR in the non-covert communication. Firstly, we observe a huge BER difference between the non-covert and covert communication schemes. This is due to the difference between constant-amplitude signaling and the proposed signaling scheme. As explained in Sec II-A, the variation in reader's transmit power is necessary to create confusion at Willie, regardless of tag's transmission state, as an essential design to achieve covertness in the proposed scheme. Unfortunately, such a design pays a significant price in terms of BER. Next, focusing on the covert communication, we see that the BER gap between a poorly covert system (i.e., $\epsilon = 0.1$) and a strongly covert system (i.e., $\epsilon = 1.1 \times 10^{-4}$) is small, roughly $1.5 - 2.5$ dB. This tells us that the price to pay for improving the covert performance from a poorly covert system is reasonably small.

VII. Conclusion

In this work, we showed how a backscatter communication system can achieve covertness in the presence of a warden Willie. The proposed scheme requires the reader to use a noise-like signal with variable transmit power drawn from a uniform distribution. By controlling the maximum and minimum transmit powers of the reader, the system is able to achieve a target level of covertness. Comparing with a conventional backscatter system with no covertness, the BER degradation from no covertness to some (poor) covertness is huge. Nevertheless, the additional BER degradation for improving covert performance is much smaller. This paper presented the first study on covert communication in backscatter systems. It is expected that future work will devise improved transmission schemes resulting in better tradeoff performance between BER and covertness.

References

[1] C. Boyer and S. Roy, "Backscatter communication and RFID: Coding, energy, and MIMO analysis," *IEEE Trans. Commun.*, vol. 62, no. 3, pp. 770–785, Mar. 2014.

[2] J. Kimionis, A. Bletsas, and J. N. Sahalos, "Increased range bistatic scatter radio," *IEEE Trans. Commun.*, vol. 62, no. 3, pp. 1091–1104, Mar. 2014.

[3] H. Hassanieh, J. Wang, D. Katabi, and T. Kohno, "Securing RFIDs by randomizing the modulation and channel," in *USENIX NSDI Symposium*, May. 2015, pp. 235–249.

[4] X. Zhou, L. Song, and Y. Zhang, *Physical Layer Security in Wireless Communications*. CRC Press, 2013.

[5] B. A. Bash, D. Goeckel, D. Towsley, and S. Guha, "Hiding information in noise: Fundamental limits of covert wireless communication," *IEEE Commun. Mag*, vol. 53, no. 12, pp. 26–31, Dec. 2015.

[6] 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.

[7] K. Shahzad, X. Zhou, and S. Yan, "Covert communication in fading channels under channel uncertainty," in *IEEE VTC Spring*, Jun. 2017, pp. 1–5.

[8] B. He, S. Yan, X. Zhou, and V. K. N. Lau, "On covert communication with noise uncertainty," *IEEE Commun. Lett.*, vol. 21, no. 4, pp. 941–944, Apr. 2017.

[9] D. Goeckel, B. A. Bash, S. Guha, and D. Towsley, "Covert communications when the warden does not know the background noise power," *IEEE Commun. Lett.*, vol. 20, no. 2, pp. 236–239, Feb. 2016.

[10] S. Lee, R. Baxley, M. Weitnauer, and B. Walkenhorst, "Achieving undetectable communication," *IEEE J. Sel. Topics Signal Process.*, vol. 9, no. 7, pp. 1195–1205, Oct. 2015.

[11] T. V. Sobers, B. A. Bash, S. Guha, D. Towsley, and D. Goeckel, "Covert communication in the presence of an uninformed jammer," *IEEE Trans. Wireless Commun.*, vol. 16, no. 19, pp. 6193–6206, Sep. 2017.

[12] R. Soltani, D. Goeckel, D. Towsley, B. A. Bash, and S. Guha, "Covert wireless communication with artificial noise generation," *IEEE Trans. Wireless Commun.*, vol. 17, no. 11, pp. 7252–7267, Nov. 2018.

[13] K. Shahzad, X. Zhou, S. Yan, J. Hu, F. Shu, and J. Li, "Achieving covert wireless communications using a full-duplex receiver," *IEEE Trans. Wireless Commun.*, vol. 17, no. 12, pp. 8517–8530, Dec. 2018.

[14] Q. Yang, H. M. Wang, Y. Zhang, and Z. Han, "Physical layer security in MIMO backscatter wireless systems," *IEEE Trans. Wireless Commun.*, vol. 15, no. 11, pp. 7547–7560, Nov. 2016.

[15] W. Saad, X. Zhou, Z. Han, and H. V. Poor, "On the physical layer security of backscatter wireless systems," *IEEE Trans. Wireless Commun.*, vol. 13, no. 6, pp. 3442–3451, Jun. 2014.

[16] X. Wang, Z. Su, and G. Wang, "Relay selection for secure backscatter wireless communications," *Electronics Letters*, vol. 51, no. 12, pp. 951–952, Jun. 2015.

[17] F. Huo, P. Mitran, and G. Gong, "Analysis and validation of active eavesdropping attacks in passive FHSS RFID systems," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 7, pp. 1528–1541, Mar. 2016.

[18] H. M. Wang, T. Zheng, and X. G. Xia, "Secure MISO wiretap channels with multiantenna passive eavesdropper: Artificial noise vs. artificial fast fading," *IEEE Trans. Wireless Commun.*, vol. 14, no. 1, pp. 94–106, Jun. 2014.

[19] B. C. Levy, *Principles of Signal Detection and Parameter Estimation*. New York: Springer, 2010.

[20] P. V. Nikitin and K. V. S. Rao, "Theory and measurement of backscattering from RFID tags," *IEEE Antennas Propag. Mag.*, vol. 48, no. 6, pp. 212–218, Dec. 2006.

[21] F. Fuschini, C. Piersanti, F. Paolazzi, and G. Falciasecca, "Analytical approach to the backscattering from UHF RFID transponder," *IEEE Antennas Wireless Propag. Lett.*, vol. 7, pp. 33–35, Feb. 2008.

[22] D. M. Dobkin, *The RF in RFID: Passive UHF RFID in Practice*. Newnes, 2007.

[23] J. D. Griffin and G. D. Durgin, "Complete link budgets for backscatter-radio and RFID systems," *IEEE Antennas Propag. Mag.*, vol. 51, no. 2, pp. 11–25, Apr. 2009.

[24] K. Krishnamoorthy, *Handbook of Statistical Distributions with Applications*. CRC Press, 2016.