Inseparability of the Multiple Access Wiretap Channel

Jianwei Xie Sennur Ulukus
Department of Electrical and Computer Engineering
University of Maryland, College Park, MD 20742
xiejw@umd.edu *ulukus@umd.edu*

***Abstract*—We examine the separability of the parallel multiple access wiretap channel. Separability, when exists, is useful as it enables us to code separately over parallel channels, and still achieve the optimum overall performance. It is well-known that the parallel single-user channel, parallel multiple access channel (MAC) and parallel broadcast channel (BC) are all separable, however, the parallel interference channel (IC) is not separable in general. In this paper, we show that, while MAC is separable MAC wiretap channel is not separable in general. We prove this via a specific linear deterministic MAC wiretap channel. We then show that even the Gaussian MAC wiretap channel is inseparable in general. Finally, we show that, when the channel gains are drawn from continuous distributions, and when the secure degrees of freedom (s.d.o.f.) region is considered, then the Gaussian MAC wiretap channel is almost surely separable.**

I. Introduction

Separability, when exists, is useful as it enables us to code separately over parallel channels, and still achieve the optimum overall performance. It is well-known that the parallel single-user channel [1], parallel multiple access channel (MAC) [2] and parallel broadcast channel (BC) [3] are all separable, however, the parallel interference channel (IC) is not separable in general [4]–[7]. In particular, reference [4] studied the two-user one-sided ergodic fading IC and showed that separation can be strictly sub-optimal in certain cases. Reference [5] studied the separability in a parallel Gaussian IC, and showed that the parallel Gaussian IC is not always separable by presenting a specific example where joint encoding over the parallel channels outperforms individually optimal encoding in each parallel channel. Reference [6] further confirmed the inseparability of the parallel IC by examining the topological interference channel where the parallel channels correspond to different network topologies some of which had asymmetric connectivity. Recently, reference [7] showed that even symmetric parallel ICs are inseparable by characterizing the capacity region of parallel symmetric linear deterministic ICs.

In this paper, we consider the MAC wiretap channel, which is a combination of a MAC to the legitimate receiver and a MAC to the eavesdropper. The MAC wiretap channel was introduced in [8], [9] and studied further in [10]–[16]. Even though, in the absence of any secrecy constraints, MAC is the most well-understood multi-user channel model [1], its wiretap version is significantly more complex. The secrecy capacity region of the MAC wiretap channel is still unknown today, and its secure degrees of freedom (s.d.o.f.) region has been fully characterized only recently [17], [18]. In this paper, we focus on the separability of the parallel MAC wiretap channel and show that it is not separable in general. Intuitively, this can be attributed to the observation that, even though MAC wiretap channel is composed of MAC legitimate and eavesdropping links, as a whole, it resembles the IC more, as it has two independent transmitters and two independent receivers.

To show the inseparability of the parallel MAC wiretap channel, we construct a specific linear deterministic MAC wiretap channel in each component channel. We find the exact secrecy capacity of each of these component MAC wiretap channels, and then determine the optimum secrecy rates achievable by separate encoding. This step is challenging as the secrecy capacity of MAC wiretap channels is unknown in general; we provide a specific achievability and converse for the capacity of each of the component channels. We then provide an encoding scheme that codes over the parallel channels which outperforms the optimum separable scheme.

Next, we consider the parallel Gaussian MAC wiretap channel. Since the secrecy capacity region of the general MAC wiretap channel, including the Gaussian MAC wiretap channel, is unknown but exact s.d.o.f. region is known [17], [18], we investigate the sum s.d.o.f. of parallel Gaussian MAC wiretap channels and prove that it is inseparable. This implies the inseparability of the secrecy region as well. Next, we observe that, if the different channel gains which give rise to different parallel channels are drawn independently from continuous distributions, then the channel gain configurations which give rise to inseparability fall into a set with zero Lebesgue measure. To confirm this observation, and prove the almost sure s.d.o.f. separability of parallel Gaussian MAC wiretap channels, we consider the *flat channel*, where we put the individual n channel uses of each component channel into a single $2n$ channel uses. We utilize the converse techniques in [17], [18] to show the separability in this case.

Finally, we note that, while inseparability in s.d.o.f. implies inseparability in the secrecy capacity, separability in s.d.o.f. does not imply separability in secrecy capacities. The almost sure separability proved for the parallel Gaussian MAC wiretap channel in this paper holds only for the s.d.o.f., which is the pre-log factor of the secrecy capacity, and is a weaker measure of separability.

This work was supported by NSF Grants CNS 09-64632, CCF 09-64645, CCF 10-18185 and CNS 11-47811.

II. System Model and Definitions

In a two-user MAC wiretap channel $p(y_1, y_2|x_1, x_2)$, each transmitter i, $i = 1, 2$, has a message W_i intended for the legitimate receiver whose channel output is Y_1. For each i, message W_i is uniformly and independently chosen from set $\mathcal{W}_i$. The rate of message i is $R_i \triangleq \frac{1}{n}\log|\mathcal{W}_i|$. Transmitter i uses a stochastic function $f_i : \mathcal{W}_i \to X_i^n$, where the n-length vector X_i^n denotes the ith user's channel input in n channel uses. All messages are needed to be kept secret from the eavesdropper whose channel output is Y_2.

A secrecy rate pair (R_1, R_2) is said to be achievable if for any $\epsilon > 0$ there exist n-length codes such that the legitimate receiver can decode the messages reliably, i.e., the probability of decoding error is less than ϵ

$$\Pr\left[(W_1, W_2) \neq (\hat{W}_1, \hat{W}_2)\right] \leq \epsilon \tag{1}$$

and the messages are kept information-theoretically secure against the eavesdropper

$$\frac{1}{n}H(W_1, W_2|Y_2^n) \geq \frac{1}{n}H(W_1, W_2) - \epsilon \tag{2}$$

where $\hat{W}_1, \hat{W}_2$ are the estimates of the messages based on the legitimate receiver's observation Y_1^n.

The secrecy capacity region $\mathcal{C}$ is the closure of the set containing all achievable secrecy rate pairs. The sum secrecy capacity is $C_\Sigma = \sup(R_1 + R_2)$, where the supremum is over all achievable secrecy rate pairs $(R_1, R_2) \in \mathcal{C}$. For Gaussian MAC wiretap channel with average power constraint P for both transmitters, the s.d.o.f. region is defined as:

$$D_s = \left\{(d_1, d_2) : (R_1, R_2) \in \mathcal{C},\ d_i \triangleq \lim_{P\to\infty} \frac{R_i}{\frac{1}{2}\log P}\right\} \tag{3}$$

and the sum s.d.o.f. is defined as:

$$D_{s,\Sigma} \triangleq \lim_{P\to\infty} \frac{C_\Sigma}{\frac{1}{2}\log P} \tag{4}$$

Let $p(y_{1a}, y_{2a}|x_{1a}, x_{2a})$ and $p(y_{1b}, y_{2b}|x_{1b}, x_{2b})$ be two two-user MAC wiretap channels. The *parallel* two-user MAC wiretap channel is a two-user MAC wiretap channel in which the channel inputs of transmitter 1 and 2 are (x_{1a}, x_{1b}) and (x_{2a}, x_{2b}), respectively, and the channel inputs are sent simultaneously in parallel. The channel outputs of the legitimate receiver and the eavesdropper are (y_{1a}, y_{1b}) and (y_{2a}, y_{2b}), respectively, and are distributed according to

$$\begin{aligned} &p\left(y_{1a}, y_{2a}, y_{1b}, y_{2b}|x_{1a}, x_{2a}, x_{1b}, x_{2b}\right) \\ &\quad = p(y_{1a}, y_{2a}|x_{1a}, x_{2a})p(y_{1b}, y_{2b}|x_{1b}, x_{2b}) \end{aligned} \tag{5}$$

We refer to each MAC wiretap channel, $p(y_{1a}, y_{2a}|x_{1a}, x_{2a})$ and $p(y_{1b}, y_{2b}|x_{1b}, x_{2b})$, as a *component* channel of the overall *parallel* MAC wiretap channel.

III. Inseparability of the MAC Wiretap Channel

In this section, we show that the parallel MAC wiretap channel is not separable in general. To this end, we provide a specific counter example.

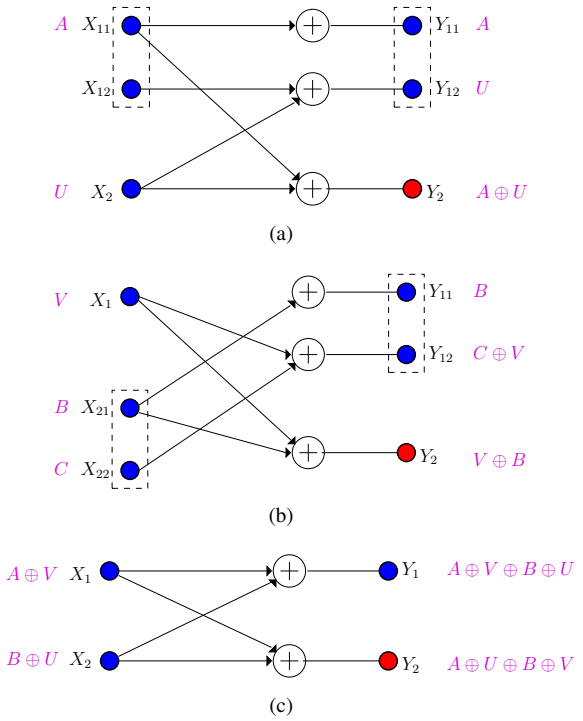

Fig. 1. An inseparable linear deterministic parallel MAC wiretap channel. There are three component channels: (a), (b) and (c). An achievable scheme that codes across the parallel channels is shown in color magenta.

Consider the linear deterministic parallel discrete memoryless MAC wiretap channel shown in Fig. 1, which has three component channels: (a), (b) and (c). In the first component channel, (a), transmitter 1 has two sub-channel inputs, i.e., (X_{11}, X_{12}), and transmitter 2 has only one sub-channel input X_2. The legitimate receiver observes (Y_{11}, Y_{12}) and the eavesdropper observes Y_2. In the second component channel, (b), the roles of the two transmitters are swapped. In the third component channel, (c), the legitimate receiver and the eavesdropper have identical observations. Specifically, the input/output relationships for sub-channel (a) are:

$$Y_{11} = X_{11}, \quad Y_{12} = X_{12} \oplus X_2, \quad Y_2 = X_{11} \oplus X_2 \tag{6}$$

where all symbols are binary, and addition is modulo-2.

While transmitters send independent data, they can each code their data jointly across their parallel channels. In the following two sub-sections, we show that the optimum separable (i.e., independent) coding yields 2 bits/channel-use for the sum secrecy rate, while through coding jointly across the component channels a sum secrecy rate of 3 bits/channel-use is achievable, and hence separation is strictly sub-optimal.

A. Optimum Sum Secrecy Rate with Separable Encoding

Due to independent coding across the component channels:

$$C_{\Sigma,\text{indep}} = C_{\Sigma,(a)} + C_{\Sigma,(b)} + C_{\Sigma,(c)} = 2C_{\Sigma,(a)} \tag{7}$$

where $C_{\Sigma,(a)} = C_{\Sigma,(b)}$ is due to symmetry, and $C_{\Sigma,(c)} = 0$ is due to the fact that the legitimate receiver and the eavesdropper have identical observations. Therefore, we only need to show $C_{\Sigma,(a)} = 1$ in order to show $C_{\Sigma,\text{indep}} = 2$. The achievability of

this follows by the following signalling: The first user sends a 1 bit (uniform) information signal in X_{12}, and sends no signal in the other sub-channel which leaks to the eavesdropper, i.e., $X_{11}=0$, and the second user does not send any information, i.e., $X_2=0$. This gives 1 bit secure rate for the first user, and hence 1 bit sum secrecy rate for the system, i.e., $C_{\Sigma,(a)}\geq 1$.

Next, we need to prove that the sum secrecy rate in the component channel (a) is upper bounded by 1, i.e., $C_{\Sigma,(a)}\leq 1$.

For convenience, let us denote $nR_\Sigma \triangleq n(R_1+R_2)-n\epsilon$ in order not to carry $+n\epsilon$ throughout the derivation. Then, by definition, and Fano's inequality, we have

$$\begin{aligned} nR_\Sigma &= nH(W_1,W_2)-n\epsilon && (8)\\ &\leq I(W_1,W_2;Y_{11}^n,Y_{12}^n)-I(W_1,W_2;Y_2^n) && (9)\end{aligned}$$

Using the chain rule on both terms on the right hand side,

$$\begin{aligned} nR_\Sigma &\leq I(W_1,W_2;Y_{11}^n)+I(W_1,W_2;Y_{12}^n|Y_{11}^n)\\ &\quad -I(W_1;Y_2^n)-I(W_2;Y_2^n|W_1) && (10)\\ &= I(W_1;Y_{11}^n)+I(W_2;Y_{11}^n|W_1)-I(W_1;Y_2^n)\\ &\quad +I(W_1,W_2;Y_{12}^n|Y_{11}^n)-I(W_2;Y_2^n|W_1) && (11)\\ &= I(W_1;Y_{11}^n)+I(W_2;Y_{11}^n,W_1)-I(W_1;Y_2^n)\\ &\quad +I(W_1,W_2;Y_{12}^n|Y_{11}^n)-I(W_2;Y_2^n|W_1) && (12)\\ &= I(W_1;Y_{11}^n)-I(W_1;Y_2^n)\\ &\quad +I(W_1,W_2;Y_{12}^n|Y_{11}^n)-I(W_2;Y_2^n|W_1) && (13)\\ &= \big[I(W_1;Y_{11}^n)-I(W_1;Y_2^n)\big]\\ &\quad +\big[I(W_1,W_2;Y_{12}^n|Y_{11}^n)-I(W_2;Y_2^n,W_1)\big] && (14)\end{aligned}$$

where (12) and (14) come from the independence of W_2 and W_1, and (13) comes from the independence of W_2 and (W_1,Y_{11}^n). For the first part in (14), we have

$$\begin{aligned} &I(W_1;Y_{11}^n)-I(W_1;Y_2^n)\\ &\quad\leq I(W_1;Y_{11}^n,Y_2^n)-I(W_1;Y_2^n) && (15)\\ &\quad= I(W_1;Y_{11}^n|Y_2^n) && (16)\\ &\quad= I(W_1;X_{11}^n|Y_2^n) && (17)\\ &\quad= H(X_{11}^n|Y_2^n)-H(X_{11}^n|Y_2^n,W_1) && (18)\end{aligned}$$

where we refer to (6). For the second part in (14), we have

$$\begin{aligned} &I(W_1,W_2;Y_{12}^n|Y_{11}^n)-I(W_2;Y_2^n,W_1)\\ &\quad= I(W_1;Y_{12}^n|Y_{11}^n)+I(W_2;Y_{12}^n|Y_{11}^n,W_1)\\ &\qquad -I(W_2;Y_2^n,W_1) && (19)\\ &\quad= I(W_1;Y_{12}^n|Y_{11}^n)+I(W_2;Y_{12}^n,Y_{11}^n,W_1)\\ &\qquad -I(W_2;Y_2^n,W_1) && (20)\\ &\quad\leq I(W_1;Y_{12}^n|Y_{11}^n)+I(W_2;Y_{12}^n,Y_{11}^n,Y_2^n,W_1)\\ &\qquad -I(W_2;Y_2^n,W_1) && (21)\\ &\quad= I(W_1;Y_{12}^n|Y_{11}^n)+I(W_2;Y_{12}^n,Y_{11}^n|Y_2^n,W_1) && (22)\\ &\quad\leq I(X_{11}^n,X_{12}^n;Y_{12}^n|Y_{11}^n)+I(X_2^n;Y_{12}^n,Y_{11}^n|Y_2^n,W_1) && (23)\\ &\quad= I(X_{12}^n;Y_{12}^n|X_{11}^n)+H(X_2^n|Y_2^n,W_1) && (24)\\ &\quad= I(X_{12}^n;Y_{12}^n|X_{11}^n)+H(X_{11}^n|Y_2^n,W_1) && (25)\end{aligned}$$

where (20) follows from the independence of W_2 and (W_1,Y_{11}^n), (23) follows from the Markov chains

$$\begin{aligned} W_1 &\to (Y_{11}^n,X_{11}^n,X_{12}^n)\to Y_{12}^n\\ W_2 &\to (X_2^n,Y_2^n,W_1)\to (Y_{12}^n,Y_{11}^n),\end{aligned}$$

we obtain (24) by using the channel model in (6) and the fact that by knowing $(Y_{11}^n,Y_2^n)=(X_{11}^n,Y_2^n)$, X_2^n can be determined, and finally, we reach (25) by using the channel model in (6) and through the following derivation

$$\begin{aligned} H(X_2^n|Y_2^n,W_1) &= H(X_2^n,Y_2^n,W_1)-H(Y_2^n,W_1) && (26)\\ &= H(X_2^n,X_{11}^n,W_1)-H(Y_2^n,W_1) && (27)\\ &= H(X_{11}^n,Y_2^n,W_1)-H(Y_2^n,W_1) && (28)\\ &= H(X_{11}^n|Y_2^n,W_1) && (29)\end{aligned}$$

Substituting (18) and (25) into (14), we obtain

$$\begin{aligned} nR_\Sigma &\leq H(X_{11}^n|Y_2^n)+I(X_{12}^n;Y_{12}^n|X_{11}^n) && (30)\\ &= H(X_{11}^n|X_{11}^n\oplus X_2^n)+I(X_{12}^n;X_{12}^n\oplus X_2^n|X_{11}^n) && (31)\end{aligned}$$

where $\oplus$ means bitwise modulo plus. Now, intuitively, as shown in (31), if transmitter 1 intends to transmit n-bit message via X_{11}^n, then to protect it, transmitter 2 must send Bernoulli $(\frac{1}{2})$ i.i.d random noise; however, by performing that, the sub-channel capacity between X_{12}^n and Y_{12}^n is constrained and reduced to zero. To confirm this, we continue from (31)

$$\begin{aligned} nR_\Sigma &\leq H(X_{11}^n|X_{11}^n\oplus X_2^n)+I(X_{12}^n;X_{12}^n\oplus X_2^n|X_{11}^n) && (32)\\ &= H(X_2^n,X_{11}^n)-H(X_{11}^n\oplus X_2^n)\\ &\quad +H(X_{12}^n\oplus X_2^n|X_{11}^n)-H(X_2^n|X_{12}^n,X_{11}^n) && (33)\\ &= H(X_2^n)+H(X_{11}^n)-H(X_{11}^n\oplus X_2^n)\\ &\quad +H(X_{12}^n\oplus X_2^n|X_{11}^n)-H(X_2^n) && (34)\\ &= H(X_{11}^n)-H(X_{11}^n\oplus X_2^n)+H(X_{12}^n\oplus X_2^n|X_{11}^n) && (35)\\ &= H(X_{11}^n|X_2^n)-H(X_{11}^n\oplus X_2^n)\\ &\quad +H(X_{12}^n\oplus X_2^n|X_{11}^n) && (36)\\ &= H(X_{11}^n\oplus X_2^n|X_2^n)-H(X_{11}^n\oplus X_2^n)\\ &\quad +H(X_{12}^n\oplus X_2^n|X_{11}^n) && (37)\\ &= H(X_{12}^n\oplus X_2^n|X_{11}^n)-I(X_2^n;X_{11}^n\oplus X_2^n) && (38)\\ &\leq H(X_{12}^n\oplus X_2^n|X_{11}^n)=H(Y_{12}^n|X_{11}^n)\leq H(Y_{12}^n) && (39)\\ &\leq n && (40)\end{aligned}$$

where we repeatedly use the independence of X_2^n and X_{11}^n, and also the independence of X_2^n and (X_{11}^n,X_{12}^n).

Finally, (40) implies $C_{\Sigma,(a)}\leq 1$, concluding, together with the achievability, that $C_{\Sigma,(a)}=1$, and hence $C_{\Sigma,\text{indep}}=2$.

B. Joint Encoding Based Achievable Scheme

Here, we provide an achievable scheme to transmit 3 bits securely by coding across the component channels, i.e., by introducing correlation between the channel inputs of component channels. Let $\{A,B,C,U,V\}$ be mutually independent Bernoulli $(\frac{1}{2})$ random variables. Here, $\{A,B,C\}$ represent the message carrying signals, and $\{U,V\}$ represent the jamming signals. The joint encoding based achievable scheme is shown

in color magenta in Fig. 1, where transmitter 1 sends A, V and $A \oplus V$ in three component channels, respectively (note that we choose $X_{12} = 0$), and transmitter 2 sends U, (B, C) and $B \oplus U$ in three component channels, respectively.

With this scheme, the legitimate receiver observes $A, U, B, C \oplus V, A \oplus V \oplus B \oplus U$ from three component channels, which means that the legitimate receiver can decode message A from transmitter 1 and messages B, C from transmitter 2 with zero probability of error, i.e., the legitimate receiver can decode 3 bits reliably. On the other hand, the eavesdropper observes $A \oplus U$, $B \oplus V$ and $A \oplus U \oplus B \oplus V$, which implies

$$\begin{aligned} &I(A, B, C; A \oplus U, B \oplus V, A \oplus U \oplus B \oplus V) \\ &\quad = I(A, B, C; A \oplus U, B \oplus V) && (41) \\ &\quad = H(A \oplus U, B \oplus V) - H(A \oplus U, B \oplus V | A, B, C) && (42) \\ &\quad = H(A \oplus U, B \oplus V) - H(U, V) && (43) \\ &\quad = 2 - 2 = 0 && (44) \end{aligned}$$

where we use the independence of $\{A, B, C, U, V\}$ and also that they are all Bernoulli $(\frac{1}{2})$. This derivation implies that the eavesdropper learns nothing about the messages, and therefore, 3 bits are sent to the legitimate receiver reliably and securely.

IV. Gaussian MAC Wiretap Channel

A. General Inseparability

In this section, we show that even the parallel Gaussian MAC wiretap channel is not separable in general. We prove this by providing a specific example. Also note that, it suffices to show the inseparability from the s.d.o.f. point of view, since it implies the inseparability of the secrecy capacity.

Consider the special two-user parallel Gaussian MAC wiretap channel shown in Fig. 2, in which each component channel is a two-user Gaussian MAC wiretap channel defined by,

$$Y_{1k} = h_{1k} X_{1k} + h_{2k} X_{2k} + N_{1k} \quad (45)$$

$$Y_{2k} = g_{1k} X_{1k} + g_{2k} X_{2k} + N_{2k} \quad (46)$$

where $k = a, b$, and (h_{ia}, h_{ib}) and (g_{ia}, g_{ib}) are the time-invariant channel gains of user i to the legitimate receiver and the eavesdropper, respectively. We let

$$h_{1b} = h_{2b} = \alpha, \quad \text{and} \quad g_{1b} = g_{2b} = \beta \quad (47)$$

Then, the six random variables $\{h_{1a}, h_{2a}, g_{1a}, g_{2a}, \alpha, \beta\}$ are mutually independently distributed according to the same continuous distribution, and N_{1a}, N_{2a}, N_{1b}, N_{2b} are mutually independent Gaussian random variables with zero-mean and unit-variance. The channel inputs of each user satisfy average power constraints, $\mathrm{E}\left[X_{ia}^2 + X_{ib}^2\right] \le P$, for $i = 1, 2$.

From [17], for almost all channel gains $\{h_{1a}, h_{2a}, g_{1a}, g_{2a}\}$, the sum s.d.o.f. for component channel (a) is $\frac{2}{3}$. From [8], component channel (b) is degraded, and its sum s.d.o.f. is zero. This implies that, by independent encoding across the component channels, the optimum sum s.d.o.f. is $\frac{2}{3}$.

On the other hand, by selecting

$$X_{1a} = \frac{1}{g_{1a}} V, \; X_{2a} = \frac{1}{g_{2a}} U, \; X_{1b} = \frac{1}{\beta} V, \; X_{2b} = \frac{1}{\beta} U \quad (48)$$

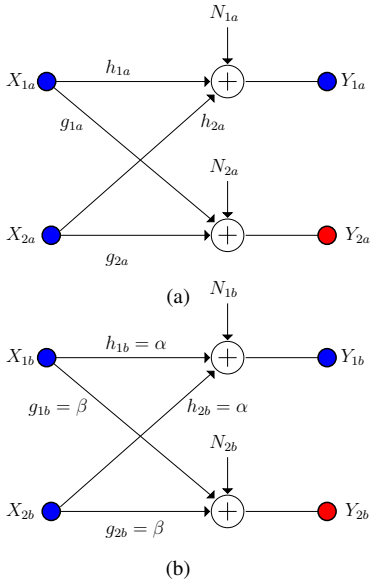

Fig. 2. An example two-user parallel Gaussian MAC wiretap channel.

where V and U are independent random variable drawn from the following discrete PAM constellation:

$$C(a, Q) = a\{-Q, -Q+1, \ldots, Q-1, Q\} \quad (49)$$

Here, V represents the message-carrying signal and U represents the jamming signal. Let us define $\hat{Y}$ as

$$\begin{aligned} \hat{Y} &= \frac{g_{2a}}{h_{2a}} Y_{1a} - \frac{\beta}{\alpha} Y_{1b} && (50) \\ &= \left[\frac{g_{2a} h_{1a}}{g_{1a} h_{2a}} - 1\right] V + \frac{g_{2a}}{h_{2a}} N_{1a} - \frac{\beta}{\alpha} N_{1b} && (51) \end{aligned}$$

The factor in front of V is non-zero for almost all channel gains. Let us define $\hat{V}$ as the estimate of V obtained by selecting the closest point in $C(a, Q)$ based on the observation $\hat{Y}$. For any small enough $\delta > 0$, let us choose $Q = P^{\frac{1-\delta}{2}}$ and $a = \gamma P^{\frac{\delta}{2}}$, where γ is a constant independent of P to meet the average power constraint. Then, due to the Markov chain $V \to (Y_{1a}, Y_{1b}) \to \hat{Y} \to \hat{V}$, we have

$$\begin{aligned} I(V; Y_{1a}, Y_{1b}) &\ge I(V; \hat{Y}) \ge I(V; \hat{V}) && (52) \\ &= H(V) - H(V|\hat{V}) && (53) \\ &= \log(2Q+1) - H(V|\hat{V}) && (54) \\ &\ge \log(2Q+1) - 1 - \Pr\left[V \ne \hat{V}\right] \log(2Q+1) && (55) \\ &\ge \left\{1 - \Pr\left[V \ne \hat{V}\right]\right\} \frac{1-\delta}{2} \log P - 1 && (56) \end{aligned}$$

Now, due to the PAM structure, probability of error is

$$\Pr\left[V \ne \hat{V}\right] \le \exp\left(-\gamma' a^2\right) \le \exp\left(-\gamma'' P^{\delta}\right) \quad (57)$$

where γ', γ'' are constants independent of P. Then, from (56) and (57), at high SNR (large enough P), we have

$$I(V; Y_{1a}, Y_{1b}) \ge \frac{1-\delta}{2} \log P + o(\log P) \quad (58)$$

where $o(\cdot)$ is the little-o function.

On the other hand, for the information leakage rate,

$$I(V;Y_{2a},Y_{2b}) \le I(V;V+U) \tag{59}$$
$$\le H(V+U)-H(V) \tag{60}$$
$$\le \log\frac{4Q+1}{2Q+1} \le 1 \tag{61}$$

By [13, Theorem 1], we can achieve the sum secrecy rate of

$$\sup(R_1+R_2) \ge I(V;Y_{1a},Y_{1b})-I(V;Y_{2a},Y_{2b}) \tag{62}$$
$$\ge \frac{1-\delta}{2}\log P + o(\log P) \tag{63}$$

for any $\delta \ge 0$, which implies that we can achieve 1 sum s.d.o.f. This means that by joint encoding across component channels, we achieve 1 sum s.d.o.f. outperforming optimum independent encoding, which can at most achieve $\frac{2}{3}$ sum s.d.o.f.

B. Separability in s.d.o.f. for Almost All Channel Gains

Although the Gaussian MAC wiretap channel is not always separable, the special construction provided in the last subsection is not "general", i.e., for almost all channel gains, the constraints in (47) are never met. Based on this observation, we show that the s.d.o.f. region of the parallel Gaussian MAC wiretap channel is separable for almost all channel gains.

From [18], the s.d.o.f. regions of the component Gaussian MAC wiretap channels are identical, i.e., $D_{s,(a)} = D_{s,(b)}$, and

$$D_{s,(a)} = \{(d_1,d_2):\ 2d_1+d_2\le 1,\ d_1+2d_2\le 1\} \tag{64}$$

Therefore, it suffices to show that for the overall parallel Gaussian MAC channel the s.d.o.f. region is

$$D_s = \{(d_1,d_2):\ 2d_1+d_2\le 2,\ d_1+2d_2\le 2\} \tag{65}$$

The achievability follows from [18] for almost all channel gains. In the achievability, we scale the power in each component channel, to meet the overall power constraint; however, this does not affect the s.d.o.f. calculations.

For the converse, we first *flatten* the parallel channel by concatenating the channel inputs and outputs of component channels into $2n$-length vectors. Instead of studying the parallel channel in n channel uses, we study the *flat channel* in $2n$ channel uses. The power constraint remains the same over $2n$ channel uses. In addition, since introducing correlation in time and in component channels has the same effect, the flat channel must have the same converse as the original one.

Then, similar to the steps in [17, Eqns. (7)-(16)], we have

$$n(R_1+R_2) \le h(\tilde{\mathbf{X}}_1,\tilde{\mathbf{X}}_2,\mathbf{Y}_1,\mathbf{Y}_2)-h(\tilde{\mathbf{X}}_1,\tilde{\mathbf{X}}_2|\mathbf{Y}_1,\mathbf{Y}_2) - h(\mathbf{Y}_2)+nc_0 \tag{66}$$

where vectors in bold-face are $2n$-length vectors. The components of $2n$-vectors $\tilde{\mathbf{X}}_j$, for $j=1,2$, are $\tilde{X}_{ji} = X_{ji}+\tilde{N}_{ji}$, for $i=1,\dots,2n$. Here, the sequence $\tilde{N}_j^{2n}$ is i.i.d. over time, is independent of all other random variables, and $\tilde{N}_{ji}$ is a Gaussian random variable with zero-mean and variance σ_{ji}^2, such that

$$\sigma_{ji}^2 < \min\left\{\frac{1}{h_{ja}^2},\frac{1}{g_{ja}^2},\frac{1}{h_{jb}^2},\frac{1}{g_{jb}^2}\right\} \tag{67}$$

Then, all the remaining steps in [17] follow, and we have

$$nR_i+nR_1+nR_2 \le h(Y_1^{2n})+nc_1 \le \left(\frac{2n}{2}\log P\right)+nc_2 \tag{68}$$

for $i=1,2$. This implies

$$2d_1+d_2\le 2, \quad \text{and} \quad d_1+2d_2\le 2 \tag{69}$$

which completes the proof of the converse for this case.

V. Conclusions

We showed that the parallel MAC wiretap channel is not always separable by providing a specific example in which the sum secrecy rate by joint encoding over parallel channels outperforms the best rate achievable by individually optimal encoding for each component channel. Then, we showed that the parallel Gaussian MAC wiretap channel is inseparable in general as well. Finally, we showed, from a s.d.o.f. point of view, that the parallel Gaussian MAC wiretap channel is separable almost surely, however, separability in s.d.o.f. is weaker than separability in secrecy capacity.

References

[1] T. M. Cover and J. A. Thomas. *Elements of Information Theory*. Wiley-Interscience, second edition, 2006.

[2] D. Tse and S. V. Hanly. Multiaccess fading channels-Part I: Polymatroid structure, optimal resource allocation and throughput capacities. *IEEE Trans. Inf. Theory*, 44(7):2796–2815, November 1998.

[3] D. Tse. Optimal power allocation over parallel Gaussian broadcast channels. In *IEEE ISIT*, June 1997.

[4] L. Sankar, X. Shang, E. Erkip, and H. V. Poor. Ergodic two-user interference channels: Is separability optimal? In *Allerton Conference*, September 2008.

[5] V. R. Cadambe and S. A. Jafar. Parallel Gaussian interference channels are not always separable. *IEEE Trans. Inf. Theory*, 55(9):3983–3990, September 2009.

[6] H. Sun, C. Geng, and S. A. Jafar. Topological interference management with alternating connectivity. Available at [arXiv:1302.4020].

[7] P. Mukherjee, R. Tandon, and S. Ulukus. Even symmetric parallel linear deterministic interference channels are inseparable. In *Allerton Conference*, October 2013.

[8] E. Tekin and A. Yener. The Gaussian multiple access wire-tap channel. *IEEE Trans. Inf. Theory*, 54(12):5747–5755, December 2008.

[9] E. Tekin and A. Yener. The general Gaussian multiple-access and two-way wiretap channels: Achievable rates and cooperative jamming. *IEEE Trans. Inf. Theory*, 54(6):2735–2751, June 2008.

[10] E. Ekrem and S. Ulukus. On the secrecy of multiple access wiretap channel. In *Allerton Conference*, September 2008.

[11] E. Ekrem and S. Ulukus. Cooperative secrecy in wireless communications. *Securing Wireless Communications at the Physical Layer*, W. Trappe and R. Liu, Eds., Springer-Verlag, 2009.

[12] X. He and A. Yener. Providing secrecy with structured codes: Two-user Gaussian channels. *IEEE Trans. Inf. Theory*, 60(4):2121–2138, April 2014.

[13] G. Bagherikaram, A. S. Motahari, and A. K. Khandani. On the secure degrees-of-freedom of the multiple-access-channel. *IEEE Trans. Inf. Theory*, submitted March 2010. Also available at [arXiv:1003.0729].

[14] R. Bassily and S. Ulukus. Ergodic secret alignment. *IEEE Trans. Inf. Theory*, 58(3):1594–1611, March 2012.

[15] N. Liu and W. Kang. The secrecy capacity region of a special class of multiple access channels. In *IEEE ISIT*, July 2011.

[16] M. Wiese and H. Boche. An achievable region for the wiretap multiple-access channel with common message. In *IEEE ISIT*, July 2012.

[17] J. Xie and S. Ulukus. Secure degrees of freedom of the Gaussian multiple access wiretap channel. In *IEEE ISIT*, July 2013.

[18] J. Xie and S. Ulukus. Secure degrees of freedom region of the Gaussian multiple access wiretap channel. In *Asilomar Conference*, November 2013.