The Capacity of a Broadcast Channel with Gaussian Jamming and a Friendly Eavesdropper

Kevin Luo, Ramy H. Gohary, and Halim Yanikomeroglu
Department of Systems and Computer Engineering, Carleton University, Ottawa, Ontario, Canada

[1] ***Abstract*—A friendly eavesdropper assists communication in a broadcast scenario in which one transmitter wishes to send a common message to two receivers in the presence of a malicious jammer. The jammer attempts to disrupt communication by transmitting a high power Gaussian signal, whereas the friendly eavesdropper 'hears' the jammer's transmission and sends an assisting signal to the destinations over an orthogonal channel in order to help them alleviate the jammer's impact. We derive an expression for capacity, i.e., the maximum data rate that can be reliably communicated from the transmitter to the receivers and we show that it is optimal for the friendly eavesdropper to send a Gaussian description of the jamming signal with the help of a scheme based on a modified compress-and-forward relaying that uses a list decoding procedure.**

I. Introduction

In various military applications a transmitter may wish to send a common message to multiple receivers in the presence of an antagonistic jammer. This situation arises, for instance in the scenario illustrated in Fig 1 when an unmanned drone wishes to send a description of the battlefield to ground troops, and the adversary attempts to disrupt communication. The impact of the jammer can be partially alleviated by an ally agent in the geographic proximity of the jammer which acts as a friendly eavesdropper that 'hears' the jammer's signal and sends a description thereof to multiple receivers over an orthogonal channel. Neither the optimal signalling strategy of the eavesdropper nor a quantification of its utility is available, and the focus of this paper is to investigate these aspects.

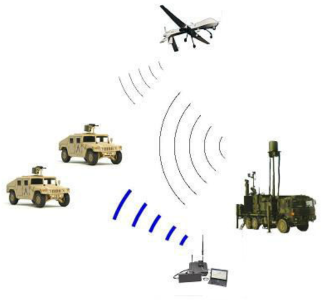

Fig. 1. An illustration of the considered communication system.

The impact of jamming has been considered in various communication scenarios. For instance, cases in which the jammer sends a correlated version of the transmitter's signal were considered in [1] from a mean-squared error perspective and in [2] from a capacity perspective. The case in which the jammer's signal are not correlated with the transmitter's signal was considered in [3]. It was shown therein that under individual average power constraints the transmitter signal that enables the highest data rate to be communicated is Gaussian distributed and the jammer's signal that minimizes the communicated rate is also Gaussian distributed. Applications of Gaussian jamming and counter jamming were studied in [4]–[6]. For instance, service disruption due to the injection of malicious signals into an all-optical-network was considered in [4], whereas the effect of multiple antenna jamming and the potential of counter jamming in multi-carrier direct-sequence spread-spectrum systems were considered in [5] and [6], respectively. Other instances of communication scenarios in the presence of jamming can be found in [7]–[9].

In this paper, we consider the situation in which a friendly eavesdropper assists communication in a broadcast scenario [10]. In this scenario one transmitter wishes to send a common message to two receivers in the presence of a malicious jammer that sends a zero mean Gaussian signal; the jammer and the transmitter's signals are uncorrelated. The received power of the jammer's signal is much higher than that of the receivers' background noises, which are therefore assumed to be negligible, see e.g., [6]. A friendly eavesdropper is able to pick the jammer's signal and attempts to assist the receivers by sending a description of the jammer's signal on an orthogonal channel. The channel between the eavesdropper and the receivers can be modelled as another Gaussian broadcast one. In fact, it is the noises on the links between the eavesdropper and the receivers that render rate-efficient communication challenging; without these noises the eavesdropper can simply forward its observation to the receivers in order to eliminate the jammer's signal. The eavesdropper has a maximum power budget which induces a constraint on its maximum transmission rate. To ensure causality, the eavesdropper's transmitted signal lags its received signal by one block. This implies that the jammer's, and subsequently the receivers' signals, are statistically independent of the eavesdropper transmitted signal. To analyze the maximum data rate that can be communicated between the transmitter and the receivers, we conceive the role of the friendly eavesdropper as that of a standard relay, but with the exception that the relay (eavesdropper) in this case has no access to the transmitter's signal. Hence, the channel between the transmitter and the receivers resembles a broadcast relay channel with strictly causal side information at the relay, but with the key difference

[1] This work was supported in part by a Discovery Grant of the Natural Sciences and Engineering Research Council (NSERC) of Canada and in part by the Ontario Ministry of Economic Development and Innovations ORF-RE (Ontario Research FundResearch Excellence) program.

with this broadcast scenario [11] being that the eavesdropper does not have access to the transmitter's codebooks, and the key difference with relaying schemes with strictly causal side information being that these schemes do not consider a broadcasting scenario [12]. A counterpart of the scenario considered herein is the one in [13]. Therein the eavesdropper was malicious and a friendly jammer (relay) forwarded noise to the eavesdropper to confuse it.

To derive an expression for the capacity of the channel considered herein, we derive an expression for the cut-set upper bound [14]. We then show that this bound can be achieved by a signalling strategy in which the friendly eavesdropper uses a scheme based on compress-and-forward (CF) [15] to send a description of the Gaussian jamming signal to the receivers. To decode the eavesdropper's signal and to subsequently use it to alleviate the effect of jamming, the receivers use a list decoding [16] scheme rather than the standard CF one.

Although other relaying techniques might be able to achieve the capacity of the channel considered herein, neither amplify-and-forward [17] nor decode-and-forward [15] does: amplify-and-forward yields a strictly lower rate, as will be shown below, and decode-and-forward can be readily excluded because the jammer does not cooperate with the eavesdropper.

Notation: Regular face upper and lower case letters will refer to random variables and their corresponding realizations, respectively. Boldface letters will refer to length-n sequences and the calligraphic font will be used to refer to codebooks. Throughout the paper, we will use $\mathcal{A}_{\epsilon}^{(n)}$ to denote the jointly ϵ-typical set of length-n sequences.

II. Channel Model

Consider the channel model depicted in Fig. 2. In this figure, the transmitter sends a common signal to two receivers that cannot collaborate. A malicious jammer attempts to disrupt communication by sending an independent Gaussian signal. The jammer's signal is 'heard' by a friendly eavesdropper, which attempts to assist the receivers by sending a description of the jammer's signal over an orthogonal channel.

Let the transmitter signal be denoted by X and let the signal sent by the eavesdropper on an orthogonal channel be denoted by X_{e}. The jamming signal is denoted by $J \sim \mathcal{N}(0, P_J)$. The jammer-eavesdropper channel gain is normalized to 1, the transmitter-receiver i channel gain is a_i and the jammer-receiver i channel gain is b_i, $i = 1, 2$. The received signal of the eavesdropper is denoted by Y_{e}. Each receiver i, receives two orthogonal signals: one from the transmitter contaminated by the jammer's signal, Y_i, and one from the friendly eavesdropper contaminated by additive Gaussian noise, $Y_{\mathrm{s},i}$, $i = 1, 2$. We denote the additive Gaussian noise component of $Y_{\mathrm{s},i}$ by $Z_i \sim \mathcal{N}(0, N_i)$, $i = 1, 2$. The friendly eavesdropper transmission rate is $R_{\mathrm{e}} \leq \sup_{p(x_{\mathrm{e}})} \max_{i=1,2} I(X_{\mathrm{e}}; Y_{\mathrm{s},i})$. Using this notation, the received signals at the eavesdropper and the receivers can be expressed as

$$\begin{aligned} &Y_{\mathrm{e}} = J, \\ &Y_1 = a_1 X + b_1 J, \quad Y_2 = a_2 X + b_2 J, \\ &Y_{\mathrm{s},1} = X_{\mathrm{e}} + Z_1, \quad\; Y_{\mathrm{s},2} = X_{\mathrm{e}} + Z_2. \end{aligned} \tag{1}$$

The average power of the jammer's Gaussian signal is given by $\mathrm{E}(J^2) = P_J$, whereas the transmitter and the friendly eavesdropper each is subject to its individual average transmit power constraint, $\mathrm{E}(X^2) \leq P$, and $\mathrm{E}(X_{\mathrm{e}}^2) \leq P_{\mathrm{e}}$, respectively. In the next section, we will show that a modified CF scheme that uses list decoding achieves the channel capacity.

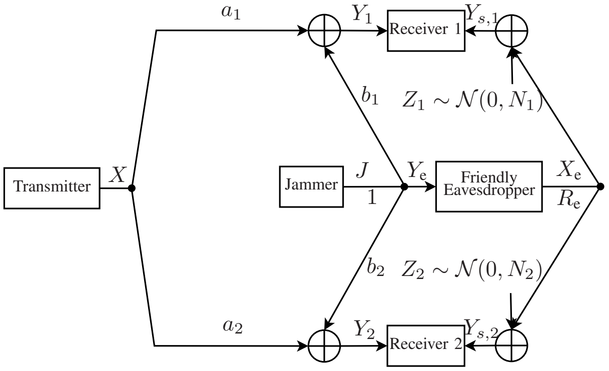

Fig. 2. A broadcast channel in the presence of a Gaussian jammer with a friendly eavesdropper, $J \sim \mathcal{N}(0, P_J)$.

III. Capacity Results

Let the maximum signal-to-jamming power ratio (SJR) of the transmitter-receiver i channel be denoted by $\gamma_i = \frac{a_i^2 P}{b_i^2 P_J}$, $i = 1, 2$, and let the maximum signal-to-noise ratio (SNR) of the eavesdropper-receiver i channel be denoted by $\gamma_{\mathrm{e},i} = \frac{P_{\mathrm{e}}}{N_i}$, $i = 1, 2$. Let $\mathcal{C}(x) \triangleq \frac{1}{2}\log_2(1 + x)$. Our main result is recorded in the following theorem.

Theorem 1: The capacity of the channel in Fig. 2 can be achieved when the eavesdropper sends a Gaussian description of the jammer's signal at a rate $R_{\mathrm{e}} = \max\{\mathcal{C}(\gamma_{\mathrm{e},1}), \mathcal{C}(\gamma_{e,2})\}$. This capacity is given by

$$C = \min\bigl\{\mathcal{C}(\gamma_1) + \mathcal{C}(\gamma_{\mathrm{e},1}), \mathcal{C}(\gamma_2) + \mathcal{C}(\gamma_{\mathrm{e},2})\bigr\}. \tag{2}$$

Proof: To prove the converse, in Appendix A-A we show that choosing X and X_{e} to be Gaussian-distributed with average powers P and P_{e}, respectively, maximizes the cut-set upper bound [18, Sect. 18.1].

To complete the proof of the theorem, in Appendix A-B we show that the cut-set upper bound can be achieved when the eavesdropper uses a strategy that resembles standard CF relaying, but with a list decoding procedure. In particular, the eavesdropper uses two Gaussian codebooks $\hat{\mathcal{Y}}_{\mathrm{e}}$ and $\mathcal{X}_{\mathrm{e}}$ with the powers and rates described in Appendix A-B. Upon receiving the jammer's signal, the eavesdropper finds a codeword in $\hat{\mathcal{Y}}_{\mathrm{e}}$ that is jointly typical with it. The eavesdropper uses Wyner-Ziv binning [19] to determine the codeword to be transmitted in the next block from $\mathcal{X}_{\mathrm{e}}$. Instead of using standard CF decoding, the receivers use a list decoding procedure similar to the one described in [16] to recover the eavesdropper's message. In list decoding, each receiver uses its knowledge of the codebooks $\hat{\mathcal{Y}}_{\mathrm{e}}$ and $\mathcal{X}$ as side information to recover the message from the eavesdropper and subsequently the message from the transmitter. (In standard CF $\hat{\mathcal{Y}}_{\mathrm{e}}$ and $\mathcal{X}$ are not used in recovering the message from the eavesdropper.) ∎

The proof of Theorem 1 assumes that both receivers use the list decoding procedure. However, the statement of the theorem holds if the receiver with less noise power on the eavesdropper link uses standard CF decoding, which is more straightforward than list decoding, to recover the eavesdropper's message.

So far, we have shown that the capacity of the channel described in Section II can be achieved when the eavesdropper sends a Gaussian description of the jammer's signal at a rate $R_{\text{e}} = \max\{\mathcal{C}(\gamma_{\text{e},1}), \mathcal{C}(\gamma_{\text{e},2})\}$. Since this rate is higher than the capacity of the link between the eavesdropper and the receiver with the higher noise, this receiver will not be able to recover the eavesdropper message if it uses standard CF decoding [12], but will be able to recover it if it uses list decoding; list decoding incorporates $\mathcal{X}$, cf. Appendix A-B.

IV. Comparison with other eavesdropping signalling schemes

We now compare the rates that can be achieved in the absence of the friendly eavesdropper, and when this eavesdropper uses either CF with standard decoding or AF relaying.

A. *No Eavesdropper Case*

In the absence of the eavesdropper, the channel capacity can be readily seen to be

$$C_{\text{No Eavesdropper}} = \min_{i=1,2} \mathcal{C}(\gamma_i). \tag{3}$$

Hence, using $\Delta \triangleq |\mathcal{C}(\gamma_1) - \mathcal{C}(\gamma_2)|$, the rate gain provided by the friendly eavesdropper can be expressed as

$$\begin{array}{ll} \min\big\{\Delta + \mathcal{C}(\gamma_{\text{e},1}), \mathcal{C}(\gamma_{\text{e},2})\big\}, & \gamma_1 \geq \gamma_2, \\ \min\big\{\mathcal{C}(\gamma_{\text{e},1}), \Delta + \mathcal{C}(\gamma_{\text{e},2})\big\}, & \gamma_1 < \gamma_2. \end{array}$$

It is of interest to note that when the transmitter (the drone) is sufficiently far from the receivers (ground troops), $\Delta \approx 0$ and the advantage of having the eavesdropper is approximately $\min\big\{\mathcal{C}(\gamma_{\text{e},1}), \mathcal{C}(\gamma_{\text{e},2})\big\}$. This is in contrast with the eavesdropper rate, which is given by $\max\big\{\mathcal{C}(\gamma_{\text{e},1}), \mathcal{C}(\gamma_{\text{e},2})\big\}$.

B. *CF With Standard Decoding Case*

Using standard CF decoding [12] at both receivers to recover the eavesdropper's message without using $\hat{\mathcal{Y}}_{\text{e}}$ and $\mathcal{X}$ induces a constraint on the eavesdropper's transmission rate, R_{e}. In particular, $R_{\text{e}} \leq \min_{i=1,2} I(X_{\text{e}}; Y_{\text{s},i})$. Using the standard approach, it can be verified that CF with Gaussian codebooks and standard decoding achieves the following rate:

$$R_{\text{CF}} \leq \min_{i=1,2} \mathcal{C}(\gamma_i) + \min_{i=1,2} \mathcal{C}(\gamma_{\text{e},i}), \tag{4}$$

which is generally less than capacity, cf. Section V.

C. *Amplify-and-Forward Case*

When the eavesdropper uses non-regenerative AF relaying, the optimal receivers' strategy can be readily seen to be using the signal received from the eavesdropper to partially cancel the jamming signal. The maximum rate that can be achieved by this scheme is given by

$$R_{\text{AF}} = \min_{i=1,2} \big\{\mathcal{C}\big(\gamma_i(1 + \gamma_{\text{e},i})\big)\big\}. \tag{5}$$

Proof: See details in Appendix. B. ■

Although the eavesdropper receives a noiseless replica of the jamming signal, AF achieves a rate strictly below capacity.

V. Numerical Comparison

To illustrate the advantage of CF with list decoding, in Fig. 3 we compare the rates achieved by the schemes outlined in Section IV with the capacity expression provided in Theorem 1. In particular, the capacity expression (2) is compared with: 1) the capacity of the broadcast channel in the absence of the friendly eavesdropper, cf. (3); 2) the rate achieved when the eavesdropper uses CF, but the receivers use standard (non-list) decoders to recover the eavesdropper message, cf. (4); and 3) the rate achieved when the eavesdropper uses AF, cf. (5). We consider instances in which the SJR of receiver 1, γ_1, varies from 0 to 4.5 and the SJR of receiver 2 is $\gamma_2 = 4$, and the SNRs of the eavesdropper to the receivers channels are $\gamma_{\text{e},1} = 3$ and $\gamma_{\text{e},2} = 2$. Fig. 3 shows that the achievable rate of CF with standard decoding is strictly below capacity in the high jamming regime, e.g., when $\gamma_1 < 4$. When the jamming signal power is relatively low, e.g., when $\gamma_1 \geq 4$, CF with standard decoding also achieves capacity. In contrast, the rate achieved by AF is strictly below capacity. The gap between the rate achieved when the eavesdropper uses AF and when it uses CF with list decoding (capacity) is reduced as γ_1 increases from 0 to 3. For $\gamma_1 \geq 3$, this gap is constant and strictly greater than zero. Without the friendly eavesdropper, the capacity is strictly below the rate achieved when the eavesdropper uses CF with either standard or list decoding.

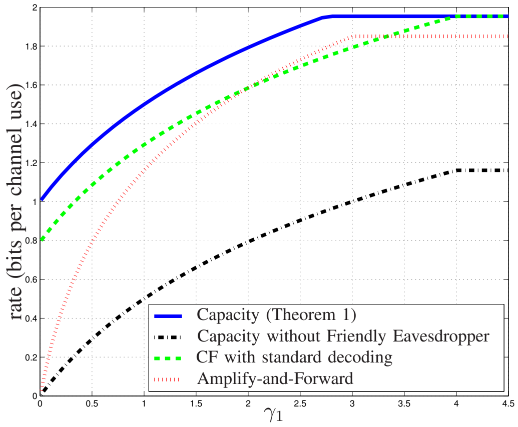

Fig. 3. Comparison between capacity (Theorem 1) and the rates achievable using the schemes in Section IV, for $\gamma_2 = 4$, $\gamma_{\text{e},1} = 3$, $\gamma_{\text{e},2} = 2$.

VI. Conclusion

We considered a two-receiver broadcast channel with a Gaussian jammer and a friendly eavesdropper. The friendly eavesdropper 'hears' the jamming signal and sends a description thereof to the receivers to help them to reduce the jammer's impact. We showed that the capacity of this channel can be achieved when the eavesdropper uses CF relaying with Gaussian codebooks and the receivers use list decoding to recover the eavesdropper's message. Our results are confirmed by analytical and numerical comparisons.

APPENDIX A
PROOF OF THEOREM 1

A. *Proof of converse*

Using the cut-set bound, the rate, R, of the common message to both receivers can be upper bounded by

$$R \leq \min_{i=1,2} I(X, X_{\mathrm{e}}; Y_i, Y_{\mathrm{s},i}). \tag{6}$$

From (6), it follows that, for $i = 1, 2$,

$$\begin{aligned} R \leq & I(X, X_{\mathrm{e}}; Y_i, Y_{\mathrm{s},i}) \\ = & h(a_i X + J, X_{\mathrm{e}} + Z_i) - h(J, Z_i). \end{aligned}$$

Since J and Z_i are independent, and X and X_{e} are independent of J and Z_i, choosing X and X_{e} to be independent maximizes $h(a_i X + J, X_{\mathrm{e}} + Z_i)$, and hence maximizes $I(X, X_{\mathrm{e}}; Y_i, Y_{\mathrm{s},i})$. The independence of (X, Y_i) and $(X_{\mathrm{e}}, Y_{\mathrm{s},i})$ implies that

$$R \leq I(X; Y_i) + I(X_{\mathrm{e}}; Y_{\mathrm{s},i}), \qquad i = 1, 2. \tag{7}$$

Since $Y_{\mathrm{s},i}$ and Y_i are received on orthogonal channels, and X and X_{e} must satisfy their respective average power constraints, it can be readily seen that choosing X and X_{e} to be independent Gaussian random variables maximizes the right hand side of (7), whence $R \leq \mathcal{C}(\gamma_i) + \mathcal{C}(\gamma_{\mathrm{e},i})$.

B. *Proof of achievability*

The proposed approach uses list instead of standard CF decoding approach, but for codebook generation and encoding it follows standard CF. Throughout the proof we will assume, without loss of generality, that $N_1 \leq N_2$.

Codebook Generation: Generate 2^{nR} i.i.d. $\mathbf{x}(m)$ following $p(\mathbf{x}) = \prod_{i=1}^{n} p(x_i)$, $m \in [1, 2^{nR}]$. Generate $2^{nI(X_{\mathrm{e}};Y_{\mathrm{s},1})}$ i.i.d. $\mathbf{x}_{\mathrm{e}}(s)$ following $p(\mathbf{x}_{\mathrm{e}}) = \prod_{i=1}^{n} p(x_{\mathrm{e}i})$, $s \in [1, 2^{nI(X_{\mathrm{e}};Y_{\mathrm{s},1})}]$. For each $\mathbf{x}_{\mathrm{e}}(s)$, generate $2^{n\hat{R}_{\mathrm{e}}}$ i.i.d. $\hat{\mathbf{y}}_{\mathrm{e}}(z|s)$ following $p(\hat{\mathbf{y}}_{\mathrm{e}}|\mathbf{x}_{\mathrm{e}}) = \prod_{i=1}^{n} p(\hat{y}_{\mathrm{e}i}|x_{\mathrm{e}i})$, $z \in [1, 2^{n\hat{R}_{\mathrm{e}}}]$.

Random Binning: The set $\{1, \cdots, 2^{n\hat{R}_{\mathrm{e}}}\}$ is randomly binned in $2^{nI(X_{\mathrm{e}};Y_{\mathrm{s},1})}$ cells. Denote the mapping by $s = \mathcal{B}(z)$.

Encoding: In block b, the eavesdropper finds an index z_b such that $(\mathbf{x}_{\mathrm{e}}(s_b), \hat{\mathbf{y}}_{\mathrm{e}}(z_b|s_b), \mathbf{y}_{\mathrm{e}}(b)) \in \mathcal{A}_{\epsilon}^{(n)}$. From the covering lemma [18], such z_b exists if n is sufficiently large and

$$\hat{R}_{\mathrm{e}} \geq I(\hat{Y}_{\mathrm{e}}; Y_{\mathrm{e}}|X_{\mathrm{e}}). \tag{8}$$

If more than one z is found, choose the smallest z and let $s_{b+1} = \mathcal{B}(z_b)$. Index m_b and s_b are transmitted by the transmitter and the eavesdropper, respectively.

Decoding: Assume that at the end of block b, receiver 1 and receiver 2 have correctly decoded m_{b-1} and s_{b-1}.

1) Decoding s_b: Receiver i, $i = 1, 2$, does two steps:
   a) The receiver determines two sets, $\mathcal{S}_z^{(b-1)}$ and $\mathcal{S}_s^{(b)}$:
      - The set $\mathcal{S}_z^{(b-1)}$ contains the indices $\hat{z}$ for which $(\mathbf{x}(m_{b-1}), \mathbf{x}_{\mathrm{e}}(s_{b-1}), \hat{\mathbf{y}}_{\mathrm{e}}(\hat{z}|s_{b-1}), \mathbf{y}_{\mathrm{s},i}(b-1), \mathbf{y}_i(b-1)) \in \mathcal{A}_{\epsilon}^{(n)}$.
      - The receiver determines the set $\mathcal{S}_s^{(b)}$ which contains the indices $\hat{s} = \mathcal{B}(\hat{z})$ for each $\hat{z} \in \mathcal{S}_z^{(b-1)}$.
   b) The receiver declares that $s_b = \hat{s}$ was sent in block b if there exists a unique index $\hat{s} \in \mathcal{S}_s^{(b)}$ such that $\big(\mathbf{x}(\hat{m}), \mathbf{x}_{\mathrm{e}}(\hat{s}), \mathbf{y}_{\mathrm{s},i}(b), \mathbf{y}_i(b)\big) \in \mathcal{A}_{\epsilon}^{(n)}$ for some $\hat{m}$.
2) Recovering m_b: Using the index s_b obtained in Step 1, receiver i constructs a set $\mathcal{S}'^{(b)}_{z,i} = \{\hat{z}|\big(\mathbf{x}_{\mathrm{e}}(s_b), \hat{\mathbf{y}}_{\mathrm{e}}(\hat{z}|s_b), \mathbf{y}_{\mathrm{s},i}(b), \mathbf{y}_i(b)\big) \in \mathcal{A}_{\epsilon}^{(n)}, \big(\mathbf{x}_{\mathrm{e}}(\hat{s}), \mathbf{y}_{\mathrm{s},i}(b+1), \mathbf{y}_i(b+1)\big) \in \mathcal{A}_{\epsilon}^{(n)}, \hat{s} = \mathcal{B}(\hat{z})\}$. The receiver declares that $m_b = \hat{m}$ was sent in block b if, for some $\hat{z} \in \mathcal{S}'^{(b)}_{z,i}$, there is a unique $\hat{m}$ such that $\big(\mathbf{x}(\hat{m}), \hat{\mathbf{y}}_{\mathrm{e}}(\hat{z}|s_b), \mathbf{x}_{\mathrm{e}}(s_b), \mathbf{y}_{\mathrm{s},i}(b), \mathbf{y}_i(b)\big) \in \mathcal{A}_{\epsilon}^{(n)}$.

Next we analyze the probability of error.

Without loss of generality, assume that the index pair $(m, s) = (1, 1)$ is transmitted in block b and block $b+1$. We define the following error events for the recovery of s_b.

$$\begin{aligned} \mathcal{E}_{\mathrm{s},i} = \{ & (\mathbf{x}(1), \mathbf{x}_{\mathrm{e}}(1), \hat{\mathbf{y}}_{\mathrm{e}}(1|1), \mathbf{y}_{\mathrm{s},i}(b-1), \mathbf{y}_i(b-1)) \\ & \notin \mathcal{A}_{\epsilon}^{(n)} \cup (\mathbf{x}(1), \mathbf{x}_{\mathrm{e}}(1), \mathbf{y}_{\mathrm{s},i}(b), \mathbf{y}_i(b)) \notin \mathcal{A}_{\epsilon}^{(n)} \\ & \text{for some } z \neq 1\}; \\ \mathcal{E}_{\mathrm{s},2} = \{ & (\mathbf{x}(1), \mathbf{x}_{\mathrm{e}}(1), \hat{\mathbf{y}}_{\mathrm{e}}(z|1), \mathbf{y}_{\mathrm{s},i}(b-1), \mathbf{y}_i(b-1)) \\ & \in \mathcal{A}_{\epsilon}^{(n)} \cap (\mathbf{x}(1), \mathbf{x}_{\mathrm{e}}(s), \mathbf{y}_{\mathrm{s},i}(b), \mathbf{y}_i(b)) \in \mathcal{A}_{\epsilon}^{(n)} \\ & \text{for some } z \neq 1, s = \mathcal{B}(z) \neq 1\}; \\ \mathcal{E}_{\mathrm{s},3} = \{ & (\mathbf{x}(1), \mathbf{x}_{\mathrm{e}}(1), \hat{\mathbf{y}}_{\mathrm{e}}(z|1), \mathbf{y}_{\mathrm{s},i}(b-1), \mathbf{y}_i(b-1)) \\ & \in \mathcal{A}_{\epsilon}^{(n)} \cap (\mathbf{x}(m), \mathbf{x}_{\mathrm{e}}(s), \mathbf{y}_{\mathrm{s},i}(b), \mathbf{y}_i(b)) \in \mathcal{A}_{\epsilon}^{(n)} \\ & \text{for some } z \neq 1, s = \mathcal{B}(z) \neq 1, m \neq 1\}. \end{aligned}$$

The receiver makes an error if any events in $\mathcal{E}_s = \cup_{j=1}^{3} \mathcal{E}_{\mathrm{s},j}$ occurs. Using the union bound, we have $P(\mathcal{E}_s) = P(\cup_{j=1}^{3} \mathcal{E}_{\mathrm{s},j}) \leq \sum_{j=1}^{3} P(\mathcal{E}_{\mathrm{s},j})$.

Let $\hat{Y}_{\mathrm{e}} = J + Z'$, where $Z' \sim \mathcal{N}(0, N')$. Define $\gamma' = \frac{N'}{P_J}$. Using $Y_{\mathrm{e}} = J$ and $Y_i = a_i X + b_i J$, we have

$$I(\hat{Y}_{\mathrm{e}}; Y_{\mathrm{e}}|X, X_{\mathrm{e}}, Y_i, Y_{\mathrm{s},i}) = h(Z') - h(Z') = 0. \tag{9}$$

Since (9) holds for any value of γ', it can be arbitrarily chosen.

Now we upper bound $P(\mathcal{E}_{\mathrm{s},j}), j = 1, 2, 3$. By the conditional joint typicality lemma [18], $P(\mathcal{E}_{\mathrm{s},1}) \to 0$ as $n \to \infty$.

The probability of $\mathcal{E}_{\mathrm{s},2}$ can be upper bounded by $P(\mathcal{E}_{\mathrm{s},2}) \leq 2^{n(\hat{R} - I(\hat{Y}_{\mathrm{e}}; X, Y_i, Y_{\mathrm{s},i}|X_{\mathrm{e}}) - I(X_{\mathrm{e}}; Y_i, Y_{\mathrm{s},i}|X))}$. Because of (9), we have $I(X_{\mathrm{e}}; Y_i, Y_{\mathrm{s},i}|X) \geq I(\hat{Y}_i; Y_{\mathrm{e}}|X, X_{\mathrm{e}}, Y_i, Y_{\mathrm{s},i})$. Hence using (8), $P(\mathcal{E}_{\mathrm{s},2}) \to 0$ as $n \to \infty$.

The probability of $\mathcal{E}_{\mathrm{s},3}$ can be upper bounded by $P(\mathcal{E}_{\mathrm{s},3}) \leq 2^{n(R + \hat{R} - I(\hat{Y}_{\mathrm{e}}; X, Y_i, Y_{\mathrm{s},i}|X_{\mathrm{e}}) - I(X, X_{\mathrm{e}}; Y_i, Y_{\mathrm{s},i}))}$. Using (8), we have $P(\mathcal{E}_{\mathrm{s},3}) \to 0$ as $n \to \infty$ if $R \leq I(X, X_{\mathrm{e}}; Y_i, Y_{\mathrm{s},i}) - I(\hat{Y}_{\mathrm{e}}; Y_{\mathrm{e}}|X, X_{\mathrm{e}}, Y_i, Y_{\mathrm{s},i})$, which using (9) yields

$$R \leq I(X, X_{\mathrm{e}}; Y_i, Y_{\mathrm{s},i}) = I(X; Y_i) + I(X_{\mathrm{e}}; Y_{\mathrm{s},i}). \tag{10}$$

Thus, when (10) is satisfied, $P(\mathcal{E}_s)$ tends to 0 as $n \to \infty$.

To analyze the probability of error for the recovery of m_b, we define the following error events for $i = 1, 2$, respectively:

$$\begin{aligned} \mathcal{E}_{m,1} = \{ & (\mathbf{x}(1), \mathbf{x}_{\mathrm{e}}(1), \hat{\mathbf{y}}_{\mathrm{e}}(1|1), \mathbf{y}_{\mathrm{s},i}(b), \mathbf{y}_i(b)) \notin \mathcal{A}_{\epsilon}^{(n)} \\ & \cup (\mathbf{x}_{\mathrm{e}}(1), \mathbf{y}_{\mathrm{s},i}(b+1), \mathbf{y}_i(b+1)) \notin \mathcal{A}_{\epsilon}^{(n)}\}; \\ \mathcal{E}_{m,2} = \{ & (\mathbf{x}(m), \mathbf{x}_{\mathrm{e}}(1), \hat{\mathbf{y}}_{\mathrm{e}}(1|1), \mathbf{y}_{\mathrm{s},i}(b), \mathbf{y}_i(b)) \in \mathcal{A}_{\epsilon}^{(n)}\}; \\ \mathcal{E}_{m,3} = \{ & (\mathbf{x}(m), \mathbf{x}_{\mathrm{e}}(1), \hat{\mathbf{y}}_{\mathrm{e}}(z|1), \mathbf{y}_{\mathrm{s},i}(b), \mathbf{y}_i(b)) \in \mathcal{A}_{\epsilon}^{(n)} \end{aligned}$$

$$\begin{aligned} &\cap (\mathbf{x}_{\mathrm{e}}(1), \mathbf{y}_{\mathrm{s},i}(b+1), \mathbf{y}_i(b+1)) \in \mathcal{A}_\epsilon^{(n)} \\ &\text{for } m \neq 1, z \neq 1\}; \\ \mathcal{E}_{m,4} = \{&(\mathbf{x}(m), \mathbf{x}_{\mathrm{e}}(1), \hat{\mathbf{y}}_{\mathrm{e}}(z|1), \mathbf{y}_{\mathrm{s},i}(b), \mathbf{y}_i(b)) \in \mathcal{A}_\epsilon^{(n)} \\ &\cap (\mathbf{x}_{\mathrm{e}}(s), \mathbf{y}_{\mathrm{s},i}(b+1), \mathbf{y}_i(b+1)) \in \mathcal{A}_\epsilon^{(n)} \\ &\text{for } m \neq 1, z \neq 1, s = \mathcal{B}(z) \neq 1\}. \end{aligned}$$

The receiver makes an error if any events in $\mathcal{E}_m = \cup_{j=1}^4 \mathcal{E}_{m,j}$ occurs. Hence, $P(\mathcal{E}_m) \leq \sum_{j=1}^4 P(\mathcal{E}_{m,j})$.

Now we bound $P(\mathcal{E}_{m,j}), j = 1,2,3,4$. By the conditional joint typicality lemma [18], $P(\mathcal{E}_{m,1}) \to 0$ as $n \to \infty$.

For $\mathcal{E}_{m,2}$, we have $P(\mathcal{E}_{m,2}) \leq 2^{n(R - I(X;\hat{Y}_{\mathrm{e}}, Y_i, Y_{\mathrm{s},i}|X_{\mathrm{e}}))}$. Hence, $P(\mathcal{E}_{m,2}) \to 0$ as $n \to \infty$ if for $i = 1,2$,

$$R \leq I(X; \hat{Y}_{\mathrm{e}}, Y_i, Y_{\mathrm{s},i}|X_{\mathrm{e}}). \tag{11}$$

The probability of $\mathcal{E}_{m,3}$ can be bounded by $P(\mathcal{E}_{m,3}) \leq 2^{n(R+\hat{R}_{\mathrm{e}} - I(X;Y_{\mathrm{s},1}) - I(X;Y_{\mathrm{s},i},Y_i|X_{\mathrm{e}}) - I(\hat{Y}_{\mathrm{e}};X,Y_{\mathrm{s},i},Y_i|X_{\mathrm{e}}))}$. Using (8), yields $P(\mathcal{E}_{m,3}) \to 0$ as $n \to \infty$ if $R \leq I(X; Y_{\mathrm{s},i}, Y_i|X_{\mathrm{e}}) - I(\hat{Y}_{\mathrm{e}}; Y_{\mathrm{e}}|X, X_{\mathrm{e}}, Y_{\mathrm{s},i}, Y_i) + I(X; Y_{\mathrm{s},1})$. Using (9), the latter condition is satisfied for $i = 1,2$, when

$$R \leq I(X;Y_{\mathrm{s},i}, Y_i|X_{\mathrm{e}}) + I(X; Y_{\mathrm{s},1}) = I(X; Y_i) + I(X_{\mathrm{e}}; Y_{\mathrm{s},1}). \tag{12}$$

The probability of $\mathcal{E}_{m,4}$ can be bounded by $P(\mathcal{E}_{m,4}) \leq 2^{n(R+\hat{R}_{\mathrm{e}} - I(X;Y_{\mathrm{s},i},Y_i|X_{\mathrm{e}}) - I(\hat{Y}_{\mathrm{e}};X,Y_i,Y_{\mathrm{s},i}|X_{\mathrm{e}}) - I(X_{\mathrm{e}};Y_i,Y_{\mathrm{s},i}))}$. Using (8), we have $P(\mathcal{E}_{m,4}) \to 0$ as $n \to \infty$ if $R \leq I(X, X_{\mathrm{e}}; Y_i, Y_{\mathrm{s},i}) - I(\hat{Y}_{\mathrm{e}}; Y_{\mathrm{e}}|X, X_{\mathrm{e}}, Y_i, Y_{\mathrm{s},i})$. Using (9), the latter condition yields the same constraint as (10).

Now we analyze the constraints in (10) and (12). We note that $I(X_{\mathrm{e}}; Y_{\mathrm{s},1}) \geq I(X_{\mathrm{e}}; Y_{\mathrm{s},2})$ since $N_1 \leq N_2$. Hence, the constraint in (10) is tighter than that in (12) for $i = 2$. Using this observation, the constraints in (12) can be dropped.

Using Gaussian codebooks (10) yields $R \leq \mathcal{C}(\gamma_i) + \mathcal{C}(\gamma_{\mathrm{e},i})$. Next, consider (11). We have

$$R \leq I(X; \hat{Y}_{\mathrm{e}}, Y_i, Y_{\mathrm{s},i}|X_{\mathrm{e}}) = \mathcal{C}\big(\gamma_i(1 + 1/\gamma')\big). \tag{13}$$

It can be shown that, when $\gamma' \geq 0$ such that

$$\gamma' \leq \min_{i=1,2} \frac{\gamma_i}{(1+\gamma_i)\gamma_{\mathrm{e},i}}$$

is satisfied, the right hand side of (13) is larger than the smaller of the two arguments of the minimization of (2). This choice of γ' renders (13) redundant and completes the proof.

Appendix B
Proof of the achievable rate by AF

Let the signal transmitted by eavesdropper be denoted by cJ, where c is the gain of the amplifier. Hence,

$$c^2 = P_{\mathrm{e}}/P_J. \tag{14}$$

At receiver i, the received signal from the eavesdropper can be expressed as $Y_{\mathrm{s},i} = cJ + Z_i$. Receiver i linearly combines the received signal Y_i and $Y_{\mathrm{s},i}$ to recover the message from the transmitter. The combined signal can be expressed as $Y_i + \alpha Y_{\mathrm{s},i} = a_i X + b_i J - \alpha(cJ + Z_i)$, where α is the combining weight to be optimized. The maximum rate that can be achieved by AF is given by

$$R_{\mathrm{AF}} = \min_{i=1,2} \max_{\alpha} \mathcal{C}\Big(\frac{a_i^2 P}{P_{J,Z_i}}\Big), \tag{15}$$

where $P_{J,Z_i} = (b_i - \alpha C)^2 P_J + \alpha^2 N_i$ is the jamming and noise power.

Optimizing α yields $P_{J,Z_i}^* = \frac{b_i^2 P_J N_i}{c^2 P_J + N_i}$. Using this result and (14) in (15) yields

$$R_{\mathrm{AF}} \leq \mathcal{C}\Big(\frac{a_i^2 P(P_{\mathrm{e}} + N)}{b_i^2 P_J N_i}\Big) = \mathcal{C}\big(\gamma_i(1 + \gamma_{\mathrm{e},i})\big), \qquad i = 1,2,$$

which completes the proof.

References

[1] T. Basar, "The Gaussian test channel with an intelligent jammer," *IEEE Trans. Inf. Theory*, vol. 29, pp. 152–157, Jan. 1983.

[2] M. Médard, "Capacity of correlated jamming channels," in *Proc. 35th Allerton Conf. Commun., Control Comput.*, (Monticello, Il), pp. 1043–1052, Sept. 1997. Also available at:http://www.mit.edu/~medard/pubs.html.

[3] R. J. McEliece and W. E. Stark, "An information theoretic study of communication in the presence of jamming," in *Proc. IEEE Int. Conf. Commun.*, (Denver, CO, USA), pp. 45.3.1–45.3.5, June 1981.

[4] M. Médard, D. Marquis, R. A. Barry, and S. J. Finn, "Security issues on all-optical-networks," *IEEE Network*, vol. 47, pp. 42–48, May 1997.

[5] E. A. Jorswieck, H. Boche, and M. Weckerle, "Optimal transmitter and jamming strategies in Gaussian MIMO channels," in *Proc. IEEE Vehic. Technol. Conf.*, (Stockholm,Sweden), pp. 978–982, May 2005.

[6] K. Cheun, K. Choi, H. Lim, and K. Lee, "Antijamming performance of a multicarrier direct-sequence spread-spectrum system," *IEEE Trans. Commun.*, vol. 47, pp. 1781–1784, Dec. 1999.

[7] A. Kashyap, T. Basar, and R. Srikant, "Correlated jamming on MIMO Gaussian fading channels," *IEEE Trans. Inf. Theory*, vol. 50, pp. 2119–2123, Sept. 2004.

[8] E. Tekin and A. Yener, "The general Gaussian multiple-access and two-way wiretap channels: Achievable rates and cooperative jamming," *IEEE Trans. Inf. Theory*, vol. 54, pp. 2735–2751, June 2008.

[9] S. Shafie and S. Ulukus, "Mutual information games in multiuser channels with correlated jamming," *IEEE Trans. Inf. Theory*, vol. 59, pp. 4598–4607, Oct. 2009.

[10] T. M. Cover, "Broadcast channels," *IEEE Trans. Inf. Theory*, vol. 18, pp. 2–14, Jan. 1972.

[11] Y. Liang and V. V. Veeravalli, "Cooperative relay broadcast channels," *IEEE Trans. Inf. Theory*, vol. 53, pp. 900–928, Mar. 2007.

[12] M. N. Khormuji, A. A. Zaidi, and M. Skoglund, "Interference management using nonlinear relaying," *IEEE Trans. Commun.*, vol. 58, pp. 1924–1930, July 2010.

[13] L. Lai and H. E. Gamal, "The relay-eavesdropper channel: Cooperation for secrecy," *IEEE Trans. Inf. Theory*, vol. 54, pp. 4005–4019, Sept. 2008.

[14] T. M. Cover and J. A. Thomas, *Elements of Information Theory*. New York: Wiley, 1991.

[15] T. M. Cover and A. A. El Gamal, "Capacity theorems for the relay channel," *IEEE Trans. Inf. Theory*, vol. IT-25, pp. 572–584, Sept. 1979.

[16] S. R. Bhaskaran, "Forward decoding over a relay channel," *Proc. IEEE Int. Symp. Inf. Theory*, pp. 2673–2677, July 2008.

[17] A. A. El Gamal, M. Mohseni, and S. Zahedi, "Bounds on capacity and minimum energy-per-bit for AWGN relay channels," *IEEE Trans. Inf. Theory*, vol. 52, pp. 1545–1561, Apr. 2006.

[18] A. El Gamal and Y.-H. Kim, *Network Information Theory*. Cambridge, UK: Cambridge University Press, 2012.

[19] A. D. Wyner and J. Ziv, "The rate-distortion function for source coding with side information at the decoder," *IEEE Trans. Inf. Theory*, vol. 22, pp. 1–10, Jan. 1976.