Jamming Modulation:
An Active Anti-Jamming Scheme

Jianhui Ma, Qiang Li, Zilong Liu, *Senior Member, IEEE*, Linsong Du,
Hongyang Chen, *Senior Member, IEEE*, and Nirwan Ansari, *Fellow, IEEE*

Abstract—Providing quality communications under adversarial electronic attacks, e.g., broadband jamming attacks, is a challenging task. Unlike state-of-the-art approaches which treat jamming signals as destructive interference, this paper presents a novel active anti-jamming (AAJ) scheme for a jammed channel to enhance the communication quality between a transmitter node (TN) and receiver node (RN), where the TN actively exploits the jamming signal as a carrier to send messages. Specifically, the TN is equipped with a programmable-gain amplifier, which is capable of re-modulating the jamming signals for jamming modulation. Considering four typical jamming types, we derive both the bit error rates (BER) and the corresponding optimal detection thresholds of the AAJ scheme. The asymptotic performances of the AAJ scheme are discussed under the high jamming-to-noise ratio (JNR) and sampling rate cases. Our analysis shows that there exists a BER floor for sufficiently large JNR. Simulation results indicate that the proposed AAJ scheme allows the TN to communicate with the RN reliably even under extremely strong and/or broadband jamming. Additionally, we investigate the channel capacity of the proposed AAJ scheme and show that the channel capacity of the AAJ scheme outperforms that of the direct transmission when the JNR is relatively high.

Index Terms—Anti-jamming communications, jamming modulation (JM), broadband jamming, programmable-gain amplifier (PGA).

I. INTRODUCTION

Jamming, also known as an intentional interference [1]–[3], is one of the most hostile threats in wireless communications. Due to their broadcasting nature, wireless networks are extremely vulnerable to jamming attacks. A jammer may dramatically disrupt the communications between two or more legitimate users by launching jamming signals to the target wireless channel [4]. As a result, the receiver may fail to decode out any useful messages from the legitimate transmitter. Since the jamming signal is generally unknown to the receiver, it is difficult to distinguish or suppress them, especially for certain extremely strong and broadband jamming signals [5]. This motivates us a radical rethinking to re-purpose the notorious jamming signals, instead of passively treating them as destructive interference.

Anti-jamming and secure communications, as an important direction in modern telecommunication engineering, has attracted extensive research attentions over the past decades [6]–[10]. The mainstream anti-jamming techniques include 1) direct sequence spread spectrum (DS-SS) [8] by spreading the signal spectrum to suppress the jamming over a narrowband; 2) frequency hopping (FH) [9] by rapidly switching a carrier over multiple frequency channels by following a pseudo-random hopping pattern known to both the transmitter and receiver to avoid the jamming attacks; and 3) interference suppression (IS) [10] by estimating and suppressing or abandoning the jammed frequency band. It is noted that these techniques generally require the legitimate users to have the jamming types and parameters from the received signal for passive anti-jamming, which is difficult in practice. A major drawback is that the desired signals may be suppressed as well when countering the jamming signals. In addition, these techniques may not be effective in mitigating extremely strong and/or broadband jamming signals.

Recently, with the emerging ambient backscatter (AmBC) techniques [11], wireless nodes are able to utilize the existing ambient radio frequency (RF) signals as a carrier to transmit additional data. As a countermeasure candidate against unknown jamming attacks, the transmitter in an AmBC communication system can modulate the impedance of transmit antenna to change the reflection of an incident signal. To validate its feasibility, [12] investigated the signal detection and bit error rate (BER) performance of AmBC communication systems. For higher transmission rates, [13] employed *M*-PSK at the backscatter node to attain high-order modulation. Recently, AmBC has been adopted in [14] to mitigate jamming attacks by developing a reinforcement learning-based algorithm to address the uncertainty of the jamming signals. However, since the backscatter node is assumed to be battery-free and the reflection factor is less than 1, it can neither guarantee a quality communication nor support a long-distance transmission. To address this

problem, we turn to a new solution, i.e., programmable-gain amplifier (PGA), which can amplify the incident signals with programmed gains. According to [15], PGA achieves a broad gain range of 30 dB over a bandwidth from 2.5 MHz to 1.17 GHz. Comparing to AmBC with passive reflecting, PGA is more suitable for anti-jamming communications, especially for broadband jamming cases and high-order modulation.

In this paper, we present a novel active anti-jamming (AAJ) scheme based on jamming modulation (JM). To improve the receiving performance and extend the communication coverage, a PGA is deployed at the transmitter node (TN) to modulate the jamming signals with the varying amplification factors, which are programmable according to the messages to be sent. Such a scheme enables us to transmit digital data over jamming signals, instead of counteracting them as in the legacy anti-jamming systems. At the receiver node (RN), the desired messages are retrieved by distinguishing different energy levels of the received signals. Under this setup, we utilize the signal-to-noise ratio (SNR) and jamming-to-noise ratio (JNR) to characterize the strengths of the desired signal and jamming signal, respectively. The transmission performance is investigated to demonstrate the feasibility and reliability of the AAJ scheme. The main contributions of this paper are summarized as follows:

- We develop the AAJ scheme to actively counter the radio jamming attacks by exploiting the jamming signal as a message carrier. In such a way, AAJ permits legitimate communications even under extremely strong or broadband jamming. Another attractive point of AAJ is that the channel state information (CSI) and the type of the jamming signal are not required at the receiver, thus making AAJ more practical in real electronic adversarial scenarios.
- We investigate the BER performance of the AAJ scheme. Both the minimum average BER and the corresponding optimal detection threshold are derived under the energy detection criterion. Moreover, considering the single-tone, multi-tone, narrowband, and broadband jamming types, we derive a general expression of the BER for these four cases. It is shown that our analytical BERs match well with the simulated ones. When the JNR under the broadband jamming case is 40 dB, as an instance shown in Section VII, the BER of the proposed AAJ scheme is about 7.38×10^{-5}. In this case, in sharp contrast, the BERs of the existing schemes approach to 0.5, leading to a decoding failure, almost surely.
- We study the asymptotic behaviors of the BER under the broadband Gaussian jamming case. In the high JNR case, we prove that there exists a BER floor for sufficiently large JNR; in the high sampling rate case, we derive an approximate expression of the BER.
- We also investigate the channel capacity of the jammed channel with the AAJ scheme and derive its optimal input distribution in a semi-closed form. Numerical results demonstrate that the channel capacity of the

proposed AAJ scheme exceeds that of the direct transmission (DT) when the JNR is relatively high. More importantly, the system performance improves as the jamming power increases.

The remainder of this paper is organized as follows. Section II introduces the system model of the jamming channel. Section III develops an energy detection method and computes the corresponding BER of the proposed AAJ scheme under the random broadband jamming case. Section IV analyzes the transmission performances of the AAJ scheme under deterministic jamming cases. Section V shows the asymptotic analysis of the system BER with the AAJ scheme. Section VI investigates the channel capacity and the corresponding optimal input distribution of the AAJ enabled jamming channel. Numerical results are presented in Section VII. Section VIII concludes this paper.

II. SYSTEM MODEL

Let us consider a wireless communications system consisting of a TN, an RN, and a jammer node (JN), as shown in Fig. 1, where the JN transmits jamming signals to attack both the TN and RN. To enable legitimate communications between the TN and RN, we take advantage of the JM method to introduce a novel AAJ scheme in which the TN is able to send messages over jamming signals.

A. JM Method

The key idea of JM is to utilize the useful messages to modulate the energy of the jamming signals. Specifically, a PGA, whose amplification factor can be programmable with digital messages [15]–[17], is adopted at the TN such that it is able to communicate with the RN by modulating its own messages over the jamming signals. The JM method can be briefly described in the following three steps:

1) First, the JN launches a jamming attack, which will be sensed and subsequently received by the TN.
2) Second, the TN re-modulates and transmits them to the RN by the PGA, which is programmed with the useful digital messages (mapping to different amplification factors)[1].
3) Finally, the RN detects the drastic change of the received signals caused by the amplification factors so as to extract the desired messages.

B. Signal Model

The channel coefficients of the JN-TN (JT), TN-RN (TR), and JN-RN (JR) links are denoted by h_1, h_2, and h_3, respectively. In this paper, we consider a frequency-flat and block-fading channel model. All channel coefficients stay constant within a channel coherent time but may vary independently in different coherent intervals. In real electronic adversarial cases, the CSI of the jamming channel, i.e., JT and JR links, and the type of jamming signal are

---

[1]The re-modulated signal can be regarded as an energy modulated signal, i.e., different energy levels of the forwarded signal may represent different messages.
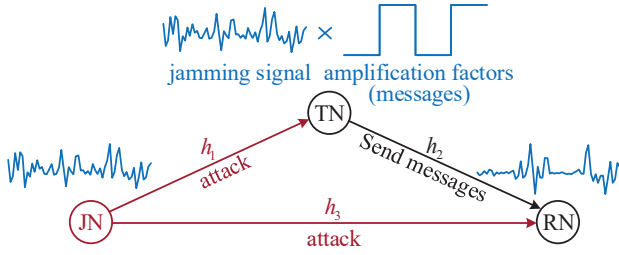
Fig. 1. Active anti-jamming communications system, with JN, TN, and RN denoting the jammer node, transmitter node, and receiver node, respectively, where the TN operates in the FD mode.

generally unavailable. Therefore, the channel coefficients h_1 and h_2 as well as the jamming signal may be unknown to the TN and RN. Without any loss of generality, the TN operates in the full-duplex (FD) mode, which enables it to receive and transmit signals at the same time slot. Next, the signal transmitting and receiving processes of the proposed AAJ scheme are described as follows.

1) Signal Transmitting: The JN broadcasts the jamming signals to both the TN and RN[2]. Therefore, the received signal $Y_T(t)$ at the TN is given by

$$Y_T(t) = h_1 X_J(t). \tag{1}$$

Here, $X_J(t)$ denotes the unknown jamming signal. For the convenience of calculation, the noise of the PGA and the self-interference introduced by the FD mode at the TN are both incorporated into the noise at the RN[3].

Under this case, the TN communicates with the RN by adopting the JM method, i.e., the messages to be sent by the TN are mapped to different amplification factors, carried by the jamming signal, and forwarded to the RN. Therefore, the transmitted signal $X_T(t)$ at the TN is given by

$$\begin{aligned} X_T(t) &= A(t)Y_T(t) \\ &= A(t)h_1 X_J(t), \end{aligned} \tag{2}$$

where $A(t) \in \{a_k\}, k = 1, 2, ..., K$, is the amplification factor corresponding to the messages to be sent by the TN with the distribution $p(A(t) = a_k) = p_k$, $\sum_{k=1}^{K} p_k = 1$.

2) Signal Receiving: As shown in Fig. 1, the RN receives the superposition of the jamming signal from the JR link and the re-modulated signal from the TR link. Therefore, the received signal $Y_R(t)$ at the RN is given by

$$\begin{aligned} Y_R(t) &= h_2 X_T(t) + h_3 X_J(t - \tau) + Z_R(t) \\ &= h_1 h_2 A(t) X_J(t) + h_3 X_J(t - \tau) + Z_R(t), \end{aligned} \tag{3}$$

where τ is the delay between the JR and JT-TR links, and $Z_R(t)$ is the independent and identical distributed (i.i.d.) circularly symmetric complex Gaussian (CSCG) noise, i.e., $Z_R(t) \sim \mathcal{CN}(0, \sigma_R^2)$.

Remark 2.1: It is observed that the received signal at the RN includes not only the additive interference and noise $h_3 X_J(t - \tau) + Z_R(t)$ but also the multiplicative interference $h_1 h_2 A(t) X_J(t)$, thus making the decoding a complex task.

Remark 2.2: Note that from (3), the desired message, i.e., $A(t)$, is only carried by the jamming signal received from the TR link. In other words, the jamming signal from the JR link, i.e., $h_3 X_J(t - \tau)$, is regarded as interference when the RN decodes the desired messages.

III. PROPOSED SIGNAL DETECTION

In this section, an energy detector [22] is introduced for the proposed AAJ scheme under the jamming attacks. Unlike conventional communications, the CSI and modulation type of the hostile jammer in anti-jamming communications are generally unknown to the receiver, and thus coherent demodulations are inapplicable in this case. However, some statistics of the jamming signal are generally fixed due to the hardware limits of the jammer. For instance, the average transmission power of the jammer is fixed[4]. This inherent property has led to the proposed energy-based detection scheme, which only relies on the statistics of the received signal to recover the desired messages.

During the duration of one transmitted symbol, the received signal at the RN is sampled for N times, which is denoted by $\boldsymbol{y}_R = [y_R[1], y_R[2], ..., y_R[N]]^T$. From (3), when the TN sends the symbol a_k, the n-th sample can be expressed as

$$y_R[n] = h[n]a_k + z[n], \tag{4}$$

where $h[n] = h_1 h_2 X_J[n]$ and $z[n] = h_3 X_J[n - n_\tau] + Z_R[n]$.

According to (4), the signal-to-interference and noise ratio (SINR) at the RN with the AAJ scheme can be given by

$$\begin{aligned} \mathrm{SINR} &= \frac{\mathbb{E}\left[|h_1 h_2 X_J[n]a_k|^2\right]}{\mathbb{E}\left[|h_3 X_J[n - n_\tau] + Z_R[n]|^2\right]} \\ &= \frac{|h_1|^2|h_2|^2|a_k|^2 P_J}{|h_3|^2 P_J + \sigma_R^2}, \end{aligned} \tag{5}$$

where P_J is the average power of the jamming signal.

Remark 3.1: One can see that unlike conventional anti-jamming communications, both the numerator and the denominator of the SINR include the term of P_J in the AAJ communications system due to the fact that we exploit the jamming signal to transmit messages[5].

---

[2]In this paper, we focus on the case of continuous jamming attack, i.e., the jammer keeps transmitting without a stop. The jamming signal can be detected by the spectrum sensing technique [18], [19]. If jamming is not detected, the TN may switch to the conventional RF chain to transmit signals, i.e., generating signal carrier by itself.

[3]Unlike conventional communications, the digital-to-analog converter (DAC), the oscillator, and the frequency mixer, etc., are not required at the TN when the AAJ scheme is adopted, and thus the noise at the TN is relatively low. In addition, according to the current self-interference cancellation techniques, the residual self-interference is also very low as compared with the strong jamming signal [20], [21]. Therefore, both of them can be regarded as background noises when the RN decodes the messages.

[4]It is worth noting that the proposed AAJ scheme is not limited to the fixed jamming power and signal type cases. Although the transmission performances may degrade, it can still work even under jamming cases with varying power levels due to the fact that the signal energy from the JT-TR link can be dramatically changed by the amplification factor a_k. The transmission performances of the AAJ scheme under the other jamming cases are thus worthy of a further study.

[5]As a future work, one may consider an adaptive scheme in terms of the jamming strength, where $A(t)$ depends on the strength of $X_J(t)$. When the jamming is strong, we can choose a smaller $A(t)$ to maintain the energy level of the re-modulated jamming signal; when the jamming is weak, we should choose a larger $A(t)$ or switch to the conventional anti-jamming scheme.

Remark 3.2: Since the jamming signal $X_J[n]$ is unknown to the RN, it may not directly extract the desired messages from the received signal. However, considering the limits of hardware, the JN is supposed to launch jamming attacks with the fixed transmission power. Consequently, the average power of the jamming signal is mostly fixed, e.g., the single-tone jamming signal with a constant envelope.

A. Energy Detection

1) Energy Detector: An energy detector measures the average energy of the received signal over one transmitted symbol period and compares it with a predefined threshold to distinguish the different symbols. The average energy of N receiver samples corresponding to one transmit symbol, i.e., the average energy of $\boldsymbol{y}_R$, is given by

$$\mathcal{Q} \triangleq \frac{1}{N} \sum_{n=1}^{N} |y_R[n]|^2. \tag{6}$$

By substituting (4) into (6), we have

$$
\begin{aligned}
&\frac{1}{N} \sum_{n=1}^{N} |y_R[n]|^2 \\
=& \frac{1}{N} \sum_{n=1}^{N} |h_1 h_2 a_k X_J[n] + h_3 X_J[n - n_\tau] + Z_R[n]|^2 \\
=& \frac{1}{N} \sum_{n=1}^{N} |h_1 h_2 a_k X_J[n] + h_3 X_J[n - n_\tau]|^2 + \frac{1}{N} \sum_{n=1}^{N} |Z_R[n]|^2,
\end{aligned}
\tag{7}
$$

where (7) is obtained by leveraging the independence between the jamming signal and noise.

For sufficiently large N, we have

$$
\begin{aligned}
&\frac{1}{N} \sum_{n=1}^{N} |h_1 h_2 a_k X_J[n] + h_3 X_J[n - n_\tau]|^2 \\
&\longrightarrow |h_1 h_2 a_k + h_3|^2 \frac{1}{N} \sum_{n=1}^{N} |X_J[n]|^2.
\end{aligned}
\tag{8}
$$

Note that we focus on the strong jamming case in this paper. By ignoring the noise term, (7) can be approximated by

$$
\begin{aligned}
\mathcal{Q} &= \frac{1}{N} \sum_{n=1}^{N} |y_R[n]|^2 \\
&\approx |h_1 h_2 a_k + h_3|^2 \frac{1}{N} \sum_{n=1}^{N} |X_J[n]|^2.
\end{aligned}
\tag{9}
$$

Therefore, the average energy of the received signal is determined by the amplification factor a_k, meaning that the RN can extract the desired message from the received signal by distinguishing its different energy levels.

Remark 3.3: For instance, if we adopt the binary modulation, i.e., on-off keying (OOK), at the TN, we have

$$
\mathcal{Q} \approx \begin{cases} |h_3|^2 \frac{1}{N} \sum_{n=1}^{N} |X_J[n]|^2, & a_1 = 0 \text{ for sending '0',} \\ |h_1 h_2 a + h_3|^2 \frac{1}{N} \sum_{n=1}^{N} |X_J[n]|^2, & a_2 = a \text{ for sending '1'.} \end{cases}
\tag{10}
$$

Obviously, the energy levels of the received signal are distinguishable at the RN as long as a is sufficiently large.

2) The Estimation of Detection Threshold: The threshold value $\mathcal{T}_{th}$ for detecting a symbol is derived by a preamble promised beforehand, e.g., '101010', in the case of binary input. When the RN receives the whole signal during one communication block, it first uses the preamble sequence to determine the average energy of '0' and '1', and then sets the threshold. The average energy of the two preamble symbols are given by

$$
\hat{\mathcal{Q}}_p = \begin{cases} (P_2 + P_4 + P_6)/3, & \text{preamble symbol is '0',} \\ (P_1 + P_3 + P_5)/3, & \text{preamble symbol is '1',} \end{cases}
\tag{11}
$$

where P_m denotes the average energy of the m-th symbol in the preamble, i.e.,

$$
P_m = \frac{1}{N} \sum_{n=1}^{N} |y_R[(m-1)N + n]|^2, 1 < m < M. \tag{12}
$$

In practice, we can choose a longer preamble, i.e., M is relatively large, to get a more precise threshold.

Therefore, the detection threshold between '0' and '1' can be formulated as

$$
\hat{\mathcal{T}}_{th} = T_{ED} \left(\hat{\mathcal{Q}}_p(a_k = a_1), \hat{\mathcal{Q}}_p(a_k = a_2) \right), \tag{13}
$$

where T_{ED} is the mapping from $\hat{\mathcal{Q}}_p$ to $\hat{\mathcal{T}}_{th}$, which is given in *Remark 3.5* of the next subsection. $\hat{\mathcal{Q}}_p(a_k = a_1)$ and $\hat{\mathcal{Q}}_p(a_k = a_2)$ correspond to the estimated average energy levels of '0' and '1', respectively, which are given in (11).

3) Message Decoding: $\hat{\mathcal{T}}_{th}$ divides the estimation space into non-intersection intervals, i.e., $\mathcal{I}_1$ and $\mathcal{I}_2$, corresponding to different amplification factors $\{a_k\}_{k=1}^2$, i.e.,

$$
\mathcal{I}_k = \begin{cases} \mathcal{Q} \in (0, \hat{\mathcal{T}}_{th}), & a_k = a_1 \text{ for sending '0',} \\ \mathcal{Q} \in (\hat{\mathcal{T}}_{th}, +\infty), & a_k = a_2 \text{ for sending '1'.} \end{cases}
\tag{14}
$$

Hence, the decoder at the RN produces

$$
\hat{k} : \{ k \in \{1, 2\} : \mathcal{Q} \in \mathcal{I}_k \}. \tag{15}
$$

Next, let us summarize the energy detection method in the following three steps:

Step 1: Compute the average energy of the received signal, i.e., $\mathcal{Q}$, by (6);

Step 2: Estimate the detection threshold, i.e., $\hat{\mathcal{T}}_{th}$, by (11) and (13);

Step 3: Decode the desired messages by the energy detection criterion. If $\mathcal{Q} \leq \hat{\mathcal{T}}_{th}$, then $a_k = a_1$; else $a_k = a_2$.

Remark 3.4: It is worth noting that the energy detection, as a non-coherent demodulation, only uses the average energy of the received signal, i.e., $\mathcal{Q} = \frac{1}{N} \sum_{n=1}^{N} |y_R[n]|^2$, to decode the desired messages. Consequently, the CSI of the anti-jamming channel and even the type of jamming signal may not be necessary for message recovering, which is the very unique feature of the AAJ scheme in practice.

B. Bit Error Rate

To estimate the performance of the proposed AAJ scheme, we next compute its average BER, which is defined as

$$P_e = \sum_{k=1}^{K} P_e(a_k), \tag{16}$$

where $P_e(a_k) = p_k \left(1 - \int_{\mathcal{I}_k} f(q) \mathrm{d}q \right)$ is the error probability when the TN transmits symbol a_k, and $f(q)$ is the probability density function (PDF) of $\mathcal{Q}$, i.e., the average energy of N receiver samples.

Since the transmit power budget of the jammer transmitter is limited, we have

$$\mathbb{E}\left[|X_{\mathrm{J}}[n]|^2\right] = \lim_{N \to \infty} \frac{1}{N} \sum_{n=1}^{N} |X_{\mathrm{J}}[n]|^2 \le P_{\mathrm{J}}. \tag{17}$$

According to the maximum entropy principle [23], the Gaussian distribution maximizes the entropy over all distributions under the same variance. Therefore, the uncertainty of the jamming signal achieves the maximum value when it subjects to the zero-mean complex Gaussian distribution, i.e., $X_{\mathrm{J}}[n] \sim \mathcal{CN}(0, P_{\mathrm{J}})$. In other words, the best strategy of the JN is to launch a Gaussian jamming signal.

In such a case, the RN received signal under $A[n] = a_k$, is also a zero-mean complex Gaussian random process, i.e.,

$$y_{\mathrm{R}}[n] \sim \mathcal{CN}\left(0, \delta_k^2\right), \tag{18}$$

where the delay at the TN is omitted, and the variance of $y_{\mathrm{R}}[n]$ is computed as

$$\begin{aligned} \delta_k^2 &= \mathrm{Var}\left[h[n]a_k + z[n]\right] \\ &= |h_1 h_2 a_k + h_3|^2 P_{\mathrm{J}} + \sigma_{\mathrm{R}}^2. \end{aligned} \tag{19}$$

It can be observed from (6) that $\mathcal{Q}$ is a sum of squares of N independent CSCG variables with identical mean and variance. By normalizing the variance of $y_{\mathrm{R}}[n]$, we have the following lemma.

Lemma 3.1: The average energy of the received signal during one transmitted symbol $\mathcal{Q}$ satisfies

$$\frac{2N}{\delta_k^2} \mathcal{Q} \sim \chi^2(2N), \tag{20}$$

where $\chi^2(2N)$ is the chi-squared distribution with $2N$ degrees of freedom.

Proof: Please see Appendix A. ∎

According to *Lemma 3.1*, the distribution of $(2\mathcal{Q}N)/\delta_k^2$ is derived, upon which we can further compute the PDF of $\mathcal{Q}$.

Lemma 3.2: The PDF of $\mathcal{Q}$ is given by

$$f_{\mathcal{Q}}(q) = \begin{cases} \frac{N}{\Gamma(N)(\delta_k^2)^N} (Nq)^{N-1} e^{-\frac{N}{\delta_k^2}q}, & q > 0, \\ 0, & \text{otherwise,} \end{cases} \tag{21}$$

where $\Gamma(N) = \int_0^{+\infty} x^{N-1} e^{-x} \mathrm{d}x$ is the Gamma function.

Proof: Please see Appendix B. ∎

By substituting the above PDF of $\mathcal{Q}$ into (16), we can compute the optimal detection threshold for the energy detector, which is given by

$$\mathcal{T}_{\mathrm{th}}^* = \arg\min_{\mathcal{T}_{\mathrm{th}}} P_e. \tag{22}$$

Considering the binary input at the TN and $\delta_1^2 < \delta_2^2$, the minimum P_e and the corresponding optimal detection threshold $\mathcal{T}_{\mathrm{th}}^*$ of the proposed AAJ scheme under the energy detection are summarized in the following proposition.

Proposition 3.1: The minimum average BER of the proposed AAJ scheme under the energy detection can be expressed as

$$\begin{aligned} P_e = & p_1 \left(1 - \int_0^{\mathcal{T}_{\mathrm{th}}^*} \frac{N}{\Gamma(N)\left(\delta_1^2\right)^N} (Nq)^{N-1} e^{-\frac{N}{\delta_1^2}q} \mathrm{d}q \right) \\ & + p_2 \left(1 - \int_{\mathcal{T}_{\mathrm{th}}^*}^{+\infty} \frac{N}{\Gamma(N)\left(\delta_2^2\right)^N} (Nq)^{N-1} e^{-\frac{N}{\delta_2^2}q} \mathrm{d}q \right), \end{aligned} \tag{23}$$

where the optimal detection threshold $\mathcal{T}_{\mathrm{th}}^*$ is determined by

$$\mathcal{T}_{\mathrm{th}}^* = \frac{1}{N} \frac{\delta_1^2 \delta_2^2}{\delta_2^2 - \delta_1^2} \ln\left(\frac{p_1}{p_2} \left(\frac{\delta_2^2}{\delta_1^2} \right)^N \right). \tag{24}$$

Proof: Please see Appendix C. ∎

Remark 3.5: Since $y_{\mathrm{R}}[n]$ is a zero mean variable, and then we have $\delta_k^2 = \mathbb{E}\left[|y_{\mathrm{R}}[n]|^2\right] \to \hat{\mathcal{Q}}_p$ when N is large enough. From (13) and (24), the mapping T_{ED} is determined by $T_{\mathrm{ED}}(x, y) = \frac{1}{N} \frac{xy}{y-x} \ln\left(\frac{p_1}{p_2} \left(\frac{y}{x} \right)^N \right)$. Consequently, when $p_1 = p_2 = 0.5$, the optimal detection threshold in practice becomes

$$\mathcal{T}_{\mathrm{th}}^* = \frac{\hat{\mathcal{Q}}_p(a_k = a_1)\hat{\mathcal{Q}}_p(a_k = a_2)}{\hat{\mathcal{Q}}_p(a_k = a_2) - \hat{\mathcal{Q}}_p(a_k = a_1)} \ln \frac{\hat{\mathcal{Q}}_p(a_k = a_2)}{\hat{\mathcal{Q}}_p(a_k = a_1)}. \tag{25}$$

It is obvious that the optimal detection threshold only relates to the average energy of the received signal samples, which can be estimated by $\hat{\mathcal{Q}}_p$.

IV. DETERMINISTIC JAMMING CASE

In the above discussions, we have analyzed the error performance of the AAJ scheme under the Gaussian jamming signal, which can be regarded as a type of random broadband jamming[6]. In this subsection, we investigate the BERs of the AAJ scheme under the deterministic jamming, which includes single-tone, multi-tone, narrowband, and broadband jamming signals. Moreover, the general expression of the system BER under the above five jamming cases is derived.

---

[6]The narrowband Gaussian jamming signal can be generated by a white Gaussian signal passing through a bandpass filter. However, the filtering operation brings correlation among the sampled symbols, which does not fit the signal model of this paper. Therefore, we will discuss this case in our next paper.

$$\mathcal{Q} = \underbrace{\frac{1}{N} \sum_{n=1}^{N} \left| h_1 h_2 a_k \sum_{j=1}^{J} a_j \cos[2\pi f_j n + \phi_j] + h_3 \sum_{j=1}^{J} a_j \cos[2\pi f_j(n - n_\tau) + \phi_j] \right|^2}_{\mathcal{Q}_{\mathrm{D},k}: \text{ Deterministic part}} + \underbrace{\frac{1}{N} \sum_{n=1}^{N} |Z_{\mathrm{R}}[n]|^2}_{\mathcal{Q}_{\mathrm{R},k}: \text{ Random part}}. \quad (30)$$

A. Single-Tone Jamming

The JN launches a single-tone jamming signal, i.e., a sinusoid signal with a certain frequency, which can be expressed as

$$X_{\mathrm{J}}(t) = a_j \cos(2\pi f_j t + \phi_j), \quad (26)$$

where a_j, f_j, and ϕ_j are the amplitude, the carrier frequency, and the initial phase of the jamming signal, respectively. From (4), the received signal after the sampling is given by

$$y_{\mathrm{R}}[n] = h_1 h_2 a_k a_j \cos[2\pi f_j n + \phi_j] + h_3 a_j \cos[2\pi f_j(n - n_\tau) + \phi_j] + Z_{\mathrm{R}}[n]. \quad (27)$$

B. Multi-Tone/Narrowband/Broadband Jamming

The deterministic multi-tone, narrowband, and broadband jamming signals can be regarded as a sum of sinusoid signals. The difference among these three jamming types are summarized as follows:

1) Multi-tone jamming: the frequencies of the multi-tone jamming signal can be arbitrarily distributed in the whole band.
2) Narrowband jamming: the frequencies of the narrowband jamming signal occupy a narrow frequency range.
3) Broadband jamming: the frequencies of the broadband jamming signal occupy a broadband frequency range.

Generally, the bandwidth of the narrowband jamming signal is less than 1% of that of the source signal while the bandwidth of the broadband jamming signal is larger than 10% of that of the source signal. All these three jamming signals can be expressed as

$$X_{\mathrm{J}}(t) = \sum_{j=1}^{J} a_j \cos(2\pi f_j t + \phi_j). \quad (28)$$

Consequently, the received signal after the sampling is given by

$$y_{\mathrm{R}}[n] = h_1 h_2 a_k \sum_{j=1}^{J} a_j \cos[2\pi f_j n + \phi_j] + h_3 \sum_{j=1}^{J} a_j \cos[2\pi f_j(n - n_\tau) + \phi_j] + Z_{\mathrm{R}}[n]. \quad (29)$$

Further, under the deterministic single-tone, multi-tone, narrowband, and broadband jamming cases, the general expression of the average energy for N received samples is given by (30), as shown at the top of this page.

C. General Expression of BER

It is worth noting that when N is large enough, the average energy of the deterministic signal part in (30), denoted by $\mathcal{Q}_{\mathrm{D},k}$, is close to a constant. The uncertainty of $\mathcal{Q}$ mainly comes from the noise part, denoted by $\mathcal{Q}_{\mathrm{R},k}$. According to *Lemma 3.2*, $\mathcal{Q}_{\mathrm{R},k}$ is a sum of squares of N complex Gaussian signals, with the following PDF

$$f_{\mathcal{Q}_{\mathrm{R},k}}(q) = \begin{cases} \frac{N}{\Gamma(N)(\sigma_{\mathrm{R}}^2)^N} (Nq)^{N-1} e^{-\frac{N}{\sigma_{\mathrm{R}}^2}q}, & q > 0, \\ 0, & \text{otherwise.} \end{cases} \quad (31)$$

Since $\mathcal{Q} = \mathcal{Q}_{\mathrm{D},k} + \mathcal{Q}_{\mathrm{R},k}$, we have

$$\begin{aligned} F_{\mathcal{Q}}(q) &= \Pr\{\mathcal{Q} \leq q\} \\ &= \Pr\{\mathcal{Q}_{\mathrm{R},k} \leq q - \mathcal{Q}_{\mathrm{D},k}\} \\ &= F_{\mathcal{Q}_{2,k}}(q - \mathcal{Q}_{\mathrm{D},k}). \end{aligned} \quad (32)$$

Therefore, the PDF of $\mathcal{Q}$ can be computed by

$$f_{\mathcal{Q}}(q) = \frac{\mathrm{d}F_{\mathcal{Q}}(q)}{\mathrm{d}q} = f_{\mathcal{Q}_{\mathrm{R},k}}(q - \mathcal{Q}_{\mathrm{D},k}). \quad (33)$$

By substituting $f_{\mathcal{Q}_{\mathrm{R},k}}(q)$ into (33), we have

$$f_{\mathcal{Q}}(q)$$
$$= \begin{cases} \frac{N}{\Gamma(N)(\sigma_{\mathrm{R}}^2)^N} (N(q - \mathcal{Q}_{\mathrm{D},k}))^{N-1} e^{-\frac{N}{\sigma_{\mathrm{R}}^2}(q - \mathcal{Q}_{\mathrm{D},k})}, & q > 0, \\ 0, & \text{otherwise.} \end{cases} \quad (34)$$

The minimum P_e and the corresponding optimal $\mathcal{T}_{\mathrm{th}}^*$ of the proposed AAJ scheme under the deterministic jamming case are summarized in the following proposition.

Proposition 4.1: The minimum BER of the proposed AAJ scheme under the deterministic jamming case is given by (35), as shown at the top of the next page, where the optimal detection threshold $\mathcal{T}_{\mathrm{th}}^*$ is determined by

$$\mathcal{T}_{\mathrm{th}}^* = \frac{\mathcal{Q}_{\mathrm{D},1} - \xi \mathcal{Q}_{\mathrm{D},2}}{1 - \xi}. \quad (36)$$

Here, $\mathcal{Q}_{\mathrm{D},1} < \mathcal{Q}_{\mathrm{D},2}$ and $\xi = \frac{p_2}{p_1} e^{\frac{N-1}{N}\left(\frac{\mathcal{Q}_{\mathrm{D},2} - \mathcal{Q}_{\mathrm{D},1}}{\sigma_{\mathrm{R}}^2}\right)}$.

Proof: The proof is similar to that of *Proposition 3.1*, and thus it is omitted for brevity. ∎

Although $\mathcal{Q}_{\mathrm{D},1}$ and $\mathcal{Q}_{\mathrm{D},2}$ in (36) cannot be derived directly, $\mathcal{Q}_{\mathrm{D},2} - \mathcal{Q}_{\mathrm{D},1}$ can be estimated by $\hat{\mathcal{Q}}_p(a_k = a_2)$ and $\hat{\mathcal{Q}}_p(a_k = a_1)$ such that $\mathcal{T}_{\mathrm{th}}^*$ can also be derived.

Notice that the BERs of the single-tone, multi-tone, narrowband, and broadband jamming (random and deterministic types) cases have a similar structure. Thus, we

$$P_e = p_1 \left(1 - \int_0^{\mathcal{T}_{\text{th}}^*} \frac{N}{\Gamma(N)\left(\sigma_{\text{R}}^2\right)^N} \left(N(q - \mathcal{Q}_{\text{D},1})\right)^{N-1} e^{-\frac{N}{\sigma_{\text{R}}^2}(q - \mathcal{Q}_{\text{D},1})} \mathrm{d}q \right)$$
$$+ p_2 \left(1 - \int_{\mathcal{T}_{\text{th}}^*}^{+\infty} \frac{N}{\Gamma(N)\left(\sigma_{\text{R}}^2\right)^N} \left(N(q - \mathcal{Q}_{\text{D},2})\right)^{N-1} e^{-\frac{N}{\sigma_{\text{R}}^2}(q - \mathcal{Q}_{\text{D},2})} \mathrm{d}q \right), \tag{35}$$

develop a general expression of the BER for the considered five jamming cases, i.e.,

$$P_e = \sum_{k=1}^K p_k \left(1 - \int_{\mathcal{I}_k} \frac{N}{\Gamma(N)A^N} \left(N(q - B)\right)^{N-1} e^{-\frac{N}{A}(q-B)} \mathrm{d}q \right). \tag{37}$$

1) When $A = \delta_k^2$ and $B = 0$, P_e is the BER of the random broadband jamming case.
2) When $A = \sigma_{\text{R}}^2$ and $B = \mathcal{Q}_{\text{D},k}$, P_e is the BER of the deterministic single-tone, multi-tone, narrow-band, or broadband jamming case.

Remark 4.1: Since the deterministic broadband, narrowband, and multi-tone jamming signals can be regarded as a sum of different single-tone jamming signals, the BER of the single-tone jamming case is generally lower than the other three cases. The reason is that the different single-tone jamming signals may cancel each other out, resulting in a decrease of signal strength. Therefore, under the same transmission power and channel conditions, the BER performances of the above four cases satisfy: $P_e^{\text{ST}} \leq P_e^{\text{MT}} \leq P_e^{\text{RB}} \leq P_e^{\text{BB,D}} \leq P_e^{\text{BB,R}}$, where P_e^{ST}, P_e^{MT}, P_e^{RB}, and $P_e^{\text{BB,D}}$ are the BERs of the deterministic single-tone, multi-tone, narrowband, and broadband jamming cases, respectively, and $P_e^{\text{BB,R}}$ is the BER of the random broadband jamming case.

V. ASYMPTOTIC ANALYSIS

To uncover more insights on the error performance of the AAJ enabled anti-jamming communications, we investigate the asymptotic behaviors of the BER, where the power of the jamming signal and the number of samples go to infinity. Here, we define the JNR as $P_{\text{J}}/\sigma_{\text{R}}^2$ to characterize the effect of the power of the jamming signal.

A. The High JNR Case

Recalling (5), we can rewrite the SINR at the RN as follows:

$$\text{SINR} = \frac{|h_1|^2 |h_2|^2 |a_k|^2}{|h_3|^2 + \sigma_{\text{R}}^2/P_{\text{J}}}. \tag{38}$$

It can be observed from (38) that the SINR monotonically increases with the JNR, meaning that the more power the JN uses, the higher SINR the RN can get, i.e., the better BER the system can obtain.

Proposition 5.1: If a_k is fixed and $P_{\text{J}}/\sigma_{\text{R}}^2 \to \infty$, SINR increases to $\left(|h_1|^2 |h_2|^2 |a_k|^2\right)/|h_3|^2$ at the following rate

$$\text{SINR} \approx O(1). \tag{39}$$

Proof: When $P_{\text{J}}/\sigma_{\text{R}}^2 \to \infty$, $\sigma_{\text{R}}^2/P_{\text{J}} \to 0$. From (38), we have

$$\text{SINR}|_{P_{\text{J}}/\sigma_{\text{R}}^2 \to \infty} \longrightarrow \frac{|h_1|^2 |h_2|^2 |a_k|^2}{|h_3|^2}, \tag{40}$$

which is $O(1)$. ∎

Remark 5.1: Based on the above analysis, we can conclude that the SINR increases and approaches the upper bound with the increase of the JNR. In this case, the BER decreases and approaches the lower bound with the increase of the JNR. In other words, there will be a BER floor with the increasing JNR. In addition, the lower bound of BER is determined by the channel conditions and the transmission power of the TN.

Remark 5.2: As we know, SINR is determined by the ratio of the strength of desired signal to the variances of jamming signal and noise. The SINR expression (38) holds when $X_{\text{J}}[n]$ is a random signal. If $X_{\text{J}}[n]$ is the deterministic single-tone, multi-tone, narrowband, or broadband jamming signal, the variance of the jamming signal $\text{Var}\left[X_{\text{J}}[n]\right] = 0$. Therefore, the SINRs of the above four deterministic jamming cases are given by

$$\text{SINR} = \frac{|h_1|^2 |h_2|^2 |a_k|^2 P_{\text{J}}}{\sigma_{\text{R}}^2}. \tag{41}$$

Unlike the random broadband jamming case, the power of the jamming signal P_{J} in (41) is not in the denominator of the SINR when the JN launches the deterministic jamming signals. In other words, the SINR monotonically increases with P_{J}, i.e., the BER monotonically decreases with P_{J} under the deterministic jamming cases.

B. The High Sampling Rate Case

We now look into the asymptotic regime, where the number of samples N is large during one symbol, i.e., the high sampling rate. It is observed from (18) that $|y_{\text{R}}[n]|^2$ is a central chi-square random variable with two degrees of freedom, which follows $\left|\sqrt{2}y_{\text{R}}[n]/\delta_k\right|^2 \sim \mathcal{X}^2(2)$. From the statistical property of the chi-square distribution, the mean and variance of $|y_{\text{R}}[n]|^2$ are δ_k^2 and δ_k^4, respectively. Consequently, $\mathcal{Q} = \frac{1}{N}\sum_{n=1}^N |y_{\text{R}}[n]|^2$ is a sum of N independent identical distributed central chi-square variables with two degrees of freedom, and we can derive the following proposition:

Proposition 5.2: For sufficiently large N, the average energy of the sampled signal $\mathcal{Q}$ approximately follows the Gaussian distribution, i.e.,

$$\mathcal{Q} \sim \mathcal{N}\left(\delta_k^2, \delta_k^4/N\right). \tag{42}$$

Proof: According to the central limit theorem [24], for sufficiently large N, we have

$$\frac{\frac{1}{N}\sum_{n=1}^{N}|y_{\mathrm{R}}[n]|^2-\mu}{\sigma/\sqrt{N}}\sim\mathcal{N}(0,1)$$

$$\longrightarrow \mathcal{Q}=\frac{1}{N}\sum_{n=1}^{N}|y_{\mathrm{R}}[n]|^2\sim\mathcal{N}(\mu,\sigma^2/N),\qquad(43)$$

where $\mu=\sigma=\delta_k^2$. Hence, *Proposition 5.2* is proved. ∎

Therefore, the BER in (23) can be rewritten as

$$P_e=p_1 P_e(a_1)+p_2 P_e(a_2)$$

$$\approx p_1\int_{\mathcal{T}_{\mathrm{th}}^*}^{+\infty}\frac{1}{\sqrt{2\pi\delta_1^4/N}}e^{-\frac{\left(q-\delta_1^2\right)^2}{2\delta_1^4/N}}\,\mathrm{d}q$$

$$+p_2\int_0^{\mathcal{T}_{\mathrm{th}}^*}\frac{1}{\sqrt{2\pi\delta_2^4/N}}e^{-\frac{\left(q-\delta_2^2\right)^2}{2\delta_2^4/N}}\,\mathrm{d}q$$

$$=p_1 Q\left(\frac{\mathcal{T}_{\mathrm{th}}^*-\delta_1^2}{\delta_1^2/\sqrt{N}}\right)+p_2 Q\left(\frac{\delta_2^2-\mathcal{T}_{\mathrm{th}}^*}{\delta_2^2/\sqrt{N}}\right),\qquad(44)$$

where $Q(x)=\frac{1}{\sqrt{2\pi}}\int_x^\infty e^{-\frac{1}{2}x^2}\,\mathrm{d}x$ is the Q-function.

VI. CAPACITY ANALYSIS

In this section, we first derive the PDF of the received signal and then calculate the information entropies. Subsequently, the channel capacity of the considered jamming channel under the AAJ scheme is derived by maximizing the mutual information over the distribution of the TN transmitted signals.

Based on the definition of the channel capacity in information theory [23], the channel capacity of the jamming channel can be given by

$$\mathcal{C}=\max_{p(a_k)}\mathrm{I}(Y_{\mathrm{R}};A)=\max_{p(a_k)}\mathrm{H}(Y_{\mathrm{R}})-\mathrm{H}(Y_{\mathrm{R}}|A),\qquad(45)$$

where $\mathrm{I}(Y_{\mathrm{R}};A)$ is the average mutual information between the input A and the output Y_{R}. $\mathrm{H}(Y_{\mathrm{R}})$ and $\mathrm{H}(Y_{\mathrm{R}}|A)$ are information entropies defined as

$$\mathrm{H}(Y_{\mathrm{R}})=-\int_{-\infty}^{\infty}f(y_{\mathrm{R}})\log f(y_{\mathrm{R}})\mathrm{d}y_{\mathrm{R}},\qquad(46)$$

$$\mathrm{H}(Y_{\mathrm{R}}|A)=-\int_{-\infty}^{\infty}\int_{-\infty}^{\infty}f(y_{\mathrm{R}},a_k)\log f_{Y_{\mathrm{R}}|A}(y_{\mathrm{R}}|a_k)\mathrm{d}a_k\mathrm{d}y_{\mathrm{R}},\qquad(47)$$

respectively.

To derive the channel capacity of the jamming channel with the AAJ scheme, we first derive the PDF of Y_{R} and $Y_{\mathrm{R}}|A$, i.e., $f(y_{\mathrm{R}})$ and $f_{Y_{\mathrm{R}}|A}(y_{\mathrm{R}}|a_k)$, respectively. From (18), the PDF of $Y_{\mathrm{R}}|A$ under the Gaussian channel can be given by

$$f_{Y_{\mathrm{R}}|A}(y_{\mathrm{R}}|a_k)=\frac{1}{\sqrt{2\pi\delta_k^2}}e^{-\frac{y_{\mathrm{R}}^2}{2\delta_k^2}}.\qquad(48)$$

Next, we compute the PDF of Y_{R}. According to the relationship between the marginal PDF and joint PDF, $f(y_{\mathrm{R}})$

can be computed as

$$f(y_{\mathrm{R}})=\sum_{k=1}^2 f(y_{\mathrm{R}},a_k)$$

$$=\sum_{k=1}^2 f_{Y_{\mathrm{R}}|A}(y_{\mathrm{R}}|a_k)p(a_k).\qquad(49)$$

Proposition 6.1: Considering the binary input at the TN, i.e., $p_1=p$ and $p_2=1-p$, the closed-form of the mutual information for the jamming channel with the AAJ scheme is given by

$$\mathrm{I}(Y_{\mathrm{R}};A)=-\int_{-\infty}^{\infty}(p\Phi_1+(1-p)\Phi_2)\log(p\Phi_1+(1-p)\Phi_2)\,\mathrm{d}y_{\mathrm{R}}$$

$$-\frac{1}{2}p\log 2\pi e\delta_1^2-\frac{1}{2}(1-p)\log 2\pi e\delta_2^2,\qquad(50)$$

where $\Phi_1=\frac{1}{\sqrt{2\pi\delta_1^2}}e^{-\frac{y_{\mathrm{R}}^2}{2\delta_1^2}}$ and $\Phi_2=\frac{1}{\sqrt{2\pi\delta_2^2}}e^{-\frac{y_{\mathrm{R}}^2}{2\delta_2^2}}$.

Proof: Please see Appendix D. ∎

Therefore, the channel capacity of the jamming channel can be reformulated as

$$\mathcal{C}=\max_p \mathrm{I}(Y_{\mathrm{R}};A).\qquad(51)$$

The optimal p and the corresponding channel capacity are summarized in the following proposition.

Proposition 6.2: The channel capacity of the jamming channel is given by

$$\mathcal{C}=-\int_{-\infty}^{\infty}(p^*\Phi_1+(1-p^*)\Phi_2)\log(p^*\Phi_1+(1-p^*)\Phi_2)\,\mathrm{d}y_{\mathrm{R}}$$

$$-\frac{1}{2}p^*\log 2\pi e\delta_1^2-\frac{1}{2}(1-p^*)\log 2\pi e\delta_2^2,\qquad(52)$$

where p^* is the optimal input distribution, which is determined by

$$\int_{-\infty}^{\infty}(\Phi_2-\Phi_1)\log(p\Phi_1+(1-p)\Phi_2)\mathrm{d}y_{\mathrm{R}}=\frac{1}{2}\log\frac{\delta_1^2}{\delta_2^2}.\quad(53)$$

Proof: Please see Appendix E. ∎

In order to solve the problem (51) to derive the precise value of p^*, we denote $\eta(p,y_{\mathrm{R}})=(\Phi_2-\Phi_1)\log(p\Phi_1+(1-p)\Phi_2)$. Therefore, the first-order derivative of $\int_{-\infty}^{\infty}\eta(p,y_{\mathrm{R}})\mathrm{d}y_{\mathrm{R}}$ can be computed as

$$\frac{\mathrm{d}\int_{-\infty}^{\infty}\eta(p,y_{\mathrm{R}})\mathrm{d}y_{\mathrm{R}}}{\mathrm{d}p}=-\int_{-\infty}^{\infty}\frac{(\Phi_1-\Phi_2)^2}{\ln 2\,(p\Phi_1+(1-p)\Phi_2)}\mathrm{d}y_{\mathrm{R}}.\qquad(54)$$

Note that $\Phi_1\neq\Phi_2$ and $(p\Phi_1+(1-p)\Phi_2)>0$. Thus, $\mathrm{d}\int_{-\infty}^{\infty}\eta(p,y_{\mathrm{R}})\mathrm{d}y_{\mathrm{R}}/\mathrm{d}p<0$, which means that $\int_{-\infty}^{\infty}\eta(p,y_{\mathrm{R}})\mathrm{d}y_{\mathrm{R}}$ monotonically decreases over p. Therefore, the solution of the problem (51), i.e., $\int_{-\infty}^{\infty}\eta(p,y_{\mathrm{R}})\mathrm{d}y_{\mathrm{R}}-\frac{1}{2}\log\frac{\delta_1^2}{\delta_2^2}=0$, can be found by bisection search in $[0,1]$.

VII. NUMERICAL RESULTS

In this section, both the BER and channel capacity performances of the AAJ scheme are evaluated with numerical simulation results. We define the SNR at the RN as P_A/σ_R^2, where P_A is the average power of the desired signal $A(t)$. Unless specifically stated, we assume that the JN launches random broadband jamming signal, i.e., CSCG signal. Furthermore, it is assumed that there exists a dominant line-of-sight (LOS) path among each of the following three links, i.e., JT, TR, and JR links. Therefore, we consider Rician fading models throughout this section. The channel coefficients of the JT link, the TR link, and the JR link are denoted by $h_1 = \sqrt{\frac{\mathcal{K}}{\mathcal{K}+1}}\overline{h}_1 + \sqrt{\frac{1}{\mathcal{K}+1}}\hat{h}_1$, $h_2 = \sqrt{\frac{\mathcal{K}}{\mathcal{K}+1}}\overline{h}_2 + \sqrt{\frac{1}{\mathcal{K}+1}}\hat{h}_2$, and $h_3 = \sqrt{\frac{\mathcal{K}}{\mathcal{K}+1}}\overline{h}_3 + \sqrt{\frac{1}{\mathcal{K}+1}}\hat{h}_3$, respectively, where the Rician factor $\mathcal{K} = 10$. $\overline{h}_1$, $\overline{h}_2$, and $\overline{h}_3$ are the LOS components, which are all set to be 1. $\hat{h}_1$, $\hat{h}_2$, and $\hat{h}_3$ are the non-line-of-sight (NLOS) components, which are generated by the i.i.d. complex Gaussian distribution $\mathcal{CN}(0,1)$. The length of the preamble sequence is set to be $m = 10$. The variance of the CSCG noise is normalized to 1, i.e., $\sigma_R^2 = 1$. A total of 10^7 Monte-Carlo runs are averaged to show the results.
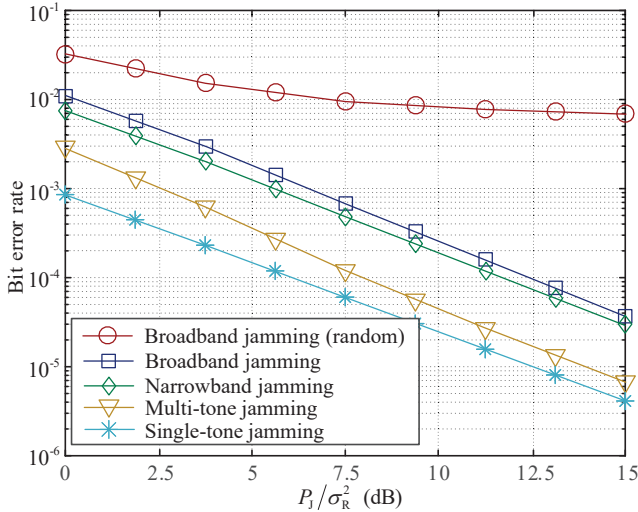

Fig. 2. BER comparison among different unmodulated jamming signals ($P_A/\sigma_R^2 = 5$ dB, $N = 10$).

Figure 2 shows how the BER performance changes with the JNR under different unmodulated jamming signals. Specifically, the broadband jamming signal (random) is generated by a band-limited CSCG signal that occupies a bandwidth of 10 MHz with the center frequency 100 MHz; the broadband jamming signal (deterministic) is a sum of sinusoid signals that also constitutes a bandwidth of 10 MHz with the center frequency 100 MHz; the narrowband jamming is a sum of sinusoid signals that constitutes a bandwidth of 100 KHz with the center frequency 100 MHz; the multi-tone jamming signal is comprised of five sinusoid signals at frequencies $\{95, 97.5, 100, 102.5, 105\}$ MHz; and the single-tone jamming signal is a sinusoid signal at the frequency of 100 MHz. The bandwidth of the baseband
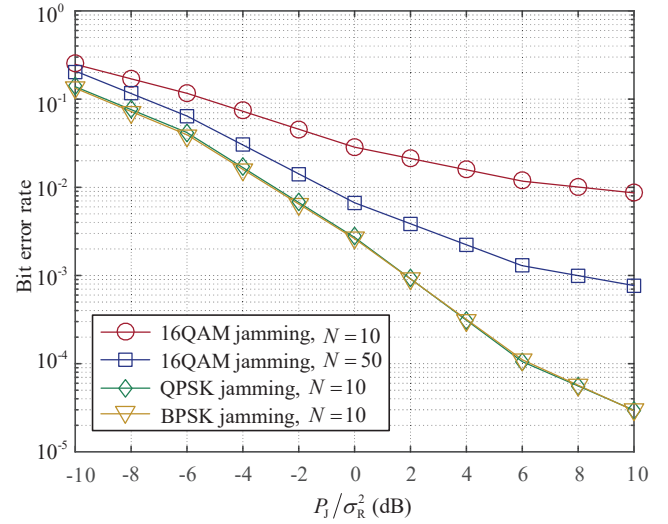

Fig. 3. BER comparison among different modulated jamming signals ($P_A/\sigma_R^2 = 5$ dB).

signal is 10 MHz. The SNR is set to be $P_A/\sigma_R^2 = 5$ dB. The number of samples collected during one symbol is set to be $N = 10$. From the figure, we can observe that the AAJ scheme works well even under different jamming attacks. More importantly, the BERs of the considered jamming cases are all monotonically decreasing with the JNR, i.e., the higher power the jammer uses, the better BER performance we can get, which is a great advantage as compared with the existing anti-jamming schemes. As shown in the previous analysis, the BER of the broadband jamming (random) case is floored with the increase of the JNR. In addition, the BER of the broadband jamming (random) case is the worst due to the fact that Gaussian signal is a random signal while the other four cases can be regarded as deterministic ones, which coincides with our analysis in Section IV and Section V.

Figure 3 shows the system BER performances under different modulated jamming signals, i.e., BPSK, QPSK, and 16QAM (jamming types). The bandwidth of the jamming signal is 10 MHz and the carrier frequency is 100 MHz. The bandwidth of the baseband signal is 1 MHz. The SNR is set to be $P_A/\sigma_R^2 = 5$ dB. It is observed that the BERs under the modulated jamming signals still monotonically decrease with the JNR. In the case of the sampling rate $N = 10$, the BER of the 16QAM jamming case performs worst due to the fact that a higher order modulation incurs higher uncertainty of the jamming power. However, one can see that the BER gets improved when N is increased to 50. In addition, the BER of the BPSK jamming case is close to that of the QPSK one. The reason is that the envelope of the phase modulated signal is constant, and thus the energy levels of the BPSK and QPSK jamming signals are the same, i.e., the BER performances of these two cases are equivalent under the energy detection criterion.

Figure 4 illustrates how the BER performance changes with the JNR under different anti-jamming schemes. The broadband (fullband) jamming attack, i.e., CSCG signal with $\mathcal{CN}(0, P_J)$, is adopted in this simulation. For a fair
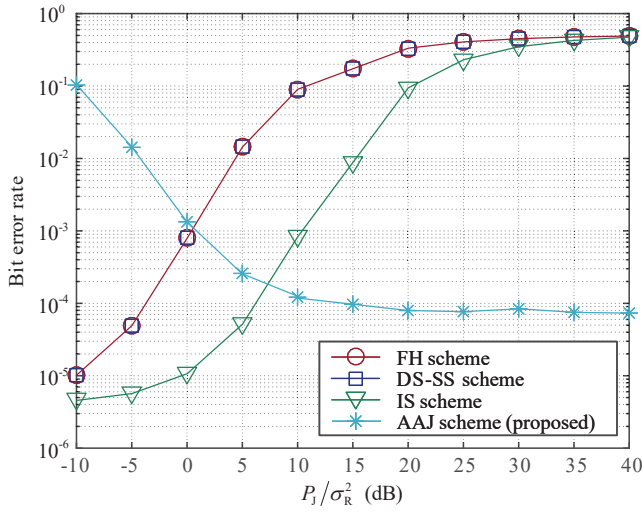
Fig. 4. BER comparison among different anti-jamming schemes ($E_\mathrm{b}/N_0 = 10$ dB, $N = 8$).
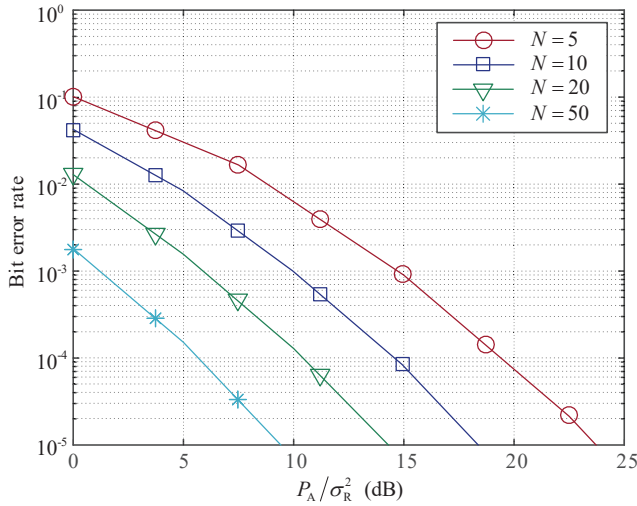

Fig. 5. BER comparison with different sampling rate ($P_\mathrm{J}/\sigma_\mathrm{R}^2 = 10$ dB).

comparison, the SNR per bit, also know as E_b/N_0 (ratio of the energy per bit to the noise power spectral density), is set to be 10 dB. The spread factor in the DS-SS and FH schemes are both set to be 8. Likewise, we adopt the number of samples collected during one symbol as $N = 8$. Since the conventional anti-jamming schemes require the instantaneous CSI, the channel coefficients are all set to be 1, i.e., $h_1 = h_2 = h_3 = 1$. From the figure, it can be observed that the BER under our proposed AAJ scheme decreases with the JNR while those of the existing schemes increase with the JNR. This is because the jamming signal is used as a carrier of the useful messages in the AAJ scheme, i.e., it can enhance the transmission of the TR link. When the JNR $P_\mathrm{J}/\sigma_\mathrm{R}^2 = 40$ dB, the BER of the AAJ scheme is about 7.38×10^{-5}. In this case, however, the BERs of the other schemes decrease to 0.5, thus failing to decode out any meaningful messages.

Figure 5 illustrates the BER performances of the different

numbers of samples, N. The JNR is set to be $P_\mathrm{J}/\sigma_\mathrm{R}^2 = 10$ dB. It is observed that the BER of the AAJ scheme significantly decreases with N. Therefore, one can not only increase the SNR but also the sampling rate to improve the transmission reliability of the legitimate communication. In this system, since the jamming signal is unknown, it is desirable to increase the interval of one symbol due to the fact that the longer the interval of one symbol is, the average energy of one symbol approaches to a constant. In other words, the bandwidth of the legitimate transmission should be narrower than the jamming signal even though it may decrease the transmission rate. Therefore, there is a tradeoff between the transmission rate and the BER performance in the AAJ scheme.
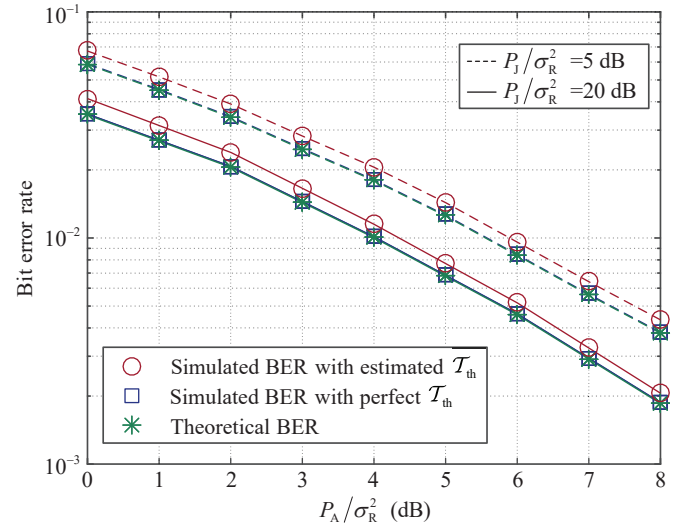

Fig. 6. BER comparison with the simulated and theoretical results ($m = 10$, $N = 10$).

The simulated and theoretical BERs are compared in Fig. 6. In this figure, $N = 10$. For the case of the simulated BER with the estimated $\mathcal{T}_\mathrm{th}$, the length of the preamble sequence $m = 10$; For the case of the simulated BER with the perfect $\mathcal{T}_\mathrm{th}$, the detection threshold $\mathcal{T}_\mathrm{th}$ is perfect estimated, i.e., $\mathcal{T}_\mathrm{th}^*$ is known. It is observed that the simulated BER coincides with the theoretical result if $\mathcal{T}_\mathrm{th}^*$ is known. Even when we use short preamble sequences, the BER is still close to the case where $\mathcal{T}_\mathrm{th}$ is perfectly known, i.e., the system can still achieve a good BER performance.

The relationship between the mutual information and the input distribution for the Gaussian jamming channel is shown in Fig. 7. In this simulation, the JNR is set to be $P_\mathrm{J}/\sigma_\mathrm{R}^2 = 10$ dB, whereas the SNRs are drawn from $\{0, 5, 10, 20\}$ dB. It is obvious that the mutual information between Y_R and A is a concave function over the input distribution, and there is only one maximum value for $p \in [0, 1]$, thus verifying our previous analysis. It is also interesting to observe that the optimal input distribution approaches a uniform distribution, i.e., $p = 0.5$, when the SNR increases. In addition, it is shown that the mutual information increases with the SNR, and thus we can still increase the SNR to improve the transmission performance.
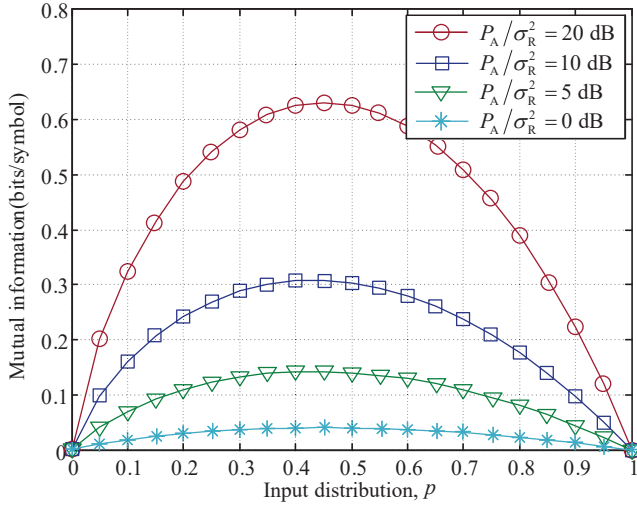
Fig. 7. Mutual information *v.s.* input distribution in the jamming channel under the AAJ scheme.
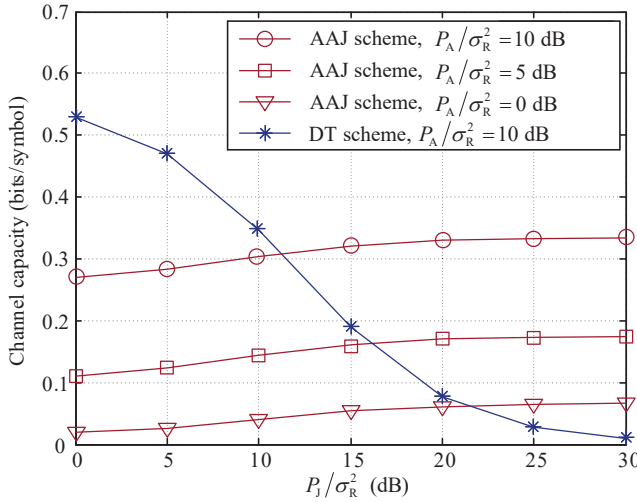

Fig. 8. Channel capacity *v.s.* JNR.

Figure 8 shows the relationship between the channel capacity and the JNR of the AAJ scheme. From the figure, it can be observed that the channel capacity of the DT scheme decreases with the JNR while the ones for the AAJ scheme increase with the JNR. For the SNR $P_A/\sigma_R^2 = 10$ dB, when the JNR is relatively large, i.e., $P_J/\sigma_R^2 > 11.8$ dB, the AAJ scheme begins to exceed the DT one, meaning that the proposed AAJ scheme has a great advantage in the strong jamming signal case. In addition, the channel capacity monotonically increases with the SNR.

VIII. CONCLUSIONS AND FUTURE WORKS

In this paper, we have proposed a novel AAJ scheme for a jammed channel to maintain the legitimate communications between the TN and RN. By exploiting the JM method, the TN is able to re-modulate the jamming signals with its own messages for new anti-jamming communications. Focusing on the binary input at the TN, we have computed the

minimum average BER of the AAJ scheme and the corresponding optimal detection threshold, where the single-tone, multi-tone, narrowband, and broadband jamming signals were all considered. Then, the semi-closed forms of both the channel capacity and the corresponding optimal input distribution of the jammed channel with the AAJ scheme have been derived. Simulation results have been presented to show that the proposed anti-jamming scheme is effective even under the extremely strong and/or broadband jamming attacks. When the JNR is relatively high, the AAJ scheme outperforms the DT one in terms of the channel capacity. Furthermore, we have revealed that there exists a BER floor with increasing JNR through the asymptotic analysis. Finally, it is interesting to point out that the RN enjoys increasingly improved error rate performance for larger JNR, making it an ideal anti-jamming candidate when the jamming attacks are hard to be suppressed.

As a pioneering work, we believe that the proposed AAJ scheme provides a new solution for anti-jamming communications. In the future, we plan to expand our work from the following perspectives: 1) Mode selection: when the jamming signal is weak or absent, the AAJ scheme may need more power to guarantee the quality of the legitimate communications. It is worthy to develop a hybrid transmission scheme, e.g., how to select the AAJ, DT, or conventional scheme according to the different jamming cases; 2) Trade-off between the BER and the transmission rate: as mentioned in Section VII, a longer symbol interval brings a lower BER but leads to reduced transmission rate at the same time. It is therefore of great interest to investigate the relationship between BER and transmission rate; 3) Multi-antenna case: in the present research, the TN and RN are equipped with one single antenna. Since multiple antennas can provide a higher diversity gain, further research is needed to study the performance limits of the AAJ scheme in the multi-antenna case; 4) Optimal detection method: optimal/enhanced detection schemes for the proposed AAJ scheme are a vital and interesting topic. For example, maximum likelihood (ML) detection and independent component analysis (ICA), are worthy of a close investigation; 5) Power-varying jamming cases: in practice, the jammer does not need to always send signals with fixed power, and thus the performance analysis of the AAJ scheme under the power-varying jamming cases will be studied in our future work.

APPENDIX A
PROOF OF *Lemma 3.1*

According to probability theory and statistics [24], the chi-square distribution with l degrees of freedom is defined as the distribution of a sum of squares of l independent

standard normal random variables. Note that $y_{\text{R}}[n]$ is a CSCG variable with zero mean and variance δ_k^2, i.e., $y_{\text{R}}[n] = r + jr$, where $r \sim \mathcal{N}\left(0, \delta_k^2/2\right)$. Therefore, the average energy of one symbol, $\mathcal{Q} = \frac{1}{N}\sum_{n=1}^{N}|y_{\text{R}}[n]|^2 = \sum_{n=1}^{2N}(r/\sqrt{N})^2$, can be regarded as a sum of squares of $2N$ CSCG variables with distribution $r/\sqrt{N} \sim \mathcal{CN}(0, \delta_k^2/2N)$.

By normalizing the variance of $r/\sqrt{N}$, we have

$$
\mathcal{Q} = \frac{1}{N}\sum_{n=1}^{N}|y_{\text{R}}[n]|^2
$$
$$
\longrightarrow \frac{2N}{\delta_k^2}\mathcal{Q} = \sum_{n=1}^{N}\left|\frac{\sqrt{2}y_{\text{R}}[n]}{\delta_k}\right|^2, \tag{55}
$$

where $\sqrt{2}r/\delta_k$ satisfies the standard normal distribution, i.e.,

$$
\frac{\sqrt{2}}{\delta_k}r \sim \mathcal{N}(0,1). \tag{56}
$$

Then, we can further derive the following result

$$
\left|\frac{\sqrt{2}y_{\text{R}}[n]}{\delta_k}\right|^2 \sim \mathcal{X}^2(2)
$$
$$
\longrightarrow \sum_{n=1}^{N}\left|\frac{\sqrt{2}y_{\text{R}}[n]}{\delta_k}\right|^2 \sim \mathcal{X}^2(2N). \tag{57}
$$

Therefore, $(2N\mathcal{Q})/\delta_k^2$ is a chi-square distributed variable with $2N$ degrees of freedom.

Hence, *Lemma 3.1* is proved.

APPENDIX B
THE PROOF OF *Lemma 3.2*

From *Lemma 3.1*, it is found out that $X = (2N\mathcal{Q})/\delta_k^2$ is a chi-square distributed variable with $2N$ degrees of freedom, whose PDF is given by

$$
f_X(x) = \begin{cases} \frac{1}{2^N\Gamma(N)}(x)^{N-1}e^{-\frac{x}{2}}, & x > 0, \\ 0, & \text{otherwise.} \end{cases} \tag{58}
$$

Next, we compute the PDF of $\mathcal{Q}$ according to the property of a function of random variables. Denote $F_X(x)$ and $F_{\mathcal{Q}(a_k)}(q)$ as the cumulative density functions (CDF) of X and $\mathcal{Q}$.

Therefore, we have $\mathcal{Q} = \left(\delta_k^2 X\right)/2N$, and then $F_{\mathcal{Q}}(q)$ is given by

$$
F_{\mathcal{Q}}(q) = \Pr\{\mathcal{Q} \le q\}
$$
$$
= \Pr\left\{X \le \frac{2Nq}{\delta_k^2}\right\}
$$
$$
= F_X\left(\frac{2Nq}{\delta_k^2}\right). \tag{59}
$$

By computing the first-order derivative of the CDF (59), we can derive its PDF as follows

$$
f_{\mathcal{Q}}(q) = \frac{dF_{\mathcal{Q}}(q)}{dq} = \frac{2N}{\delta_k^2}f_X\left(\frac{2Nq}{\delta_k^2}\right). \tag{60}
$$

Therefore, by substituting (58) into (60), we have

$$
f_{\mathcal{Q}}(q) = \begin{cases} \frac{N}{\Gamma(N)\left(\delta_k^2\right)^N}(Nq)^{N-1}e^{-\frac{N}{\delta_k^2}q}, & q > 0, \\ 0, & \text{otherwise.} \end{cases} \tag{61}
$$

Hence, *Lemma 3.2* is proved.

APPENDIX C
THE PROOF OF *Proposition 3.1*

To compute the minimum average BER of the energy detection under the AAJ scheme, we first need to determine the optimal detection threshold.

First, by substituting the PDF $f_{\mathcal{Q}}(q)$ into (16), the BER can be rewritten as

$$
P_e = \sum_{k=1}^{2}p_k\left(1 - \int_{\mathcal{I}_k}f_{\mathcal{Q}}(q)dq\right)
$$
$$
= p_1\left(1 - \int_0^{\mathcal{T}_{\text{th}}^*}\frac{N}{\Gamma(N)\left(\delta_1^2\right)^N}(Nq)^{N-1}e^{-\frac{N}{\delta_1^2}q}dq\right)
$$
$$
+ p_2\left(1 - \int_{\mathcal{T}_{\text{th}}^*}^{+\infty}\frac{N}{\Gamma(N)\left(\delta_2^2\right)^N}(Nq)^{N-1}e^{-\frac{N}{\delta_2^2}q}dq\right). \tag{62}
$$

Then, we compute the first-order derivative of P_e, i.e.,

$$
\frac{dP_e}{d\mathcal{T}_{\text{th}}} = p_1 \times \frac{N}{\Gamma(N)\left(\delta_1^2\right)^N}(N\mathcal{T}_{\text{th}})^{N-1}e^{-\frac{N}{\delta_1^2}\mathcal{T}_{\text{th}}}
$$
$$
- p_2 \times \frac{N}{\Gamma(N)\left(\delta_2^2\right)^N}(N\mathcal{T}_{\text{th}})^{N-1}e^{-\frac{N}{\delta_2^2}\mathcal{T}_{\text{th}}}. \tag{63}
$$

When $dP_e/d\mathcal{T}_{\text{th}} = 0$, by performing some algebraic manipulation, we can derive the expression of the optimal detection threshold $\mathcal{T}_{\text{th}}^*$, as presented in (24).

Therefore, the minimum average BER of the energy detection under the AAJ scheme is derived and given in (23).

Hence, *Proposition 3.1* is proved.

APPENDIX D
PROOF OF *Proposition 6.1*

According to (45), to derive the mutual information for the jamming channel, we need to compute the information entropies $\text{H}(Y_{\text{R}})$ and $\text{H}(Y_{\text{R}}|A)$.

From (47) and (48), the information entropy of $Y_{\text{R}}|A = a_k$ can be computed as

$$
\text{H}(Y_{\text{R}}|A = a_k)
$$
$$
= -\int_{-\infty}^{\infty}f_{Y_{\text{R}}|A}(y_{\text{R}}|a_k)\log f_{Y_{\text{R}}|A}(y_{\text{R}}|a_k)dy_{\text{R}}
$$
$$
= -\int_{-\infty}^{\infty}\frac{1}{\sqrt{2\pi\delta_k^2}}e^{-\frac{y_{\text{R}}^2}{2\delta_k^2}}\log\left(\frac{1}{\sqrt{2\pi\delta_k^2}}e^{-\frac{y_{\text{R}}^2}{2\delta_k^2}}\right)dy_{\text{R}}
$$
$$
= -\int_{-\infty}^{\infty}\frac{1}{\sqrt{2\pi\delta_k^2}}e^{-\frac{y_{\text{R}}^2}{2\delta_k^2}}\left(\log\frac{1}{\sqrt{2\pi\delta_k^2}} - \frac{y_{\text{R}}^2\log e}{2\delta_k^2}\right)dy_{\text{R}}
$$
$$
= \frac{1}{2}\log 2\pi\delta_k^2 + \frac{\mathbb{E}\left[Y_{\text{R}}^2\right]\log e}{2\delta_k^2}
$$
$$
= \frac{1}{2}\log 2\pi e\delta_k^2. \tag{64}
$$

Further, the information entropy of $Y_\mathrm{R}|A$ is given by

$$\mathrm{H}(Y_\mathrm{R}|A) = \sum_{k=1}^{2} p(a_k)\mathrm{H}(Y_\mathrm{R}|A=a_k)$$

$$= \frac{1}{2}\sum_{k=1}^{2} p(a_k)\log 2\pi e\delta_k^2. \qquad (65)$$

Likewise, from (46), (48), and (49), the information entropy of Y_R is given by

$$\mathrm{H}(Y_\mathrm{R}) = -\int_{-\infty}^{\infty} f(y_\mathrm{R})\log f(y_\mathrm{R})\mathrm{d}y_\mathrm{R}$$

$$= -\int_{-\infty}^{\infty}\sum_{k=1}^{2} f_{Y_\mathrm{R}|A}(y_\mathrm{R}|a_k)p(a_k)$$

$$\times \log\left(\sum_{k=1}^{2} f_{Y_\mathrm{R}|A}(y_\mathrm{R}|a_k)p(a_k)\right)\mathrm{d}y_\mathrm{R}$$

$$= -\int_{-\infty}^{\infty}\sum_{k=1}^{2} p(a_k)\frac{1}{\sqrt{2\pi\delta_k^2}}e^{-\frac{y_\mathrm{R}^2}{2\delta_k^2}}$$

$$\times \log\left(\sum_{k=1}^{2} p(a_k)\frac{1}{\sqrt{2\pi\delta_k^2}}e^{-\frac{y_\mathrm{R}^2}{2\delta_k^2}}\right)\mathrm{d}y_\mathrm{R}. \qquad (66)$$

Substituting (65) and (66) into (45), and thus the mutual information between Y_R and A for the considered jamming channel with the AAJ scheme is given in (52).

Therefore, this proposition is proved.

APPENDIX E
PROOF OF *Proposition 6.2*

To derive the channel capacity, i.e., the maximum mutual information $\mathrm{I}(Y_\mathrm{R};A)$, we first compute the first-order derivative of $\mathrm{I}(Y_\mathrm{R};A)$ as follows

$$\frac{\mathrm{dI}(Y_\mathrm{R};A)}{\mathrm{d}p}$$

$$= -\int_{-\infty}^{\infty}(\Phi_1-\Phi_2)\log(p\Phi_1+(1-p)\Phi_2)+\frac{1}{\ln 2}(\Phi_1-\Phi_2)\mathrm{d}y_\mathrm{R}$$

$$- \frac{1}{2}\log 2\pi e\delta_1^2 + \frac{1}{2}\log 2\pi e\delta_2^2$$

$$= -\int_{-\infty}^{\infty}(\Phi_1-\Phi_2)\log(p\Phi_1+(1-p)\Phi_2)\mathrm{d}y_\mathrm{R} - \frac{1}{2}\log\frac{\delta_1^2}{\delta_2^2}. \qquad (67)$$

Since $\mathrm{I}(Y_\mathrm{R};A)$ is continuous and bounded for $p\in[0,1]$, there must exist a maximum value in the feasible set. Moreover, $\mathrm{I}(Y_\mathrm{R};A)|_{p=0} = \mathrm{I}(Y_\mathrm{R};A)|_{p=1} = 0$ and $\frac{\mathrm{dI}(Y_\mathrm{R};A)}{\mathrm{d}p}|_{p=0} > 0$, and thus the maximum $\mathrm{I}(Y_\mathrm{R};A)$ is achieved at the stationary point of the objective function in (51), which is equivalent to the root of equation (67), i.e., $\mathrm{dI}(Y_\mathrm{R};A)/\mathrm{d}p = 0$.

Therefore, the mutual information of the jamming channel achieves the maximum value when $p_1 = p^*$ and $p_2 = 1 - p^*$.

Hence, *Proposition 6.2* is proved.

REFERENCES

[1] X. Wang *et al.*, "Dynamic spectrum anti-jamming communications: challenges and opportunities," *IEEE Commun. Mag.*, vol. 58, no. 2, pp. 79-85, Feb. 2020.

[2] L. Du, J. Ma, Q. Liang, C. Li, and Y. Tang, "Capacity characterization for reconfigurable intelligent surfaces assisted wireless communications with interferer," *IEEE Trans. Commun.*, vol. 70, no. 3, pp. 1546-1558, Mar. 2022.

[3] L. Du, J. Ma, C. Fan, Q. Liang, C. Li, and Y. Tang, "Spatial domain suppression of co-channel interference: a reflection amplifiers surface (RAS) approach," TechRxiv. Preprint, https://doi.org/10.36227/techrxiv.15677823.v1.

[4] H. Jung, B. Nguyen, I. Song, and K. Kim, "Design of anti-jamming waveforms for time-hopping spread spectrum systems in tone jamming environments," *IEEE Trans. Veh. Technol.*, vol. 69, no. 1, pp. 728-737, Jan. 2020.

[5] M. Arefl, S. Jayaweeral, and E. Yepezl, "Survey on cognitive anti-jamming communications," *IET Commun.*, vol. 14, no. 18, pp. 3110-3127, Nov. 2020.

[6] F. Cheng, G. Gui, N. Zhao, Y. Chen, J. Tang, and H. Sari, "UAV-relaying-assisted secure transmission with caching," *IEEE Trans. Commun.*, vol. 67, no. 5, pp. 3140-3153, May 2019.

[7] Y. Cao, N. Zhao, F. Yu, M. Jin, Y. Chen, J. Tang, and V. Leung, "Optimization or alignment: secure primary transmission assisted by secondary networks," *IEEE Journal Sel. Areas Commun.*, vol. 36, no. 4, pp. 905-917, Apr. 2018.

[8] C. Popper, M. Strasser, and S. Capkun, "Anti-jamming broadcast communication using uncoordinated spread spectrum techniques," *IEEE J. Sel. Areas Commun.*, vol. 28, no. 5, pp. 703-715, Jun. 2010.

[9] M. Letafati, A. Kuhestani, H. Behroozi, and D. Ng, "Jamming-resilient frequency hopping-aided secure communication for internet-of-things in the presence of an untrusted relay," *IEEE Trans. Wireless Commun.*, vol. 19, no. 10, pp. 6771-6785, Oct. 2020.

[10] L. Zhao and A. Haimovich, "Performance of ultra-wideband communications in the presence of interference," *IEEE J. Sel. Areas Commun.*, vol. 20, no. 9, pp. 1684-1691, Dec. 2002.

[11] V. Liu *et al.*, "Ambient backscatter: wireless communication out of thin air," *in Proc. ACM SIGCOMM*, Hong Kong, Aug. 2013, pp. 39-50.

[12] G. Wang, F. Gao, R. Fan, and C. Tellambura, "Ambient backscatter communication systems: detection and performance analysis," *IEEE Trans. Commun.*, vol. 64, no. 11, pp. 4836-4846, Nov. 2016.

[13] J. Qian, A. Parks, J. Smith, F. Gao, and S. Jin, "IoT communications with M-PSK modulated ambient backscatter: algorithm, analysis, and implementation," *IEEE Internet Things J.*, vol. 6, no. 1, pp. 844-855, Feb. 2019.

[14] N. Huynh, D. Nguyen, D. Hoang, E. Dutkiewicz, and M. Mueck, "Ambient backscatter: a novel method to defend jamming attacks for wireless networks," *IEEE Wireless Commun. Lett.*, vol. 9, no. 2, pp. 175-178, Feb. 2020.

[15] T. Kumar, K. Ma, K. Yeo, and W. Yang, "A 35-mW 30-dB gain control range current mode linear-in-decibel programmable gain amplifier with bandwidth enhancement," *IEEE Trans. Microw. Theo. Tech.,* vol. 62, no. 12, pp. 3465-3475, Dec. 2014.

[16] H. Liu, X. Zhu, and C. Boon, "A reconfigurable programmable-gain amplifier with gain step adjustment and binary-weighted power consumption," *in Proc. IEEE MTT-S Int. Microw. Symp. Dig.*, Phoenix, AZ, USA, 2015, pp. 1-4.

[17] S. Y. Kang, J. Jang, I. Oh, and C. Park, "A 2.16 mW low power digitally-controlled variable gain amplifier," *IEEE Microw. Wireless Compon. Lett.*, vol. 20, no. 3, pp. 172-174, Mar. 2010.

[18] Y. Liang, Y. Zeng, E. Peh, and A. Hoang, "Sensing-throughput tradeoff for cognitive radio networks," *IEEE Trans. Wireless Commun.*, vol. 7, no. 4, pp. 1326-1337, Apr. 2008.

[19] E. Axell, G. Leus, E. Larsson, and H. V. Poor, "Spectrum sensing for cognitive radio: state-of-the-art and recent advances," *IEEE Signal Process. Mag.*, vol. 29, no. 3, pp. 101-116, May 2012.

[20] J. Ma, C. Huang, and Q. Li, "Energy efficiency of full-and half-duplex decode-and-forward relay channels," *IEEE Internet Things J.*, vol. 9, no. 12, pp. 9730-9748, Jun. 2022.

[21] Y. Liu, P. Roblin, X. Quan, W. Pan, S. Shao, and Y. Tang, "A full-duplex transceiver with two-stage analog cancellations for multipath self-interference," *IEEE Trans. Microw. Theo. Tech.*, vol. 65, no. 12, pp. 5263-5273, Dec. 2017.

[22] A. Manolakos, M. Chowdhury, and A. Goldsmith, "Energy-based modulation for noncoherent massive SIMO systems," *IEEE Trans. Wireless Commun.*, vol. 15, no. 11, pp. 7831-7846, Nov. 2016.

[23] T. Cover and J. Thomas, *Elements of Information Theory*. New York: Wiley, 1991.
[24] A. Papoulis and S. Pillai, *Probability, Random Variables, and Stochastic Processes,* 4th ed. New York: McGraw-Hill, 2002.