entropy

MDPI

Article

Gaussian Multiuser Wiretap Channels in the Presence of a Jammer-Aided Eavesdropper †

Rémi A. Chou [1,*] and Aylin Yener [2,*]

[1] Department of Electrical Engineering and Computer Science, Wichita State University, Wichita, KS 67260, USA [2] Department of Electrical and Computer Engineering, The Ohio State University, Columbus, OH 43210, USA * Correspondence: remi.chou@wichita.edu (R.A.C.); yener@ece.osu.edu (A.Y.)

† This paper is an extended version of our paper published in Chou, R.; Yener, A. The Gaussian multiple access wiretap channel when the eavesdropper can arbitrarily jam. In Proceedings of the IEEE International Symposium on Information Theory (ISIT), Aachen, Germany, 25–30 June 2017.

Abstract: This paper considers secure communication in the presence of an eavesdropper and a malicious jammer. The jammer is assumed to be oblivious of the communication signals emitted by the legitimate transmitter(s) but can employ any jamming strategy subject to a given power constraint and shares her jamming signal with the eavesdropper. Four such models are considered: (i) the Gaussian point-to-point wiretap channel; (ii) the Gaussian multiple-access wiretap channel; (iii) the Gaussian broadcast wiretap channel; and (iv) the Gaussian symmetric interference wiretap channel. The use of pre-shared randomness between the legitimate users is not allowed in our models. Inner and outer bounds are derived for these four models. For (i), the secrecy capacity is obtained. For (ii) and (iv) under a degraded setup, the optimal secrecy sum-rate is characterized. Finally, for (iii), ranges of model parameter values for which the inner and outer bounds coincide are identified.

Keywords: Gaussian wiretap channel; Gaussian multiple-access wiretap channel; Gaussian broadcast wiretap channel; jamming; secure communication

Citation: Chou, R.A.; Yener, A. Gaussian Multiuser Wiretap Channels in the Presence of a Jammer-Aided Eavesdropper. Entropy **2022**, 24, 1595. https://doi.org/10.3390/e24111595

Academic Editor: Eduard Jorswieck

Received: 29 September 2022
Accepted: 28 October 2022
Published: 2 November 2022

1. Introduction

Consider secure communication over wireless channels between legitimate parties in the presence of an eavesdropper and a malicious jammer. The jammer is assumed to be oblivious of the legitimate users' communication but can employ any jamming strategy subject to a given power constraint. Consequently, the main channel between the legitimate users is arbitrarily varying [1]. Unlike most works that consider arbitrarily varying channels, however, pre-shared randomness is not available to the legitimate users in our scenario. Additionally, the jammer shares her jamming signal with the eavesdropper who can thus perfectly cancel the effect of the jamming signal on her channel. In this paper, we study the fundamental limits of secure communication rates in the presence of such a jammer-aided eavesdropper over four Gaussian wiretap channel models: the Gaussian wiretap channel [2], the Gaussian multiple-access wiretap channel [3], the Gaussian broadcast wiretap channel [4], and the Gaussian symmetric interference wiretap channel.

1.1. Contributions

Our contributions are summarized as follows.

- For secure communication over Gaussian point-to-point, multiple-access, broadcast, and symmetric interference wiretap channels in the presence of a jammer-aided eavesdropper as described above, we determine inner and outer bounds on the secrecy capacity region.
- We show that our bounds are tight for the point-to-point setting, tight for sum-rates for the multiple-access and interference settings under degraded setups, and tight for some ranges of model parameter values for the broadcast setting.

Our main strategy to handle our multiuser settings is to reduce the problem to single-user coding. Previous known techniques for such a reduction, such as rate-splitting [5] and successive cancellation decoding [5] [Appendix C], that have been developed for multiple-access settings without security constraints, do not easily apply to wiretap channel models. These techniques consist in achieving the corner points of achievability regions that can be described by polymatroids whose corner points have positive components. However, regions described by polymatroids whose corner points have negative components, as in our wiretap channel models, prevent the applications of these techniques. We overcome this roadblock by proposing novel time-sharing strategies coupled with appropriate secret-key exchanges between the legitimate users. As seen in the proofs of our results, eavesdropping and arbitrary jamming are not easy to decouple in the secrecy analysis. In particular, the analysis of the secrecy in our proposed model does not follow from a standard secrecy analysis in the absence of jamming, as we need to consider (i) codewords uniformly distributed over spheres, which we use to handle an arbitrarily varying main channel; and (ii) block-Markov coding and specific time-sharing strategies (to allow the reduction of multiuser coding to single-user coding) which create inter-dependencies between coding blocks. Note that our achievability schemes also rely on point-to-point codes developed in [1]. One of the benefits of reducing multiuser coding to point-to-point coding techniques is that despite the fact that our setting involves multiple transmitters and an arbitrarily varying channel between the legitimate users, pre-shared randomness among the legitimate users will not be needed in our achievability schemes. Our strategy for the converse consists of reducing the problem of determining a converse for our model to the problem of determining a converse for a related model in the absence of a jammer.

1.2. Related Works

Related works that consider simultaneous eavesdropping and oblivious jamming threats for the point-to-point discrete memoryless wiretap channel include [6–11]. The proof techniques used in these references to obtain security, such as random binning [12,13], resolvability/soft covering [10,14,15], or typicality arguments, are challenging to apply to a Gaussian setting in the absence of shared randomness at the legitimate user. Specifically, for the Gaussian point-to-point channel in the presence of an adversary that arbitrarily jams [1], the only known coding mechanism to obtain reliability in the absence of pre-shared randomness relies on codewords uniformly drawn on a unit sphere [1], which are challenging to integrate with the above techniques to obtain security because their components are not independent and identically distributed.

Another line of work [16] considers Gaussian channel models where the eavesdropper channel can vary arbitrarily, but the main channel is not. The setting considered in the present paper, where the main channel between the legitimate users is arbitrarily varying, prevents the use of analyses similar to those in [16] for the same reasons described above.

Several other works have considered continuous channel models, including the Gaussian MIMO wiretap channel [17], the Gaussian multiple-access wiretap channel [18], where deviating users can be viewed as active adversary, and continuous point-to-point wiretap channels [19,20], where the adversary can choose between eavesdropping or jamming. These references differ from the above-mentioned references on arbitrarily varying channels as they assume a specific signaling strategy for the jammer.

Finally, note that for point-to-point channels, stronger jamming strategies that depend on the signals of the legitimate transmitters have been studied in [21–23].

1.3. Organization of the Paper

The remainder of the paper is organized as follows. We describe the models in Section 2. We present our results for the Gaussian point-to-point wiretap channel, the Gaussian multiple-access wiretap channel, the Gaussian broadcast wiretap channel, and the Gaussian symmetric interference wiretap channel in Sections 3–6, respectively. We discuss in Section 4.2 a way to avoid, at least for some channel parameters, time-sharing for the

multiple-access setting. We also discuss in Section 4.3 an extension of the multiple-access setting to more than two transmitters. We detail the proofs for the multiple-access setting in Sections 7 and 8. We end the paper with concluding remarks in Section 9.

2. Problem Statement

2.1. Notation

For $a, b \in \mathbb{R}$, define $[a, b] \triangleq [\lceil a \rceil, \lfloor b \rfloor] \setminus \mathbb{N}$, $]a, b[\triangleq [a, b] \setminus \{a, b\}$, $[a, b[\triangleq [a, b] \setminus \{b\}$, and $]a, b] \triangleq [a, b] \setminus \{a\}$. The components of a vector, X^n, of size $n \in \mathbb{N}$, are denoted by subscripts, i.e., $X^n \triangleq (X_1, X_2, \ldots, X_n)$. For $x \in \mathbb{R}$, define $[x]^+ \triangleq \max(0, x)$. The notation $x \mapsto y$ describes a function that associates y to x when the domain and the image of the function are clear from the context. The power set of a finite set S is denoted by 2^S. The convex hull of a set S is denoted by $\mathrm{Conv}(S)$. Unless specified otherwise, capital letters designate random variables, whereas lowercase letters designate realizations of associated random variables, e.g., x is a realization of the random variable X. For $R \in \mathbb{R}_+$, $\mathcal{B}_0^n(R)$ denotes the ball of radius R centered in 0 in $\mathbb{R}^n$ under the Euclidian norm.

2.2. Gaussian Multiuser Wiretap Channel in the Presence of a Jammer-Aided Eavesdropper

Consider the Gaussian memoryless wiretap channel model with two transmitters and two legitimate receivers

$$Y_1^n \triangleq \sqrt{g_{11}} X_1^n + \sqrt{g_{12}} X_2^n + \sqrt{g_{13}} S^n + N_1^n, \tag{1a}$$

$$Y_2^n \triangleq \sqrt{g_{21}} X_1^n + \sqrt{g_{22}} X_2^n + \sqrt{g_{23}} S^n + N_2^n, \tag{1b}$$

$$Z^n \triangleq \sqrt{h_1} X_1^n + \sqrt{h_2} X_2^n + N_Z^n, \tag{1c}$$

where Y_1^n, Y_2^n are the channel outputs observed by the legitimate receivers, and Z^n is the channel output observed by the eavesdropper. For $l \in \{1, 2\}$, X_l^n is the signal emitted by Transmitter l satisfying the power constraint $\|X_l^n\|^2 \triangleq \sum_{i=1}^n (X_l)_i^2 \leq nG_l$, S^n is an arbitrary jamming sequence transmitted by the jammer that is oblivious of the communication of the legitimate users and satisfies the power constraint $\|S^n\|^2 \triangleq \sum_{i=1}^n S_i^2 \leq nL$, and $N^n \sim \mathcal{N}(0, \sigma^2)$, $N_1^n \sim \mathcal{N}(0, \sigma_1^2)$, $N_2^n \sim \mathcal{N}(0, \sigma_2^2)$ are sequences of independent and identically distributed Gaussian noise with variances σ^2, σ_1^2, σ_2^2, respectively. The channel coefficients g_{11}, g_{12}, g_{13}, g_{21}, g_{22}, g_{23}, h_1, h_2 are fixed and known to all parties. Note that we assume that the jammer helps the eavesdropper by sharing her jamming sequence, which allows the eavesdropper to perfectly cancel S^n from Z^n. Coding schemes and achievable rates are defined as follows.

Definition 1. Let $n, k \in \mathbb{N}$. A $(2^{nR_1}, 2^{nR_2}, n, k)$ code $\mathcal{C}_n$ consists, for each block $j \in [\![1, k]\!]$, of

- Two message sets $\mathcal{M}_l^{(j)} \triangleq [\![1, 2^{nR_l^{(j)}}]\!]$, $l \in \{1, 2\}$;
- Two stochastic encoders, $e_l^{(j)} : \mathcal{M}_l^{(j)} \to \mathcal{B}_0^n(\sqrt{nG_l})$, $l \in \{1, 2\}$;
- Two decoders, $g_l^{(j)} : \mathbb{R}^n \to \mathcal{M}_l^{(j)}$, $l \in \{1, 2\}$;

where for any $l \in \{1, 2\}$, $R_l = \frac{1}{k} \sum_{j=1}^k R_l^{(j)}$, and operates as follows. For each block $j \in [\![1, k]\!]$, transmitter $l \in \{1, 2\}$ encodes with $e_l^{(j)}$ a uniformly distributed message $M_l^{(j)} \in \mathcal{M}_l^{(j)}$ to a codeword of length n, which is sent to the legitimate receiver over the channel described by Equation (1a), Equation (1b), Equation (1c) with the power constraint nL for the jamming signal S_i^n. Note that all the power constraints at the transmitters and the jammer hold for a given transmission block of length n, which is relevant when the power constraints hold within any time window corresponding to n channel uses. Then, the legitimate receiver $l \in \{1, 2\}$ forms an estimate $\hat{M}_l^{(j)} \triangleq g_l^{(j)}(Y_l^n)$ of the message $M_l^{(j)}$. We define $\hat{\mathcal{M}} \triangleq \hat{\mathcal{M}}_1^{(j)}, \hat{\mathcal{M}}_2^{(j)}{}_{j \in [\![1,k]\!]}$, $\mathcal{M} \triangleq \mathcal{M}_1^{(j)}, \mathcal{M}_2^{(j)}{}_{j \in [\![1,k]\!]}$, $S \triangleq (S_i^n)_{i \in [\![1,nk]\!]}$, and $\mathcal{S} \triangleq \{(S_i^n)_{i \in [\![1,nk]\!]} : \|S_i^n\|^2 \leq nL, \forall i \in [\![1, nk]\!]\}$.

Definition 2. A rate pair (R_1, R_2) is achievable, if there exists a sequence of $2^{nR_1}, 2^{nR_2}, n, k$ codes such that

$$\lim_{n \to \infty} \sup_{s \in S} P[\hat{M} \neq M] = 0 \text{ (reliability)}, \tag{2a}$$

$$\lim_{n \to \infty} \frac{1}{nk} H(M | Z^{kn}) \geq R_1 + R_2 \text{ (equivocation)}. \tag{2b}$$

2.3. Special Case 1: The Gaussian Wiretap Channel in the Presence of a Jammer-Aided Eavesdropper

Assume that the two transmitters are colocated and the two receivers are colocated in Section 2.2. More specifically, as depicted in Figure 1, the channel model of Section 2.2 becomes

$$Y^n = X^n + S^n + N_1^n, \tag{3a}$$

$$Z^n = \sqrt{h} X^n + N_Z^n, \tag{3b}$$

where $s_1^2 = s_Z^2 = 1$. We term this model as Gaussian Wiretap channel with Jammer-Aided eavesdropper (Gaussian WT-JA in short form). Note that this model recovers as a special case the Gaussian wiretap channel [2].

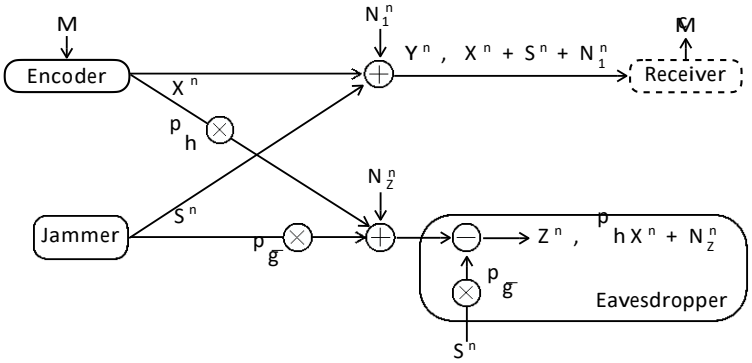

Figure 1. The Gaussian wiretap channel in the presence of a jammer-aided eavesdropper.

2.4. Special Case 2: The Gaussian Multiple-Access Wiretap Channel in the Presence of a Jammer-Aided Eavesdropper

Assume that the two receivers are colocated in Section 2.2. More specifically, as depicted in Figure 2, the channel model of Section 2.2 becomes

$$Y^n = X_1^n + X_2^n + S^n + N_1^n, \tag{4a}$$

$$Z^n = \sqrt{\bar{h}_1} X_1^n + \sqrt{\bar{h}_2} X_2^n + N_Z^n, \tag{4b}$$

where $s_1^2 = s_Z^2 = 1$. We term the model as Gaussian Multiple-Access Wiretap channel with Jammer-Aided eavesdropper (Gaussian MAC-WT-JA in short form) with the parameters $(G_1, G_2, h_1, h_2, L, s_1^2, s_Z^2)$. This model recovers as special cases the model in [24] in the absence of the security constraint (2b), and the Gaussian multiple-access wiretap channel [3]. Note that the model in [24] was introduced to study the presence of selfish transmitters via cooperative game theory, and that, similarly, the Gaussian MAC-WT-JA can be used to study the presence of selfish transmitters via coalitional game theory [25].

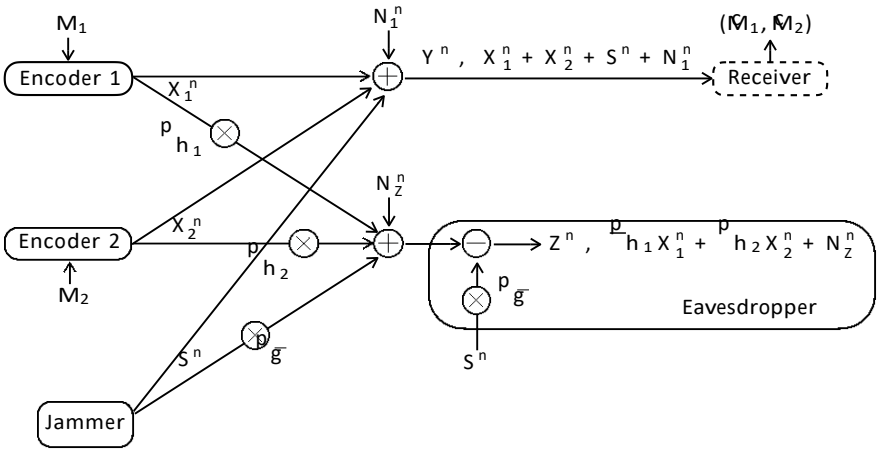

Figure 2. The Gaussian multiple-access wiretap channel in the presence of a jammer-aided eavesdropper.

2.5. Special Case 3: The Gaussian Broadcast Wiretap Channel in the Presence of a Jammer-Aided Eavesdropper

Assume that the two transmitters are colocated in Section 2.2. More specifically, as depicted in Figure 3, the channel model of Section 2.2 becomes

$$Y_1^n, \quad X^n + \sqrt{\bar{g}_1} S^n + N_1^n, \tag{5a}$$

$$Y_2^n, \quad X^n + \sqrt{\bar{g}_2} S^n + N_2^n, \tag{5b}$$

$$Z^n, \quad \sqrt{h} X^n + N_Z^n, \tag{5c}$$

where $s_Z^2 = 1$. We term the model as Gaussian Broadcast Wiretap channel with Jammer-Aided eavesdropper (Gaussian BC-WT-JA in short form). Note that this model recovers as special cases the multi-receiver wiretap channel [26] and the model in [27] in the absence of the security constraint (2b).

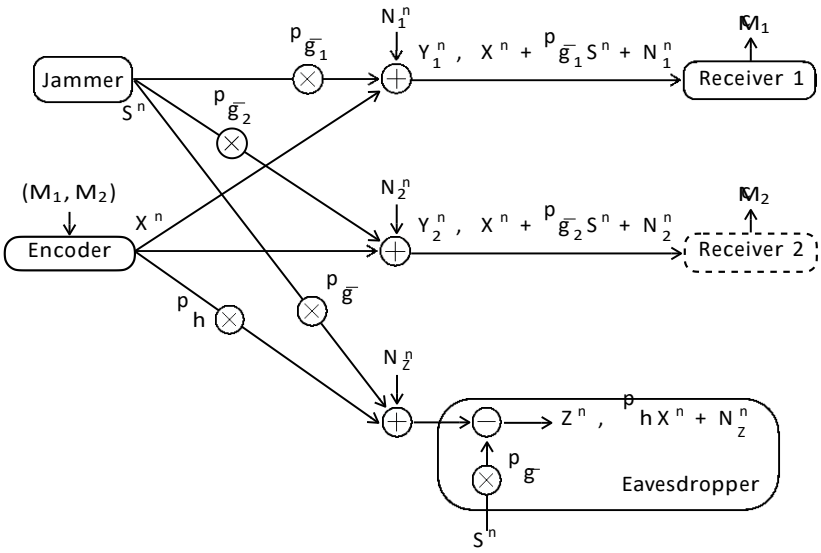

Figure 3. The Gaussian broadcast wiretap channel in the presence of a jammer-aided eavesdropper.

2.6. Special Case 4: The Gaussian Symmetric Interference Wiretap Channel in the Presence of a Jammer-Aided Eavesdropper

Consider the following special case of the channel model of Section 2.2

$$Y_1^n = X_1^n + X_2^n + S^n + N_1^n, \tag{6a}$$
$$Y_2^n = X_1^n + X_2^n + S^n + N_2^n, \tag{6b}$$
$$Z^n = \sqrt{h_1}X_1^n + \sqrt{h_2}X_2^n + N_Z^n, \tag{6c}$$

where $s_1^2 = s_2^2 = s_Z^2 = 1$. We term the model as Gaussian Symmetric Interference Wiretap channel with Jammer-Aided eavesdropper (Gaussian SI-WT-JA in short form). In the absence of the security constraint (2b) and the jamming sequence, this model recovers a special case of the Gaussian interference channel under strong interference [28].

3. The Gaussian Wiretap Channel in the Presence of a Jammer-Aided Eavesdropper

We present a capacity result for the Gaussian WT-JA model described in Section 2.3.

Theorem 1. The secrecy capacity of the Gaussian WT-JA is

$$C(L) = \begin{cases} \frac{1}{2}\log\frac{1+(1+L)^{-1}G}{1+hG} & \text{if } G > L \\ 0 & \text{if } G \le L \end{cases}. \tag{7}$$

Observe that $C(L)$ is non-zero if and only if $G > L$ and $(1+L)^{-1} > h$. When $G > L$, Theorem 1 means that arbitrary oblivious jamming is no more harmful than Gaussian jamming, i.e., when the jamming sequence is obtained from independent and identical realizations of a zero-mean Gaussian random variable with variance equal to the power constraint L.

The proof of Theorem 1 follows as a special case of the achievability and converse bounds derived in the next section in Theorems 2 and 3, respectively, for the Gaussian MAC-WT-JA.

4. The Gaussian Multiple-Access Wiretap Channel in the Presence of a Jammer-Aided Eavesdropper

4.1. Inner and Outer Bounds for the Gaussian MAC-WT-JA

We derive inner and outer bounds for the Gaussian MAC-WT-JA in Theorems 2 and 3. Their proofs are provided in Sections 7 and 8, respectively.

Theorem 2 (Achievability)**.** We consider three cases.

1. When $G_1 > L$ and $G_2 \le L$,

$$\mathcal{R}_1^{MAC} = \left\{(R_1, 0) : R_1 \le \max_{0 \le P \le G_2 - L} \frac{1}{2}\log\frac{1+G_1(L+P)}{1+G_1 h_1(1+h_2 P)}\right\} \tag{8}$$

is achievable.

2. When $G_2 > L$ and $G_1 \le L$,

$$\mathcal{R}_2^{MAC} = \left\{(0, R_2) : R_2 \le \max_{0 \le P \le G_1 - L} \frac{1}{2}\log\frac{1+G_2(L+P)}{1+G_2 h_2(1+h_1 P)}\right\} \tag{9}$$

is achievable.

3. When $\min(G_1, G_2) > L$,

$$\mathcal{R}^{MAC} = \mathrm{Conv}\left(\mathcal{R}_1^{MAC} \cup \mathcal{R}_2^{MAC} \cup \left[\bigcup_{\substack{L \le P_1 \le G_1 - L \\ L \le P_2 \le G_2 - L}} \mathcal{R}_{1,2}^{MAC}(P_1, P_2)\right]\right) \tag{10}$$

is achievable, where

$$R_{1,2}^{\mathrm{MAC}}(P_1, P_2), \quad (R_1, R_2) : R_1 \le \frac{1}{2}\log\left(\frac{1+{}_1P\,(1+L)^{\,1}}{1+P\,h^1(1+h\,P^2)^{2\,1}}\right)^{+},$$
$$R_2 \le \frac{1}{2}\log\left(\frac{1+P_2(1+L)^{\,1}}{1+P_2h_2(1+h_1P_1)^{\,1}}\right)^{+},$$
$$R_1 + R_2 \le -\log\left(1+P\,h_1^1+P^2h_2\right)\left(\frac{1+(P_1+P_2)(1+L)^{\,1}}{1+P_1h_1+P_2h_2}\right)^{1+1}{}^{2}\Big)^{+}. \tag{11}$$

Theorem 3 (Partial Converse)**.**

1. If $\max(G_1, G_2) \le L$, then no positive rate is achievable.
2. When $\min(G_1, G_2) > L$ and $h_1 = h_2$, the sum-rate bound of $R_{1,2}^{\mathrm{MAC}}(G_1, G_2)$ described in Equation (11) is tight by choosing $(P_1, P_2) = (G_1, G_2)$.

Observe that in the achievability scheme for R_1^{MAC}, choosing a transmission power smaller than G_1 for Transmitter 1 would result in a smaller region, since for a fixed P_2, $x \mapsto \log\frac{1+x(1+L+P_2)}{1+xh_1(1+h_2P_2)}$ is either negative when $(1+L+P_2)^{-1} > h_1(1+h_2P_2)^{-1}$, or non-decreasing when $(1+L+P_2)^{-1} \le h_1(1+h_2P_2)^{-1}$. By exchanging the role of the transmitters, we have the same observation for R_2^{MAC}.

4.2. Discussion of Rate-Splitting

Rate-splitting [5] can be adapted to the Gaussian MAC-WT-JA to avoid time-sharing, however, the entire region in Equation (11) cannot be achieved as splitting the power of one user precludes reliable communication. Assuming that

$$I(X_1X_2;Y) \le I(X_1X_2;Z) \le \max[I(X_1;Y|X_2) \le I(X_1;Z), I(X_2;Y|X_1) \le I(X_2;Z)], \tag{12}$$

then one can split the power of Transmitter 1 in $(P_1 - d)$ and d, where $d \in [0, P_1]$, and define the following functions from $[0, P_1]$ to $\mathbb{R}$

$$R_U : d \mapsto \frac{1}{2}\log\frac{1+(P_1-d)(1+L+d+P_2)^{-1}}{1+h_1^1(P_1-d)^{-1}}, \tag{13a}$$
$$R_V : d \mapsto \frac{1}{2}\log\frac{1+d(1+L)^{-1}}{1+h_1d(1+h_1(P_1-d)+h_2P_2)^{-1}}, \tag{13b}$$
$$R_2 : d \mapsto \frac{1}{2}\log\frac{1+P_2(1+L+d)^{-1}}{1+h_2P_2(1+h_1(P_1-d))^{-1}}. \tag{13c}$$

Lemma 1. For any $d \in [0, P_1]$, we have $(R_U + R_V + R_2)(d) = I(X_1X_2;Y) - I(X_1X_2;Z)$. Moreover, for any point (x_0, y_0) in

$$D(P^1, P^2), \quad (R_1, R_2) \in R_{1,2}^{\mathrm{MAC}}(P_1, P_2) : R_1 + R_2 = \frac{1}{2}\log\left(\frac{1+(P_1+P_2)(1+L)^{-1}}{1+P_1h_1+P_2h_2}\right)^{+}, \tag{14}$$

there exists $d_0 \in [0, P_1]$ such that $x_0 = (R_U + R_V)(d_0)$ and $y_0 = R_2(d_0)$.

Proof. Define

$$Y' = U + V + X_2 + N_Y, \tag{15a}$$
$$Z' = \sqrt{h_1}(U + V) + \sqrt{h_2}X_2 + N_Z, \tag{15b}$$

where V, U, X_2, N_Y, N_Z are independent zero-mean Gaussian random variables with variances $d \in [0, P_1]$, $P_1 - d$, P_2, $(1 + L)$, 1, respectively. Additionally, define

$$R_U(d) \triangleq I(U;Y) - I(U;Z|V,X_2) = \frac{1}{2}\log\frac{1+(P_1-d)(1+L+d+P_2)^{-1}}{1+h_1(P_1-d)}, \tag{16a}$$

$$R_V(d) \triangleq I(V;Y|U,X_2) - I(V;Z) = \frac{1}{2}\log\frac{1+d(1+L)^{-1}}{1+h_1 d(1+h_1(P_1-d)+h_2P_2)^{-1}}, \tag{16b}$$

$$R_2(d) \triangleq I(X_2;Y|U) - I(X_2;Z|V) = \frac{1}{2}\log\frac{1+P_2(1+L+d)^{-1}}{1+h_2P_2(1+h_1(P_1-d))^{-1}}. \tag{16c}$$

By the chain rule, we have, for any $d \in [0, P_1]$, $(R_U + R_V + R_2)(d) = I(X_1X_2;Y) - I(X_1X_2;Z)$. Finally, since $(R_U + R_V)(0) = I(X_1;Y) - I(X_1;Z|X_2)$ and $(R_U + R_V)(P_1) = I(X_1;Y|X_2) - I(X_1;Z)$, by continuity of $d \mapsto (R_U + R_V)(d)$, there exists $d_0 \in [0, P_1]$ such that $x_0 = (R_U + R_V)(d_0)$ and $y_0 = R_2(d_0)$ for any point (x_0, y_0) in $\mathcal{D}(P_1, P_2)$. □

As remarked in [29], a potential issue is that $R_U(d_0)$ or $R_V(d_0)$ can be negative in Lemma 1. We have the following achievability result.

Proposition 1. Let $(x_0, y_0) \in \mathcal{D}(P_1, P_2)$ and d_0 be as in Lemma 1. Then, (x_0, y_0) can be achieved without time-sharing if $R_U(d_0) \geq 0$ and $R_V(d_0) \geq 0$ and $\min(d_0, P_1 - d_0) > L$. $(x_0, y_0) \in \mathcal{D}(P_1, P_2)$ can also be achieved without time-sharing if similar conditions (obtained by exchanging the role of the two transmitters) are satisfied when splitting the power of Transmitter 2.

Proof idea: Transmitter 1 is split into two virtual users that transmit at rate $R_U(d)$ with power d and at rate $R_V(d)$ with power $P_1 - d$. Encoding for User 2 and the two virtual users is similar to Case 1 in the proof of Theorem 2. The receiver adopts a minimum distance decoding rule as in Theorem 2 to first decode the message associated with the virtual user that transmits at rate R_V, then to decode the message associated with User 2, and finally, to decode the message associated with the virtual user that transmits at rate R_U. A similar procedure can be performed if one decides to split the power of Transmitter 2. □

An illustration of Proposition 1 is depicted in Figure 4. Note that for some model parameters, the set of points achievable with Proposition 1 can be empty and, unfortunately, it does not seem easy to obtain a simple analytical characterization of the rate pairs achievable with Proposition 1.

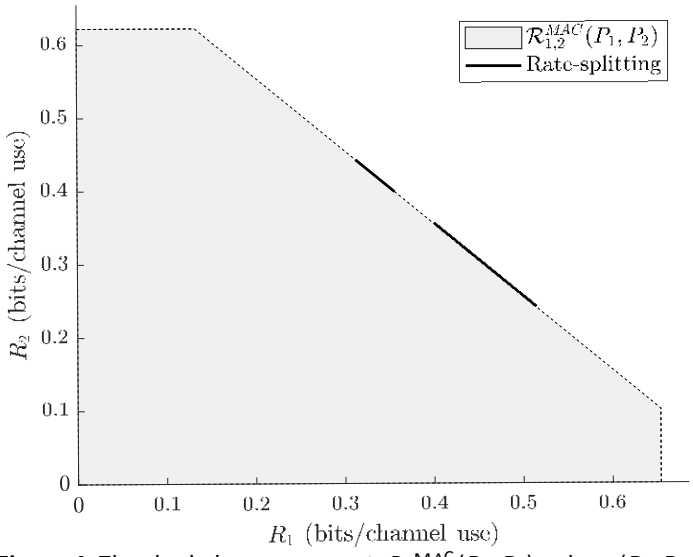

Figure 4. The shaded area represents $\mathcal{R}_{1,2}^{MAC}(P_1, P_2)$, where $(P_1, P_2, L, h_1, h_2) = (4, 3.3, 1.5, 0.12, 0.11)$. The solid segments represent the rate pairs achievable with Proposition 1.

4.3. Extension to More Than Two Transmitters

We extend our result for the MAC-WT-JA to the case of an arbitrary number of transmitters. The problem is more involved than the case of two transmitters and requires new time-sharing strategies that leverage extended polymatroid properties.

Consider the model of Section 2.4 with L transmitters instead of two transmitters. We let $\mathcal{L} = \{1, \dots, L\}$ denote the set of transmitters. More specifically, the channel model of Section 2.4 becomes

$$Y^n = \sum_{l \in \mathcal{L}} X_l^n + S^n + N_1^n, \tag{17a}$$

$$Z^n = \sum_{l \in \mathcal{L}} \sqrt{h_l} X_l^n + N_Z^n, \tag{17b}$$

where $s_1^2 = s_Z^2 = 1$. We term the model as Gaussian MAC-WT-JA with parameters $((G_l)_{l \in \mathcal{L}}, (h_l)_{l \in \mathcal{L}}, L, s_1^2, s_Z^2)$. When the channel gains $(h_l)_{l \in \mathcal{L}}$ are all equal to $h \in [0, 1[$, we refer to this model as the degraded MAC-WT-JA with parameters $((G_l)_{l \in \mathcal{L}}, h, L, s_1^2, s_Z^2)$. Given $L \in \mathbb{R}_+$ and $(G_l)_{l \in \mathcal{L}}$, we define $h_L = (1 + L)^{-1}$, $\mathcal{L}(L) = \{l \in \mathcal{L} : G_l > L\}$, and $\mathcal{L}^c(L) = \mathcal{L} \setminus \mathcal{L}(L)$. The following achievability result is proven in Appendix B.

Theorem 4. Assume that for all $l \in \mathcal{L}(L)$, $h_L > h_l$. The following region is achievable for the Gaussian MAC-WT-JA with parameters $((G_l)_{l \in \mathcal{L}}, (h_l)_{l \in \mathcal{L}}, L, 1, 1)$

$$\mathcal{R} = \bigcup_{(P_l)_{l \in \mathcal{L}} : \forall l \in \mathcal{L}(L), L < P_l G_l} \left\{ (R_l)_{l \in \mathcal{L}} : \forall l \in \mathcal{L}^c(L), R_l = 0 \text{ and } \forall T \subset \mathcal{L}(L), R_T \le \frac{1}{2} \log \frac{1 + h_L P_T}{1 + (\sum_{l \in T} h_l P_l)(1 + \sum_{l \in T^c} h_l P_l)^{-1}} \right\}^+, \tag{18}$$

where for any $(P_l)_{l \in \mathcal{L}}$ and $T \subset \mathcal{L}$, we use the notation $P_T = \sum_{l \in T} P_l$.

We immediately obtain the following corollary.

Corollary 1. The following region is achievable for the degraded Gaussian MAC-WT-JA with parameters $((G_l)_{l \in \mathcal{L}}, h, L, 1, 1)$

$$\mathcal{R} = \bigcup_{(P_l)_{l \in \mathcal{L}} : \forall l \in \mathcal{L}(L), L < P_l G_l} \left\{ (R_l)_{l \in \mathcal{L}} : \forall l \in \mathcal{L}^c(L), R_l = 0 \text{ and } \forall T \subset \mathcal{L}(L), R_T \le \frac{1}{2} \log \frac{1 + h_L P_T}{1 + hP_T(1 + hP_{T^c})^{-1}} \right\}^+. \tag{19}$$

Note that the achievability strategy used in the proof of Theorem 4 is different than the achievability strategy used in the proof of Theorem 2. While Theorem 4 gains in generality by considering an arbitrary number of users, it requires the assumption $\forall l \in \mathcal{L}(L), h_L > h_l$, which is not needed in Theorem 2. We also have the following optimality result, which is proven in Appendix C.

Theorem 5. The maximal secrecy sum-rate $R_L = \sum_{l \in \mathcal{L}} R_l$ achievable for the degraded Gaussian MAC-WT-JA with parameters $((G_l)_{l \in \mathcal{L}}, h, L, 1, 1)$ is

$$\left\{ \frac{1}{2} \log \frac{1 + h_L G_{\mathcal{L}(L)}}{1 + hG_{\mathcal{L}(L)}} \right\}^+. \tag{20}$$

Note that the optimal secrecy sum-rate is positive if and only if $h_L > h$ and $\mathcal{L}(L) \neq \emptyset$.

5. The Gaussian Broadcast Wiretap Channel in the Presence of a Jammer-Aided Eavesdropper

Theorems 6 and 7 provide inner and outer bounds, respectively, for the Gaussian BC-WT-JA.

Theorem 6 (Achievability)**.** We have the following inner bounds.

1. When $g_2 \geq G$ and $g_1 < G$,

$$R_1^{BC} \triangleq \left\{ (R_1, 0) : R_1 \leq \frac{1}{2} \log\left(\frac{1 + \frac{G}{s_1^2 + g_1}}{1 + hG} \right) \right\}, \tag{21}$$

   is achievable.
2. When $g_1 \geq G$ and $g_2 < G$,

$$R_2^{BC} \triangleq \left\{ (0, R_2) : R_2 \leq \frac{1}{2} \log\left(\frac{1 + \frac{G}{s_2^2 + g_2}}{1 + hG} \right) \right\}, \tag{22}$$

   is achievable.
3. When $\max(g_1, g_2) < G$, and, without loss of generality, $s_1^2 + g_1 \geq s_2^2 + g_2$ (exchange the role of the receivers if $s_1^2 + g_1 > s_2^2 + g_2$),

$$\mathrm{Conv}\left(R_1^{BC} \cup R_2^{BC} \cup \bigcup_{\alpha \in [\max(g_1, g_2) G^{-1}, 1]} R^{BC}(\alpha) \right), \tag{23}$$

   is achievable where we have defined for $\alpha \in [0, 1]$

$$R^{BC}(\alpha) \triangleq \left\{ (R_1, R_2) : R_1 \leq \frac{1}{2} \log\left(\frac{1 + \frac{(1-\alpha)G}{s_1^2 + g_1}}{1 + h(1-\alpha)G} \right), \right.$$
$$\left. R_2 \leq \frac{1}{2} \log\left(\frac{1 + \frac{\alpha G}{(1-\alpha)G + s_2^2 + g_2}}{1 + \frac{h\alpha G}{h(1-\alpha)G + 1}} \right) \right\}. \tag{24}$$

Note that $R^{BC}(\alpha = 0) = R_1^{BC}$ and $R^{BC}(\alpha = 1) = R_2^{BC}$. The achievability scheme of Theorem 6 is similar to the proof of Theorem 2 and [27] [Theorem 3].

Theorem 7 (Partial converse)**.**

1. If $G \leq \min(g_1, g_2)$, then no positive rate is achievable;
2. When $g_2 \geq G$ and $g_1 < G$, the achievability region R_1^{BC} in Theorem 6 is tight; 3.
   When $g_1 \geq G$ and $g_2 < G$, the achievability region R_2^{BC} in Theorem 6 is tight; 4.
   When $G > \max(g_1, g_2)$, the following region is an outer bound

$$\bigcup_{\alpha \in [0,1]} R^{BC}(\alpha), \tag{25}$$

   where $R^{BC}(\alpha)$ has been defined in Theorem 6.

The proof of Theorem 7 is similar to the proof of Theorem 3 using [26] in place of [30]. Observe that the gap between the inner and outer bounds of Theorems 6 and 7 when $G > \max(g_1, g_2)$ comes from the fact that our achievability scheme is limited to $\alpha \in]\max(g_1, g_2) G^{-1}, 1] \cup \{0\}$.

6. The Symmetric Interference Wiretap Channel in the Presence of a Jammer-Aided Eavesdropper

By the symmetry in Equation (6a) and Equation (6b), a code for the Gaussian MAC-WT-JA allows Receiver $i \in \{1,2\}$ to securely recover the message of Transmitter i. Hence, from the achievability result for the Gaussian MAC-WT-JA, we have the following achievability result for the Gaussian SI-WT-JA.

Theorem 8 (Achievability)**.** We consider three cases.

1. When $G_1 > L$ and $G_2 \leq L$, $R^{SI}_1 \triangleq R^{MAC}_1$ is achievable; 2. When $G_2 > L$ and $G_1 \leq L$, $R^{SI}_2 \triangleq R^{MAC}_2$ is achievable; 3. When $\min(G_1, G_2) > L$, $R^{SI} \triangleq R^{MAC}$ is achievable;

where R^{MAC}_1, R^{MAC}_2, and R^{MAC} are defined in Theorem 2.

Next, by the symmetry in Equations (6a) and (6b), we have that any code for the Gaussian SI-WT-JA allows Receiver $i \in \{1,2\}$ to securely recover the messages from both transmitters, meaning that an outer bound for the Gaussian SI-WT-JA can be obtained by considering an outer bound for a Gaussian MAC-WT-JA. Hence, from the partial converse for the Gaussian MAC-WT-JA, we obtain the following partial converse for the Gaussian SI-WT-JA.

Theorem 9 (Partial converse)**.**

1. If $\max(G_1, G_2) \leq L$, then no positive rate is achievable.
2. When $\min(G_1, G_2) > L$ and $h_1 = h_2$, the sum-rate achieved in R^{SI} is tight by choosing $(P_1, P_2) = (G_1, G_2)$.

7. Proof of Theorem 2

To prove Theorem 2, it is sufficient to prove the achievability of the dominant face

$$D(P_1, P_2) \triangleq \left\{(R_1, R_2) \in R^{MAC}_{1,2}(P_1, P_2) : R_1 + R_2 = \frac{1}{2}\log\left(1 + \frac{(P_1 + P_2)(1 + L)}{1 + P_1 h_1 + P_2 h_2}\right)\right\} \tag{26}$$

of $R^{MAC}_{1,2}(P_1, P_2)$ to prove the achievability of $R^{MAC}_{1,2}(P_1, P_2)$ when $\min(G_1, G_2) > L$ and where $(P_1, P_2) \in]L, G_1]]L, G_2]$. The achievability of R^{MAC}_i, $i \in \{1,2\}$, when $G_i > L$ and $G_{3-i} \leq L$ is obtained similarly by having Transmitter i, $\bar{3}-i$ send Gaussian noise. Observe that the rate constraints in $R^{MAC}_{1,2}(P_1, P_2)$ can be expressed as

$$R_1 \leq [I(X_1; Y|X_2) - I(X_1; Z)]^+, \tag{27a}$$

$$R_2 \leq [I(X_2; Y|X_1) - I(X_2; Z)]^+, \tag{27b}$$

$$R_1 + R_2 \leq [I(X_1 X_2; Y) - I(X_1 X_2; Z)]^+, \tag{27c}$$

where

$$Y \triangleq X_1 + X_2 + N_Y, \tag{28a}$$

$$Z \triangleq \sqrt{h_1} X_1 + \sqrt{h_2} X_2 + N_Z, \tag{28b}$$

and X_1, X_2, N_Y, N_Z are independent zero-mean Gaussian random variables with variances P_1, P_2, $(1 + L)$, 1, respectively. As remarked in [29], the set function $\mathcal{T} \mapsto I(X_{\mathcal{T}}; Y|X_{\mathcal{T}^c}) - I(X_{\mathcal{T}}; Z)$ is submodular but not necessarily non-decreasing, where $\forall \mathcal{T} \subseteq \{1,2\}$, $X_{\mathcal{T}} \triangleq (X_t)_{t \in \mathcal{T}}$. This is the main reason why achieving the corner points of $R^{MAC}_{1,2}(P_1, P_2)$ by means of point-to-point codes via the successive decoding method [5] [Appendix C] does

not easily translate to our setting. Before we provide our solution, we summarize our proof strategy in the three cases below. Figure 5 illustrates these cases.

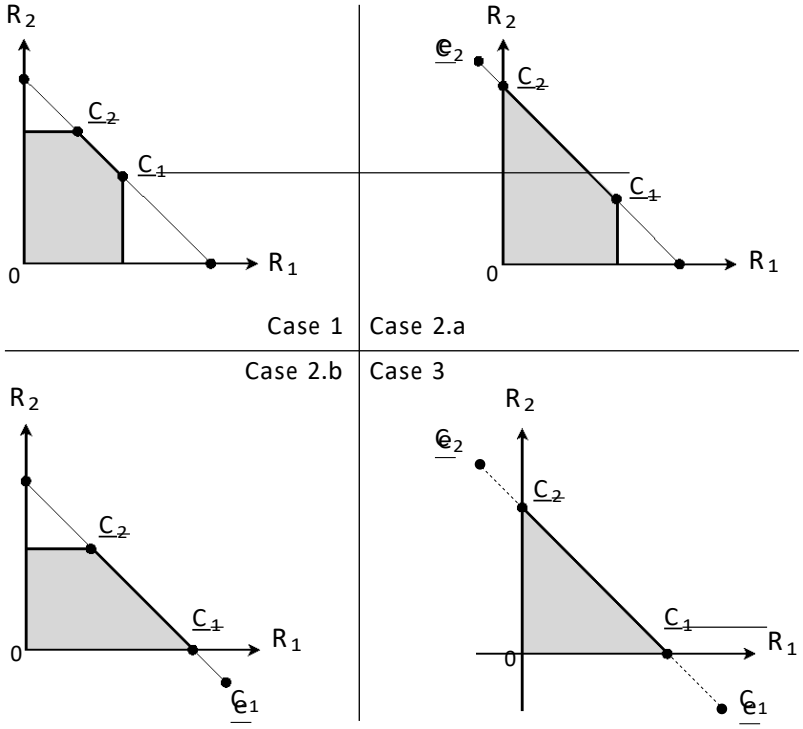

Figure 5. Region $R_{1,2}(P_1, P_2)$.

Case 1: Assume

$$I(X_1X_2;Y) \quad I(X_1X_2;Z) \quad \max[I(X_1;YjX_2) \quad I(X_1;Z), I(X_2;YjX_1) \quad I(X_2;Z)]. \tag{29}$$

The corner points of $R_{1,2}^{MAC}$ are given by

$$\underline{C}_1 \ , \ (I(X_1;YjX_2) \quad I(X_1;Z), I(X_2;Y) \quad I(X_2;ZjX_1)), \tag{30a}$$

$$\underline{C}_2 \ , \ (I(X_1;Y) \quad I(X_1;ZjX_2), I(X_2;YjX_1) \quad I(X_2;Z)). \tag{30b}$$

We will achieve each corner point with point-to-point coding techniques and perform time-sharing to achieve $D(P_1, P_2)$. Specifically, to achieve $\underline{C}_i$, $i \ 2 \ f1, 2g$, the encoders will be designed such that the decoder can first estimate the codeword sent by Transmitter $\bar{i}$, $3 \quad i$ (by considering the codewords of Transmitter i as noise), which is in turn used to estimate the codeword sent by Transmitter i. This approach is similar to the successive decoding method [5] [Appendix C] for a multiple-access channel in the absence of a security constraint.

Case 2.a: Assume

$$I(X_1X_2;Y) \quad I(X_1X_2;Z) \ I(X_1;YjX_2) \quad I(X_1;Z), \tag{31a}$$

$$I(X_1X_2;Y) \quad I(X_1X_2;Z) < I(X_2;YjX_1) \quad I(X_2;Z). \tag{31b}$$

Hence,

$$\underline{e}_2 \ , \ (I(X_1;Y) \quad I(X_1;ZjX_2), I(X_2;YjX_1) \quad I(X_2;Z)) \tag{32}$$

has a negative x-coordinate and the method of Case 1 cannot be directly applied here. Now, the corner points of $R_{1,2}^{MAC}$ are

$$\underline{C}_1 , \quad (I(X_1;Y|X_2) \quad I(X_1;Z), I(X_2;Y) \quad I(X_2;Z|X_1)), \tag{33a}$$

$$\underline{C}_2 , \quad (0, I(X_1X_2;Y) \quad I(X_1X_2;Z))). \tag{33b}$$

The idea to achieve $\underline{C}_1$ is, as in Case 1, a successive decoding approach by decomposing the sum rate $I(X_1X_2;Y) \quad I(X_1X_2;Z)$ as the sum of $I(X_2;Y) \quad I(X_2;Z|X_1)$, which represents the secret message rate for Transmitter 2, and $I(X_1;Y|X_2) \quad I(X_1;Z)$, which represents the secret message rate for Transmitter 1. However, $\underline{C}_2$ cannot be decomposed in a similar manner and thus cannot be achieved with the same method. Instead, to achieve any point in $D(P_1, P_2)$, we rely on a strategy over several transmission blocks. First, in an appropriate number of transmission blocks, the transmitters can send secret messages with rates $\underline{C}_1$ as in Case 1. Part of the secret messages of Transmitter 1, with a rate equal to the absolute value of the x-coordinate of the point $\underline{\mathbf{e}}_2$, is dedicated to the exchange of a secret key between Transmitter 1 and the legitimate receiver. Then, for the remaining transmission blocks, Transmitter 2 transmits a secret message with rate $I(X_1X_2;Y) \quad I(X_1X_2;Z)$, while Transmitter 1 uses the previously generated secret key to produce a jamming signal, which can be canceled out by the legitimate receiver but not by the eavesdropper who does not know the secret key.

Case 2.b: Assume

$$I(X_1X_2;Y) \quad I(X_1X_2;Z) \quad I(X_2;Y|X_1) \quad I(X_2;Z), \tag{34a}$$

$$I(X_1X_2;Y) \quad I(X_1X_2;Z) < I(X_1;Y|X_2) \quad I(X_1;Z). \tag{34b}$$

This case is handled as Case 2.a by exchanging the role of the two transmitters.

Case 3: Assume

$$I(X_1X_2;Y) \quad I(X_1X_2;Z) < \min[I(X_1;Y|X_2) \quad I(X_1;Z), I(X_2;Y|X_1) \quad I(X_2;Z)]. \tag{35}$$

Hence,

$$\underline{\mathbf{e}}_1 , \quad (I(X_1;Y|X_2) \quad I(X_1;Z), I(X_2;Y) \quad I(X_2;Z|X_1)), \tag{36a}$$

$$\underline{\mathbf{e}}_2 , \quad (I(X_1;Y) \quad I(X_1;Z|X_2), I(X_2;Y|X_1) \quad I(X_2;Z)), \tag{36b}$$

have a negative y-component and a negative x-component, respectively, and the strategy of Case 1 or Case 2 cannot be directly applied here. The corner points of the region are

$$\underline{C}_1 , \quad (I(X_1X_2;Y) \quad I(X_1X_2;Z), 0), \tag{37a}$$

$$\underline{C}_2 , \quad (0, I(X_1X_2;Y) \quad I(X_1X_2;Z)). \tag{37b}$$

These corner points do not seem to be easily achievable using the method for Case 1. We will first show that it is possible to achieve a point $\underline{R} \ 2 \ D(P_1, P_2)$, where $\underline{R}$ has strictly positive components. All the other points in $D(P_1, P_2)$ will then be achieved as in Case 2 by doing the substitutions $\underline{C}_1 \quad \underline{R}$ and $\underline{C}_2 \quad \underline{R}$ in Case 2.a and Case 2.b, respectively.

Note that it is sufficient to consider the case

$$\min[I(X_1;Y|X_2) \quad I(X_1;Z), I(X_2;Y|X_1) \quad I(X_2;Z)] \ 0. \tag{38}$$

Indeed, for $i \ 2 \ \{1, 2\}$ and $\bar{i} , \quad 3 \quad i$, when $I(X_i;Y|X_{\bar{i}}) \quad I(X_i;Z) > 0$ and $I(X_{\bar{i}};Y|X_i) \quad I(X_{\bar{i}};Z) \quad 0$, we have $R_{\bar{i}} = 0$ and $R_i \quad I(X_1X_2;Y) \quad I(X_1X_2;Z) \quad I(X_i;Y|X_{\bar{i}})$ $I(X_i;Z|X_{\bar{i}}) = \frac{1}{2}\log \frac{1+P_i(1+L)^{\ 1}}{1+P_ih_i}$. These cases correspond to Theorem 1 and can be treated as in Case 1.

7.1. Case 1

We show the achievability of $\underline{C}_2$. The achievability of $\underline{C}_1$ is obtained by exchanging the role of the transmitters.

Codebook construction: For Transmitter $i \in \{1,2\}$, construct a codebook $C_n^{(i)}$ with $\lceil 2^{nR_i} \rceil \lceil 2^{n\tilde{R}_i} \rceil$ codewords drawn independently and uniformly on the sphere of radius $\sqrt{nP_i}$ in $\mathbb{R}^n$. The codewords are labeled $x_i^n(m_i, \tilde{m}_i)$, where $m_i \in \{1, 2^{nR_i}\}$, $\tilde{m}_i \in \{1, 2^{n\tilde{R}_i}\}$. We define $C_n := (C_n^{(1)}, C_n^{(2)})$ and choose for $d > 0$

$$R_1 > I(X_1;Y) - I(X_1;Z|X_2) + d, \tag{39a}$$

$$\tilde{R}_1 > I(X_1;Z|X_2) + d, \tag{39b}$$

$$R_2 > I(X_2;Y|X_1) - I(X_2;Z) + d, \tag{39c}$$

$$\tilde{R}_2 > I(X_2;Z) + d. \tag{39d}$$

Encoding at Transmitter $i \in \{1,2\}$: Given $(m_i, \tilde{m}_i)$, transmit $x_i^n(m_i, \tilde{m}_i)$. In the remainder of the paper, we use the term randomization sequence for $\tilde{m}_i$.

Decoding: The receiver performs minimum distance decoding to first estimate $(\hat{m}_1, \hat{\tilde{m}}_1)$ and then to estimate $(m_2, \tilde{m}_2)$, i.e., given y^n, it determines $(\hat{m}_1, \hat{\tilde{m}}_1) := f_1(y^n, 0)$, and $(\hat{m}_2, \hat{\tilde{m}}_2) := f_2(y^n, x_1^n(\hat{m}_1, \hat{\tilde{m}}_1))$ where for $i \in \{1,2\}$

$$f_i(y^n, x) := \begin{cases} (m_i, \tilde{m}_i) & \text{if } \|y^n - x - x_i^n(m_i, \tilde{m}_i)\|^2 < \|y^n - x - x_i^n(m_i', \tilde{m}_i')\|^2 \\ & \text{for } (m_i', \tilde{m}_i') \neq (m_i, \tilde{m}_i), \\ 0 & \text{if no such } (m_i, \tilde{m}_i) \in \{1, 2^{nR_i}\} \times \{1, 2^{n\tilde{R}_i}\} \text{ exists} \end{cases} \tag{40}$$

Define $e(C_n, s^n) := P\left[(\hat{M}_1, \hat{M}_2) \neq (M_1, M_2) \middle| C_n\right]$. We now prove that $\mathbb{E}_{C_n}[\sup_{s^n} e(C_n, s^n)] \to 0$ as $n \to \infty$ if $R_1 + \tilde{R}_1 < I(X_1;Y) + \frac{1}{n} I(M_1 M_2; Z^n | C_n)$. We will thus conclude by Markov's inequality that there exists a sequence of realizations $(C_n)_{n\geq 1}$ of $(C_n)_{n\geq 1}$ such that both $\sup_{s^n} e(C_n, s^n)$ and $\frac{1}{n} I(M_1 M_2; Z^n | C_n)$ can be made arbitrarily close to zero as $n \to \infty$.

Average probability of error: We have

$$e(C_n, s^n) := P\left[(\hat{M}_1, \hat{M}_2) \neq (M_1, M_2) \text{ or } (\hat{\tilde{M}}_1, \hat{\tilde{M}}_2) \neq (\tilde{M}_1, \tilde{M}_2) \middle| C_n\right] \tag{41a}$$

$$\leq e_1(C_n, s^n, x_2^n(M_2, \tilde{M}_2)) + e_2(C_n, s^n, 0), \tag{41b}$$

where for $i \in \{1,2\}$

$$e_i(C_n, s^n, x) := \frac{1}{\lceil 2^{nR_i} \rceil \lceil 2^{n\tilde{R}_i} \rceil} \sum_{m_i} \sum_{\tilde{m}_i} P\left[\|x_i^n(m_i, \tilde{m}_i) + s^n + x + N^n - x_i^n(m_i', \tilde{m}_i')\|^2 \leq \|s^n + x + N^n\|^2 \text{ for some } (m_i', \tilde{m}_i') \neq (m_i, \tilde{m}_i)\right]. \tag{42}$$

Next, we have

$$\mathbb{E}_{C_n}[e_1(C_n, s^n, x_2^n(M_2, \tilde{M}_2))] \leq \mathbb{E}_{C_n}[e_1(C_n, s^n, x_2^n(M_2, \tilde{M}_2)) | C_n^{(1)} \in \mathcal{C}_1] + P[C_n^{(1)} \notin \mathcal{C}_1] \tag{43a}$$

$$\to 0, \tag{43b}$$

where, in Equation (43a), $\mathcal{C}_1$ represents all the sets of unit norm vectors scaled by $\sqrt{nP_1}$ that satisfy the two conditions of Lemma A1 (in Appendix A), Equation (43b) holds because $P[C_n^{(1)} \in \mathcal{C}_1] \to 1$ by Lemma A1, and $\mathbb{E}_{C_n}[e_1(C_n, s^n, x_2^n(M_2, \tilde{M}_2)) | C_n^{(1)} \in \mathcal{C}_1] \to 0$ by Theorem A1 (in Appendix A) using that $R_1 + \tilde{R}_1 < I(X_1;Y) = \frac{1}{2}\log\left(1 + \frac{P_1}{1+L+P_2}\right)$ and by interpreting the signal of Transmitter 2 as noise. Then,

$$E_{C_n}[e_2(C_n, s^n, 0)] \le E_{C_n}[e_2(C_n, s^n, 0)|C_n^{(2)} \in C_2] + P[C_n^{(2)} \notin C_2] \tag{44a}$$

$$\to 0, \quad n \to \infty \tag{44b}$$

where, in Equation (44a), C_2 represents all the sets of unit norm vectors scaled by $\sqrt{nP_2}$ that satisfy the two conditions of Lemma A1, Equation (44b) holds because $P[C_n^{(2)} \notin C_2] \to 0$, $n \to \infty$ by Lemma A1, and $E_{C_n}[e_2(C_n, s^n, 0)|C_n^{(2)} \in C_2] \to 0$, $n \to \infty$ by Theorem A1 using that $R_2 < I(X_2; Y|X_1) = \frac{1}{2}\log\left(1 + \frac{P_2}{1+L}\right)$. Hence, by Equations (41b), (43b) and (44b), we have

$$E_{C_n}[e(C_n, s^n)] \to 0, \quad n \to \infty. \tag{45}$$

Equivocation: We first study the average error probability of decoding (m_1, m_2) given (z^n, m_1, m_2) with the following procedure. Given (z^n, m_1, m_2), determine $\check{m}_2 = y_2(z^n, 0)$, and $\check{m}_1 = y_1(z^n, \sqrt{h_2}x_2^n(m_2, \check{m}_2))$ where

$$y_i(z^n, x) = \begin{cases} m_i & \text{if } \|z^n - x - \sqrt{h_i}x_i^n(m_i, m_i')\|^2 < \|z^n - x - \sqrt{h_i}x_i^n(m_i, m_i^0)\|^2 \\ & \text{for } m_i^0 = m_i \\ 0 & \text{if no such } m_i \in [1, 2^{nR_i}] \text{ exists} \end{cases}. \tag{46}$$

We define $e(C_n) = P[(\check{M}_1, \check{M}_2) = (M_1, M_2)|C_n]$ and for $i \in \{1, 2\}$,

$$e_i(C_n, x) = \frac{1}{(2^{nR_i} - 1)} \sum_{m_i} P\left[\|\sqrt{h_i}x_i^n(m_i, m_i') + x + N_Z^n - \sqrt{h_i}x_i^n(m_i, m_i^0)\|^2 \right.$$
$$\left. \le \|x + N_Z^n\|^2 \text{ for some } m_i^0 \ne m_i\right]. \tag{47}$$

Then, with the same notation as in Equations (43) and (44), we have

$$E_{C_n}[e(C_n)] \le E_{C_n}[e_1(C_n, 0)] + E_{C_n}[e_2(C_n, \sqrt{h_1}x_1(M_1, M_1'))] \tag{48a}$$

$$\le E_{C_n}[e_1(C_n, 0)|C_n^{(1)} \in C_1] + P[C_n^{(1)} \notin C_1]$$
$$+ E_{C_n}[e_2(C_n, \sqrt{h_1}x_1^n(M_1, M_1'))|C_n^{(2)} \in C_2] + P[C_n^{(2)} \notin C_2] \tag{48b}$$

$$\to 0, \quad n \to \infty, \tag{48c}$$

where Equation (48c) holds because $P[C_n^{(1)} \notin C_1] \to 0$, $n \to \infty$ and $P[C_n^{(2)} \notin C_2] \to 0$, $n \to \infty$ by Lemma A1, $E_{C_n}[e_1(C_n, 0)|C_n^{(1)} \in C_1] \to 0$, $n \to \infty$ by Theorem A1 using that $R_1 < I(X_1; Z|X_2) = \frac{1}{2}\log(1 + h_1P_1)$, and $E_{C_n}[e_2(C_n, \sqrt{h_1}x_1^n(M_1, M_1'))|C_n^{(2)} \in C_2] \to 0$ by Theorem A1 using that $R_2 < I(X_2; Z) = \frac{1}{2}\log\left(1 + \frac{h_2P_2}{1+h_1P_1}\right)$ and by interpreting the signal of Transmitter 1 as noise.

Define $M = (M_1, M_2)$, $M' = (M_1', M_2')$. Let the superscript T denote the transpose operation and define $\mathbf{X} = [\sqrt{h_1}(X_1^n)^T \ \sqrt{h_2}(X_2^n)^T]^T \in \mathbb{R}^{2n1}$, such that

$$Z^n = G\mathbf{X} + N_Z^n, \tag{49}$$

with $G = [I_n, I_n] \in \mathbb{R}^{n2n}$ and I_n the identity matrix with dimension n. Let $K_{\mathbf{X}}$ denote the covariance matrix of $\mathbf{X}$. Note that, by independence between X_1^n and X_2^n, we have $K_{\mathbf{X}} = \begin{bmatrix} K_{\sqrt{h_1}X_1^n} & 0_n \\ 0_n & K_{\sqrt{h_2}X_2^n} \end{bmatrix}$, where $0_n = 0 \, I_n$ and $K_{\sqrt{h_i}X_i^n}$ is the covariance matrix of $\sqrt{h_i}X_i^n$, $i \in \{1, 2\}$. Then, for $i \in \{1, 2\}$, since X_i^n is chosen uniformly at random over a sphere of radius $\sqrt{nP_i}$, the off-diagonal elements of $K_{\sqrt{h_i}X_i^n}$ are all equal to 0 by symmetry, and the

diagonal elements are all equal (also by symmetry) and sum to nh_iP_i. Hence, $K^{\sqrt{h_i}X_i^n} = h_iP_iI_n$, $i \in \{1,2\}$, and

$$K_{\mathbf{X}} = \begin{bmatrix} h_1P_1I_n & 0_n \\ 0_n & h_2P_2I_n \end{bmatrix}. \tag{50}$$

Then, we have

$$\begin{aligned}
I(M;Z^n|C_n) &= I(M\hat{M};Z^n|C_n) - I(\hat{M};Z^n|MC_n) && (51a)\\
&= I(M\hat{M};Z^n|C_n) - H(\hat{M}|C_n) + H(\hat{M}|Z^nMC_n) && (51b)\\
&\le I(\mathbf{X};Z^n|C_n) - H(M|C_n) + H(M|Z^nMC_n) && (51c)\\
&= I(\mathbf{X};Z^n) - H(M|C_n) + H(M|Z^nMC_n) && (51d)\\
&= h(Z^n) - h(N_Z^n) - H(\hat{M}|C_n) + H(\hat{M}|Z^nMC_n) && (51e)\\
&= \frac{1}{2}\log|GK_{\mathbf{X}}G^T + I_n| - H(M|C_n) + H(M|Z^nMC_n) && (51f)\\
&= \frac{n}{2}\log(1 + h_1P_1 + h_2P_2) - H(M|C_n) + H(M|Z^nMC_n) && (51g)\\
&= nI(X_1X_2;Z) - H(\hat{M}|C_n) + H(\hat{M}|Z^nMC_n) && (51h)\\
&\le nI(X_1X_2;Z) - n(I(X_1X_2;Z) - 2\delta) + O(nE_{C_n}[\epsilon(C_n)]) && (51i)\\
&= 2\delta n + o(n), && (51j)
\end{aligned}$$

where Equation (51b) holds by independence between M and $\hat{M}$; Equation (51c) holds because $(M, \hat{M}) - (\mathbf{X}, C_n) - Z^n$ forms a Markov chain; Equation (51d) holds because $C_n - \mathbf{X} - Z^n$ forms a Markov chain; Equation (51f) holds because $h(N_Z^n) = \frac{1}{2}\log((2\pi e)^n)$ and because $h(Z^n) \le \frac{1}{2}\log((2\pi e)^n|GK_{\mathbf{X}}G^T + I_n|)$ by Equation (49) and the maximal differential entropy lemma (e.g., [31]) [Eq. (2.6)]; Equation (51g) holds by Equation (50); in Equation (51i), we used the definition of $\epsilon_1 + \epsilon_2$ and the uniformity of $\hat{M}$ to obtain the second term, and Fano's inequality to obtain the third term; Equation (51j) holds by Equation (48c).

Note that the idea of considering a fictitious decoder at the eavesdropper to use Fano's inequality in Equation (51i) is a standard technique that already appeared in [32].

7.2. Case 2

We only consider Case 2.a; Case 2.b is handled by exchanging the role of the transmitters. Let $\underline{R} \in \mathcal{D}(R_1, R_2) \in \mathcal{D}(P_1, P_2)$. There exists $\alpha \in [0,1[$ such that $\underline{R} = (1-\alpha)\underline{C}_1 + \alpha\overline{C}_2$. The corner point $\underline{C}_1$ is achievable by Case 1, however, recall that since the first component of $\overline{C}_2$ is negative, it thus cannot be achieved as in Case 1, and one cannot perform time-sharing between $\underline{C}_1$ and $\overline{C}_2$ to achieve $\underline{R}$. Instead, we achieve $\underline{R}$ as follows. We define $k, k' \in \mathbb{N}$ such that $k'/k = (1-\alpha)^{-1}(1+\varepsilon)$, $\varepsilon > 0$, this is possible by density of $\mathbb{Q}$ in $\mathbb{R}$. We realize a first transmission T_1 as in Case 1 of a pair of confidential messages of length $nk\underline{C}_1$. Part of these confidential messages is dedicated to exchange a secret key of length $nk(I(X_1;Z|X_2) - I(X_1;Y)) > 0$ between Transmitter 1 and the receiver, which is possible because $(1-\alpha)\underline{C}_1 + \alpha\overline{C}_2 = \underline{R}$ has positive components. We then realize a second transmission T_2 of a pair of confidential messages of length $nk(0, I(X_2;Y|X_1) - I(X_2;Z))$ assisted with the secret key that is shared between Transmitter 1 and the receiver. Hence, the overall transmission rate of confidential messages is $\frac{k}{k+k'}\underline{C}_1 + \frac{k'}{k+k'}\overline{C}_2$, which is arbitrarily close to $\underline{R}$ by choosing a sufficiently small ε. We now explain how transmission T_2 is performed. We repeat k' times the following coding scheme.

Codebook construction: Perform the same codebook construction as in Case 1 for Transmitter 2. For Transmitter 1, construct a codebook with $\lfloor 2^{n\hat{R}_1} \rfloor \lceil 2^{n\hat{R}_1} \rceil$ codewords drawn independently and uniformly on the sphere of radius $\sqrt{nP_1}$ in $\mathbb{R}^n$. The codewords

are labeled $x_1^n(\check{m}_1, \hat{m}_1)$, where $\check{m}_1 \in [1, 2^{n\check{R}_1}]$, $\hat{m}_1 \in [1, 2^{n\hat{R}_1}]$. We define the rates $\check{R}_1 = I(X_1;Y) - d$, $\hat{R}_1 = I(X_1;Z|X_2) - I(X_1;Y) - d$, and $R_1 = \check{R}_1 + \hat{R}_1 = I(X_1;Z|X_2) - 2d$.

Encoding at Transmitters: Encoding for Transmitter 2 is as in Case 1. Given $(\check{m}_1, \hat{m}_1)$, Transmitter 1 forms $x_1^n(\check{m}_1, \hat{m}_1)$, where $\hat{m}_1$ is seen as a secret key known at the receiver and that has been shared through transmission T_1 described above. In the following, we define $m_1 = (\check{m}_1, \hat{m}_1)$.

Decoding and average probability of error: As in Case 1, using minimum distance decoding, one can show that on average over the codebooks, the receiver can reconstruct $x_1^n(\check{m}_1, \hat{m}_1)$ with a vanishing average probability of error because $\hat{m}_1$ is known at the receiver and because $\check{R}_1 < I(X_1;Y)$. The receiver can then reconstruct x_2^n as in Case 1.

Equivocation: The equivocation computation for transmission T_2 is as in Case 1 by remarking that it is possible on average over the codebooks to reconstruct with vanishing average probability of error first x_2^n given (z^n, m_2) and then x^n given (z^n, x_2^n) by using that $R_1 \leq I(X_1;Z|X_2)$.

Finally, to conclude that $\underline{R}$ is achievable, we need to show that the secrecy constraint is satisfied for the joint transmissions T_1 and T_2. We use the superscript (T_i) to denote random variables associated with transmission T_i, $i \in \{1,2\}$. Define $M^{(T_1)} = M_1^{(T_1)} \cap \mathring{M}_1^{(T_1)}, M_2^{(T_1)}$, the confidential messages sent during transmission T_1 excluding $\mathring{M}_1^{(T_1)}$, defined as all the confidential messages sent during transmission T_1 and used during transmission T_2. We define $M^{(T_2)} = \check{M}, M_2^{(T_2)}$ as the confidential messages sent during transmission T_2. We define $\hat{M}^{(T_i)} = \hat{M}_1^{(T_i)}, \hat{M}_2^{(T_i)}$ as the randomization sequences used by both transmitters in Transmission T_i, $i \in \{1,2\}$. We also define $\mathbf{X}^{(T_i)}$ as all the channel inputs from both transmitters in Transmission T_i, $i \in \{1,2\}$, and $\mathbf{Z}^{(T_i)}$ as all the channel outputs observed by the eavesdropper in Transmission $i \in \{1,2\}$. Finally, we define $M^{(T_1,T_2)} = M^{(T_1)}, M^{(T_2)}$, $\hat{M}^{(T_1,T_2)} = \hat{M}^{(T_1)}, \hat{M}^{(T_2)}$, $\mathbf{Z}^{(T_1,T_2)} = \mathbf{Z}^{(T_1)}, \mathbf{Z}^{(T_2)}$, $\mathbf{X}^{(T_1,T_2)} = \mathbf{X}^{(T_1)}, \mathbf{X}^{(T_2)}$, $C_n^{(T_1,T_2)} = C_n^{(T_1)}, C_n^{(T_2)}$. We have

$$
\begin{aligned}
& I(M^{(T_1,T_2)}; \mathbf{Z}^{(T_1,T_2)} | C_n^{(T_1,T_2)}) \\
&= I(M^{(T_1,T_2)}\hat{M}^{(T_1,T_2)}; \mathbf{Z}^{(T_1,T_2)} | C_n^{(T_1,T_2)}) - I(\hat{M}^{(T_1,T_2)}; \mathbf{Z}^{(T_1,T_2)} | M^{(T_1,T_2)} C_n^{(T_1,T_2)}) && \text{(52a)} \\
&= I(M^{(T_1,T_2)}\hat{M}^{(T_1,T_2)}; \mathbf{Z}^{(T_1,T_2)} | C_n^{(T_1,T_2)}) - H(\hat{M}^{(T_1,T_2)} | C_n^{(T_1,T_2)}) \\
&\quad + H(\hat{M}^{(T_1,T_2)} | \mathbf{Z}^{(T_1,T_2)} M^{(T_1,T_2)} C_n^{(T_1,T_2)}) && \text{(52b)} \\
& I(\mathbf{X}^{(T_1,T_2)}; \mathbf{Z}^{(T_1,T_2)} | C^{(T_1,T_2)}_n) - H(M^{(T_1,T_2)} | C^{(T_1,T_2)}_n) \\
&\quad + H(\hat{M}^{(T_1,T_2)} | \mathbf{Z}^{(T_1,T_2)} M^{(T_1,T_2)} C_n^{(T_1,T_2)}) && \text{(52c)} \\
& I(\mathbf{X}^{(T_1,T_2)}; \mathbf{Z}^{(T_1,T_2)}) - H(M^{(T_1,T_2)} | C^{(T_1,T_2)}_n) + H(M^{(T_1,T_2)} | \mathbf{Z}^{(T_1,T_2)} M^{(T_1,T_2)} C^{(T_1,T_2)}_n) && \text{(52d)} \\
& n(k + k') I(X_1 X_2; Z) - H(M^{(T_1,T_2)} | C^{(T_1,T_2)}_n) + H(M^{(T_1,T_2)} | \mathbf{Z}^{(T_1,T_2)} M^{(T_1,T_2)} C^{(T_1,T_2)}_n) && \text{(52e)} \\
& 3nd(k + k') + H(M^{(T_1,T_2)} | \mathbf{Z}^{(T_1,T_2)} M^{(T_1,T_2)} C^{(T_1,T_2)}_n) && \text{(52f)} \\
& 3nd(k + k') + O\left(n E_{C_n^{(T_1,T_2)}}[e(C_n^{(T_1,T_2)})]\right), && \text{(52g)}
\end{aligned}
$$

where Equation (52b) holds because we defined $M^{(T_1,T_2)}$ such that $M^{(T_1,T_2)}$ is independent from $\hat{M}^{(T_1,T_2)}$, Equation (52c) holds because $(M^{(T_1,T_2)}, \hat{M}^{(T_1,T_2)}) - C_n^{(T_1,T_2)} - \mathbf{X}^{(T_1,T_2)} - \mathbf{Z}^{(T_1,T_2)}$ forms a Markov chain, Equation (52d) holds because $C_n^{(T_1,T_2)} - \mathbf{X}^{(T_1,T_2)} - \mathbf{Z}^{(T_1,T_2)}$ forms a Markov chain, Equation (52e) holds similar to Equation (51h), Equation (52f) holds because by definition $R_1 + R_2 \leq I(X_1X_2;Z) - 3d$, Equation (52g) holds by Fano's

inequality with $e(C_n^{(T_1,T_2)})$ defined as the probability of error to reconstruct $M^{(T_1,T_2)}$ given $Z^{(T_1,T_2)}$, $M^{(T_1,T_2)}$ using minimum distance decoding as in Case 1. Then, define $e^{(1)}(C_n^{(T_1,T_2)})$ as the error probability to reconstruct $M^{(T_2)}$ from $Z^{(T_2)}$, $M^{(T_2)}$ using minimum distance decoding, and $e^{(2)}(C_n^{(T_1,T_2)})$ as the error probability to reconstruct $M^{(T_1)}$ from $Z^{(T_1)}$, $M^{(T_1)}$, $M^{(T_2)}$ using minimum distance decoding. As in the analysis of Case 1 and by observing that $M_1^{(T_1)}$ is included in $M^{(T_2)}$, we have

$$E_{C_n^{(T_1,T_2)}}[e(C_n^{(T_1,T_2)})] \leq E_{(C_n^{T_1},C_n^{T_2})}[e^{(1)}(C_n^{(T_1,T_2)})] + E_{(C_n^{T_1},C_n^{T_2})}[e^{(2)}(C_n^{(T_1,T_2)})] \tag{53a}$$

$$\leq n\,!\,\infty\ 0. \tag{53b}$$

We conclude from Equations (52g) and (53b)

$$I(M^{(T_1,T_2)};Z^{(T_1,T_2)}|C_n^{(T_1,T_2)}) = 3nd(k+k^0)+o(n). \tag{54}$$

7.3. Case 3

We have $I(X_1;Z|X_2) \geq I(X_1;Y) > 0$ and $I(X_2;Z|X_1) \geq I(X_2;Y) > 0$ as depicted in Figure 5. Assume $I(X_1X_2;Y) \geq I(X_1X_2;Z) > 0$, otherwise $R_{1,2}^{MAC}(P_1,P_2) = \{(0,0)\}$. We will use the following lemma.

Lemma 2. Define $h_L \triangleq (1+L)^{-1}$. We have

1. $I(X_1;Z|X_2) \geq I(X_1;Y)$ $I(X_1;Y|X_2) \geq I(X_1;Z)$ or $I(X_2;Z|X_1) \geq I(X_2;Y)$ $I(X_2;Y|X_1) \geq I(X_2;Z)$. 2. $h_1 < h_L$ or $h_2 < h_L$.
3. Assume $I(X_1;Z|X_2) \geq I(X_1;Y)$ $I(X_1;Y|X_2) \geq I(X_1;Z)$. There exists $m,m^0 \in \mathbb{N}$, such that

$$m^0(I(X_1;Y|X_2) \geq I(X_1;Z)) \leq m(I(X_1;Z|X_2) \geq I(X_1;Y)), \tag{55a}$$

$$m(I(X_2;Y|X_1) \geq I(X_2;Z)) > m^0(I(X_2;Z|X_1) \geq I(X_2;Y)). \tag{55b}$$

Proof. (i) Assume that

$$I(X_1;Z|X_2) \geq I(X_1;Y) > I(X_1;Y|X_2) \geq I(X_1;Z), \tag{56a}$$

$$I(X_2;Z|X_1) \geq I(X_2;Y) > I(X_2;Y|X_1) \geq I(X_2;Z). \tag{56b}$$

Then,

$$\begin{aligned} &I(X_1;Z|X_2) \geq I(X_1;Y) + I(X_2;Z|X_1) \geq I(X_2;Y) \\ &> I(X_1;Y|X_2) \geq I(X_1;Z) + I(X_2;Y|X_1) \geq I(X_2;Z), \end{aligned} \tag{57}$$

which contradicts the fact that $I(X_1;Z|X_2) \geq I(X_1;Y) < I(X_2;Y|X_1) \geq I(X_2;Z)$ and $I(X_2;Z|X_1) \geq I(X_2;Y) < I(X_1;Y|X_2) \geq I(X_1;Z)$.

(ii) By contradiction, if $h_1 \geq h_L$ and $h_2 \geq h_L$, then $I(X_1X_2;Y) \geq I(X_1X_2;Z)$ 0. (iii) Choose $m \in \mathbb{N}$ such that

$$I(X_1;Z|X_2) \geq I(X_1;Y) \leq m^0(I(X_1X_2;Y) \geq I(X_1X_2;Z)). \tag{58}$$

Then, there exists $m \in \mathbb{N}$ and $r \in [0, I(X_1;Z|X_2) \geq I(X_1;Y)[$ such that

$$m^0(I(X_1;Y|X_2) \geq I(X_1;Z)) = m(I(X_1;Z|X_2) \geq I(X_1;Y)) + r. \tag{59}$$

Then, we have

$$\begin{aligned}
& m(I(X_2;Y|X_1) - I(X_2;Z)) \\
&= m(I(X_1;Z|X_2) - I(X_1;Y)) + m(I(X_1X_2;Y) - I(X_1X_2;Z)) && \text{(60a)}\\
&= m'(I(X_1;Y|X_2) - I(X_1;Z)) + m(I(X_1X_2;Y) - I(X_1X_2;Z)) - r && \text{(60b)}\\
&= m'(I(X_2;Z|X_1) - I(X_2;Y)) + (m+m')(I(X_1X_2;Y) - I(X_1X_2;Z)) - r && \text{(60c)}\\
&> m'(I(X_2;Z|X_1) - I(X_2;Y)) + m(I(X_1X_2;Y) - I(X_1X_2;Z)) && \text{(60d)}\\
&> m'(I(X_2;Z|X_1) - I(X_2;Y)), && \text{(60e)}
\end{aligned}$$

where Equation (60b) holds by Equation (59), and Equation (60d) holds because $r < I(X_1;Z|X_2) - I(X_1;Y) - m'(I(X_1X_2;Y) - I(X_1X_2;Z))$. □

By (i) in Lemma 2, assume without loss of generality that $I(X_1;Z|X_2) - I(X_1;Y) \le I(X_1;Y|X_2) - I(X_1;Z)$ by exchanging the role of the transmitters if necessary. We let m, m' be as in (iii) of Lemma 2. $D(P_1, P_2)$ is achieved in four steps.

Step 1. During a first transmission T_0, Transmitter 2 transmits a confidential message of length $nm'(I(X_2;Z|X_1) - I(X_2;Y))$ to the receiver. This is possible with a point-to-point wiretap code; as in Case 1, when Transmitter 1 remains silent and when $h_L > h_2$. If, on the other hand, $h_L \le h_2$, then by (ii) in Lemma 2, $h_L > h_1$ and Transmitter 2 can transmit a confidential message of length $nm'(I(X_2;Z|X_1) - I(X_2;Y))$ as follows. Transmitter 1 transmits a confidential message of length $nk(I(X_1;Z|X_2) - I(X_1;Y))$, where $k \in \mathbb{N}$ is such that $nk(I(X_2;Y|X_1) - I(X_2;Z)) \le nm'(I(X_2;Z|X_1) - I(X_2;Y))$. Using this secret key shared by Transmitter 1 and the receiver, Transmitter 2 can transmit a confidential message of length $nk(I(X_2;Y|X_1) - I(X_2;Z))$ as in Case 2. Note that Step 1 is operated in a fixed number of blocks of length n.

Step 2. As in Case 2, the transmitters achieve transmission T_1 of confidential messages of length $(nm'(I(X_1;Y|X_2) - I(X_1;Z)), 0)$ by using the secret key exchanged during T_0 between Transmitter 2 and the receiver. Then, as in Case 2 and because $m'(I(X_1;Y|X_2) - I(X_1;Z)) \le m(I(X_1;Z|X_2) - I(X_1;Y)) \le 0$ by (iii) in Lemma 2, the transmitters achieve a transmission T_2 of confidential messages of length $(0, nm(I(X_2;Y|X_1) - I(X_2;Z)))$ using a secret key of length $nm(I(X_1;Z|X_2) - I(X_1;Y))$ exchanged between Transmitter 1 and the receiver during T_1. Hence, after T_1 and T_2, the transmitters achieved the transmission of confidential messages of length $(nm'(I(X_1;Y|X_2) - I(X_1;Z)) - nm(I(X_1;Z|X_2) - I(X_1;Y)), nm(I(X_2;Y|X_1) - I(X_2;Z)))$.

Step 3. The transmitters repeat T_1 and T_2 t times, where t is arbitrary, since $m(I(X_2;Y|X_1) - I(X_2;Z)) - m'(I(X_2;Z|X_1) - I(X_2;Y)) > 0$ by (iii) in Lemma 2. After these t repetitions, the rate pair achieved is arbitrarily close to

$$\begin{aligned}
\underline{R} = \frac{1}{m+m'}\big(& m'(I(X_1;Y|X_2) - I(X_1;Z)) - m(I(X_1;Z|X_2) - I(X_1;Y)), \\
& m(I(X_2;Y|X_1) - I(X_2;Z)) - m'(I(X_2;Z|X_1) - I(X_2;Y))\big) && \text{(61)}
\end{aligned}$$

provided that t is large enough since Step 1 only requires a fixed number of transmission blocks. Observe that $\underline{R} \in D(P_1, P_2)$.

Step 4. Any point of $D(P_1, P_2)$ can then be achieved as in Case 2 by doing the substitutions $\underline{C}_1 \to \underline{R}$ and $\underline{C}_2 \to \underline{R}$ in Case 2.a and Case 2.b, respectively.

The proof that secrecy holds over the joint transmissions is similar to Case 2 and thus omitted.

8. Proof of Theorem 3

We first show that determining a converse for our model reduces to determining a converse for a similar model when the jammer is inactive, i.e., when $L = 0$.

Lemma 3. Let $\mathcal{O}' \triangleq \{(R_1, R_2) : R_1 \le B_1, R_2 \le B_2, R_1 + R_2 \le B_{1,2}\}$ be an outer bound, i.e., a set that contains all possibly achievable rate pairs, for the Gaussian MAC-WT-JA with parameters $(G_1, G_2, h_1, h_2, 0, s^2 + \Lambda, s_Y^2)$. Then,

$$\left\{(R_1, R_2) : R_1 \le \begin{cases} B_1 & \text{if } G_1 > \Lambda \\ 0 & \text{if } G_2 \le \Lambda \end{cases}, R_2 \le \begin{cases} B_2 & \text{if } G_2 > \Lambda \\ 0 & \text{if } G \le \Lambda \end{cases}, R_1 + R_2 \le B_{1,2}\right\}$$

is an outer bound for the Gaussian MAC-WT-JA with parameters $(G_1, G_2, h_1, h_2, \Lambda, s_Y^2, s_Z^2)$.

Proof. Consider any encoders and decoder for the Gaussian MAC-WT-JA with the parameters $(G_1, G_2, h_1, h_2, \Lambda, s_Y^2, s_Z^2)$ that achieve the rate pair (R_1, R_2). Note that by [24] [Theorem 2.3], for any $l \in \{1, 2\}$ such that $G_l \le \Lambda$, we must have $R_l = 0$, since an outer bound for the model in [24] is also an outer bound for the Gaussian MAC-WT-JA, which has the additional security constraint (2b). Then, to derive an outer bound, it is sufficient to consider a specific jamming strategy and study the best achievable rates for this jamming strategy, since the boundaries of the capacity region correspond to the best (from the jammer's point of view) jamming strategies and any other jamming strategy can only enlarge the set of achievable rates. We assume that in each transmission block, the jamming sequence is S^n with the components independent and identically distributed according to a zero-mean Gaussian random variable with the variance $\Lambda' < \Lambda$. The average probability of error at the legitimate receiver is thus upper-bounded by $\sup_{S \in \mathcal{S}} P[\hat{M} \ne M] + \mathbb{P}[\|S^n\|^2 > n\Lambda] \le n \to \infty \to 0$ where we used the notation of Definition 1 and the fact that $\mathbb{P}[\|S^n\|^2 > n\Lambda] \xrightarrow{n \to \infty} 0$ since $\Lambda' < \Lambda$. Hence, since the secrecy constraint is independent of Λ', we obtain the reliability and secrecy constraints for a Gaussian MAC-WT-JA with parameters $(G_1, G_2, h_1, h_2, 0, s^2 + \Lambda', s_Y^2)$, meaning that $(R_1, R_2) \in \mathcal{O}'$, where $\mathcal{O}'$ is an outer bound for the Gaussian MAC-WT-JA with parameters $(G_1, G_2, h_1, h_2, 0, s_Y^2 + \Lambda', s_Z^2)$. Finally, we conclude the proof by choosing Λ' arbitrarily close to Λ. □

We now obtain Theorem 3 as follows. (i) holds from Lemma 3. (ii) holds from Lemma 3 and [33] [Theorem 6] by remarking that $x \to \log \frac{1+x(1+\Lambda)^{-1}}{1+xh}$ is non-decreasing when $(1+\Lambda)^{-1} > h$ and negative when $(1+\Lambda)^{-1} < h$.

9. Concluding Remarks

In this paper, we defined Gaussian wiretap channels in the presence of an eavesdropper aided by a jammer. The jamming signal is power-constrained and assumed to be oblivious of the legitimate users' communication but is not restricted to be Gaussian. We studied several models in this framework, namely point-to-point, multiple-access, broadcast, and symmetric interference settings. We derived inner and outer bounds for these settings, and identified conditions for these bounds to coincide. We stress that no shared randomness among the legitimate users is required in our coding schemes.

Our achievability scheme for the Gaussian MAC-WT-JA relies on novel time-sharing strategies and an extension of successive decoding for multiple-access channels to multiple-access wiretap channels via secret-key exchanges. An open problem remains to provide a scheme that avoids time-sharing. Section 4.2 provides such a scheme for some rate pairs and channel parameters; however, it might not be possible to achieve the entire region of Theorem 2 by solely relying on point-to-point codes, in which case the design of multi-transmitter codes for arbitrarily varying multiple-access channels would be necessary.

Finally, beyond proving the existence of achievability schemes for our models, finding explicit coding schemes largely remains an open problem. We note that [34] investigates this problem for short communication blocklengths over point-to-point channels via a practical approach that relies on deep learning. Another open problem is to achieve the same regions as that derived in this paper under strong and semantic security guarantees.

Author Contributions: The ideas in this work were formed by the discussions between R.A.C. and A.Y. Both authors collaborated on the writing of the manuscript. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported in part by NSF grants CIF-1319338, CNS-1314719, CCF-2105872, and CCF-2047913.

Institutional Review Board Statement: Not applicable.

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

Appendix A. Supporting Results

Lemma A1 ([1]). Let $e > 0$, $h \in]8^{p}e, 1[$, $K > 2e$, $R \in [2e, K]$, and $N \doteq e^{nR}$. Let $X_1^n, \ldots, X_N^n$ be independent random variables uniformly distributed on the unit sphere. With probability arbitrarily close to one as $n \to \infty$, we have

1. $|\{j : |\langle X_j^n, u^n\rangle| \geq a\}| \leq e^{n\left[R + \frac{1}{2}\log(1-a^2) + \frac{1}{2}e\right]^+}$ for any unit vector $u^n \in \mathbb{R}^n$, $a > 0$.
2. $\frac{1}{N}|\{i : |\langle X_j^n, X_i^n\rangle| \geq a, |\langle X^n, u^n\rangle| \geq b, \text{ for some } j = i\}| \leq e^{ne}$ for any unit vector $u^n \in \mathbb{R}^n$, $a, b \in [0,1]$ such that $a \sqrt{h}, a^2 + b^2 > 1 + h - e^{-2R}$.

Theorem A1 ([1,24]). Consider a channel whose output is defined as $Y^n = X^n + V^n + s^n$, where X^n is the input such that $\|X^n\|^2 \leq n$, V^n represents noise (to be defined next), and s^n is a state unknown to the encoder and decoder such that $\|s^n\|^2 \leq nL$, $L < 1$. Let $s, d > 0$. Consider a codebook C_n made of $N \doteq e^{n(\frac{1}{2}\log(1+(L+s^2)^{-1})-d)}$ codewords $(x_1^n, \ldots, x_N^n)$ that satisfy the two conditions of Lemma A1, and define the average probability of error $e(C_n)$ of a minimum distance decoder as $e(C_n) \doteq \frac{1}{N}\sum_{i=1}^{N} P[\|x_i^n + s^n + V^n - x_j^n\|^2 \leq \|s^n + V^n\|^2, \text{ for some } j \neq i]$.

1. (From [1]). If V^n is a vector with i.i.d. zero-mean Gaussian coordinates with variance s^2, then $\lim_{n\to\infty} e(C_n) = 0$.
2. (From [24]). If $V^n \doteq W^n + U$, where W^n is a vector with i.i.d. zero-mean Gaussian coordinates with variance a^2 and U is independently distributed uniformly at random on a sphere with radius $\sqrt{nb^2}$ such that $a^2 + b^2 = s^2$, then $\lim_{n\to\infty} e(C_n) = 0$.

Appendix B. Proof of Theorem 4

We first recall some definitions and results on polymatroids.

Definition A1 ([35]). Let $f : 2^M \to \mathbb{R}$. $P(f) \doteq \{(R_i)_{i\in M} \in \mathbb{R}^M : R_S \leq f(S), \forall S \subseteq M\}$ associated with the function f is an extended polymatroid if f is submodular, i.e., $\forall S, T \subseteq M$, $f(S \cup T) + f(S \cap T) \leq f(S) + f(T)$.

Property A1 ([29] [Property 1]). Define $g : 2^{L(L)} \to \mathbb{R}, T \to I(X_T; Y|X_{T^c}) - I(X_T; Z)$, where $Y \doteq \sum_{l\in L(L)} X_l + N_Y$, $Z \doteq \sum_{l\in L(L)} \sqrt{h_l} X_l + N_Z$, with $(X_l)_{l\in L(L)}$, N_Y, N_Z independent zero-mean Gaussian random variables with variances $(P_l)_{l\in L(L)}$, $(1+L)$, 1, respectively.

$$C(L) \doteq \left\{(R_l)_{l\in L(L)} \in \mathbb{R}^{|L(L)|} : \forall T \subseteq L(L), R_T \leq g(T)\right\} \tag{A1}$$

associated with g is an extended polymatroid.

Property A2 ([35]). Define the dominant face $D(L)$ of $C(L)$ as

$$D(L) \doteq \left\{(R_l)_{l\in L(L)} \in C(L) : R_{L(L)} = g(L(L))\right\}. \tag{A2}$$

For $p \in \mathrm{Sym}(|L(L)|)$, where $\mathrm{Sym}(|L(L)|)$ is the symmetric group on $L(L)$, for $i, j \in L(L)$, define $p^{i:j} \doteq (p(k))_{k\in\{i,\ldots,j\}}$. $D(L)$ is the convex hull of the vertices

$\mathcal{V} \triangleq \{(C_{p(i)})_{i\in[1,|L(L)|]} : p \in \mathrm{Sym}(|L(L)|)\}$, where for $p \in \mathrm{Sym}(|L(L)|)$, for $i \in [1,|L(L)|]$, $C_{p(i)} = \mathcal{G} \setminus \mathcal{F}^{p^{[i:|L(L)|]}}\mathcal{G} \setminus \mathcal{G} \setminus \mathcal{F}^{p^{[i+1:|L(L)|]}}\mathcal{G}$.

Define $\mathcal{D}_+(L) \triangleq \mathcal{D}(L) \setminus \mathcal{R}_+^{|L(L)|}$. By Property A2, for any $\underline{R} \in \mathcal{D}_+(L)$, for any $\underline{V} = (V_l)_{l\in L(L)} \in \mathcal{V}$, there exists $\alpha_{\underline{V}} \in [0,1]$, such that $\sum_{\underline{V}\in\mathcal{V}} \alpha_{\underline{V}} = 1$ and $\underline{R} = \sum_{\underline{V}\in\mathcal{V}} \alpha_{\underline{V}}\underline{V}$. As remarked in [29], g is, in general, not non-decreasing; hence, some $\underline{V} \in \mathcal{V}$ might have negative components and the successive decoding method [5] [Appendix C] cannot be applied to the multiple-access wiretap channel. We show in the following how to overcome this issue. For $l \in L(L)$, define $R_l \triangleq \sum_{\underline{V}\in\mathcal{V}} \alpha_{\underline{V}} \mathbb{1}\{V_l > 0\}$, and $\underline{R} \triangleq (R_l)_{l\in L(L)}$. Our coding scheme operates in three steps, the idea of which is described below.

Step 1. For $l \in L(L)$, a secret message of length nR_l is exchanged between Transmitter l and the receiver.

Step 2. For all $\underline{V} \in \mathcal{V}$, secret messages of length $n(\alpha_{\underline{V}}\mathbb{1}\{V_l > 0\})_{l\in L(L)}$ are exchanged between the transmitters and the receiver, provided that secret sequences of length $n\underline{R}$ are shared between the transmitters and the receiver, which is ensured by Step 1. The overall length of secret communication is $n(\sum_{\underline{V}\in\mathcal{V}} \alpha_{\underline{V}}\mathbb{1}\{V_l > 0\})_{l\in L(L)}$, i.e., $n(\underline{R} + \underline{R}')$.

Step 3. Repeat t times Step 2. It is possible to do so because secret sequences of length at least $n\underline{R}$ were exchanged between the transmitters and the receiver in Step 2. The overall rate of secret sequences exchanged between the transmitters and the receiver is thus $\underline{R}$, provided that t is large enough, since Step 1 only requires the transmission of a finite number of blocks.

The coding schemes and their analyses to realize Steps 1 and 2 are described in Appendix B.1 and Appendix B.2, respectively. In the remainder of the section, Y and Z are defined as in Property A1 with $(X_l)_{l\in L(L)}$ zero-mean Gaussian random variables with variances $(P_l)_{l\in L(L)}$.

Appendix B.1. Proof of Step 1

The proof of Step 1 directly follows from the point-to-point setting, i.e., Theorem 1, applied to each $l \in L(L)$ since we assumed $h_l < h_L$.

Appendix B.2. Proof of Step 2

We fix $\underline{V} \in \mathcal{V}$. The following procedure must be reiterated for each $\underline{V} \in \mathcal{V}$ by applying a permutation $p \in \mathrm{Sym}(|L(L)|)$ on the labeling of the transmitters. For convenience, we relabel the transmitter from 1 to $|L(L)|$ and redefine $L(L)$ as $[1,|L(L)|]$. We show how to exchange secret messages with rate $(\mathbb{1}\{V_l > 0\})_{l\in L(L)}$ between the transmitters and the receiver, when they have access to pre-shared secrets (obtained from Step 1) with rate $(\mathbb{1}\{V_l < 0\})_{l\in L(L)}$. Define $\mathcal{I} \triangleq \{l \in L(L) : V_l \neq 0\}$ and $\mathcal{I}^c \triangleq L(L)\setminus\mathcal{I}$. We also use the notation $X_{L(L)} \triangleq (X_l)_{l\in L(L)}$, $X_{\mathcal{I}} \triangleq (X_l)_{l\in\mathcal{I}}$, and for $i, j \in L(L)$, $X_{i:j} \triangleq (X_l)_{l\in[i,j]}$.

Codebook construction: For Transmitter $i \in \mathcal{I}^c$, construct a codebook $\mathcal{C}_n^{(i)}$ with $\lceil 2^{nR_i}\rceil\lceil 2^{n\breve{R}_i}\rceil$ codewords drawn independently and uniformly on the sphere of radius $\sqrt{nP_i}$ in $\mathbb{R}^n$. The codewords are labeled $x_i^n(m_i, \breve{m}_i)$, where $m_i \in [1, 2^{nR_i}]$, $\breve{m}_i \in [1, 2^{n\breve{R}_i}]$. We choose the rates as $R_i \triangleq I(X_i;Y|X_{1:i-1}) - I(X_i;Z|X_{i+1:|L(L)|}) - d$, $\breve{R}_i \triangleq I(X_i;Z|X_{i+1:|L(L)|}) - d$. For Transmitter $i \in \mathcal{I}$, construct a codebook $\mathcal{C}_n^{(i)}$ with $\lceil 2^{n\breve{R}_i}\rceil\lceil 2^{n\hat{R}_i}\rceil$ codewords drawn independently and uniformly on the sphere of radius $\sqrt{nP_i}$ in $\mathbb{R}^n$. The codewords are labeled $x_i^n(\breve{m}_i, \hat{m}_i)$, where $\breve{m}_i \in [1, 2^{n\breve{R}_i}]$, $\hat{m}_i \in [1, 2^{n\hat{R}_i}]$. We define the rates $\breve{R}_i \triangleq I(X_i;Y|X_{1:i-1}) - d$, $\hat{R}_i \triangleq I(X_i;Z|X_{i+1:|L(L)|}) - I(X_i;Y|X_{1:i-1}) - d$, and $\breve{R}_i \triangleq \breve{R}_i + \hat{R}_i = I(X_i;Z|X_{i+1:|L(L)|}) - 2d$. Define $\mathcal{C}_n \triangleq (\mathcal{C}_n^{(i)})_{i\in L(L)}$.

Encoding at the transmitters: For Transmitter $i \in \mathcal{I}^c$, given $(m_i, \breve{m}_i)$, transmit $x_i^n(m_i, \breve{m}_i)$. For Transmitter $i \in \mathcal{I}$, given $(\breve{m}_i, \hat{m}_i)$, transmit $x_i^n(m_i, \hat{m}_i)$, where m_i is assumed to be known at the receiver by the transmissions in Step 1. In the following, we define for $i \in \mathcal{I}$,

$\tilde{m}_i \triangleq (\tilde{m}_i, \hat{m}_i)$. By convention, define for $i \in I$, $m_i \triangleq \check{m}$. Also define $m \triangleq (m_i)_{i \in L(L)}$, $\tilde{m} \triangleq (\tilde{m}_i)_{i \in L(L)}$. In the following, we refer to $\tilde{m}$ as randomization sequence.

Decoding: The receiver performs minimum distance decoding, i.e., given y^n, determine starting from $i = 1$ to $i = |L(L)|$, $(\hat{m}_i, \hat{\tilde{m}}_i) \triangleq f_i(y^n, \sum_{j=1}^{i-1} x_j^n(\hat{m}_j, \hat{\tilde{m}}_j))$ where

$$f_i : (y^n, x) \to \begin{cases} (m_i, \tilde{m}_i) & \text{if } \|y^n - x - x_i^n(m_i, \tilde{m}_i)\|^2 < \|y^n - x - x_i^n(m_i', \tilde{m}_i')\|^2 \\ & \text{for } (m_i', \tilde{m}_i') = (m_i, \tilde{m}_i). \\ 0 & \text{if no such } (m_i, \tilde{m}_i) \in [1, 2^{nR_i}] \times [1, 2^{n\tilde{R}_i}] \text{ exists} \end{cases} \tag{A3}$$

Define $\hat{m} \triangleq (\hat{m}_i)_{i \in L(L)}$, $\hat{\tilde{m}} \triangleq (\hat{\tilde{m}}_i)_{i \in L(L)}$. Let $e(C_n, s^n) \triangleq P\left[\hat{M} \neq M \,|\, C_n\right]$, we now prove that on average on C_n, we have $E_{C_n}[\sup_{s^n} e(C_n, s^n)] + \frac{1}{n} I(M; Z^n | C_n) \xrightarrow{n \to \infty} 0$. We will thus conclude that there exists a sequence of realizations (C_n) of (C_n) such that both $\sup_{s^n} e(C_n, s^n)$ and $\frac{1}{n} I(M; Z^n | C_n)$ can be made arbitrarily close to zero as $n \to \infty$.

Average probability of error: We have

$$e(C_n, s^n) \triangleq P\left[\hat{M} \neq M \text{ or } \hat{\tilde{M}} \neq \tilde{M} \,|\, C_n\right] \tag{A4a}$$

$$= \sum_{i \in L(L)} e_i\left(C_n, s^n, \sum_{j=i+1}^{|L(L)|} x^n(M_j, \tilde{M}_j)\right), \tag{A4b}$$

where for $i \in L(L)$

$$e_i(C_n, s^n, x) \triangleq \frac{1}{2^{n\tilde{R}_i} \prod_{j \neq i} 2^{nR_j}} \sum_{m_i} \sum_{\tilde{m}_i} P\left[\|x^n(m_i, \tilde{m}_i) + s^n + x + N^n - x^n(m_i', \tilde{m}_i')\|^2 \leq \|s^n + x + N^n\|^2 \text{ for some } (m_i', \tilde{m}_i') \neq (m_i, \tilde{m}_i)\right]. \tag{A5}$$

Assume that the receiver has reconstructed $(m_j, \tilde{m}_j)_{j \in [1, i-1]}$, for $i \in L(L)$. Assume first that $i + 1 \in I^c$. Using minimum distance decoding, on average over the codebooks, we show that the receiver can reconstruct x_{i+1}^n. We have

$$E_{C_n}\left[e_i\left(C_n, s^n, \sum_{j=i+1}^{|L(L)|} x^n(M_j, \tilde{M}_j)\right)\right]$$

$$E_{C_n}\left[e_i\left(C_n, s^n, \sum_{j=i+1}^{|L(L)|} x_j^n(M_j, \tilde{M}_j)\right) \,\middle|\, C_n^{(i)} \in \mathcal{C}_i\right] + P\left[C_n^{(i)} \notin \mathcal{C}_i\right] \tag{A6a}$$

$$\xrightarrow{n \to \infty} 0, \tag{A6b}$$

where in Equation (A6a) $\mathcal{C}_i$ represents all the sets of unit norm vectors scaled by $\sqrt{n P_i}$ that satisfy the two conditions of Lemma A1 (in Appendix A), Equation (A6b) holds because $P[C_n^{(i)} \notin \mathcal{C}_i] \xrightarrow{n \to \infty} 0$ by Lemma A1, and $E_{C_n}\left[e_i\left(C_n, s^n, \sum_{j=i+1}^{|L(L)|} x_j^n(M_j, \tilde{M}_j)\right) \,\middle|\, C_n^{(i)} \in \mathcal{C}_i\right] \xrightarrow{n \to \infty} 0$ by Theorem A1 (in Appendix A) using the definition of $R_i + \tilde{R}_i$ and by interpreting the signal of transmitters in $[i+1, |L(L)|]$ as noise.

Similarly, when $i + 1 \in I$, using minimum distance decoding, on average over the codebooks, the receiver can reconstruct $x_{i+1}^n(\tilde{m}_{i+1}, \hat{m}_{i+1})$ with a vanishing average probability of error because $\hat{m}_{i+1}$ is known at the receiver and by definition of $\tilde{R}_{i+1}$, hence,

$$E_{C_n}[e(C_n, s^n)] \xrightarrow{n \to \infty} 0. \tag{A7}$$

Equivocation: We first study the average error probability of decoding $\hat{m}_i$ given (z^n, m) with the following procedure. From $i = |L(L)|$ to $i = 1$, given (z^n, m), determine m_i or $\hat{m}_i$ as $y_i(z^n, \sum_{j=i+1}^{|L(L)|} \sqrt{h_j} x_j^n(m_j, \hat{m}_j))$, where for $i \in L(L)$

$$y_i : (z^n, x) \to \begin{cases} m_i & \text{if } \|z^n - x - \sqrt{h_i} x_i^n(m_i, \hat{m}_i)\|^2 < \|z^n - x - \sqrt{h_i} x_i^n(m_i, \hat{m}_i')\|^2 \\ & \text{for } \hat{m}_i' \neq \hat{m}_i \\ 0 & \text{if no such } \hat{m}_i \in [1, 2^{nR_i}] \text{ exists} \end{cases}. \quad \text{(A8)}$$

We define $e(C_n) \triangleq P[\hat{M} \neq M | C_n]$. We have

$$e(C_n) = \sum_{i \in L(L)} e_i(C_n, \sum_{j=1}^{i-1} \sqrt{h_j} x_j^n(M_j, \hat{M}_j)), \quad \text{(A9)}$$

where for $i \in L(L)$

$$e_i(C_n, x) \triangleq \frac{1}{2^{nR_i}} \sum_{\hat{m}_i} P[\|\sqrt{h_i} x_i(m_i, \hat{m}_i) + x + Z^n - \sqrt{h_i} x_i(m_i, m_i')\|^2 \leq \|x + Z^n\|^2 \text{ for some } m_i' \neq m_i]. \quad \text{(A10)}$$

Similar to the justifications for obtaining Equation (A6b), $E_{C_n}[e_i(C_n, \sum_{j=1}^{i-1} \sqrt{h_j} x_j^n(M_j, \hat{M}_j))]$ vanishes to zero as $n \to \infty$ by interpreting the signal of transmitters in $[1, i-1]$ as noise and by using the definition of R_i. We thus obtain

$$E_{C_n}[e(C_n)] \xrightarrow{n \to \infty} 0. \quad \text{(A11)}$$

Let the superscript T denote the transpose operation and define $\mathbf{X} \triangleq [\sqrt{h_1}(X_1^n)^T \sqrt{h_2}(X_2^n)^T \ldots \sqrt{h_{|L(L)|}}(X_{|L(L)|}^n)^T]^T \in \mathbb{R}^{n|L(L)|1}$, such that

$$Z^n = G\mathbf{X} + N_Z^n, \quad \text{(A12)}$$

with $G \triangleq [I_n, I_n, \ldots, I_n] \in \mathbb{R}^{n \times n|L(L)|}$ and I_n the identity matrix with dimension n. Let $K_{\mathbf{X}}$ denote the covariance matrix of $\mathbf{X}$. Similar to Equation (50), we have

$$K_{\mathbf{X}} = \text{diag}(h_1 P_1 I_n, \ldots, h_{|L(L)|} P_{|L(L)|} I_n). \quad \text{(A13)}$$

Then, we have

$$I(M; Z^n | C_n) \geq I(\mathbf{X}; Z^n) - H(M|\hat{M}C_n) + H(M|Z^n M C_n) \quad \text{(A14a)}$$

$$\geq \frac{1}{2} \log \frac{|GK_{\mathbf{X}}G^T + I_n|}{|I_n|} - H(M|\hat{M}C_n) + H(M|Z^n M C_n) \quad \text{(A14b)}$$

$$= \frac{n}{2} \log\left(1 + \sum_{l \in L(L)} \frac{h_l P_l}{1}\right) - e(M|C_n) + eH(M|Z^n M C_n) \quad \text{(A14c)}$$

$$\geq n I(X_{L(L)}; Z) - n(I(X_{L(L)}; Z) - 2|L(L)|d) + O(nE_{C_n}[e(C_n)]) \quad \text{(A14d)}$$

$$= 2|L(L)|d + o(n), \quad \text{(A14e)}$$

where Equation (A14a) holds similar to Equation (51d), Equation (A14b) holds similar to Equation (51f), Equation (A14c) holds by Equation (A13), in Equation (A14d), we used the definition of $\sum_{i \in L(L)} R_i$ and the uniformity of M to obtain the second term, and Fano's inequality to obtain the third term, Equation (A14e) holds by Equation (A11).

The proof of joint secrecy for Step 1 and the repetitions of Step 2 is similar to the proof of Theorem 2.

Appendix C. Proof of Theorem 5

The proof that Equation (20) is an upper bound on the secrecy sum-rate is similar to the case $L = 2$ in Theorem 3.

Remark that from the statement of Corollary 1, it is unclear whether the sum-rate of Theorem 5 is achievable. However, by inspecting the proof of Theorem 4, observe that we achieve a point in $D_+(L)$, $D(L) \setminus R_+^{jL(L)j}$, where $D(L)$ is defined in Equation (A2). Hence, the sum-rate of Theorem 5 is indeed achievable.

References

1. Csiszár, I.; Narayan, P. Capacity of the Gaussian arbitrarily varying channel. IEEE Trans. Inf. Theory **1991**, 37, 18–26. [CrossRef]
2. Leung-Yan-Cheong, S.; Hellman, M. The Gaussian wire-tap channel. IEEE Trans. Inf. Theory **1978**, 24, 451–456. [CrossRef]
3. Tekin, E.; Yener, A. The general Gaussian multiple-access and two-way wiretap channels: Achievable rates and cooperative jamming. IEEE Trans. Inf. Theory **2008**, 54, 2735–2751. [CrossRef]
4. Bagherikaram, G.; Motahari, A.S.; Khandani, A.K. Secure broadcasting: The secrecy rate region. In Proceedings of the Communication, Control, and Computing, 2008 46th Annual Allerton Conference, Monticello, IL, USA, 23–26 September 2008; pp. 834–841.
5. Grant, A.; Rimoldi, B.; Urbanke, R.; Whiting, P. Rate-splitting multiple access for discrete memoryless channels. IEEE Trans. Inf. Theory **2001**, 47, 873–890. [CrossRef]
6. MolavianJazi, E.; Bloch, M.; Laneman, J. Arbitrary jamming can preclude secure communication. In Proceedings of the 47th Annual Allerton Conference on Communication, Control, and Computing, Monticello, IL, USA, 1–3 October 2009; pp. 1069–1075.
7. Bjelaković, I.; Boche, H.; Sommerfeld, J. Capacity results for arbitrarily varying wiretap channels. In Information Theory, Combinatorics, and Search Theory; Springer: Berlin/Heidelberg, Germany, 2013; pp. 123–144.
8. Nötzel, J.; Wiese, M.; Boche, H. The Arbitrarily Varying Wiretap Channel: Secret Randomness, Stability, and Super-Activation. IEEE Trans. Inf. Theory **2016**, 62, 3504–3531. [CrossRef]
9. Wiese, M.; Notzel, J.; Boche, H. A Channel Under Simultaneous Jamming and Eavesdropping Attack—Correlated Random Coding Capacities Under Strong Secrecy Criteria. IEEE Trans. Inf. Theory **2016**, 62, 3844–3862. [CrossRef]
10. Goldfeld, Z.; Cuff, P.; Permuter, H.H. Arbitrarily varying wiretap channels with type constrained states. IEEE Trans. Inf. Theory **2016**, 62, 7216–7244. [CrossRef]
11. Chou, R. Explicit Wiretap Channel Codes via Source Coding, Universal Hashing, and Distribution Approximation, When the Channels Statistics are Uncertain. IEEE Trans. Inf. Forensics Secur. **2022**, 17. [CrossRef]
12. Csiszár, I. Almost Independence and Secrecy Capacity. Probl. Inf. Transm. **1996**, 32, 40–47.
13. Yassaee, M.; Aref, M.; Gohari, A. Achievability proof via output statistics of random binning. IEEE Trans. Inf. Theory **2014**, 60, 6760–6786. [CrossRef]
14. Hayashi, M. General nonasymptotic and asymptotic formulas in channel resolvability and identification capacity and their application to the wiretap channel. IEEE Trans. Inf. Theory **2006**, 52, 1562–1575. [CrossRef]
15. Bloch, M.; Laneman, J.N. Strong secrecy from channel resolvability. IEEE Trans. Inf. Theory **2013**, 59, 8077–8098. [CrossRef]
16. He, X.; Yener, A. MIMO wiretap channels with unknown and varying eavesdropper channel states. IEEE Trans. Inf. Theory **2014**, 60, 6844–6869. [CrossRef]
17. Mukherjee, A.; Swindlehurst, A.L. Jamming games in the MIMO wiretap channel with an active eavesdropper. IEEE Trans. Sig. Process. **2013**, 61, 82–91. [CrossRef]
18. Banawan, K.; Ulukus, S. Achievable secrecy rates in the multiple access wiretap channel with deviating users. In Proceedings of the IEEE International Symposium on Information Theory, Barcelona, Spain, 10–15 July 2016; pp. 2814–2818.
19. Amariucai, G.T.; Wei, S. Half-duplex active eavesdropping in fast-fading channels: A block-Markov Wyner secrecy encoding scheme. IEEE Trans. Inf. Theory **2012**, 58, 4660–4677. [CrossRef]
20. Basciftci, Y.O.; Gungor, O.; Koksal, C.E.; Ozguner, F. On the secrecy capacity of block fading channels with a hybrid adversary. IEEE Trans. Inf. Theory **2015**, 61, 1325–1343. [CrossRef]
21. Zhang, Y.; Vatedka, S.; Jaggi, S.; Sarwate, A.D. Quadratically constrained myopic adversarial channels. IEEE Trans. Inf. Theory **2022**, 68, 4901–4948. [CrossRef]
22. Zhang, Y.; Vatedka, S.; Jaggi, S. Quadratically constrained two-way adversarial channels. In Proceedings of the IEEE International Symposium on Information Theory (ISIT), Los Angeles, CA, USA, 21–26 June 2020; pp. 1587–1592.
23. Li, T.; Dey, B.K.; Jaggi, S.; Langberg, M.; Sarwate, A.D. Quadratically constrained channels with causal adversaries. In Proceedings of the IEEE International Symposium on Information Theory (ISIT), Vail, CO, USA, 17–22 June 2018; pp. 621–625.
24. La, R.; Anantharam, V. A game-theoretic look at the Gaussian multiaccess channel. DIMACS Ser. Discret. Math. Theor. Comput. Sci. **2004**, 66, 87–106.

25. Chou, R.A.; Yener, A. The degraded Gaussian multiple access wiretap channel with selfish transmitters: A coalitional game theory perspective. In Proceedings of the IEEE International Symposium on Information Theory (ISIT), Aachen, Germany, 25–30 June 2017; pp. 1703–1707.
26. Ekrem, E.; Ulukus, S. Secrecy capacity region of the Gaussian multi-receiver wiretap channel. In Proceedings of the IEEE International Symposium on Information Theory (ISIT), Seoul, Korea, 28 June–3 July 2009; pp. 2612–2616.
27. Sarwate, A.D.; Gastpar, M. Randomization Bounds on Gaussian arbitrarily varying channels. In Proceedings of the IEEE International Symposium on Information Theory (ISIT), Seattle, WA, USA, 9–14 July 2006; pp. 2161–2165.
28. Sato, H. The capacity of the Gaussian interference channel under strong interference. IEEE Trans. Inf. Theory **1981**, 27, 786–788. [CrossRef]
29. Chou, R.; Yener, A. Polar coding for the multiple access wiretap channel via rate-splitting and cooperative jamming. IEEE Trans. Inf. Theory **2018**, 64, 7903–7921. [CrossRef]
30. Ekrem, E.; Ulukus, S. On the secrecy of multiple access wiretap channel. In Proceedings of the Annual Allerton Conf. on Communication Control and Computing, Monticello, IL, USA, 23–26 September 2008; pp. 1014–1021.
31. El Gamal, A.; Kim, Y.H. Network Information Theory; Cambridge University Press: Cambridge, UK, 2011.
32. Wyner, A. The wire-tap channel. Bell Syst. Tech. J. **1975**, 54, 1355–1387. [CrossRef]
33. Tekin, E.; Yener, A. The Gaussian multiple access wire-tap channel. IEEE Trans. Inf. Theory **2008**, 54, 5747–5755. [CrossRef]
34. Rana, V.; Chou, R.A. Short Blocklength Wiretap Channel Codes via Deep Learning: Design and Performance Evaluation. arXiv **2022**, arXiv:2206.03477.
35. Schrijver, A. Combinatorial Optimization: Polyhedra and Efficiency; Springer Science & Business Media: Berlin/Heidelberg, Germany, 2003; Volume 24.