Defeating Smart and Reactive Jammers with Unlimited Power

Nguyen Van Huynh[1], Dinh Thai Hoang[1], Diep N. Nguyen[1], Eryk Dutkiewicz[1], and Markus Mueck[2]
[1] School of Electrical and Data Engineering, University of Technology Sydney, Australia
[2] Intel Corporation

Abstract—**Among all wireless jammers, dealing with reactive ones is most challenging. This kind of jammer attacks the channel whenever it detects transmission from legitimate radios. With recent advances in self-interference suppression or in-band full-duplex radios, a reactive jammer can jam and simultaneously sense/discern/detect the legitimate transmission. Such a jammer is referred to as a smart reactive jammer. However, all existing solutions, e.g., frequency hopping and rate adaptation, cannot effectively deal with this type of jammer. This is because a smart reactive jammer with sufficient power budget can theoretically jam most, if not all, frequency channels at sufficiently high power. This work proposes to augment the transmitter with an ambient backscatter tag. Specifically, when the jammer attacks the channel, the transmitter deceives it by continuing to transmit data to attract the jammer while the tag backscatters data based on both the jamming signals and active signals from the jammer and transmitter, respectively. However, backscattering signals from multiple radio sources results in a high bit error rate (BER). Thus, we propose to use multiple antennas at the receiver. The theoretical analysis and simulation results show that by using multiple antennas at the receiver, the BER and hence the throughput of the system can be significantly improved. More importantly, we demonstrate that with our proposed solutions, the average throughput increases and the BER decreases when the jammer attacks with higher power levels. We believe this is the first anti-jamming solution that can cope effectively with a high- or even unlimited-power jammers.**

Index Terms—**Anti-jamming, unlimited power jammer, ambient backscatter, signal detection, smart and reactive jammer.**

I. Introduction

Due to the open medium of wireless links, radios are extremely vulnerable to adversaries (e.g., jamming, eavesdropping). In particular, by injecting high-power interference signals into wireless channels, a jammer can decrease the signal-to-interference-plus-noise ratio (SINR) at the receiver, and thus interrupting or even preventing the legitimate communications of wireless systems. Additionally, such an attack can be easily launched by using commercial off-the-shelf components.

There is a rich literature in anti-jamming. The most common type of jammers is the proactive jammer which attacks the wireless channel with a given strategy that is often optimized w.r.t. the victim devices' communications pattern. To deal with this kind of jamming attack, the simplest solution is regulating the transmit power of wireless devices [1]. Specifically, a transmitter can either transmit at very low power (e.g., using ultra wideband methods so that the jammer cannot detect its transmission) or at very high levels to dominate jamming signals. However, this method is inefficient especially when the jammer often attacks the channel with high power. Another approaches widely adopted in the literature are the frequency-hopping (FH) and the rate adaptation (RA) technology [2]-[5]. In particular, the FH mechanism allows a wireless device to quickly switch its operating frequency to other channels while being attacked. On the other hand, in the RA technique, the transmitter can adapt its data rate to leave margin for interference from jammers (i.e., low rates are used when being jammed). In [5], the authors combined the RA and FH techniques to mitigate attacks from a reactive-sweep jammer that can jam/sweep a given set of channels at a time. The authors modeled the arm-race between the jammers and the node as a zero-sum Markov game and obtained the optimal policies for the transmitters by solving a constrained Nash equilibrium problem. Similarly, in [7], the authors proposed a stochastic game framework to study the strategic interaction between jammers and legitimate users. The principle behind all the above methods is the assumption that the jammer is limited or constrained in power. For that, they are ineffective to combat powerful jammers that can jam a large frequency band (e.g., most channels in FH) with significant power to thwart the transmission even the lowest rate (e.g., in RA [4]).

Given the above, in this paper, we consider a wireless system with the presence of a smart and reactive jammer with high or even hypothetically unlimited power budget. Specifically, using the latest advances in self-interference suppression (SiS) [6], the reactive jammer can discern the victims' activities (even while jamming) and then adapts its attack strategy to maximize the disruption. To address the disadvantages of existing solutions, the authors in [8] adopted the RF energy harvesting technology to allow the transmitter to harvest energy from the strong jamming signals while being attacked. By using the ambient backscatter communication technology [9], [10], the authors in [11] proposed to backscatter/modulate information on the jamming signals so that the nodes can communicate even under jamming attacks. However, with a smart and reactive jammer which stops attacking the channel once no active transmission from the transmitter is detected, these solutions are not applicable. One may argue that when the jamming ceases, nodes can switch back to active transmission (instead of backscattering). However, with the SiS capability and sufficiently high power budget, the jammer can quickly start jamming (as soon as active transmission is detected) to damage the very first bits.

To the best of our knowledge, all current anti-jamming approaches cannot efficiently deal with this kind of jamming attack. To solve this problem, similar to [11] we augment the conventional transmitter with a backscatter tag [9], [10]. Then, when the jammer attacks the channel, the transmitter keeps transmitting to attract the jammer while the tag backscatters the information to the receiver through the strong jamming signals as well as the transmitter's signals. However, backscattering signals from multiple radio sources (e.g., the jammer and the legitimate transmitters) results in a higher bit error rate (BER), compared with the case of a single source. To deal with this problem, we propose to use multiple antennas at the receiver. Through theoretical analysis and simulation results, we prove that our proposed solution can significantly improve the system performance under jamming attacks. In particular, we show that the maximum achievable backscattered rate increases, and the BER decreases when the jammer attacks the channels with higher power levels.

Notation: The lowercase, boldface lowercase, and boldface uppercase letters g, $\mathbf{g}$, $\mathbf{G}$ denote a scalar variable, vector, and matrix, respectively. $\mathbb{E}[.]$ denotes the statistical expectation. $\mathcal{CN}(\mu, \xi^2)$ denotes the circularly symmetric complex Gaussian (CSCG) distribution with mean μ and variance ξ^2. $|\mathbf{G}|$, $\mathbf{G}^T$ and $\mathbf{G}^H$ denote the determinant, transpose and conjugate transpose of matrix $\mathbf{G}$, respectively. $\mathbf{I}_M$ denotes the $M \times M$ identical matrix. $I(X;Y)$ denotes the mutual information of random variables X and Y.

II. System Model

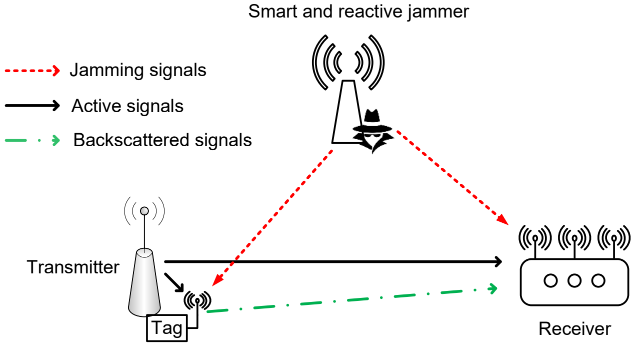

Fig. 1: System model.

In this paper, we consider scenarios in which the transmitter transmits information to the receiver in the presence of a smart and reactive jammer with hypothetically unlimited power budget. With the SiS capability [6], the jammer can observe active transmissions from the transmitter to adapt its attack strategy. Specifically, once the transmitter actively transmits data, the jammer immediately attacks the channel with its highest power level. The attack is ceased when there is no active transmission. To cope with this kind of attack, we deploy a low-cost tag with ambient backscatter capability connected to the transmitter as shown in Fig. 1. Specifically, when the jammer attacks the channel, the transmitter will continue its active transmissions[1] to lure the jammer. At the same time, the tag is activated to backscatter data to the receiver by backscattering the RF signals from the jammer and the transmitter. In other words, the tag considers the transmitter and the jammer as two RF sources to support its backscattering transmissions. Note that the transmitter can easily detect the jamming attacks by measuring packet delivery ratio (PDR), packet send ratio (PSR), bad packet ratio (BPR) or signal to noise ratio (SNR) [1].

If the tag chooses to backscatter to transmit data to the receiver, it will modulate and reflect the ambient RF signals or the jamming signals by using the load modulator [10]. Specifically, the controller modulates the information as a stream of zero and one bits. This stream is the input of the load modulator which is directly connected to the antenna. The main component of the load modulator is an RF switch such as ADG902 [9] with two loads Z_1 and Z_2. When the input bit is one, the load modulator switches to load Z_2, and thus the tag is at the reflecting state. Otherwise, the load modulator turns to load Z_1, and thus the tag is at the absorbing state. In this way, the tag can backscatter information to the receiver. It is worth noting that although we consider a single tag in this paper, the proposed model and analysis can be extended to the case with multiple tags. In this case, tags can backscatter information at different rates [9], [10]. As such, by distinguishing the difference in communication rates, the receiver can successfully decode the information sent from tags.

III. Channel Model

As mentioned in [9], [10], the tag should backscatter information at a lower rate than the RF source signals to make sure that the receiver can properly decode the backscattered signals. Thus, in this paper, we assume that each backscatter symbol period spans over N RF source symbol periods. The receiver is equipped with M antennas ($M \geq 1$). The received signals at the m-th antenna of the receiver consist of three components: (i) the direct link signals $d^{\mathrm{t}}_{m,n}$ directly transmitted from the transmitter to the receiver, (ii) the direct link signals $d^{\mathrm{a}}_{m,n}$ directly sent from the jammer to the receiver, and (iii) the backscattered signals $b_{m,n}$ backscattered from the tag to the receiver, $n = 1, \dots, N$. The received signals at the m-th antenna of the receiver can be expressed as follows [10]:

$$y_{m,n} = \underbrace{d^{\mathrm{t}}_{m,n} + d^{\mathrm{a}}_{m,n}}_{\text{direct links}} + \underbrace{b_{m,n}}_{\text{backscatter links}} + \sigma_{m,n}, \qquad (1)$$

where $\sigma_{m,n} \sim \mathcal{CN}(0,1)$ is the additive white Gaussian noise (AWGN) [13].

A. Direct Links

We first denote $s_{r,n}$ and $s_{a,n}$ as the RF signals from the transmitter and the jammer at time n, respectively. Similar to several studies in the literature [12], we assume that $s_{r,n}$ are independent and identically distributed (i.i.d) at every time instant n. Similarly, $s_{a,n}$ is also i.d.d w.r.t n. As the RF signals are unknown at the receiver and are usually random, we assume that $s_{r,n}$ and $s_{a,n}$ follow the standard CSCG distribution with zero mean and unit variance [13]. The direct link signals from the transmitter received at the m-th antenna of the receiver at time instant n then can be expressed as follows:

$$d^{\mathrm{t}}_{m,n} = f_{r,m}\sqrt{P_{t,r}}s_{r,n}, \qquad (2)$$

[1] Note that the transmitter does not need to transmit the real data, it can transmit random signals to just lure the jammer to keep the jamming signals on.

where $P_{t,r}$ is the average received power from the transmitter-receiver direct link and $f_{r,m}$ is the small-scale fading from the transmitter to the receiver with $\mathbb{E}[|f_{r,m}|^2] = 1$. The average received power $P_{t,r}$ is calculated as follows:

$$P_{t,r} = \frac{P_t G_t G_r \lambda^2}{(4\pi)^2 {L_r}^{\upsilon}}, \tag{3}$$

where λ is the wavelength, P_t is the transmit power of the transmitter, G_t and G_r are the antenna gains of the transmitter and the receiver, respectively. L_r is the distance between the transmitter and the receiver and υ is the path loss exponent. Denote $\kappa = \left(\frac{\lambda}{4\pi}\right)^2$, we have

$$P_{t,r} = \frac{\kappa P_t G_t G_r}{{L_r}^{\upsilon}}. \tag{4}$$

Similarly, the direct link signals from the jammer received at the receiver are expressed as follows:

$$d^{\mathrm{a}}_{m,n} = f_{a,m}\sqrt{P_{t,a}}s_{a,n}, \tag{5}$$

where $f_{a,m}$ is the small-scale fading from the jammer to the receiver with $\mathbb{E}[|f_{a,m}|^2] = 1$ and $P_{t,a}$ is the average received power from the jammer-receiver direct link which is expressed as follows:

$$P_{t,a} = \frac{\kappa P_a G_a G_r}{{L_a}^{\upsilon}}, \tag{6}$$

where P_a is the transmit power of the jammer, G_a is the antenna gain of the jammer, and L_a is the distance between the jammer and the receiver.

B. Backscatter Link

As mentioned, the tag backscatters the jamming signals and the active signals sent from the transmitter to transmit information to the receiver. In the following, we present the fundamental of the backscattering process. Specifically, the average power from the transmitter received at the tag before backscattering can be expressed as follows:

$$P_{b,r} = \frac{\kappa P_t G_t G_b}{{L_b}^{\upsilon}}, \tag{7}$$

where L_b is the distance between the transmitter and the tag, and G_b is the antenna gain of the tag. Then, the RF signals sent from the transmitter received at the tag are as follows:

$$z_{r,n} = l_r\sqrt{P_{b,r}}s_{r,n}, \tag{8}$$

where l_r is the small-scale fading from the transmitter to the tag with $\mathbb{E}[|l_r|^2] = 1$. Similarly, we can derive the RF signals sent from the jammer received at the tag as follows:

$$z_{a,n} = l_a\sqrt{P_{b,a}}s_{a,n}, \tag{9}$$

where l_a is the small-scale fading from the jammer to the tag with $\mathbb{E}[|l_a|^2] = 1$, and $P_{b,a}$ is the average power from the jammer received at the tag. $P_{b,a}$ is expressed as follows:

$$P_{b,a} = \frac{\kappa P_a G_a G_b}{{L_s}^{\upsilon}}, \tag{10}$$

where L_s is the distance between the jammer and the tag. The total RF signals received at the tag are expressed as follows:

$$z_n = z_{r,n} + z_{a,n} = l_r\sqrt{P_{b,r}}s_{r,n} + l_a\sqrt{P_{b,a}}s_{a,n}. \tag{11}$$

In this paper, we adopt the *on-off keying (OOK)* modulation technique as in several studies in the literature [9]. In particular, the tag has two backscatter states: (i) non-reflecting state denoted by $c = 0$ and (ii) reflecting state denoted by $c = 1$. To allow the receiver to be able to decode the backscattered signals, the backscattered rate of the tag must be lower than the data rate of the ambient RF signals (from the transmitter and the jammer). Thus, the backscattering state c remains unchanged for N consecutive source symbols. During one backscatter symbol period, the backscattered signals of the tag can be expressed as follows:

$$s_{b,n} = \gamma z_n c, \tag{12}$$

where γ is the reflection coefficient and $0 < |\gamma|^2 < 1$. Then, the backscatter link signals received at the m-th antenna of the receiver can be expressed as follows:

$$b_{m,n} = f_{b,m}\sqrt{\frac{G_b G_r \kappa}{{L_e}^{\upsilon}}}s_{b,n}, \tag{13}$$

where $f_{b,m}$ is the small-scale fading from the tag to the receiver with $\mathbb{E}[|f_{b,m}|^2] = 1$, L_e is the distance between the tag and the receiver. Note that (13) does not have the transmit power of the tag as the tag only reflects the RF signals from the jammer and the transmitter to backscatter data to the receiver. Substituting (11) and (12) into (13), we have

$$\begin{aligned} b_{m,n} &= f_{b,m}\sqrt{\frac{G_b G_r \kappa}{{L_e}^{\upsilon}}}\gamma c\Big(l_r\sqrt{P_{b,r}}s_{r,n} + l_a\sqrt{P_{b,a}}s_{a,n}\Big) \\ &= f_{b,m}\gamma c\Big(l_r\sqrt{\frac{\kappa P_{t,r}{G_b}^2{L_r}^{\upsilon}}{{L_b}^{\upsilon}{L_e}^{\upsilon}}}s_{r,n} + l_a\sqrt{\frac{\kappa P_{t,a}{G_b}^2{L_a}^{\upsilon}}{{L_s}^{\upsilon}{L_e}^{\upsilon}}}s_{a,n}\Big). \end{aligned} \tag{14}$$

We then define $\tilde{\alpha}_r = \frac{\kappa|\gamma|^2{G_b}^2{L_r}^{\upsilon}}{{L_b}^{\upsilon}{L_e}^{\upsilon}}$ and $\tilde{\alpha}_a = \frac{\kappa|\gamma|^2{G_b}^2{L_a}^{\upsilon}}{{L_s}^{\upsilon}{L_e}^{\upsilon}}$. Thus, (14) is rewritten as follows:

$$b_{m,n} = f_{b,m}c\Big(l_r\sqrt{\tilde{\alpha}_r P_{t,r}}s_{r,n} + l_a\sqrt{\tilde{\alpha}_a P_{t,a}}s_{a,n}\Big). \tag{15}$$

C. Received Signals at the Receiver

Based on (2), (5), and (15), we rewrite (1) as follows:

$$\begin{aligned} y_{m,n} &= d^{\mathrm{t}}_{m,n} + d^{\mathrm{a}}_{m,n} + b_{m,n} + \sigma_{m,n} \\ &= f_{r,m}\sqrt{P_{t,r}}s_{r,n} + f_{a,m}\sqrt{P_{t,a}}s_{a,n} \\ &\quad + f_{b,m}c\Big(l_r\sqrt{\tilde{\alpha}_r P_{t,r}}s_{r,n} + l_a\sqrt{\tilde{\alpha}_a P_{t,a}}s_{a,n}\Big) + \sigma_{m,n}. \end{aligned} \tag{16}$$

We then denote $\alpha_{d,t} \triangleq P_{t,r}$ and $\alpha_{d,a} \triangleq P_{t,a}$ as the average SNR of the direct links from the transmitter and from the jammer to the receiver, respectively. We denote $\alpha_{b,t} \triangleq \tilde{\alpha}_r P_{t,r}$ and $\alpha_{b,a} \triangleq \tilde{\alpha}_a P_{t,a}$ as the average SNR of the backscatter links, i.e., transmitter-tag-receiver and jammer-tag-receiver links, respectively. Thus, we have

$$\begin{aligned} y_{m,n} = &\underbrace{f_{r,m}\sqrt{\alpha_{d,t}}s_{r,n} + f_{a,m}\sqrt{\alpha_{d,a}}s_{a,n}}_{\text{direct links}} \\ &+ \underbrace{f_{b,m}c\Big(l_r\sqrt{\alpha_{b,t}}s_{r,n} + l_a\sqrt{\alpha_{b,a}}s_{a,n}\Big)}_{\text{backscatter links}} + \sigma_{m,n}. \end{aligned} \tag{17}$$

Note that $\tilde{\alpha}_r$ and $\tilde{\alpha}_a$ are the relative SNRs which are the ratios of $\alpha_{b,t}$ and $\alpha_{b,a}$. As the receiver is equipped with M antennas, we denote the channel response vectors as follows:

$$\mathbf{f}_r = [f_{r,1}, \dots, f_{r,m}, \dots, f_{r,M}]^T, \tag{18}$$

$$\mathbf{f}_a = [f_{a,1}, \dots, f_{a,m}, \dots, f_{a,M}]^T, \tag{19}$$

$$\mathbf{f}_b = [f_{b,1}, \dots, f_{b,m}, \dots, f_{b,M}]^T. \tag{20}$$

Thus, the signals collected by M antennas at the receiver can be given as follows:

$$\begin{aligned} \mathbf{y}_n = & \underbrace{\mathbf{f}_r \sqrt{\alpha_{d,t}} s_{r,n} + \mathbf{f}_a \sqrt{\alpha_{d,a}} s_{a,n}}_{\text{direct links}} \\ & + \underbrace{\mathbf{f}_b c \Big(l_r \sqrt{\alpha_{b,t}} s_{r,n} + l_a \sqrt{\alpha_{b,a}} s_{a,n} \Big)}_{\text{backscatter links}} + \boldsymbol{\sigma}_n, \end{aligned} \tag{21}$$

where

$$\mathbf{y}_n = [y_{1,n}, \dots, y_{m,n}, \dots, y_{M,n}]^T, \tag{22}$$

$$\boldsymbol{\sigma}_n = [\sigma_{1,n}, \dots, \sigma_{m,n}, \dots, \sigma_{M,n}]^T. \tag{23}$$

In this work, we assume that each backscatter frame consists of T information bits $\mathbf{b} = [b^{(1)}, \dots, b^{(t)}, \dots, b^{(T)}]$ where $b^{(t)} \in \{0,1\}, \forall t = 1, 2, \dots, T$. These original bits are then encoded at the tag as follows:

$$c^{(t)} = c^{(t-1)} \oplus b^{(t)}, \tag{24}$$

where $\oplus$ is the modulo-2 operator [12] and $\mathbf{c} = [c^{(1)}, \dots, c^{(t)}, \dots, c^{(T)}]$ are the modulated symbols with the reference symbol $c^{(0)} = 1$. As mentioned, each backscatter symbol $c^{(t)}$ contains N RF source symbols. Thus, the n-th received sample in the t-th backscatter symbol period is expressed as follows:

$$\begin{aligned} \mathbf{y}_n^{(t)} = & \mathbf{f}_r \sqrt{\alpha_{d,t}} s_{r,n}^{(t)} + \mathbf{f}_a \sqrt{\alpha_{d,a}} s_{a,n}^{(t)} \\ & + \mathbf{f}_b c^{(t)} \Big(l_r \sqrt{\alpha_{b,t}} s_{r,n}^{(t)} + l_a \sqrt{\alpha_{b,a}} s_{a,n}^{(t)} \Big) + \boldsymbol{\sigma}_n^{(t)}, \end{aligned} \tag{25}$$

where $n = 1, 2, \dots, N$ and $t = 1, 2, \dots, T$. Denote $\mathbf{Y}^{(t)} = [\mathbf{y}_1^{(t)}, \dots, \mathbf{y}_n^{(t)}, \dots, \mathbf{y}_N^{(t)}]^T$ as the received signal sequence in the i-th symbol period. In the following, we present how the receiver can recover all the original bits from $\mathbf{Y}^{(t)}$.

IV. Decoding at the Receiver

A. *Recovering the Soft Message of* $\mathbf{c}$

To decode the information backscattered from the tag, the receiver first recovers the received signals at its antennas. In particular, during one symbol period, $c^{(t)}$ is equal to "0" if there is no backscattered signals, and $c^{(t)}$ is equal to "1" otherwise. In the following, we present the recovering process at the receiver. First, the channel statistical covariance matrices [15] are obtained as follows:

$$\begin{aligned} \mathbf{K}_1 &= (\mathbf{h}_1 + \mathbf{h}_2)(\mathbf{h}_1 + \mathbf{h}_2)^H + (\mathbf{h}_3 + \mathbf{h}_4)(\mathbf{h}_3 + \mathbf{h}_4)^H + \mathbf{I}_M, \\ \mathbf{K}_0 &= \mathbf{h}_1 \mathbf{h}_1^H + \mathbf{h}_3 \mathbf{h}_3^H + \mathbf{I}_M, \end{aligned} \tag{26}$$

where $\mathbf{h}_1 = \mathbf{f}_r \sqrt{\alpha_{d,t}}$, $\mathbf{h}_2 = l_r \mathbf{f}_b \sqrt{\alpha_{b,t}}$, $\mathbf{h}_3 = \mathbf{f}_a \sqrt{\alpha_{d,a}}$, $\mathbf{h}_4 = l_a \mathbf{f}_b \sqrt{\alpha_{b,a}}$. As both the RF signals from the jammer and the transmitter as well as the noise follow the CSCG distribution, $\mathbf{y}_n^{(t)}$ is a CSCG distributed vector. Then, the conditional probability density functions (PDFs) of $\mathbf{y}_n^{(t)}$ given $c^{(t)}$ are derived as follows [14]:

$$\begin{aligned} p(\mathbf{y}_n^{(t)} | c^{(t)} = 0) &= \frac{1}{\pi^M |\mathbf{K}_0|} e^{-\mathbf{y}_n^{(t)H} \mathbf{K}_0^{-1} \mathbf{y}_n^{(t)}}, \\ p(\mathbf{y}_n^{(t)} | c^{(t)} = 1) &= \frac{1}{\pi^M |\mathbf{K}_1|} e^{-\mathbf{y}_n^{(t)H} \mathbf{K}_1^{-1} \mathbf{y}_n^{(t)}}. \end{aligned} \tag{27}$$

Based on (27), we obtain the likelihood functions of the received signals sequence $\mathbf{Y}^{(t)} = [\mathbf{y}_1^{(t)}, \dots, \mathbf{y}_n^{(t)}, \dots, \mathbf{y}_N^{(t)}]^T$ given $c^{(t)}$, i.e., the soft message of $c^{(t)}$, as follows:

$$\begin{aligned} \mathcal{L}(\mathbf{Y}^{(t)} | c^{(t)} = 0) &= \prod_{n=1}^{N} \frac{1}{\pi^M |\mathbf{K}_0|} e^{-\mathbf{y}_n^{(t)H} \mathbf{K}_0^{-1} \mathbf{y}_n^{(t)}}, \\ \mathcal{L}(\mathbf{Y}^{(t)} | c^{(t)} = 1) &= \prod_{n=1}^{N} \frac{1}{\pi^M |\mathbf{K}_1|} e^{-\mathbf{y}_n^{(t)H} \mathbf{K}_1^{-1} \mathbf{y}_n^{(t)}}. \end{aligned} \tag{28}$$

B. *Maximum Likelihood Detector*

Based on the soft message of $c^{(t)}$, we can obtain the original symbol $b^{(t)}$ by using a conventional maximum likelihood (ML) detector. Specifically, the hard decision of $c^{(t)}$ is obtained based on the following ML criterion.

$$\hat{c}^{(t)} = \begin{cases} 0, & \mathcal{L}(\mathbf{Y}^{(t)} | c^{(t)} = 0) > \mathcal{L}(\mathbf{Y}^{(t)} | c^{(t)} = 1), \\ 1, & \mathcal{L}(\mathbf{Y}^{(t)} | c^{(t)} = 0) < \mathcal{L}(\mathbf{Y}^{(t)} | c^{(t)} = 1), \end{cases} \tag{29}$$

where $\hat{c}^{(t)}$ is the decision result of $c^{(t)}$. By substituting the likelihood functions in (28) and using the logarithm operation, (29) is expressed as follows:

$$\hat{c}^{(t)} = \begin{cases} 0, & \sum_{n=1}^{N} \mathbf{y}_n^{(t)H} (\mathbf{K}_0^{-1} - \mathbf{K}_1^{-1}) \mathbf{y}_n^{(t)} < N \ln \frac{|\mathbf{K}_1|}{|\mathbf{K}_0|}, \\ 1, & \sum_{n=1}^{N} \mathbf{y}_n^{(t)H} (\mathbf{K}_0^{-1} - \mathbf{K}_1^{-1}) \mathbf{y}_n^{(t)} > N \ln \frac{|\mathbf{K}_1|}{|\mathbf{K}_0|}. \end{cases} \tag{30}$$

Based on $\hat{c}^{(t)}$, we then can derive the original bit $b^{(t)}$.

C. *Maximum Achievable Backscattered Rate*

We denote R_b as the achievable backscattered rate of the tag by using the OOK modulation mechanism. Obviously, R_b is the mutual information between the OOK modulated c and the received signals at the receiver, i.e., $R_b = I(c; \mathbf{y})$. Nevertheless, it is impossible to obtain the close-form expression of R_b [9], [12]. Thus, in this section, we present a numerical method to derive the maximum achievable backscattered rate $R_b^{\dagger}$ which can be expressed as $R_b^{\dagger} = \mathbb{E}[I(c, \mathbf{y})]$. The mutual information $I(c, \mathbf{y})$ is expressed as follows [15]:

$$I(c, \mathbf{y}) = H(\theta_0) - \mathbb{E}_{\mathbf{y}_0}[H(c|\mathbf{y}_0)], \tag{31}$$

where $\mathbf{y}_0$ is a realization of $\mathbf{y}$, θ_0 is the prior probability when "$c = 0$" (the prior probability when "$c = 1$" is $\theta_1 = 1 - \theta_0$), $H(c|\mathbf{y}_0)$ is the conditional entropy of c given $\mathbf{y}_0$, and $H(\theta_0)$ is the binary entropy function denoted as follows [15]:

$$H(\theta_0) \triangleq -\theta_0 \log_2 \theta_0 - \theta_1 \log_2 \theta_1, \tag{32}$$

where $0 \log_2 0$ is taken to be 0. As $H(\theta_0)$ is independent of all the channel coefficients, the maximum achievable backscattered rate can be expressed as follows:

$$R_b^{\dagger} = \mathbb{E}[I(c, \mathbf{y})] = H(\theta_0) - \mathbb{E}_{\mathbf{y}_0}[H(c|\mathbf{y}_0)]. \tag{33}$$

We then define $p(c=j|\mathbf{y}_0)$ with $j \in \{0,1\}$ as the posterior probability of c when receiving $\mathbf{y}_0$ which is expressed in (34).

$$p(c=j|\mathbf{y}_0) = \frac{\theta_j p(\mathbf{y}|c=j)}{p(\mathbf{y}_0)}, \tag{34}$$

with $j \in \{0,1\}$ and $p(\mathbf{y}_0) = \theta_0 p(\mathbf{y}_0|c=0) + \theta_1 p(\mathbf{y}_0|c=1)$. We define $\omega_j = p(c=j|\mathbf{y}_0)$ with $j \in \{0,1\}$. Thus, we have the conditional entropy as follows:

$$H(c|\mathbf{y}_0) = -\sum_{j=0}^{1} \omega_j \log_2 \omega_j = H(\omega_0). \tag{35}$$

Finally, we obtain the average maximum achievable backscattered rate $R_b^\dagger$ as follows:

$$R_b^\dagger = H(\theta_0) - \mathbb{E}_{\mathbf{y}_0}[H(\omega_0)] = H(\theta_0) - \int_{\mathbf{y}_0} H(\omega_0) d\mathbf{y}_0. \tag{36}$$

V. Simulation Results

All the channels are assumed to experience independent Rayleigh fading. Unless otherwise stated, the SNRs of the direct links from the transmitter $\alpha_{d,t}$ and the jammer $\alpha_{d,a}$ are set at 20 dB and 30 dB, respectively. The relative SNRs of the backscatter links from the transmitter ($\tilde{\alpha}_r$) and the jammer ($\tilde{\alpha}_a$) are set at -25 dB. The number of bits per backscatter frame is 100. Each backscattered symbol spans over 50 RF source symbols. The number of antennas at the receiver is varied from 2 to 6 to observe the performance of the proposed solution. In particular, we first investigate the maximum achievable backscattered rate of the tag with the presence of the jammer based on the analysis in Section IV-C. Then, the BER performance of the proposed solution is analyzed under different settings.

A. Maximum Achievable Backscattered Rate

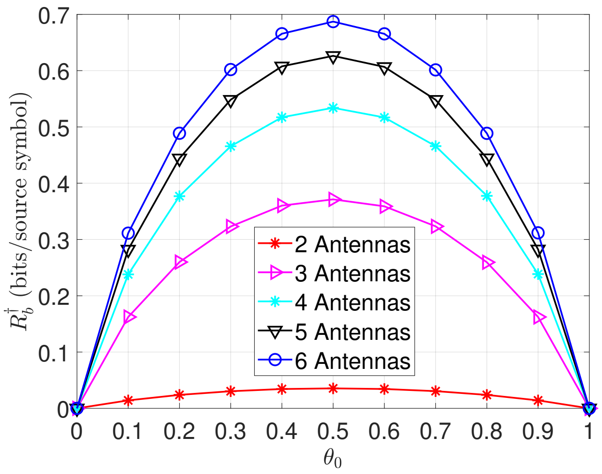

Fig. 2: Maximum average throughput vs. prior probability when the tag backscatters bit "0".

In Fig. 2, we illustrate the effects of the number of antennas at the receiver and the prior probability of transmitted bit "0" on the maximum achievable backscattered rate of the tag. In particular, we vary the prior probability that the tag backscatters bit "0" from 0 to 1 and observe the maximum achievable backscattered rate under different numbers of the receiver's antennas through 10^6 Monte Carlo runs. Clearly, as the number of antennas at the receiver increases, the tag can backscatter at higher rates. This is stemmed from the fact that with multiple antennas, the receiver can reduce the fading effects as well as the direct link interference, and thus enhancing the received signals in the presence of the jammer. This also implies that under the jamming attack with our proposed solution, one can employ multiple antennas at the receiver to improve the average throughput of the system. Moreover, with the prior probability of backscattering bit "0" equals 0.5, i.e., transmitting equiprobable symbols, the backscattered rate is maximized. In the rest of the simulation, we set $\theta_0 = \theta_1 = 0.5$.

B. BER Performance

In this subsection, we investigate the BER performance of the system under different settings. First, we vary the average SNR of the direct link from the jammer as shown in Fig. 3. Clearly, as $\alpha_{d,a}$ increases, the BERs reduce for most of the cases. This is due to the fact that when the jammer attacks the channel with higher power levels, the backscattered signals at the receiver are improved, resulting in lower BERs. In other words, with our proposed solution, the more frequent and power the jammer uses to attack the channel, the higher BER performance we can achieve. Note that when the receiver equips with only 2 or 3 antennas, the BER increases when $\alpha_{d,a} < 20$ dB and $\alpha_{d,a} < 10$, respectively. This is due to the fact that with lower numbers of antennas, the receiver cannot deal with the direct link interference from both the jammer and the transmitter, resulting in a poor performance. Again, the more antennas the receiver has, the lower BERs we can achieve.

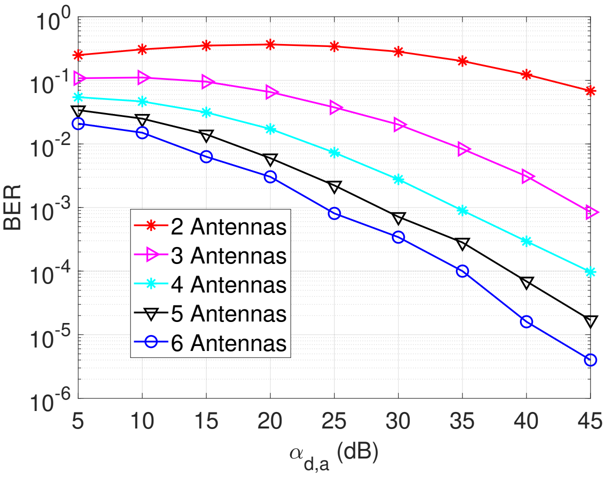

Fig. 3: BER vs. $\alpha_{d,a}$ when $\alpha_{d,t} = 20$ dB, $\tilde{\alpha}_a = \tilde{\alpha}_r = -25$ dB.

Next, we vary the relative SNRs of the backscatter links from the jammer and observe the BER performance as shown in Fig. 4. In particular, as $\tilde{\alpha}_a$ increases, the BERs of the system are reduced as the backscattered signals received at the receiver are stronger, resulting in more reliable transmissions. It is also worth noting that the BER performance is significantly improved when the number of antennas increases.

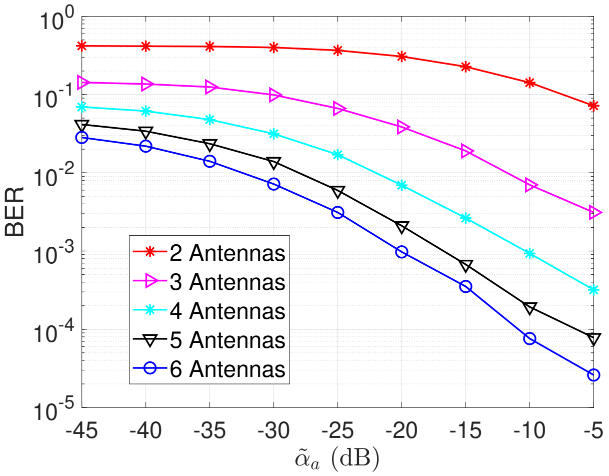

Fig. 4: BER vs. $\tilde{\alpha}_a$ when $\alpha_{d,t} = \alpha_{d,a} = 20$ dB, $\tilde{\alpha}_r = -25$ dB.

Finally, we vary the number of RF source symbols per backscatter symbol and observe the BER performance under different settings. As mentioned, to guarantee that the backscattered signals do not interfere with the jamming signals and the active signals from the transmitter, the backscattered rate must be lower than the data rate of the transmitter and the jammer. Thus, one backscatter symbol should be transmitted during a number of RF source symbol. As shown in Fig. 5, with N, i.e., the number of RF source symbol per each backscatter symbol increases, the BERs of all the cases decrease. Nevertheless, with higher values of N, the backscattered rates are reduced, resulting in a low system throughput. Thus, one needs to consider the trade-off between the backscattered rate and the value of N.

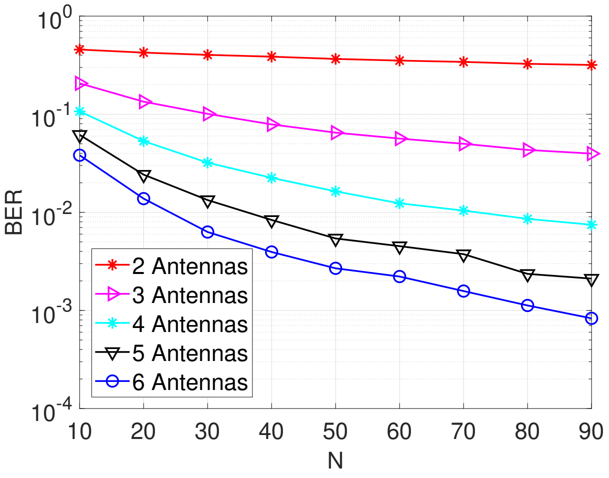

Fig. 5: BER vs. N.

VI. Conclusion

In this paper, we have proposed the state-of-the-art solution to deal with the smart and reactive jammer with high or even unlimited power budget. This is the most difficult type of jammer which has not been addressed effectively in the literature. To overcome this problem, a tag is deployed at the transmitter's side. When the jammer attacks the channel, the transmitter keeps actively transmitting signals to lure the jammer while the backscatter tag backscatters the jamming signal as well as the transmitter's signal to send data to the receiver. Through the theoretical analysis and simulation results, we have demonstrated that our proposed solution can significantly improve the system performance in terms of throughput and BER performance under the jamming attacks. Importantly, the more frequent and power the jammer uses to attack, the better BER performance we can achieve.

References

[1] W. Xu, K. Ma, W. Trappe, and Y. Zhang, "Jamming sensor networks: attack and defense strategies," *IEEE Network*, vol. 20, no. 3, May 2006, pp. 41-47.

[2] R. T. Yazicigil, P. Nadeau, D. Richman, C. Juvekar, K. Vaidya, and A. P. Chandrakasan, "Ultra-fast bit-level frequency-hopping transmitter for securing low-power wireless devices," *2018 IEEE Radio Frequency Integrated Circuits Symposium (RFIC)*, PA, USA, Aug. 2018.

[3] H. Quan, H. Zhao, and P. Cui, "Anti-jamming frequency hopping system using multiple hopping patterns," *Wireless Personal Communications*, vol. 81, no. 3, Apr. 2015, pp. 1159-1176.

[4] K. Firouzbakht, G. Noubir, and M. Salehi,"On the capacity of rate-adaptive packetized wireless communication links under jamming," in*Proceedings of the fifth ACM conference on Security and Privacy in Wireless and Mobile Networks*, Tucson, AZ, USA, 2012, pp. 3-14.

[5] M. K. Hanawal, M. J. Abdel-Rahman, and M. Krunz, "Joint adaptation of frequency hopping and transmission rate for anti-jamming wireless systems," *IEEE Transactions on Mobile Computing*, vol. 15, no. 9, Sept. 2016, pp. 2247-2259.

[6] A. Sabharwal, P. Schniter, D. Guo, D. W. Bliss, S. Rangarajan, and R. Wichman, "In-band full-duplex wireless: Challenges and opportunities," *IEEE Journal on Selected Areas in Communications*, vol. 32, no. 9, Jun. 2014, pp. 1637-1652.

[7] B. Wang, Y. Wu, K. R. Liu, and T. C. Clancy, "An anti-jamming stochastic game for cognitive radio networks," *IEEE Journal on Selected Areas in Communications*, vol. 29, no. 4, Apr. 2011, pp. 877-889.

[8] J. Guo, N. Zhao, F. R. Yu, X. Liu, and V. C. Leung, "Exploiting adversarial jamming signals for energy harvesting in interference networks," *IEEE Transactions on Wireless Communications*, vol. 16, no. 2, pp. 1267-1280, Feb. 2017.

[9] N. V. 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 , Fourthquarter 2018, pp. 2889-2922.

[10] V. Liu, A. Parks, V. Talla, S. Gollakota, D. Wetherall, and J. R. Smith, "Ambient backscatter: Wireless communication out of thin air," *ACM SIGCOMM*, Hong Kong, China, Aug. 2013.

[11] N. V. Huynh, D. N. Nguyen, D. T. Hoang and E. Dutkiewicz, "Jam Me If You Can: Defeating Jammer with Deep Dueling Neural Network Architecture and Ambient Backscattering Augmented Communications," *IEEE Journal on Selected Areas in Communications*, Early access.

[12] H. Guo, Q. Zhang, D. Li, and Y.-C. Liang, "Noncoherent Multiantenna Receivers for Cognitive Backscatter System with Multiple RF Sources," [Online]. Available: arXiv:1808.04316.

[13] J. Qian, F. Gao, G. Wang, S. Jin, and H. Zhu, "Noncoherent detections for ambient backscatter system," *IEEE Transactions on Wireless Communications*, vol. 16, no. 3, Mar. 2017, pp. 1412-1422.

[14] R. G. Gallager, "Circularly-symmetric Gaussian random vectors," preprint, 2008.

[15] T. M. Cover and J. A. Thomas, *Elements of Information Theory*. John Wiley & Sons, 2012.