The Gaussian Multiple Access Wiretap Channel when the Eavesdropper can Arbitrarily Jam

Remi A. Chou and Aylin Yener

Wireless Communications and Networking Laboratory (WCAN)
The School of Electrical Engineering and Computer Science
The Pennsylvania State University, University Park, PA 16802.
remi.chou@psu.edu *yener@engr.psu.edu*

***Abstract*—We study the Gaussian multiple access channel in presence of an adversary, who is simultaneously able to eavesdrop and jam, i.e., an active wiretapper. We assume that the adversary has a power constraint, which she can utilize to have any arbitrary jamming strategy. The multiple access channel between the legitimate transmitters and the receiver thus becomes arbitrarily varying. We derive inner and outer bounds on the secrecy rate region of our model. In the case of a degraded channel, we characterize the optimal secrecy sum-rate, and within 0.5 bits per channel use the optimal individual rate constraints. As a special case, we obtain the secrecy capacity of the point-to-point Gaussian wiretap channel when the eavesdropper is able to arbitrarily jam.**

I. Introduction

We study secure communication over a Gaussian multiple access wiretap channel [1], [2]. We assume an active adversary who is not only able to eavesdrop but also is able to perform jamming. The adversary is able to choose any jamming strategy she wishes subject to a power constraint. Consequently, the main channel between the legitimate users becomes *arbitrarily varying* [3]. We study the fundamental limits of information theoretically secure communication in this multiple access channel.

Related works include [4]–[9] for the point-to-point and discrete memoryless wiretap channel. Note that the proof techniques used in these references, such as random binning [10], resolvability/soft covering [9], [11], or typicality arguments do not seem easily applicable to the Gaussian case, even for the point-to-point scenario. Indeed, the known coding mechanisms used to obtain reliability for an arbitrarily varying point-to-point Gaussian channel [3] rely on a codebook whose codewords are uniformly drawn on a unit sphere, so that the components of the codewords cannot be considered independent and identically distributed as it is the case in [4]–[9].

Related work for the point-to-point Gaussian channel includes [12], which considers a Gaussian channel model with an arbitrarily varying *eavesdropper* channel. Our setting is different in that the main channel between the legitimate users is arbitrarily varying. The use of analyses similar to the ones in [12] are not appropriate for the present model for the same reasons described above.

This work was supported in part by NSF grants CIF-1319338 and CNS-1314719.

Several other works have considered continuous channel models with active adversaries who are able to jam, including the Gaussian MIMO wiretap channel [13], the Gaussian multiple access wiretap channel [14], where deviating users can be viewed as active adversaries, point-to-point wiretap channels [15], [16], where the adversary can choose between eavesdropping or jamming. These references differ from references [4]–[9] on arbitrarily varying channels as they assume a specific strategy for the jammer. By contrast, our model only foresees a power constraint for the jamming signal and does not assume any specific jamming strategy.

Our contribution can be summarized as follows. We propose a model for secure communication over Gaussian multiple access channels in presence of an eavesdropper who is able to arbitrarily jam the multiple access channel between the legitimate parties. We determine inner and outer bounds on the secrecy capacity region. For the case when the resulting multiple access wiretap channel is degraded the secrecy capacity region is determined up to a constant gap. Our achievability scheme relies on point-to-point codes developed in [3], time sharing, and an extension of the successive decoding method for multiple access channels without secrecy constraint [17, Appendix C] to multiple access wiretap channels. As a special case, we obtain the secrecy capacity of the point-to-point Gaussian wiretap channel when the eavesdropper is able to arbitrarily jam. Note that secrecy capacity results are already known for the point-to-point *discrete* memoryless channels when both the main channel and the eavesdropper channel are arbitrarily varying [6].

The remainder of the paper is organized as follows. We define the problem in Section II. We present our results in Section III, and sketch our achievabilty proof in Section IV. We end the paper with concluding remarks in Section V. Some proofs are omitted due to space constraints.

Notation: Define for $a, b \in \mathbb{R}$, $[\![a, b]\!] \triangleq [\lfloor a \rfloor, \lceil b \rceil] \cap \mathbb{N}$. 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 power set of $\mathcal{S}$ is denoted by $2^{\mathcal{S}}$. 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.

978-1-5090-4096-4/17/$31.00 ©2017 IEEE

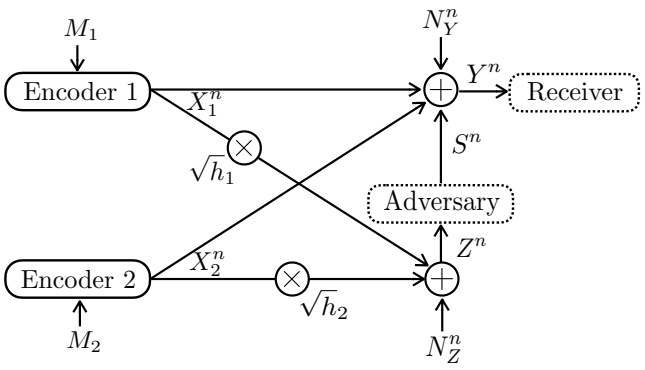

Fig. 1: G-AV-MAC-WT

II. Problem Statement

We consider a Gaussian multiple access channel with two legitimate transmitters, and an adversary who can simultaneously jam and eavesdrop on the communication. The adversary is a full-duplex node that can perfectly cancel the self-interference, i.e., its own jamming signal. Jamming is prescribed by a power constraint but no specific jamming strategy is assumed. Note that the adversary could represent an entity made of an eavesdropper and several non-collocated jammers, as long as the jamming signals are shared within the entity and can be canceled out from the eavesdropped signal.

Specifically, as depicted in Figure 1, we consider the following channel model (put under standard form similar to [2]),

$$Y^n \triangleq X_1^n + X_2^n + S^n + N_Y^n, \tag{1a}$$

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

where Y^n is the channel output observed by the legitimate receiver, Z^n is the channel output observed by the adversary, S^n is an arbitrary jamming sequence emitted by the adversary satisfying the power constraint $\|S^n\|^2 \triangleq \sum_{i=1}^n S_i^2 \leqslant n\Lambda$, for $l \in \{1,2\}$, X_l^n is the signal of transmitter l satisfying the power constraint $\|X_l^n\|^2 \triangleq \sum_{i=1}^n (X_l)_i^2 \leqslant n\Gamma_l$, and N_Y^n and N_Z^n are sequences of i.i.d. Gaussian noises with variances $\sigma_Y^2 = 1$, $\sigma_Z^2 = 1$, respectively. We define a coding scheme and achievable rates for our channel model following the scheme over multiple blocks of [18] to allow time-sharing.

Definition 1. *Let $n, k \in \mathbb{N}$. A $\left(2^{nR_1}, 2^{nR_2}, n, k\right)$ code $\mathcal{C}_n$ for the Gaussian arbitrarily varying multiple access wiretap channel (G-AV-MAC-WT) consists for each block $j \in [\![1,k]\!]$ of*

- *Two messages sets $\mathcal{M}_l^{(j)} \triangleq [\![1, 2^{nR_l^{(j)}}]\!]$, $l \in \{1,2\}$;*
- *Two stochastic encoders, $e_l^{(j)} : \mathcal{M}_l^{(j)} \to \mathbb{B}_0^n(\sqrt{n\Gamma_l})$, $l \in \{1,2\}$, where $\mathbb{B}_0^n(\sqrt{n\Gamma_l})$ is the ball of radius $\sqrt{n\Gamma_l}$ centered in 0 in $\mathbb{R}^n$ under the Euclidian norm;*
- *One decoder, $g^{(j)} : \mathbb{R}^n \to \mathcal{M}_1^{(j)} \times \mathcal{M}_2^{(j)}$;*

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 (1a), (1b) *with power constraint $n\Lambda$ for the jamming signal. Then, the legitimate receiver forms from his n channel output observations an estimate $(\widehat{M}_1^{(j)}, \widehat{M}_2^{(j)})$ of the messages $(M_1^{(j)}, M_2^{(j)})$. We define $\widehat{M} \triangleq \left(\widehat{M}_1^{(j)}, \widehat{M}_2^{(j)}\right)_{j\in[\![1,k]\!]}$ and $M \triangleq \left(M_1^{(j)}, M_2^{(j)}\right)_{j\in[\![1,k]\!]}$.*

Definition 2. *A rate pair $(2^{nR_1}, 2^{nR_2})$ is achievable, if there exists a sequence of $\left(2^{nR_1}, 2^{nR_2}, n, k\right)$ codes for the G-AV-MAC-WT such that*

$$\lim_{n\to\infty} \mathbb{P}[\widehat{M} \neq M] = 0 \text{ (reliability)}, \tag{2a}$$

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

The largest achievable rate region constitutes the secrecy capacity region. Note also that our model recovers the model in [18] in the absence of the security constraint (2b).

III. Results

A. Special case: point-to-point channels

As a special case of our model, we study the point-to-point Gaussian arbitrarily varying wiretap channel (G-AV-WT), i.e., we consider the model described in Section II with the substitutions $h_2 \leftarrow \emptyset$, $R_2 \leftarrow \emptyset$, $X_2 \leftarrow \emptyset$. For convenience, we drop the subscript 1 for h_1, Γ_1.

Theorem 1. *Define $h_\Lambda \triangleq (1+\Lambda)^{-1}$. The secrecy capacity of the G-AV-WT is given by*

$$C(\Lambda) = \mathbb{1}\{\Gamma > \Lambda\} \left[\frac{1}{2}\log\left(\frac{1+h_\Lambda\Gamma}{1+h\Gamma}\right)\right]^+, \tag{3}$$

where $\mathbb{1}\{\Gamma > \Lambda\} = 1$ if $\Gamma > \Lambda$ and 0 otherwise.

Observe that $C(\Lambda)$ is non zero if and only if $\Gamma > \Lambda$ and $h_\Lambda > h$. Theorem 1 follows as special cases of the achievability and converse bounds derived for the G-AV-MAC-WT in Theorems 2 and 3, respectively.

B. General case

We derive in Theorems 2 and 3, inner and outer bounds for the G-AV-MAC-WT, respectively. We assume in Theorems 2 and 3 that transmitters are not altruistic in the sense that a user that cannot achieve a positive secrecy rate will not use power to help the other user, as it is done in [2].

Theorem 2 (Achievability)**.** *Define h_Λ as in Theorem 1 and, for $x \in \mathbb{R}_+$, define $h_{1,2}(x) \triangleq h_1(1+h_2x)^{-1}$, $h_{2,1}(x) \triangleq h_2(1+h_1x)^{-1}$. We consider three cases.*

- *Assume $\Gamma_1 > \Lambda$ and $\Gamma_2 \leqslant \Lambda$. Then, $\mathcal{R}_1$ is achievable, where*
$$\mathcal{R}_1 = \left\{(R_1, 0) : R_1 \leqslant \left[\frac{1}{2}\log\left(\frac{1+\Gamma_1 h_\Lambda}{1+\Gamma_1 h_1}\right)\right]^+\right\}. \tag{4}$$
- *Assume $\Gamma_2 > \Lambda$ and $\Gamma_1 \leqslant \Lambda$. Then, $\mathcal{R}_2$ is achievable, where $\mathcal{R}_2$ is defined as $\mathcal{R}_1$ by exchanging the role of the transmitters.*
- *Assume $\min(\Gamma_1, \Gamma_2) > \Lambda$. Then, the convex hull of $\mathcal{R}_1 \cup \mathcal{R}_2 \cup \bigcup_{\substack{\Lambda<P_1\leqslant\Gamma_1\\ \Lambda<P_2\leqslant\Gamma_2}} \mathcal{R}_{1,2}(P_1,P_2)$ is achievable, where*

$$\mathcal{R}_{1,2}(P_1,P_2) \triangleq \left\{(R_1,R_2) : R_1 \leqslant \left[\frac{1}{2}\log\left(\frac{1+P_1h_\Lambda}{1+P_1h_{1,2}(P_2)}\right)\right]^+,\right.$$

$$R_2 \leqslant \left[\frac{1}{2}\log\left(\frac{1+P_2h_\Lambda}{1+P_2h_{2,1}(P_1)}\right)\right]^+,$$
$$R_1+R_2 \leqslant \left[\frac{1}{2}\log\left(\frac{1+(P_1+P_2)h_\Lambda}{1+P_1h_1+P_2h_2}\right)\right]^+\Bigg\}. \quad (5)$$

Observe that the region achievable when $\min(\Gamma_1,\Gamma_2)>\Lambda$ is the same as the best known achievable region when $\Lambda \leftarrow 0$ and $\sigma_Y^2 \leftarrow 1+\Lambda$ [2], which means that the arbitrary jamming signal is no more harmful than a Gaussian noise with variance Λ. Coding schemes to actually obtain this result are, however, more involved than those when the jamming signal is indeed Gaussian.

Theorem 3 (Converse)**.** *We have the following outer bounds.*

(i) If $\max(\Gamma_1,\Gamma_2)\leqslant\Lambda$*, then no positive rate is achievable.*
(ii) For $\min(\Gamma_1,\Gamma_2)\leqslant\Lambda$*, the achievability regions of Theorem 2 are tight.*
(iii) For $\min(\Gamma_1,\Gamma_2)>\Lambda$ *and when* $\max(h_1,h_2)<h_\Lambda$*, the individual rate bounds described in* (5) *are tight within a constant gap of* 0.5 *bits per channel use.*
(iv) For $\min(\Gamma_1,\Gamma_2)>\Lambda$ *and when* $h_1=h_2$*, the sum-rate bound of* $\mathcal{R}_{1,2}(\Gamma_1,\Gamma_2)$ *described in* (5) *is tight.*

Hence, for the degraded G-AV-MAC-WT, i.e., when $h_1=h_2$ [1], the capacity region is determined up to a constant gap of 0.5 bits per channel use on the individual rate bounds, and the secrecy capacity is obtained for point-to-point channels. The proof of Theorem 2 is sketched in Section IV. The proof of Theorem 3 relies on [3], [19] and is omitted for brevity.

IV. Proof of Theorem 2

It is sufficient to prove the achievability of the dominant face

$$\mathcal{D}(P_1,P_2)\triangleq\{(R_1,R_2)\in\mathcal{R}_{1,2}(P_1,P_2):$$
$$R_1+R_2=\left[\frac{1}{2}\log\left(\frac{1+(P_1+P_2)h_\Lambda}{1+P_1h_1+P_2h_2}\right)\right]^+\Bigg\} \quad (6)$$

of $\mathcal{R}_{1,2}(P_1,P_2)$ to prove achievability of $\mathcal{R}_{1,2}(P_1,P_2)$ when $\min(\Gamma_1,\Gamma_2)>\Lambda$. The achievability of $\mathcal{R}_1$ and $\mathcal{R}_2$ is obtained as special cases. Observe that the rate constraints in $\mathcal{R}_{1,2}(P_1,P_2)$ can be expressed as $[g(\{1\})]^+$, $[g(\{2\})]^+$, and $[g(\{1,2\})]^+$, with $g:2^{\{1,2\}}\to\mathbb{R},\mathcal{T}\mapsto I(X_\mathcal{T};Y|X_{\mathcal{T}^c})-I(X_\mathcal{T};Z)$, where $Y\triangleq X_1+X_2+N_Y$, $Z\triangleq\sqrt{h_1}X_1+\sqrt{h_2}X_2+N_Z$, and X_1, X_2, N_Y, N_Z are independent zero-mean Gaussian random variables with variances P_1, P_2, $(1+\Lambda)$, 1 respectively. As remarked in [20], g is submodular but not necessarily non-decreasing, which is the main reason why achieving the corner points of $\mathcal{R}_{1,2}(P_1,P_2)$ by means of point-to-point codes via the successive decoding method [17, Appendix C] does not easily translate to our setting. We summarize our proof strategy in the three following cases.

Case 1: Assume $g(\{1,2\})\geqslant\max(g(\{1\}),g(\{2\}))$. The corner points of $\mathcal{R}_{1,2}$ are given by $(g(\{1,2\})-g(\{2\}),g(\{2\}))$ and $(g(\{1\}),g(\{1,2\})-g(\{1\}))$. We will achieve each corner point with point-to-point coding techniques and perform time-sharing to achieve $\mathcal{D}(P_1,P_2)$.

Case 2.a: Assume $g(\{1,2\})\geqslant g(\{1\})$ and $g(\{1,2\})<g(\{2\})$. The corner points of $\mathcal{R}_{1,2}$ are $\underline{C}_1\triangleq(g(\{1\}),g(\{1,2\})-g(\{1\}))$ and $\underline{C}_2\triangleq(0,g(\{1,2\}))$. While $\underline{C}_1$ can be achieved as in Case 1, $\underline{C}_2$ does not decompose to allow single-user coding. Instead of achieving $\underline{C}_2$, we will achieve the virtual corner point $\widetilde{\underline{C}}_2\triangleq(g(\{1,2\})-g(\{2\}),g(\{2\}))$, keeping in mind that $g(\{1,2\})-g(\{2\})<0$.

Case 2.b: Assume $g(\{1,2\})\geqslant g(\{2\})$ and $g(\{1,2\})<g(\{1\})$. This case is handled as Case 2.a by exchanging the role of the two transmitters.

Case 3: Assume $g(\{1,2\})<\min(g(\{1\}),g(\{2\}))$. The corner points of the region are $(0,g(\{1,2\}))$ and $(g(\{1,2\}),0)$. We will show achievability of a point $\underline{R}\in\mathcal{D}(P_1,P_2)$, where $\underline{R}$ has strictly positive components. All the other points of $\mathcal{D}(P_1,P_2)$ can then be achieved as in Case 2 by time sharing between $\underline{R}$ and the virtual corner points $\widetilde{\underline{C}}_1$, $\widetilde{\underline{C}}_2$ defined as in Case 2.

A. Case 1

We show achievability of $(g(\{1,2\})-g(\{2\}),g(\{2\}))$. The achievability of $(g(\{1\}),g(\{1,2\})-g(\{1\}))$ is obtained by exchanging the role of the transmitters.

Codebook construction: For transmitter $i\in\{1,2\}$, construct a codebook $C_n^{(i)}$ with $\lceil 2^{nR_i}\rceil\lceil 2^{n\widetilde{R}_i}\rceil$ codewords drawn independently and uniformly on the sphere of radius $\sqrt{P_i}$ in $\mathbb{R}^n$. The codewords are labeled $x_i^n(m_i,\widetilde{m}_i)$, where $m_i\in[\![1,2^{nR_i}]\!]$, $\widetilde{m}_i\in[\![1,2^{n\widetilde{R}_i}]\!]$. We define $C_n\triangleq(C_n^{(1)},C_n^{(2)})$ and choose $R_1\triangleq g(\{1,2\})-g(\{2\})-\delta=I(X_1;Y)-I(X_1;Z|X_2)-\delta$, $\widetilde{R}_1\triangleq I(X_1;Z|X_2)-\delta$, $R_2\triangleq g(\{2\})-\delta=I(X_2;Y|X_1)-I(X_2;Z)-\delta$, $\widetilde{R}_2\triangleq I(X_2;Z)-\delta$, $\delta>0$.

Encoding: For Transmitter $i\in\{1,2\}$, given $(m_i,\widetilde{m}_i)$, transmit $x_i^n(m_i,\widetilde{m}_i)$. In the remainder of the paper, we term $\widetilde{m}_1$ and $\widetilde{m}_2$ as randomization sequences.

Decoding: The receiver performs minimum distance decoding to first estimate $(m_1,\widetilde{m}_1)$ and then estimate $(m_2,\widetilde{m}_2)$, i.e., given y^n, determine $(\hat{m}_1,\hat{\widetilde{m}}_1)=\phi_1(y^n,0)$, and $(\hat{m}_2,\hat{\widetilde{m}}_2)=\phi_2(y^n,x_1^n(\hat{m}_1,\hat{\widetilde{m}}_1))$ where for $i\in\{1,2\}$

$$\phi_i:(y^n,x)\mapsto$$
$$\begin{cases}(m_i,\widetilde{m}_i)\text{ if }\|y^n-x-x_i^n(m_i,\widetilde{m}_i)\|^2\\ \qquad<\|y^n-x-x_i^n(m_i',\widetilde{m}_i')\|^2\text{ for }(m_i',\widetilde{m}_i')\neq(m_i,\widetilde{m}_i)\\ 0\text{ if no such }(m_i,\widetilde{m}_i)\in[\![1,2^{nR_i}]\!]\times[\![1,2^{n\widetilde{R}_i}]\!]\text{ exists}\end{cases} \quad (7)$$

Average probability of error: The term $e(C_n,s^n)\triangleq\mathbb{P}\left[(\widehat{M}_1,\widehat{M}_2)\neq(M_1,M_2)|C_n\right]$ is upper-bounded by

$$\mathbb{P}\left[(\widehat{M}_1,\widehat{M}_2)\neq(M_1,M_2)\text{ or }(\widehat{\widetilde{M}}_1,\widehat{\widetilde{M}}_2)\neq(\widetilde{M}_1,\widetilde{M}_2)|C_n\right]$$
$$=e_1(C_n,s^n,x_2^n(m_2,\widetilde{m}_2))+e_2(C_n,s^n,0),$$

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

$$e_i(C_n,s^n,x)\triangleq\frac{1}{\lceil 2^{nR_i}\rceil\lceil 2^{n\widetilde{R}_i}\rceil}\sum_{m_i}\sum_{\widetilde{m}_i}$$
$$\mathbb{P}\left[\|x_i^n(m_i,\widetilde{m}_i)+s^n+x+N_Y^n-x_i^n(m_i',\widetilde{m}_i')\|^2\right.$$

$$\leqslant \|s^n + x + N_Y^n\|^2 \text{ for some } (m_i', \widetilde{m}_i') \neq (m_i, \widetilde{m}_i)\big].$$

Next, we have

$$\begin{aligned}
&\mathbb{E}_{C_n}[e_1(C_n, s^n, x_2^n(m_2, \widetilde{m}_2))] \\
&\leqslant \mathbb{E}_{C_n}[e_1(C_n, s^n, x_2^n(m_2, \widetilde{m}_2))|C_n^{(1)} \in \mathcal{C}_1^*] + \mathbb{P}[C_n^{(1)} \notin \mathcal{C}_1^*] \\
&\leqslant \alpha_n, \qquad (8)
\end{aligned}$$

where in the first inequality $\mathcal{C}_1^*$ represents all the sets of unit norm vectors scaled by $\sqrt{P_1}$ that satisfy the technical conditions of [3, Lemma 1], where in (8) $\alpha_n \xrightarrow{n\to\infty} 0$ because $C_n^{(1)} \in \mathcal{C}_1^*$ with probability one when $n \to \infty$ by [3], and because $\mathbb{E}_{C_n}[e_1(C_n, s^n, x_2^n(m_2, \widetilde{m}_2))|C_n^{(1)} \in \mathcal{C}_1^*] \xrightarrow{n\to\infty} 0$ by [3] using the definition of $R_1 + \widetilde{R}_1$ and by interpreting the signal of Transmitter 2 as noise, which is indeed possible by remarking that the result in [3] is valid for a noise model $N + U$, where N is Gaussian and U is uniformly distributed on a sphere of $\mathbb{R}^n$. Note that this argument has also been used in [18]. With similar justifications and by using the definition of $R_2 + \widetilde{R}_2$, we have for some (β_n) such that $\beta_n \xrightarrow{n\to\infty} 0$, $\mathbb{E}_{C_n}[e_2(C_n, s^n, 0)] \leqslant \beta_n$, hence, $\mathbb{E}_{C_n}[e(C_n, s^n)] \xrightarrow{n\to\infty} 0$.

Equivocation: We first study the average error probability $\widetilde{e}(C_n)$ of decoding $(\widetilde{m}_1, \widetilde{m}_2)$ given (z^n, m_1, m_2) with a procedure similar to (7). We omit the details due to space constraints. We define $M \triangleq (M_1, M_2)$. Similar to the justifications to obtain (8), one can show that $\mathbb{E}_{C_n}[\widetilde{e}(C_n)] \xrightarrow{n\to\infty} 0$, which leads with standard arguments to $I(M; Z^n|C_n) = o(n)$.

B. Case 2

We only consider Case 2.a since Case 2.b will follow by exchanging the role of the transmitters. Let $\underline{R} \triangleq (R_1, R_2)$ belong to $\mathcal{D}(P_1, P_2)$. There exists $\alpha \in [0, 1[$ such that $\underline{R} = (1-\alpha)\underline{C}_1 + \alpha\widetilde{\underline{C}}_2$. The corner point $\underline{C}_1$ can be achieved as in Case 1, however, recall that the first component of $\widetilde{\underline{C}}_2$ is negative, it thus cannot be achieved similarly.

We achieve $\underline{R}$ with time-sharing as follows. We define $k, k' \in \mathbb{N}$ such that $k'/k = (1-\alpha)^{-1} - 1 + \epsilon$, $\epsilon > 0$, it 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 with length $nk\underline{C}_1$. We then realize a second transmission T_2 of a pair of confidential messages with length $nk'(0, g(\{2\}))$ with the help of a secret key, shared between Transmitter 1 and the receiver, of length $nk'(g(\{2\}) - g(\{1,2\})) > 0$, which is interpreted as achieving the virtual corner point $\widetilde{\underline{C}}_2$ since the overall transmission rate of confidential messages is $\frac{k}{k+k'}\underline{C}_1 + \frac{k'}{k+k'}\widetilde{\underline{C}}_2$. Note that Transmitter 1 and the receiver share a secret key of sufficient length from the first transmission because $(1-\alpha)\underline{C}_1 + \alpha\widetilde{\underline{C}}_2 = \underline{R}$ has positive components. We now explain how transmission T_2 is done. 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 $\lceil 2^{n\breve{R}_1}\rceil\lceil 2^{n\mathring{R}_1}\rceil$ codewords drawn independently and uniformly on the sphere of radius $\sqrt{P_1}$ in $\mathbb{R}^n$. The codewords are labeled $x_1^n(\breve{m}_1, \mathring{m}_1)$, where $\breve{m}_1 \in [\![1, 2^{n\breve{R}_1}]\!]$, $\mathring{m}_1 \in [\![1, 2^{n\mathring{R}_1}]\!]$. We define the rates $\breve{R}_1 \triangleq I(X_1; Y) - \delta$, $\mathring{R}_1 \triangleq g(\{2\}) - g(\{1,2\}) - \delta = I(X_1; Z|X_2) - I(X_1; Y) - \delta$, and $\widetilde{R}_1 \triangleq \breve{R}_1 + \mathring{R}_1 = I(X_1; Z|X_2) - 2\delta$.

Encoding at Transmitters: Encoding for Transmitter 2 is as in Case 1. Given $(\breve{m}_1, \mathring{m}_1)$ Transmitter 1 forms $x_1^n(\breve{m}_1, \mathring{m}_1)$, where $\mathring{m}_1$ is assumed to be known at the receiver by the transmission T_1 described above. In the following, we define $\widetilde{m}_1 \triangleq (\breve{m}_1, \mathring{m}_1)$.

Decoding and average probability of error: Similar to case 1, using minimum distance decoding, one can show that on average over the codebooks, the receiver can reconstruct $x_1^n(\breve{m}_1, \mathring{m}_1)$ with vanishing average probability of error because $\mathring{m}_1$ is known at the receiver and by definition of $\breve{R}_1$. The receiver can then reconstruct x_2^n as in Case 1.

Equivocation: The computation of the equivocation is similar to 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_1^n given (z^n, x_2^n) by definition of $\widetilde{R}_1$.

Finally, to conclude that $\underline{R}$ is achieved, we need to show secrecy over the joint transmissions T_1 and T_2. We use the notation $'$ to designate random variables associated with transmission T_2. We define $M \triangleq (M_1 \backslash \mathring{M}_1, M_2)$, the confidential messages sent during transmission T_1, where we exclude $\mathring{M}_1$, all the confidential messages sent during transmission T_1 and used during transmission T_2. We define $M' \triangleq (\emptyset, M_2')$ the confidential messages sent during transmission T_2. Similarly, we define $\widetilde{M} \triangleq (\widetilde{M}_1, \widetilde{M}_2)$ and $\widetilde{M}' \triangleq (\widetilde{M}_1', \widetilde{M}_2')$ the randomization sequences used by both transmitters in transmissions T_1 and T_2, respectively. We also define $X^{kn} \triangleq (X_1^{kn}, X_2^{kn})$, $X^{k'n} \triangleq (X_1^{k'n}, X_2^{k'n})$. We have

$$\begin{aligned}
&I(MM'; Z^{nk}Z^{nk'}|C_nC_n') \\
&= I(X^{kn}X^{k'n}; Z^{nk}Z^{nk'}|C_nC_n') - H(\widetilde{M}\widetilde{M}'|C_nC_n') \\
&\quad + H(\widetilde{M}\widetilde{M}'|Z^{nk}Z^{nk'}MM'C_nC_n') \\
&\leqslant I(X^{kn}X^{k'n}; Z^{nk}Z^{nk'}) - n(k+k')I(X_1X_2; Z) + o(n) \\
&= o(n),
\end{aligned}$$

where in the inequality we have used $(C_nC_n') - (X^{kn}X^{k'n}) - (Z^{nk}Z^{nk'})$ to obtain the first term, the definition of $\widetilde{R}_1 + \widetilde{R}_2$ to obtain the second term, and Fano's inequality to obtain the third term, indeed, using the analyses for transmissions T_1, T_2, and a union bound, we have that on average over the codebooks the average probability of error for reconstructing $(\widetilde{M}\widetilde{M}')$ given $(Z^{nk}, Z^{nk'}, M, M')$ vanishes as $n \to \infty$. Note that we have excluded $\mathring{M}_1$ from M, but one can first determine $\widetilde{M}'$ from $(Z^{nk'}, M')$, and then $\widetilde{M}$ from $(Z^{nk}, M, \mathring{M}_1)$, since $\mathring{M}_1$ is included in $\widetilde{M}'$.

C. Case 3

We define $g_1^* \triangleq g(\{2\}) - g(\{1,2\}) > 0$ and $g_2^* \triangleq g(\{1\}) - g(\{1,2\}) > 0$. Assume $g(\{1,2\}) > 0$, otherwise $\mathcal{R}_{1,2}(P_1, P_2) = \{(0,0)\}$. We will need the following lemma, whose proof is omitted due to space constraint.

Lemma 1. *We have*

(i) $g_1^* \leqslant g(\{1\})$ *or* $g_2^* \leqslant g(\{2\})$.

(ii) $h_1 < h_\Lambda$ *or* $h_2 < h_\Lambda$.

(iii) Assume $g_1^* \leqslant g(\{1\})$. *There exists* $m, m' \in \mathbb{N}^*$, *such that* $m'g(\{1\}) - mg_1^* \geqslant 0$, *and* $mg(\{2\}) - m'g_2^* > 0$.

By (i) in Lemma 1, assume without loss of generality that $g_1^* \leqslant g(\{1\})$ by exchanging the role of the transmitters if necessary. We let m, m' be as in (iii) of Lemma 1. Achievability of $\mathcal{D}(P_1, P_2)$ is made in four steps.

Step 1. During a first transmission T_0, Transmitter 2 transmits a confidential message with length $nm'g_2^*$ to the receiver. This is possible with a point-to-point wiretap code (similar to Case 1) when Transmitter 1 remains silent and when $h_\Lambda > h_2$. If $h_\Lambda \leqslant h_2$, then by (ii) in Lemma 1, $h_\Lambda > h_1$ and Transmitter 2 can transmits a confidential message with length $nm'g_2^*$ as follows. Transmitter 1 transmits a confidential message with length nkg_1^*, where $k \in \mathbb{N}^*$ is such that $nkg(\{2\}) \geqslant nm'g_2^*$. Using this secret key shared by Transmitter 1 and the receiver, Transmitter 2 can transmit a confidential message with length $nkg(\{2\})$ as in Case 2. Note that Step 1 is operated in a fixed number of blocks of length n.

Step 2. Similar to Case 2, the transmitters achieve a transmission T_1 of confidential messages with length $(nm'g(\{1\}), 0)$ by using the secret key exchange during T_0 between Transmitter 2 and the receiver. Then, similar to Case 2 and because $m'g(\{1\}) - mg_1^* \geqslant 0$ by (iii) in Lemma 1, the transmitters achieve a transmission T_2 of confidential messages with length $(nm'g(\{1\}) - nmg_1^*, nmg(\{2\}))$ by using a secret key with length nmg_1^* exchange between Transmitter 1 and the receiver during T_1.

Step 3. The transmitters can repeat T_1 and T_2 t times, where t is arbitrary, since $mg(\{2\}) - m'g_2^* > 0$ by (iii) in Lemma 1. Hence, after these t repetitions, the rate pair achieved is arbitrarily close to $\underline{R} = \frac{1}{m+m'}(m'g(\{1\}) - mg_1^*, mg(\{2\}) - m'g_2^*)$ provided that t is large enough since Step 1 only requires a fixed number of transmission blocks. Observe that $\underline{R} \in \mathcal{D}(P_1, P_2)$.

Step 4. Any point of $\mathcal{D}(P_1, P_2)$ can then be achieved as in Case 2 by time sharing between $\underline{R}$ and one of the virtual corner points $\underline{\widetilde{C}}_1$, $\underline{\widetilde{C}}_2$.

The proof that secrecy holds is similar to Case 2.

V. Concluding Remarks

We have defined a Gaussian multiple access wiretap channel under simultaneous eavesdropping and jamming attack. Unlike previous work, the jamming signal is arbitrary and, in particular, not restricted to be Gaussian. Our achievability scheme relies on time-sharing and an extension of the successive decoding method for multiple access channels to multiple access wiretap channels. An open problem remains to provide a scheme that avoids time-sharing. Rate-splitting [17] can be adapted to our setting following [20] to avoid time-sharing, however, the entire region in (5) cannot be achieved as splitting the power of one user precludes reliable communication. It is unclear whether or not the entire region of Section III can be achieved without time-sharing and by solely relying on point-to-point codes. If not, the design of multi-transmitter codes for arbitrarily varying multiple access channels would be necessary. Another open problem is to obtain tight outer-bounds for non-degraded channels. This problem is as hard as finding tight outer bounds for the general Gaussian multiple access wiretap channel [2]. Lastly, we consider weak secrecy in this work. Strong and semantic security regions for this scenario are open. Although the scheme in [21] can be applied to point-to-point channels, the analysis does not seem extendable in a straightforward fashion to the multiple-access case.

References

[1] E. Tekin and A. Yener, "The Gaussian multiple access wire-tap channel," *IEEE Trans. Inf. Theory*, vol. 54, no. 12, pp. 5747–5755, 2008.

[2] 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, no. 6, pp. 2735–2751, 2008.

[3] I. Csiszár and P. Narayan, "Capacity of the Gaussian arbitrarily varying channel," *IEEE Trans. Inf. Theory*, vol. 37, no. 1, pp. 18–26, 1991.

[4] E. MolavianJazi, M. Bloch, and J. Laneman, "Arbitrary jamming can preclude secure communication," in *Allerton Conf. on Communication, Control, and Computing*, 2009, pp. 1069–1075.

[5] H. Boche and R. Schaefer, "Capacity results and super-activation for wiretap channels with active wiretappers," *IEEE Trans. Inf. Forensics and Security*, vol. 8, no. 9, pp. 1482–1496, 2013.

[6] I. Bjelaković, H. Boche, and J. Sommerfeld, "Capacity results for arbitrarily varying wiretap channels," in *Information Theory, Combinatorics, and Search Theory*. Springer, 2013, pp. 123–144.

[7] J. Nötzel, M. Wiese, and H. Boche, "The arbitrarily varying wiretap channel: Secret randomness, stability, and super-activation," *IEEE Trans. Inf. Theory*, vol. 62, no. 6, pp. 3504–3531, 2016.

[8] M. Wiese, J. Notzel, and H. Boche, "A channel under simultaneous jamming and eavesdropping attack—correlated random coding capacities under strong secrecy criteria," *IEEE Trans. Inf. Theory*, vol. 62, no. 7, pp. 3844–3862, 2016.

[9] Z. Goldfeld, P. Cuff, and H. Permuter, "Arbitrarily varying wiretap channels with type constrained states," *arXiv:1601.03660*, 2016.

[10] M. Yassaee, M. Aref, and A. Gohari, "Achievability proof via output statistics of random binning," *IEEE Trans. Inf. Theory*, vol. 60, no. 11, pp. 6760–6786, 2014.

[11] M. Bloch and J. N. Laneman, "Strong secrecy from channel resolvability," *IEEE Trans. Inf. Theory*, vol. 59, no. 12, pp. 8077–8098, 2013.

[12] X. He and A. Yener, "MIMO wiretap channels with unknown and varying eavesdropper channel states," *IEEE Trans. Inf. Theory*, vol. 60, no. 11, pp. 6844–6869, 2014.

[13] A. Mukherjee and A. L. Swindlehurst, "Jamming games in the MIMO wiretap channel with an active eavesdropper," *IEEE Trans. Sig. Processing*, vol. 61, no. 1, pp. 82–91, 2013.

[14] K. Banawan and S. Ulukus, "Achievable secrecy rates in the multiple access wiretap channel with deviating users," in *IEEE Int. Symp. Inf. Theory*, 2016, pp. 2814–2818.

[15] G. T. Amariucai and S. Wei, "Half-duplex active eavesdropping in fast-fading channels: a block-Markov Wyner secrecy encoding scheme," *IEEE Trans. Inf. Theory*, vol. 58, no. 7, pp. 4660–4677, 2012.

[16] Y. O. Basciftci, O. Gungor, C. E. Koksal, and F. Ozguner, "On the secrecy capacity of block fading channels with a hybrid adversary," *IEEE Trans. Inf. Theory*, vol. 61, no. 3, pp. 1325–1343, 2015.

[17] A. Grant, B. Rimoldi, R. Urbanke, and P. Whiting, "Rate-splitting multiple access for discrete memoryless channels," *IEEE Trans. Inf. Theory*, vol. 47, no. 3, pp. 873–890, 2001.

[18] R. La and V. Anantharam, "A game-theoretic look at the Gaussian multiaccess channel," *DIMACS series in discrete mathematics and theoretical computer science*, vol. 66, pp. 87–106, 2004.

[19] E. Ekrem and S. Ulukus, "On the secrecy of multiple access wiretap channel," in *Proc. of the Annual Allerton Conf. on Communication Control and Computing*, 2008, pp. 1014–1021.

[20] R. Chou and A. Yener, "Polar coding for the multiple access wiretap channel via rate-splitting and cooperative jamming," in *Proc. of IEEE Int. Symp. Info. Theory*, 2016.

[21] H. Tyagi and A. Vardy, "Explicit capacity-achieving coding scheme for the Gaussian wiretap channel," in *IEEE Int. Symp. Inf. Theory*, 2014, pp. 956–960.