Performance Analysis of Reactive Symbol-Level Jamming Techniques

Han Seung Jang, *Member, IEEE*,
and Bang Chul Jung, *Senior Member, IEEE*

***Abstract*—The reactive symbol-level jamming (SLJ) technique is a simple but practical technique to disable or disrupt malicious communication links. After sensing the transmission and detecting the digital modulation scheme of the malicious transmitter, a communication node with the reactive SLJ technique, called a reactive jammer, generates random digital modulation symbols and then sends them to the malicious receiver. In this correspondence, we mathematically analyze both uncoded and coded bit error rate (BER) at the malicious receiver under not only *reactive* SLJ, but also Gaussian SLJ techniques. In particular, we consider the partial jamming scenario, in which a portion of symbols in a data frame are affected by the SLJ, which is a practical scenario under the reactive jamming techniques. We also consider the effect of imperfect power control and channel estimation error of the reactive jammer on the BER performance at the malicious receiver.**

***Index Terms*—Reactive symbol-level jamming, bit error rate (BER), channel codes, power control, channel estimation error.**

I. Introduction

Due to broadcast nature of wireless communications, the wireless air interface is open and accessible to both authorized and illegitimate users [1], [2]. Recently, Lichtman *et al.* [3] considered physical-layer security threats and proposed the mitigation methods by analyzing various types of physical channels and signals in LTE/LTE-A and 5G NR systems. The security problems are even worse in infrastructure-free mobile communication systems [4]. Wu *et al.* [5] also provided a survey of the physical layer security studies on various recent 5G technologies such as physical layer security coding, non-orthogonal multiple access, millimeter wave communications, etc.

On the flip side of security, proactive actions to malicious communication nodes such as jamming or spoofing via wireless medium have also been actively investigated. The symbol-level spoofing technique has been proposed to replace an original message of the malicious communication link with a target message, where authorized transmitter called spoofer is assumed to know the original message of the malicious link even before the malicious transmitter does not send it [6], [7]. However, this assumption seems not to be feasible in practical communication systems. The *symbol-level jamming (SLJ)* techniques have been investigated as a simple but practical jamming method in literature. For example, the optimal jamming signal is derived for various digital modulation schemes under additive white Gaussian noise (AWGN) channels, where it was shown that the optimal jamming signals against BPSK and QPSK modulation schemes are BPSK and QPSK themselves, respectively [8]. However, there exists no bit error rate (BER) analysis of the SLJ with channel coding (CC) techniques even though most communication systems adopt the CC to protect the information bits from interference, noise, and jamming signals.

In this paper, we investigate the reactive SLJ technique where the jammer senses the transmission of the malicious transmitter, detects the modulation scheme used at the malicious transmitter, and then sends a random digital modulation symbols to the malicious receiver. We summarize the main contribution of this paper as follows:

- We consider the partial jamming scenario where a certain portion of the data frame are affected by the SLJ technique, while most studies in literature assume that whole data frame are interfered from the jammer. It is worth noting that the partial jamming scenario is much more practical due to the sensing-and-go property of the reactive jamming technique.
- We mathematically analyze both uncoded and coded BER performances of reactive SLJ techniques with QPSK modulation at the malicious receiver in AWGN channels, which is the first theoretic result to the best our knowledge. Repetition code and convolutional code are considered as the CC techniques. We also derive the BER of the reactive Gaussian SLJ technique.
- We consider the effect of imperfect power control and channel estimation error on the BER performance of the reactive SLJ techniques at the malicious receiver.

II. Reactive Symbol-Level Jamming Systems

Fig. 1 shows the system model of the *reactive* SLJ (R-SLJ) technique, which is also known as a time-correlated jamming technique [9]. There exists a single malicious communication link from Alice to Bob and a single R-SLJ transmitter called Jack tries to disable the malicious link.[1] Alice is assumed to utilize a QPSK modulation scheme, i.e., $x = \pm 1/\sqrt{2} \pm j1/\sqrt{2}$. In addition, Fig. 2 shows a timing diagram of data frame from Alice to Bob and jamming data frame from Jack to Bob. Alice's signal x is received at both of Bob and Jack after experiencing respective propagation delays. Then, Jack senses the transmission of Alice and tries to identify the modulation scheme used at Alice with automatic modulation classification (AMC) techniques [10], [11]. During the undisrupted period, the received signal at Bob is expressed as

$$y = \sqrt{E}x + w, \tag{1}$$

[1]We assume that both Alice and Bob exchange data frames with each other. Thus, the overhearing link and the jamming link can be interchanged and Jack is assumed to identify two links via overhearing.

Manuscript received May 28, 2018; revised September 18, 2018; accepted October 16, 2018. Date of publication October 22, 2018; date of current version December 14, 2018. This work was supported by the Future Combat System Network Technology Research Center Program of Defense Acquisition Program Administration and Agency for Defense Development under Grant UD160070BD. The review of this paper was coordinated by Prof. Y. Li. *(Corresponding author: Bang Chul Jung.)*

H. S. Jang is with the Information Systems Technology and Design Pillar, Singapore University of Technology and Design, Singapore, 487372 (e-mail: hanseung_jang@sutd.edu.sg).

B. C. Jung is with the Department of Electronics Engineering, Chungnam National University, Daejeon 34134, South Korea (e-mail: bcjung@cnu.ac.kr).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TVT.2018.2877435

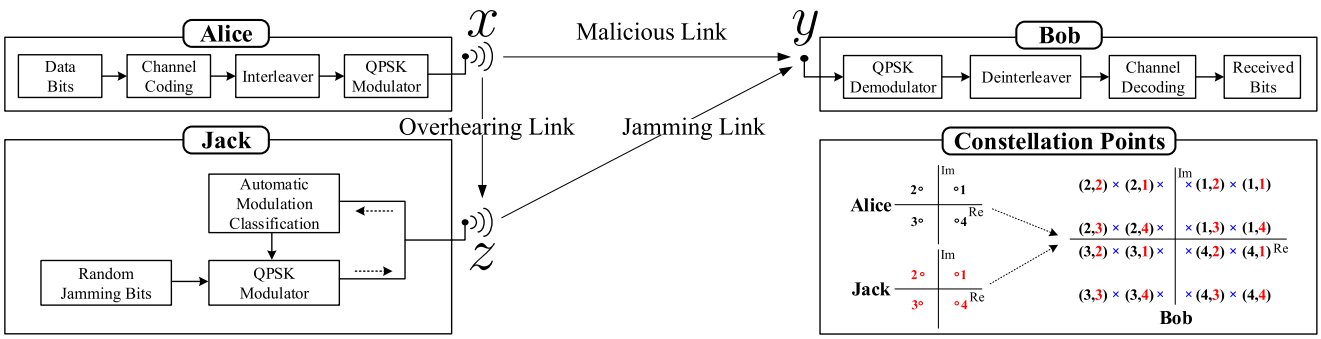

Fig. 1. System model of an SLJ system. There exist 16 candidates of constellation point at Bob, each of which is made from combination of constellation points of Alice and Jack. For example, $(1,3)$ represents that Alice's constellation points is 1 and Jack's constellation point is 3. In this figure, the phase offset is assumed to be 0 for convenience.

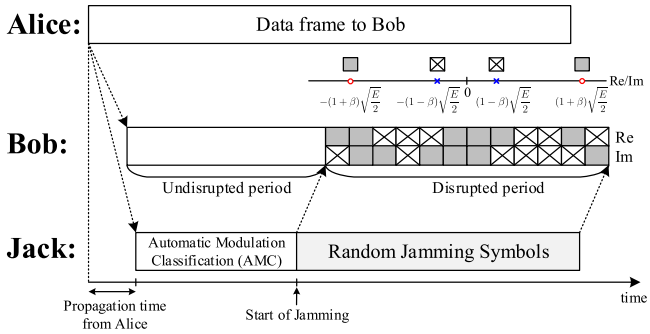

Fig. 2. Timing diagram of data frames of malicious link and jamming link.

where $\sqrt{E}$ and w represent the transmit power and the thermal noise signal at Bob following zero-mean complex Gaussian distribution with variance of $2\sigma^2$, i.e., $w \sim \mathcal{CN}(0, 2\sigma^2)$, respectively. After the AMC, Jack sends *randomly-generated* QPSK modulated symbol for the R-SLJ, i.e., $z = \pm 1/\sqrt{2} \pm j1/\sqrt{2}$. During the disrupted (jamming) period, the received signal at Bob is expressed as

$$y = \sqrt{E}x + \beta\sqrt{E}\exp(j\theta)z + w, \tag{2}$$

where β and θ represent power difference ratio and phase offset between the received signals from Alice and Jack, respectively. The jamming ratio is defined as

$$\alpha = \frac{\text{disrupted (jamming) period}}{\text{data frame period of malicious link}} \in (0,1), \tag{3}$$

where the concept of jamming ratio has been widely adopted in reactive jamming systems due to sensing-and-go property of the reactive jamming techniques [12]. In general a random interleaver is exploited as a channel interleaver for the coded bits to maximize diversity gain in communication systems. Hence, the effect of jamming is randomly spread over the entire data frame even though the symbols in a consecutive time period are affected by the R-SLJ signals. With the interleaver, we obtain the probability that a certain received symbol at Bob is disrupted by the jamming symbol is given by $P_{\mathsf{d}} = \alpha$ and the probability that a symbol is not disrupted is given by $P_{\mathsf{u}} = 1 - \alpha$, respectively.

With QPSK modulation scheme, (2) can be rewritten as (4),

$$\begin{aligned} y = &\Big\{1 + \text{sgn}[\mathsf{Re}(x)\mathsf{Re}(z)]\beta\cos(\theta) - \text{sgn}[\mathsf{Re}(x)\mathsf{Im}(z)]\beta\sin(\theta)\Big\} \\ &\times \sqrt{E}\mathsf{Re}(x) \\ &+ j\Big\{1 + \text{sgn}[\mathsf{Im}(x)\mathsf{Im}(z)]\beta\cos(\theta) - \text{sgn}[\mathsf{Re}(x)\mathsf{Im}(z)]\beta\sin(\theta)\Big\} \\ &\times \sqrt{E}\mathsf{Im}(x) + w \end{aligned} \tag{4}$$

where $\text{sgn}[\cdot]$ represents a sign function. Let $Y = Y_{\mathsf{R}} + jY_{\mathsf{I}}$ denote a complex random variable (RV) representing the received symbol at Bob consisting of two real-valued RVs, Y_{R} and Y_{I}. We adopt a traditional mapping rule for QPSK symbol in which the first and the second bit among two bits correspond to imaginary and real value of QPSK symbol, respectively. In addition, 0 and 1 are mapped to positive and negative signs, respectively. Then, Y_{R} and Y_{I} are given by

$$Y_{\mathsf{I}} = Y_{\mathsf{R}} = \begin{cases} \mathcal{N}\Big(\pm\sqrt{E/2}, \sigma^2\Big) & \text{with probability(w.p.) } 1-\alpha, \\ \mathcal{N}\Big(\pm\Upsilon_1(\beta,\theta)\sqrt{E/2}, \sigma^2\Big) & \text{w.p. } \frac{\alpha}{4}, \\ \mathcal{N}\Big(\pm\Upsilon_2(\beta,\theta)\sqrt{E/2}, \sigma^2\Big) & \text{w.p. } \frac{\alpha}{4}, \\ \mathcal{N}\Big(\pm\Upsilon_3(\beta,\theta)\sqrt{E/2}, \sigma^2\Big) & \text{w.p. } \frac{\alpha}{4}, \\ \mathcal{N}\Big(\pm\Upsilon_4(\beta,\theta)\sqrt{E/2}, \sigma^2\Big) & \text{w.p. } \frac{\alpha}{4}, \end{cases}$$

where $\mathcal{N}(\mu, \sigma^2)$ represents a Gaussian random variable with mean μ and variance σ^2, and

$$\begin{aligned} \Upsilon_1(\beta,\theta) &= 1 + \beta\cos(\theta) + \beta\sin(\theta), \\ \Upsilon_2(\beta,\theta) &= 1 + \beta\cos(\theta) - \beta\sin(\theta), \\ \Upsilon_3(\beta,\theta) &= 1 - \beta\cos(\theta) + \beta\sin(\theta), \\ \Upsilon_4(\beta,\theta) &= 1 - \beta\cos(\theta) - \beta\sin(\theta). \end{aligned}$$

Cumulative distribution functions (CDFs) of Y_{R} and Y_{I} are given by

$$\begin{aligned} F_{Y_{\mathsf{R}}}(y) = F_{Y_{\mathsf{I}}}(y) &= (1-\alpha)\Phi\left(\frac{y \mp \sqrt{E/2}}{\sigma}\right) \\ &+ \sum_{i=1}^{4}\left(\frac{\alpha}{4}\right)\Phi\left(\frac{y \mp \Upsilon_i(\beta,\theta)\sqrt{E/2}}{\sigma}\right), \end{aligned} \tag{5}$$

where $\Phi\left(\frac{y-\mu}{\sigma}\right) = \int_{-\infty}^{y} \frac{1}{\sqrt{2\pi\sigma^2}} e^{-\frac{(y-\mu)^2}{2\sigma^2}} dy$.

With Gaussian SLJ (G-SLJ) techniques, Jack sends complex Gaussian noise symbol to Bob, which is modeled as $z \sim \mathcal{CN}(0,1)$. Then, real and imaginary parts of the received signal at Bob is given by

$$Y_{\mathsf{I}} = Y_{\mathsf{R}} = \begin{cases} \mathcal{N}\left(\pm\sqrt{E/2}, \sigma^2\right) & \text{w.p. } 1-\alpha, \\ \mathcal{N}\left(\pm\sqrt{E/2}, \sigma^2 + \beta^2 E/2\right) & \text{w.p. } \alpha. \end{cases}$$

The CDFs of them are also given by

$$F_{Y_{\mathsf{R}}}(y) = F_{Y_{\mathsf{I}}}(y) = (1-\alpha)\Phi\left(\frac{y \mp \sqrt{E/2}}{\sigma}\right) + \alpha\Phi\left(\frac{y \mp \sqrt{E/2}}{\sqrt{\sigma^2 + \beta^2 E/2}}\right). \quad (6)$$

III. Performance Analysis

To obtain the BER performance at Bob, without loss of generality, we assume that a symbol $x = +1/\sqrt{2} + j1/\sqrt{2}$ is transmitted by Alice for bits 00. In this case, a bit error occurs when the received real-axis symbol has a negative phase or the received imaginary-axis the symbol has a negative phase.

A. Uncoded BER

1) Reactive Symbol-Level Jamming: The uncoded first bit-error rate under the R-SLJ is given by

$$B_{\mathsf{uncoded}}^{\mathsf{RSLJ}} = \Pr\{Y_{\mathsf{I}} < 0\} = F_{Y_{\mathsf{I}}}(0) = (1-\alpha)Q\left(\sqrt{\frac{2E_{\mathsf{b}}}{N_0}}\right) + \sum_{i=1}^{4}\left(\frac{\alpha}{4}\right)Q\left(\Upsilon_i(\beta,\theta)\sqrt{\frac{2E_{\mathsf{b}}}{N_0}}\right), \quad (7)$$

where $E_{\mathsf{b}} = E/2$, $N_0 = 2\sigma^2$, and $Q(\cdot)$ denotes a Q-function. The uncoded second bit-error rate under the R-SLJ is given as $B_{\mathsf{uncoded}}^{\mathsf{RSLJ}} = \Pr\{Y_{\mathsf{R}} < 0\} = F_{Y_{\mathsf{R}}}(0)$, which is the same as (7). Especially, when $\beta = 1$ and $\theta = 0$ (perfect power and sync control), as E_{b}/N_0 (SNR) increases, Q-function values become zero except $i = 3$ and $i = 4$, and thus, the uncoded BER under the R-SLJ is saturated by $\frac{\alpha}{2}Q(0) = \frac{\alpha}{4}$.

2) Gaussian Symbol-Level Jamming: The uncoded first bit-error rate under the G-SLJ is given by

$$B_{\mathsf{uncoded}}^{\mathsf{GSLJ}} = \Pr\{Y_{\mathsf{I}} < 0\} = F_{Y_{\mathsf{I}}}(0) = (1-\alpha)Q\left(\sqrt{\frac{2E_{\mathsf{b}}}{N_0}}\right) + \alpha Q\left(\sqrt{\frac{2\frac{E_{\mathsf{b}}}{N_0}}{1+2\beta^2\frac{E_{\mathsf{b}}}{N_0}}}\right), \quad (8)$$

and the uncoded second bit-error rate under the G-SLJ is given as $P_{\mathsf{uncoded}}^{\mathsf{GSLJ}} = \Pr\{Y_{\mathsf{R}} < 0\} = F_{Y_{\mathsf{R}}}(0)$, which is the same as (8). As E_{b}/N_0 increases, the first term in (8) becomes zero, and the uncoded BER under the G-SLJ is approximated as

$$P_{\mathsf{uncoded}}^{\mathsf{GSLJ}} \approx \alpha Q\left(\sqrt{\frac{2\frac{E_{\mathsf{b}}}{N_0}}{1+2\beta^2\frac{E_{\mathsf{b}}}{N_0}}}\right) \approx \alpha Q\left(\frac{1}{\beta}\right). \quad (9)$$

B. Coded BER With Repetition Codes

In this subsection, Alice is assumed to utilize the repetition codes (RC). With the RC, the same information bit is repeated n-times, and thus, the corresponding code rate is equal to $R_{\mathsf{c}} = 1/n$. First, we briefly review the BER performance of the n-RC without SLJ, and then we derive the BER performance of the n-RC under R-SLJ and G-SLJ.

In a binary RC, there exist two code words: $\mathbf{c}_0 = \{0,0,\ldots,0\}$ and $\mathbf{c}_1 = \{1,1,\ldots,1\}$. Let $\mathbf{y}_{\mathsf{R}} = \{\mathsf{Re}(y_1), \mathsf{Re}(y_2), \ldots, \mathsf{Re}(y_n)\}$ and $\mathbf{y}_{\mathsf{I}} = \{\mathsf{Im}(y_1), \mathsf{Im}(y_2), \ldots, \mathsf{Im}(y_n)\}$ denote the received real-axis signal vector and the received imaginary-axis signal vector, respectively, and each received symbol in $\mathbf{y}_{\mathsf{R}}$ and $\mathbf{y}_{\mathsf{I}}$ is independently and identically distributed (i.i.d). The maximum-likelihood decoder compares the likelihood of each codeword for a given received vector. Hence, the log-likelihood ratio (LLR) of the first bit of QPSK symbol is given by

$$\mathcal{L}(\mathbf{y}_{\mathsf{I}}) = \ln\frac{\Pr\{\mathbf{y}_{\mathsf{I}}|\mathbf{c}_0\}}{\Pr\{\mathbf{y}_{\mathsf{I}}|\mathbf{c}_1\}} = \ln\frac{\prod_{i=1}^{n}\exp\left\{-\frac{(\mathsf{Im}(y_i)-\sqrt{E/2})^2}{2\sigma^2}\right\}}{\prod_{i=1}^{n}\exp\left\{-\frac{(\mathsf{Im}(y_i)+\sqrt{E/2})^2}{2\sigma^2}\right\}} = \sum_{i=1}^{n}\frac{\sqrt{2E}}{\sigma^2}\mathsf{Im}(y_i), \quad (10)$$

and the LLR of the second bit of QPSK symbol is given by

$$\mathcal{L}(\mathbf{y}_{\mathsf{R}}) = \ln\frac{\Pr\{\mathbf{y}_{\mathsf{R}}|\mathbf{c}_0\}}{\Pr\{\mathbf{y}_{\mathsf{R}}|\mathbf{c}_1\}} = \ln\frac{\prod_{i=1}^{n}\exp\left\{-\frac{(\mathsf{Re}(y_i)-\sqrt{\frac{E}{2}})^2}{2\sigma^2}\right\}}{\prod_{i=1}^{n}\exp\left\{-\frac{(\mathsf{Re}(y_i)+\sqrt{\frac{E}{2}})^2}{2\sigma^2}\right\}} = \sum_{i=1}^{n}\frac{\sqrt{2E}}{\sigma^2}\mathsf{Re}(y_i). \quad (11)$$

If the $\mathcal{L}(\mathbf{y}_{\mathsf{I}})$ is larger than zero, the first decoded bit becomes zero, and otherwise, the first decoded bit becomes one. Hence, the first bit-error rate of the RC without SLJ is given by

$$B_{\mathsf{RC}} = \Pr\{\mathcal{L}(\mathbf{y}_{\mathsf{I}}) < 0|\mathbf{c}_0 \text{ transmitted}\} = \Pr\{Z_{\mathsf{I}} < 0\}, \quad (12)$$

where $Z_{\mathsf{I}} = \sum_{i=1}^{n}\mathsf{Im}(y_i)$ is the sum of n independent Gaussian random variables, each with mean $\sqrt{E/2}$ and variance σ^2. In other words, Z_{I} is a Gaussian random variable with mean $n\sqrt{E/2}$ and variance $n\sigma^2$, whose CDF is

$$F_{Z_{\mathsf{I}}}(z) = \Phi\left(\frac{z - n\sqrt{E/2}}{\sqrt{n\sigma^2}}\right). \quad (13)$$

In a similar way, the second bit-error rate of the RC without SLJ is given as

$$B_{\mathsf{RC}} = \Pr\{\mathcal{L}(\mathbf{y}_{\mathsf{R}}) < 0|\mathbf{c}_0 \text{ transmitted}\} = \Pr\{Z_{\mathsf{R}} < 0\}, \quad (14)$$

where $Z_{\mathsf{R}} = \sum_{i=1}^{n}\mathsf{Re}(y_i)$ with the same CDF of (13). As a result, the BER of the RC without SLJ is rewritten as

$$B_{\mathsf{RC}} = F_{Z_{\mathsf{I}}}(0) = Q\left(\sqrt{\frac{nE}{2\sigma^2}}\right) = Q\left(\sqrt{\frac{2E_{\mathsf{b}}}{N_0}}\right), \quad (15)$$

which is exactly the same as the uncoded BER of QPSK modulation in AWGN channels. Thus, the BER performance of the RC without SLJ is not improved compared to the uncoded BER. However, we will show that the RC can improve the BER performance under the R-SLJ and G-SLJ techniques.

1) RC Under R-SLJ: For the analysis of BER performance of n-RC under the R-SLJ, we utilize the characteristic function of a Gaussian random variable $x \sim \mathcal{N}(\mu, \sigma^2)$, $\Psi_X(\omega) = \exp\{j\omega\mu - \sigma^2\omega^2/2\}$. Hence, the characteristic functions of $\mathsf{Re}(y_i)$ and $\mathsf{Im}(y_i)$ for $i = 1, \ldots, n$ are obtained by

$$\Psi_{Y_\mathsf{R}}(\omega) = \Psi_{Y_\mathsf{I}}(\omega) = (1-\alpha)\exp\left\{j\omega\sqrt{E/2} - \sigma^2\omega^2/2\right\} + \sum_{i=1}^{4}\left(\frac{\alpha}{4}\right)\exp\left\{j\omega\Upsilon_i(\beta,\theta)\sqrt{E/2} - \sigma^2\omega^2/2\right\}. \quad (16)$$

Then, the characteristic functions of $Z_\mathsf{R} = \sum_{i=1}^{n}\mathsf{Re}(y_i)$ and $Z_\mathsf{I} = \sum_{i=1}^{n}\mathsf{Im}(y_i)$ are expressed as a multiplication of n independent characteristic functions $\Psi_{Y_\mathsf{R}}(\omega)$ and $\Psi_{Y_\mathsf{I}}(\omega)$: $\Psi_{Z_\mathsf{R}}(\omega) = [\Psi_{Y_\mathsf{R}}(\omega)]^n$ and $\Psi_{Z_\mathsf{I}}(\omega) = [\Psi_{Y_\mathsf{I}}(\omega)]^n$. Using multinomial theorem, $\Psi_{Z_\mathsf{R}}(\omega)$ and $\Psi_{Z_\mathsf{I}}(\omega)$ are given by (17).

$$\Psi_{Z_\mathsf{R}}(\omega) = \Psi_{Z_\mathsf{I}}(\omega) = \sum_{k_\mathsf{u}+k_1+k_2+k_3+k_4=n}\binom{n}{k_\mathsf{u}\,k_1\,k_2\,k_3\,k_4}(1-\alpha)^{k_\mathsf{u}} \times\left(\frac{\alpha}{4}\right)^{n-k_\mathsf{u}}\cdot\exp\left\{j\omega\left(k_\mathsf{u}\sqrt{\frac{E}{2}} + \sum_{i=1}^{4}k_i\Upsilon_i(\beta,\theta)\sqrt{\frac{E}{2}}\right) - \frac{n\sigma^2\omega^2}{2}\right\}. \quad (17)$$

The CDFs of them are given by

$$F_{Z_\mathsf{R}}(z) = F_{Z_\mathsf{I}}(z) = \sum_{k_\mathsf{u}+k_1+k_2+k_3+k_4=n}\binom{n}{k_\mathsf{u}\,k_1\,k_2\,k_3\,k_4} \times(1-\alpha)^{k_\mathsf{u}}\left(\frac{\alpha}{4}\right)^{n-k_\mathsf{u}}\Phi\left(\frac{z - k_\mathsf{u}\sqrt{\frac{E}{2}} - \sum_{i=1}^{4}k_i\Upsilon_i(\beta,\theta)\sqrt{\frac{E}{2}}}{\sqrt{n\sigma^2}}\right). \quad (18)$$

As a result, the BER of the n-RC under the R-SLJ is expressed as

$$B_{\mathsf{RC}}^{\mathsf{RSLJ}} = F_{Z_\mathsf{R}}(0) = \sum_{k_\mathsf{u}+k_1+k_2+k_3+k_4=n}\binom{n}{k_\mathsf{u}\,k_1\,k_2\,k_3\,k_4}\cdot (1-\alpha)^{k_\mathsf{u}}\left(\frac{\alpha}{4}\right)^{n-k_\mathsf{u}}\cdot Q\left(\frac{k_\mathsf{u}}{n}\sqrt{\frac{2E_\mathsf{b}}{N_0}} + \sum_{i=1}^{4}\frac{k_i}{n}\Upsilon_i(\beta,\theta)\sqrt{\frac{2E_\mathsf{b}}{N_0}}\right). \quad (19)$$

Especially, when $\beta = 1$ and $\theta = 0$ (perfect power and sync control), as the E_b/N_0 increases, Q-function values become 0 except of $k_3 + k_4 = n$, and thus, the BER of the n-RC under the R-SLJ is saturated by $\left(\frac{\alpha}{2}\right)^n \cdot Q(0) = \left(\frac{\alpha}{2}\right)^n \frac{1}{2}$.

2) RC Under G-SLJ: The characteristic function of the received signal $\mathsf{Re}(y_i)$ and $\mathsf{Im}(y_i)$ for $i = 1, \ldots, n$ under the G-SLJ is obtained by

$$\Psi_{Y_\mathsf{R}}(\omega) = \Psi_{Y_\mathsf{I}}(\omega) = (1-\alpha)\exp\left\{j\sqrt{E/2}\omega - \sigma^2\omega^2/2\right\} + \alpha\exp\left\{j\sqrt{E/2}\omega - (\sigma^2 + \beta^2E/2)\omega^2/2\right\}. \quad (20)$$

Then, in the similar way to the BER of the n-RC under R-SLJ, the BER of the n-RC under the G-SLJ is expressed as

$$B_{\mathsf{RC}}^{\mathsf{GSLJ}} = F_{Z_\mathsf{R}}(0) = F_{Z_\mathsf{I}}(0) = \sum_{k=0}^{n}\binom{n}{k}(1-\alpha)^{(n-k)}\alpha^k\cdot Q\left(\sqrt{\frac{2n\frac{E_\mathsf{b}}{N_0}}{n + 2\beta^2\frac{k}{n}\frac{E_\mathsf{b}}{N_0}}}\right). \quad (21)$$

As the E_b/N_0 increases, the BER of the n-RC under the G-SLJ is approximated as

$$B_{\mathsf{RC}}^{\mathsf{GSLJ}} \approx \sum_{k=1}^{n}\binom{n}{k}(1-\alpha)^{(n-k)}\alpha^k\cdot Q\left(\sqrt{\frac{n^2}{\beta^2 k}}\right). \quad (22)$$

C. Coded BER With Convolution Codes

In this subsection, Alice is assumed to utilize the convolutional codes (CC) with the code rate of $R_\mathsf{c} = 1/n$.

1) CC Under R-SLJ: Similar to the repetition codes, when all-zero codewords are transmitted, $Z_\mathsf{R} = \sum_{i=1}^{d}\mathsf{Re}(y_i)$ and $Z_\mathsf{I} = \sum_{i=1}^{d}\mathsf{Im}(y_i)$ are the sum of d independent Gaussian random variables, each with mean $\sqrt{E/2}$ and variance σ^2, respectively. For a soft-decision Viterbi decoder, the pairwise error probability of two distinct paths with d different coded bits is expressed as [13]

$$P_{\mathsf{CC}}(d) = Q\left(\sqrt{2dR_\mathsf{c}\frac{E_\mathsf{b}}{N_0}}\right), \quad (23)$$

where $R_\mathsf{c} = 1/n$ denotes the code rate of the CC encoder. Using (23), the BER bound of the CC without SLJ is expressed as [13]

$$B_{\mathsf{CC}} < \sum_{d=d_{\mathsf{free}}}^{\infty}K_d\cdot P_{\mathsf{CC}}(d), \quad (24)$$

where K_d and d_{free} denote the total number of nonzero information bits on all weight d codewords and the free distance of CC, respectively.

Under the R-SLJ, the first-event-error probability with the CC is expressed as

$$P_{\mathsf{CC}}^{\mathsf{RSLJ}}(d) = \sum_{k_\mathsf{u}+k_1+k_2+k_3+k_4=d}\binom{d}{k_\mathsf{u}\,k_1\,k_2\,k_3\,k_4}(1-\alpha)^{k_\mathsf{u}} \cdot\left(\frac{\alpha}{4}\right)^{d-k_\mathsf{u}}\cdot Q\left(\sqrt{\frac{2k_\mathsf{u}^2}{nd}\frac{E_\mathsf{b}}{N_0}} + \sum_{i=1}^{4}\Upsilon_i(\beta,\theta)\sqrt{\frac{2k_i^2}{nd}\frac{E_\mathsf{b}}{N_0}}\right). \quad (25)$$

Then, the BER bound of the CC under the R-SLJ is expressed as

$$B_{\mathsf{CC}}^{\mathsf{RSLJ}} < \sum_{d=d_{\mathsf{free}}}^{\infty}K_d\cdot P_{\mathsf{CC}}^{\mathsf{RSLJ}}(d), \quad (26)$$

where K_d is determined by the CC encoder structure [14]. Especially, when $\beta = 1$ and $\theta = 0$ (perfect power and sync control), as E_b/N_0 increases, Q-function values become 0 except of $k_3 + k_4 = d$ in (25), and thus, the BER of CC under the R-SLJ is saturated by $\sum_{d=d_{\mathsf{free}}}^{\infty}K_d\left(\frac{\alpha}{2}\right)^d Q(0)$.

2) CC Under G-SLJ: Under the G-SLJ, the first-event-error probability with the CC is expressed as

$$P_{\mathsf{CC}}^{\mathsf{GSLJ}}(d) = \sum_{k=0}^{d}\binom{d}{k}(1-\alpha)^{(d-k)}\alpha^k Q\left(\sqrt{\frac{2\frac{d^2}{n}\frac{E_\mathsf{b}}{N_0}}{d + 2\beta^2\frac{k}{n}\frac{E_\mathsf{b}}{N_0}}}\right). \quad (27)$$

Then, the BER bound of CC under the G-SLJ is expressed as

$$B_{\mathsf{CC}}^{\mathsf{GSLJ}} < \sum_{d=d_{\mathsf{free}}}^{\infty}K_d\cdot P_{\mathsf{CC}}^{\mathsf{GSLJ}}(d). \quad (28)$$

As E_b/N_0 increases, the BER bound of the CC under the G-SLJ is approximated as

$$B_{\mathsf{RC}}^{\mathsf{GSLJ}} \lessapprox \sum_{d=d_{\mathsf{free}}}^{\infty}\sum_{k=1}^{d}K_d\binom{d}{k}(1-\alpha)^{(d-k)}\alpha^k Q\left(\sqrt{\frac{d^2}{\beta^2 k}}\right). \quad (29)$$

TABLE I
SIMULATION PARAMETERS AND VALUES

Parameters	Values
Jamming ratio, α	$0 \sim 1$
Power ratio, β	0.8, 1.0, 1.2
Phase offset, θ	$\pi/4$, $\pi/6$, 0
Modulation scheme	QPSK
E_b/N_0 [dB]	$0 \sim 14$
Coding rate for repetition codes, R_c	$1/3$
Coding rate for convolution codes, R_c	$1/3$

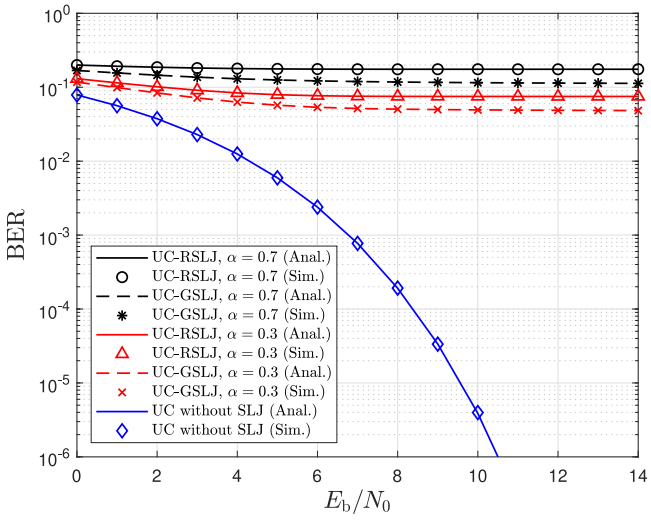

Fig. 3. Uncoded BER performance under the R-SLJ and the G-SLJ.

IV. NUMERICAL RESULTS

Table I summarizes simulation parameters utilized for performance evaluations. Fig. 3 shows the uncoded BER performance of malicious link at Bob under both the R-SLJ and the G-SLJ techniques when $\beta = 1$ and $\theta = 0$ (perfect power control and no phase offset). Our mathematical analysis matches well with the simulation results. The uncoded BER performances under both the R-SLJ and the G-SLJ become saturated to $\frac{\alpha}{2} \cdot Q(0) = \frac{\alpha}{4}$ and $\alpha \cdot Q(1) = \alpha \cdot 0.1587$, respectively, as E_b/N_0 increases. In addition, even though Alice transmits data with a higher E_b/N_0, it cannot achieve a lower BER than 10^{-2} even with a small jamming ratio α of 0.3 under the R-SLJ and the G-SLJ. The R-SLJ technique results in higher BER at Bob compared with the G-SLJ for the same jamming ratio α.

Fig. 4 shows the coded BER performance of malicious link at Bob with 3-RC ($n = 3$) under both the R-SLJ and the G-SLJ techniques when $\beta = 1$ and $\theta = 0$ (perfect power control and no phase offset). Compared with the uncoded BER performances, the BER performances of the 3-RC under both the R-SLJ and the G-SLJ are improved due to channel coding gain. Note that the mathematical analysis provided in this paper also matches well with the simulation results. Different from the uncoded BER performance, the G-SLJ technique outperforms the R-SLJ technique for the same jamming ratio α at the cost of expensive hardware for implementing G-SLJ technique. When $\alpha = 0.7$, however, the BER performances under the R-SLJ and the G-SLJ are

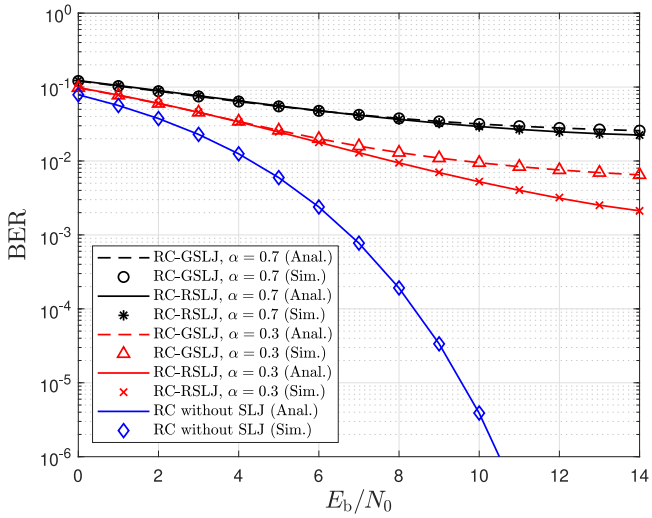

Fig. 4. BER performance of the 3-RC under the R-SLJ and the G-SLJ.

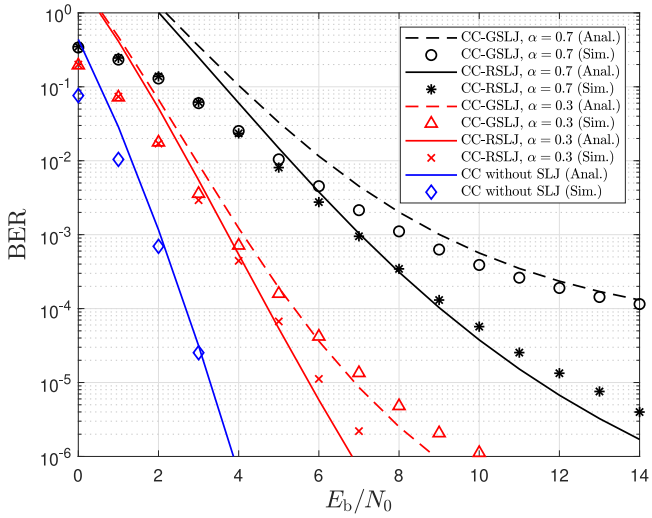

Fig. 5. BER performance of the CC under the R-SLJ and the G-SLJ.

almost the same, which implies that symbol-level jammer with a typical communication device can achieve the similar jamming performance as the Gaussian jammer with a special jamming device with the high-linearity power amplifier. Moreover, we observe that the BER of the 3-RC under the R-SLJ and the G-SLJ becomes saturated to $Q(0) \cdot (\frac{\alpha}{2})^3 = \alpha^3/16$ and $\sum_{k=1}^{3} \binom{3}{k} (1-\alpha)^{(3-k)} \alpha^k \cdot Q(\sqrt{9/k})$ as E_b/N_0 increases.

Fig. 5 shows the coded BER performance of malicious link at Bob with the CC under the R-SLJ and the G-SLJ techniques when $\beta = 1$ and $\theta = 0$ (perfect power control and no phase offset). For the CC, we utilize the generator polynomials of $(557, 663, 711)$ in octal number, the free distance d_free of 18, and K_d provided in [14]. Compared to the BER performances of the 3-RC, the overall BER performances of the CC is improved due to the stronger coding gain. Especially in high SNR regime, our analysis on BER is quite well-matched with the simulation results. The G-SLJ technique results in higher BER than the R-SLJ technique.

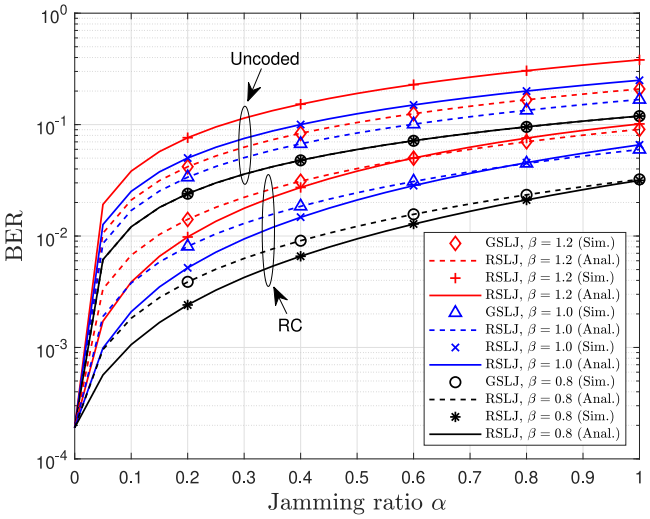

Fig. 6. Uncoded and coded BER performances under the R-SLJ and the G-SLJ with $\beta = 1.2$, 1.0, and 0.8 when $E_b/N_0 = 8$ dB and $\theta = 0$.

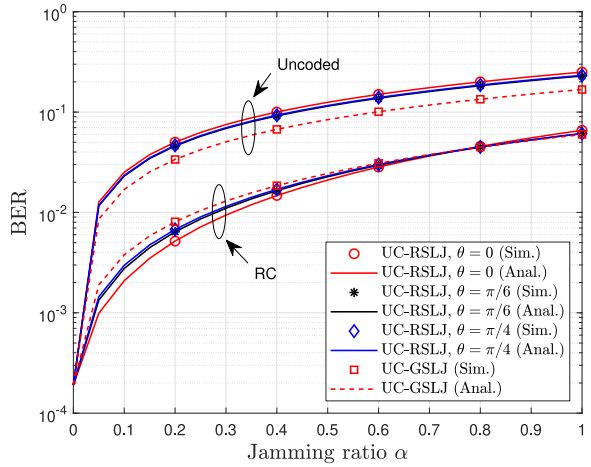

Fig. 7. Uncoded and coded BER performances under the R-SLJ and the G-SLJ with $\theta = \pi/4, \pi/6$, and 0 when $E_b/N_0 = 8$ dB and $\beta = 1$.

Fig. 6 shows the uncoded and coded BER performances under the R-SLJ and the G-SLJ for varying jamming ratio α at $\beta = 0.8$, $\beta = 1.0$, and $\beta = 1.2$. Here, Alice's E_b/N_0 is set to 8 dB and the RC is considered. This figure shows the effect of power difference ratio on the BER performance of malicious link at Bob, and we assume that $\theta = 0$. The BER performance gets worse as β increases. Higher β implies higher jamming–to–noise (JNR) ratio at Bob, and thus higher β requires the higher power consumption at Jack. The mathematical analysis matches well with the simulation results for this case as well.

Fig. 7 shows the uncoded and the coded BER performances under the R-SLJ and the G-SLJ for varying jamming ratio α at $\theta = 0$, $\theta = \pi/6$, and $\theta = \pi/4$ when $E_b/N_0 = 8$ dB and $\beta = 1$. The RC is considered as in Fig. 6. In particular, this figure shows the effect of phase offset on the BER performance of malicious link at Bob. Note that the BER performances under G-SLJ are not affected by the phase offset. Different from Fig. 6, the phase offset θ does not significantly affect the BER performance of the malicious link. Interestingly, the uncoded BER under the R-SLJ technique becomes worst when $\theta = 0$ whereas the coded BER with the RC under the R-SLJ technique becomes worst when $\theta = \pi/4$.

V. Conclusion

In this paper, we investigated a reactive symbol-level jamming (SLJ) technique and analyzed uncoded and coded BER performances of malicious communication links under both the reactive SLJ and Gaussian SLJ techniques for a given jamming ratio in additive white Gaussian noise channels. In addition, we considered the effect of power-level difference and phase offset of received signals from the malicious transmitter and the jammer at the malicious receiver. Mathematical analysis on BER performance matches well with the simulations. Somewhat interestingly, the R-SLJ technique outperforms the G-SLJ in terms of uncoded BER performance, while the G-SLJ technique outperforms the R-SLJ technique in terms of coded BER performance. We leave it for a further study to apply the SLJ techniques to multi-carrier/multi-antenna systems.

References

[1] H. Rahbari and M. Krunz, "Secrecy beyond encryption: Obfuscating transmission signatures in wireless communications," *IEEE Commun. Mag.*, vol. 53, no. 12, pp. 54–60, Dec. 2015.

[2] Y. Zou, J. Zhu, X. Wang, and L. Hanzo, "A survey on wireless security: Technical challenges, recent advances, and future trends," *Proc. IEEE*, vol. 104, no. 9, pp. 1727–1765, Sep. 2016.

[3] M. Lichtman, R. P. Jover, M. Labib, R. Rao, V. Marojevic, and J. H. Reed, "LTE/LTE-A jamming, spoofing, and sniffing: Threat assessment and mitigation," *IEEE Commun. Mag.*, vol. 54, no. 4, pp. 54–61, Apr. 2016.

[4] J. Xu, L. Duan, and R. Zhang, "Surveillance and intervention of infrastructure-free mobile communications: A new wireless security paradigm," *IEEE Wireless Commun.*, vol. 24, no. 4, pp. 152–159, Aug. 2017.

[5] Y. Wu, A. Khisti, C. Xiao, G. Caire, K.-K. Wong, and X. Gao, "A survey of physical layer security techniques for 5G wireless networks and challenges ahead," *IEEE J. Sel. Areas Commun.*, vol. 36, no. 4, pp. 679–695, Apr. 2018.

[6] J. Xu, L. Duan, and R. Zhang, "Fundamental rate limits of physical layer spoofing," *IEEE Wireless Commun. Lett.*, vol. 6, no. 2, pp. 154–157, Apr. 2017.

[7] J. Xu, L. Duan, and R. Zhang, "Transmit optimization for symbol-level spoofing," *IEEE Trans. Wireless Commun.*, vol. 17, no. 1, pp. 41–55, Jan. 2018.

[8] S. Amuru and R. M. Buehrer, "Optimal jamming against digital modulation," *IEEE Trans. Inf. Forensics Secur.*, vol. 10, no. 10, pp. 2212–2224, Oct. 2015.

[9] M. Lichtman *et al.*, "A communications jamming taxonomy," *IEEE Secur. Privacy*, vol. 14, no. 1, pp. 47–54, Jan./Feb. 2016.

[10] O. A. Dobre, A. Abdi, Y. Bar-Ness, and W. Su, "Survey of automatic modulation classification techniques: Classical approaches and new trends," *IET Commun.*, vol. 1, no. 2, pp. 137–156, Apr. 2007.

[11] S. Peng *et al.*, "Modulation classification based on signal constellation diagrams and deep learning," *IEEE Trans. Neural Netw. Learn. Syst.*, to be published, doi: 10.1109/TNNLS.2018.2850703.

[12] M. Wilhelm, I. Martinovic, J. B. Schmitt, and V. Lenders, "Reactive jamming in wireless networks: How realistic is the threat?" in *Proc. 4th ACM Conf. Wireless Netw. Secur.*, Jun. 2011, pp. 47–52.

[13] A. J. Viterbi, "Convolutional codes and their performance in communication systems," *IEEE Trans. Commun. Technol.*, vol. COM-19, no. 5, pp. 751–772, Oct. 1971.

[14] J. Conan, "The weight spectra of some short low-rate convolutional codes," *IEEE Trans. Commun.*, vol. COM-32, no. 9, pp. 1050–1053, Sep. 1984.