Optimal Secure GDoF of Symmetric Gaussian Wiretap Channel with a Helper

Jinyuan Chen and Chunhua Geng

Abstract

We study a symmetric Gaussian wiretap channel with a helper, where a confidential message is sent from a transmitter to a legitimate receiver, in the presence of a helper and an eavesdropper. For this setting, we characterize the optimal secure generalized degrees-of-freedom (GDoF). The result reveals that, adding a helper can significantly increase the secure GDoF of the wiretap channel. The result is supported by a new converse and a new scheme. In the proposed scheme, the helper sends a cooperative jamming signal at a specific power level and direction. In this way, it minimizes the penalty in GDoF incurred by the secrecy constraint. In the secure rate analysis, the techniques of noise removal and signal separation are used.

I. INTRODUCTION

The study of information-theoretic secrecy dates back to Shannon’s work of [1] in 1949. Since then, information-theoretic secrecy has been investigated in varying communication channels, for example, the wiretap channels [2]–[4], multiple access channels with confidential messages and wiretap multiple access channels [5]–[11], the broadcast channels with confidential messages [12]–[16], and the interference channels with confidential messages [12], [17]–[37]. In those settings, the messages are transmitted over the channels with secrecy constraints, which often incur a penalty in capacity (cf. [9], [12], [17], [22], [23], [26], [27], [29], [31], [34], [35]). One way to minimize the capacity penalty incurred by secrecy constraints is to add helper(s) into the channels (see, e.g., [23], [31]–[33], [37]–[40]). Specifically, the work in [37] recently showed that adding a helper can totally remove the penalty in sum generalized degrees-of-freedom (GDoF), in a two-user symmetric Gaussian interference channel.

In this work, we focus on a secure communication over a symmetric Gaussian wiretap channel with a helper. In this setting, a confidential message sent from a transmitter to a legitimate receiver needs to be secure from an eavesdropper, in the presence of a helper. The wiretap channel and its variations have been considered as the basic channels for the investigation of information-theoretic secrecy. For example, the wiretap channel with a helper can be considered as a specific case of an interference channel with only one confidential message. The insights gained from the former can be very helpful in understanding the fundamental limits of the latter. In the wiretap channel with M helpers, the works in [23], [38] showed that the secure degrees-of-freedom (DoF) is $M / (M+1)$ for almost all channel gains. The result is derived under the assumption that perfect channel state information (CSI) is available at the transmitters. The work in [33], [39] then showed that the same secure DoF of $M / (M+1)$ is still achievable when the eavesdropper CSI is not available at the transmitters. Another work in [40] studied a Gaussian wiretap channel with a helper, where a single antenna is equipped at each of the transmitter and the legitimate receiver, while multiple antennas are equipped at each of the helper and the eavesdropper. The result in [40] revealed that the secure DoF 1/2 is achievable irrespective of the number of antennas at the eavesdropper, as long as the number of antennas at the helper is the same as the number of antennas at the eavesdropper. In the setting of wiretap channel with a helper, the previous DoF results were generalized in [31] to the multiple-antenna scenario, where the eavesdropper has $K$ antennas and the other nodes have $N$ antennas, under the assumption that the eavesdropper CSI is not available at the transmitters. In all of those previous works in [23], [31], [33], [38]–[40], the authors considered the secure DoF performance of the channels. The DoF metric is a
form of capacity approximation. Under the DoF metric, all the non-zero channel gains are treated equally strong, at the regime of high signal-to-noise ratio (SNR). However, in the communication channels the capacity is usually affected by different channel strengths of different links. Therefore, it motivates us to go beyond the DoF metric and consider a better form of capacity approximation. GDoF metric is a generalization of DoF, which is able to capture the capacity behavior when different links have different channel strengths and is very helpful in understanding the capacity to within a constant gap (cf. [41]). The work in [32] studied the secure GDoF and secure capacity of the Gaussian wiretap channel with a helper, as well as the Gaussian multiple access wiretap channel, where channel gain from the first transmitter to the eavesdropper is the same as the channel gain from the second transmitter to the eavesdropper, i.e., with symmetric channel gains at the wiretapper. However, the secure GDoF upper bound and the lower bound provided in [32] are not matched for a large range of channel parameters. In this work, we seek to characterize the optimal secure GDoF of a wiretap channel with a helper.

Specifically, the main contribution of this work is the optimal secure GDoF characterization of a symmetric wiretap channel with a helper, for all the channel parameters. The result reveals that, adding a helper can significantly increase the secure GDoF of the wiretap channel (see Fig. 1). The result is supported by a new converse and a new scheme. The converse is derived for the wiretap channel with a helper under the general channel parameters, i.e., the converse holds for the symmetric and asymmetric channels. In the proposed scheme, the helper sends a cooperative jamming signal at a specific power level and direction. In this way, it minimizes the penalty in GDoF incurred by the secrecy constraint. In the proposed scheme, the signal of the transmitter is a superposition of a common signal, middle signal, and a private signal. The power of private signal is low enough such that this signal arrives at the eavesdropper under the noise level. The power of the common signal and middle signal is above the noise level. However, each of the common signal and middle signal is aligned at a specific power level and direction with the jamming signal sent from the helper, which minimizes the penalty in GDoF incurred by the secrecy constraint. The optimal secure GDoF is described in different expressions for different interference regimes. For each interference regime, the power and rate levels of the signals in the proposed scheme are set to the optimal values, so as to achieve the optimal secure GDoF. In the secure rate analysis, the techniques of noise removal and signal separation are used (cf. [42], [43]). The secure GDoF result derived in this work can be extended to understand the secure capacity to within a constant gap, which will be investigated in the future work.

We will organize the rest of this work as follows. In Section II we will describe the channel model. In Section III, the main results of this work will be provided. The converse proof will be described in Section IV and some appendices. The achievability proof will be shown in Section V. Section VI and
some appendices. In Section VII we will provide the conclusion. In terms of notations, we use $\mathbb{H}(\bullet)$ and $\mathbb{I}(\bullet)$ to represent the entropy and mutual information, respectively, and use $h(\bullet)$ to represent differential entropy. $\mathcal{Z}$ and $\mathcal{Z}^+$ are used to denote the sets of integers and positive integers, respectively, while $\mathcal{R}$ is used to denote the set of real numbers. $(\bullet)^+ = \max\{0, \bullet\}$. When $f(s) = o(g(s))$ is used, it suggests that $\lim_{s \to \infty} f(s)/g(s) = 0$. All the logarithms are considered with base 2.

II. System Model

This work focuses on a Gaussian wiretap channel with a helper (see Fig. 2). In this setting, transmitter 1 sends a confidential message to receiver 1 (the legitimate receiver), in the presence of a helper (transmitter 2) and an eavesdropper (receiver 2). The channel input-output relationship of this setting is described by

$$
\begin{align*}
y_1(t) &= \sqrt{P\alpha_{11}}h_{11}x_1(t) + \sqrt{P\alpha_{12}}h_{12}x_2(t) + z_1(t) \\
y_2(t) &= \sqrt{P\alpha_{21}}h_{21}x_1(t) + \sqrt{P\alpha_{22}}h_{22}x_2(t) + z_2(t)
\end{align*}
$$

where $y_k(t)$ denotes the received signal of receiver $k$ at time $t$, $x_k(t)$ denotes the transmitted signal of transmitter $k$ with a normalized power constraint $E|x_k(t)|^2 \leq 1$, and $z_k(t) \sim \mathcal{N}(0, 1)$ denotes the additive white Gaussian noise. $\sqrt{P\alpha_{k\ell}}h_{k\ell}$ represents the channel gain of the link from transmitter $\ell$ to receiver $k$, for $\ell, k = 1, 2$. The nonnegative parameter $\alpha_{k\ell}$ captures the link strength of the channel from transmitter $\ell$ to receiver $k$. $h_{k\ell} \in [1, 2]$ represents the channel coefficient after normalization. In this setting, $P \geq 1$ captures the base of signal-to-noise ratio of all the links. Since the form of $\sqrt{P\alpha_{k\ell}}h_{k\ell}$ can describe any real channel gain no less than 1, the above model can describe the general channels in terms of capacity approximation. In this setting, all the nodes are assumed to know all the channel parameters $\{\alpha_{k\ell}, h_{k\ell}\}_{k,\ell}$.

When we consider the symmetric case, we will assume that

$$
\alpha_{12} = \alpha_{21} = \alpha, \quad \alpha_{22} = \alpha_{11} = 1, \quad \alpha \geq 0.
$$

In this setting, transmitter 1 sends a message $w$ to its legitimate receiver over $n$ channel uses, where $w$ is chosen uniformly from the set $\mathcal{W} \triangleq \{1, 2, 3, \ldots, 2^n\}$. When transmitting the confidential message from transmitter 1, a stochastic function

$$
f_1: \mathcal{W}_0 \times \mathcal{W} \to \mathcal{R}^n
$$

maps $w \in \mathcal{W}$ to the signal $x_1^n = f_1(w_0, w) \in \mathcal{R}^n$, where the randomness in this mapping is represented by $w_0 \in \mathcal{W}_0$. We assume that $w_0$ and $w$ are independent. At the helper (transmitter 2), another function

$$
f_2: \mathcal{W}_h \to \mathcal{R}^n
$$

generates a random signal $x_2^n = f_2(w_h) \in \mathcal{R}^n$, where $w_h \in \mathcal{W}_h$ is a random variable that is independent of $w_0$ and $w$. We assume that $w_0$ is available at the first transmitter only, while $w_h$ is available at the
second transmitter only. We say a secure rate $R$ is achievable if there exists a sequence of codes with $n$-length, such that the legitimate receiver can reliably decode the message $w$, i.e.,

$$\Pr[w \neq \hat{w}] \leq \epsilon$$

for any $\epsilon > 0$, and the message is secure from the eavesdropper, i.e.,

$$\mathbb{I}(w; y^n_2) \leq n\epsilon.$$ (3)

We will use $C$ to denote the secure capacity, which is defined as the maximal secure rate that is achievable. We will use $d$ to denote the secure generalized degrees-of-freedom (GDoF), which is defined as

$$d \triangleq \lim_{P \to \infty} \frac{C}{\frac{1}{2}\log P}.$$ (4)

GDoF is a form of the approximation of capacity. In this setting, DoF is a particular case of GDoF by considering only one point with $\alpha_{12} = \alpha_{21} = \alpha_{22} = \alpha_{11} = 1$.

**III. Main Result**

This section provides the main result for the wiretap channel with a helper defined in Section II.

**Theorem 1.** Consider the symmetric Gaussian wiretap channel with a helper defined in Section II. For almost all channel coefficients $\{h_{kt}\} \in (1, 2]^{2 \times 2}$, the optimal secure GDoF is characterized as

$$d = \begin{cases} 
1 & \text{for } 0 \leq \alpha \leq 1/2 \\
2 - 2\alpha & \text{for } 1/2 \leq \alpha \leq 3/4 \\
2\alpha - 1 & \text{for } 3/4 \leq \alpha \leq 5/6 \\
3/2 - \alpha & \text{for } 5/6 \leq \alpha \leq 1 \\
\alpha/2 & \text{for } 1 \leq \alpha \leq 4/3 \\
2 - \alpha & \text{for } 4/3 \leq \alpha \leq 2 \\
0 & \text{for } 2 \leq \alpha. 
\end{cases}$$ (5)

**Proof.** The converse follows from Lemma 1 and Corollary 2 described in Section IV. Specifically, Lemma 1 provides some upper bounds on the secure rate of the Gaussian wiretap channel with a helper, under general channel parameters. Corollary 2 is the GDoF result derived from Lemma 1 in the setting of symmetric Gaussian wiretap channel with a helper. The optimal secure GDoF is achieved by the proposed scheme with cooperative jamming, described in Sections V and VI as well as in Appendices B and C. □

Fig. 1 depicts the optimal secure GDoF for the symmetric Gaussian wiretap channels with and without a helper. For the wiretap channel without a helper (removing transmitter 2), the secure GDoF, denoted by $d_{no}$, is characterized as

$$d_{no} = (1 - \alpha)^+ \quad \forall \alpha \in [0, \infty)$$

(see in Appendix D for the analysis). One can see that, adding a helper can significantly increase the secure GDoF of the wiretap channel.
IV. Converse

For the Gaussian wiretap channel with a helper defined in Section II, we provide a general upper bound on the secure rate, which is stated in the following lemma.

Lemma 1. For the Gaussian wiretap channel with a helper defined in Section II, and let \( \phi_1 \triangleq (\alpha_{12} - (\alpha_{22} - \alpha_{21})^+) \) and \( \phi_3 \triangleq \min\{\alpha_{21}, \alpha_{12}, (\alpha_{11} - \phi_1)^+\} \), the secure rate is upper bounded by

\[
R \leq \frac{1}{2} \log \left( 1 + P^{\alpha_{11} - \phi_3} \cdot \frac{|h_{11}|^2}{|h_{21}|^2} + P^{\alpha_{12} - (\alpha_{22} - \alpha_{21})^+} \cdot \frac{|h_{12}|^2}{|h_{22}|^2} \right) + \frac{1}{2} \log \left( 1 + P^{\phi_3 - \phi_1} |h_{22}|^2 \right) + 7.3 \tag{6}
\]

\[
R \leq \frac{1}{2} \left( \frac{1}{2} \log \left( 1 + \frac{P^{(\alpha_{11} - \alpha_{21})^+}}{|h_{21}|^2} \right) + \frac{1}{2} \log \left( 1 + \frac{P^{(\alpha_{22} - \alpha_{12})^+}}{|h_{12}|^2} \right) + \frac{1}{2} \log \left( 1 + P^{\alpha_{11} |h_{11}|^2} + P^{\alpha_{12} |h_{12}|^2} \right) \right) + \log 9 \tag{7}
\]

\[
R \leq \frac{1}{2} \log \left( 1 + P^{\alpha_{11} - \alpha_{21}} \cdot \frac{|h_{11}|^2}{|h_{21}|^2} + P^{\alpha_{22} + \alpha_{11} - \alpha_{21}} \cdot \frac{|h_{11}|^2 |h_{12}|^2}{|h_{21}|^2} \right) \tag{8}
\]

The proof of Lemma 1 is provided in the following subsections. Based on Lemma 1, we provide the secure GDoF upper bound in the following corollary.

Corollary 1. For the Gaussian wiretap channel with a helper defined in Section II, the secure GDoF is upper bounded by

\[
d \leq \min \left\{ \max \{\phi_1, (\alpha_{11} - \phi_3)^+\} + (\phi_3 - \phi_1)^+, \right. \\
\left. \frac{1}{2} \left( (\alpha_{11} - \alpha_{21})^+ + (\alpha_{22} - \alpha_{12})^+ + \max \{\alpha_{11}, \alpha_{12}\} \right), \right. \\
\left. \max \{ (\alpha_{11} - \alpha_{21})^+, (\alpha_{22} + \alpha_{11} - \alpha_{21})^+ \} \right\} \tag{9}
\]

Proof. The first bound \( d \leq \max \{\phi_1, (\alpha_{11} - \phi_3)^+\} + (\phi_3 - \phi_1)^+ \) follows from the bound in (6). The second bound follows from the bound in (7) and the last bound follows from the bound in (8). \( \square \)

The following result is a simplified version of Corollary 1 for the symmetric setting with \( \alpha_{11} = \alpha_{22} = 1, \alpha_{21} = \alpha_{12} = \alpha \).

Corollary 2. For the symmetric Gaussian wiretap channel with a helper defined in Section II with \( \alpha_{11} = \alpha_{22} = 1, \alpha_{21} = \alpha_{12} = \alpha \), the secure GDoF is upper bounded by

\[
d \leq \begin{cases} 
1 \quad \text{for } 0 \leq \alpha \leq 1/2 \\
2 - 2\alpha \quad \text{for } 1/2 \leq \alpha \leq 3/4 \\
2\alpha - 1 \quad \text{for } 3/4 \leq \alpha \leq 5/6 \\
3/2 - \alpha \quad \text{for } 5/6 \leq \alpha \leq 1 \\
\alpha/2 \quad \text{for } 1 \leq \alpha \leq 4/3 \\
2 - \alpha \quad \text{for } 4/3 \leq \alpha \leq 2 \\
0 \quad \text{for } 2 \leq \alpha \end{cases}
\]

Proof. See Appendix E \( \square \)
In what follows, we provide the proof of Lemma 1. At first we define that

\[
\begin{align*}
\phi_1 & \triangleq (\alpha_{12} - (\alpha_{22} - \alpha_{21})^+) \\
\phi_2 & \triangleq (\alpha_{11} - \phi_1^+) \\
\phi_3 & \triangleq \min\{\alpha_{21}, \alpha_{12}, \phi_2\}
\end{align*}
\]

and

\[
\begin{align*}
s_{kk}(t) & \triangleq \sqrt{P^{(s_{kk} - \alpha_{kk})^+}} h_{kk} x_k(t) + \tilde{z}_k(t) \\
s_{\ell k}(t) & \triangleq \sqrt{P^{(s_{\ell k} - \alpha_{\ell k})^+}} h_{\ell k} x_k(t) + z_{\ell}(t) \\
\bar{x}_1(t) & \triangleq \sqrt{P^{\min\{\alpha_{21}, \alpha_{12}, \alpha_{11} - \phi_1\}} h_{21} x_1(t) + \tilde{z}_3(t)} \\
\bar{x}_2(t) & \triangleq \sqrt{P^{\phi_3} \bar{z}_2(t) + \tilde{z}_4(t)}
\end{align*}
\]

for \( k, \ell \in \{1, 2\}, k \neq \ell \), where \( \tilde{z}_1(t), \tilde{z}_2(t), \tilde{z}_3(t), \tilde{z}_4(t) \sim \mathcal{N}(0, 1) \) are i.i.d. noise random variables that are independent of the other noise random variables and transmitted signals \( \{x_1(t), x_2(t)\} \). Let \( s_{kk}^n \triangleq \{s_{kk}(t)\}_{t=1}^n, s_{\ell k}^n \triangleq \{s_{\ell k}(t)\}_{t=1}^n, \bar{x}_k^n \triangleq \{\bar{x}_k(t)\}_{t=1}^n \) and \( \bar{y}_2^n \triangleq \{\bar{y}_2(t)\}_{t=1}^n \).

A. Proof of bound (6)

Let us focus on the proof of bound (6). For the channel defined in Section 11, the secure rate is bounded as follows:

\[
nR = \mathbb{H}(w) = \mathbb{H}(w; y_1^n) + \mathbb{H}(w|y_1^n) \\
\leq \mathbb{H}(w; y_1^n) + n\epsilon_{1,n}
\]

(19)

(20)

(21)

(22)

where (19) follows from Fano’s inequality, \( \lim_{n \to \infty} \epsilon_{1,n} = 0 \); (20) results from secrecy constraint in (3), i.e., \( \mathbb{I}(w; y_2^n) \leq n\epsilon \) for an arbitrary small \( \epsilon \); (21) uses the fact that adding information will not reduce the mutual information; (22) follows from the fact that \( w \) is independent of \( x_2^n \) and \( s_{22}^n \) (cf. (14)).

Let us first focus on the term \( \mathbb{I}(w; y_2^n) \) in (22). From the definition in (18), we note that \( w \to y_2^n \to \bar{y}_2^n \) forms a Markov chain, which implies that

\[
\mathbb{I}(w; y_2^n) = \mathbb{I}(w; \bar{y}_2^n) \\
= \mathbb{I}(w; \bar{y}_2^n | s_{22}^n) + \mathbb{I}(w; s_{22}^n) - \mathbb{I}(w; \bar{y}_2^n | s_{22}^n) \\
= \mathbb{I}(w; \bar{y}_2^n | s_{22}^n) - \mathbb{I}(w; s_{22}^n | \bar{y}_2^n)
\]

(23)

(24)
where (23) results from the Markov chain $w \rightarrow y^n_2 \rightarrow \tilde{y}^n_2$; (24) follows from the independence between $w$ and $s^n_{22}$. For the term $\mathbb{I}(w; s^n_{22} | \tilde{y}^n_2)$ in (24), it can be bounded by

$$\mathbb{I}(w; s^n_{22} | \tilde{y}^n_2) = h(s^n_{22} | \tilde{y}^n_2, w) - h(s^n_{22} | \tilde{y}^n_2)$$

$$\leq \sum_{t=1}^{n} h(s_{22}(t) | \tilde{y}_2(t)) - h(s^n_{22} | \tilde{y}^n_2, w, x^n_2)$$

$$= \sum_{t=1}^{n} h(s_{22}(t) | \tilde{y}_2(t)) - \frac{1}{2} \log(2\pi e)$$

$$\leq \sum_{t=1}^{n} h(\tilde{z}_2(t) - h_{21}x_1(t) - \sqrt{P_{\phi_3}} h_{22}z_2(t) - \sqrt{P_{\phi_3}} \tilde{z}_2(t))$$

$$\leq \sum_{t=1}^{n} \left[ (\sqrt{P_{\phi_3}} - \sqrt{P_{\phi_3}} h_{22}x_2(t) | \tilde{y}_2(t)) - \frac{n}{2} \log(2\pi e) \right]$$

$$\leq \frac{n}{2} \log 14$$

where (25) follows from chain rule and the fact that conditioning reduces differential entropy; (26) uses the identity that $h(\tilde{z}^n_2) = \frac{n}{2} \log(2\pi e)$; (27) results from the fact that Gaussian input maximizes the differential entropy, and that conditioning reduces differential entropy.

Then, by incorporating (24) and (28) into (22), it gives

$$nR - \frac{n}{2} \log 14 - n\epsilon_{1,n} - n\epsilon$$

$$\leq \mathbb{I}(w; y^n_1 | s^n_{22}) - \mathbb{I}(w; \tilde{y}^n_2 | s^n_{22})$$

$$= h(y^n_1 | s^n_{22}) - h(\tilde{y}^n_2 | s^n_{22}) + h(\tilde{y}^n_2 | s^n_{22}, w) - h(y^n_1 | s^n_{22}, w)$$

$$= h(y^n_1 | s^n_{22}) - h(\tilde{y}^n_2 | s^n_{22}) + h(y^n_1 | s^n_{22}, w) - h(\tilde{y}^n_2 | s^n_{22}, w)$$

$$\leq h(y^n_1 | s^n_{22}) - h(\tilde{y}^n_2 | s^n_{22}, w)$$

where (29) uses the identities that $h(\tilde{y}^n_2 | s^n_{22}, w) = h(\tilde{y}^n_2, s^n_{22} | w) - h(s^n_{22} | w)$ and $h(y^n_1 | s^n_{22}, w) = h(y^n_1, s^n_{22} | w) - h(s^n_{22} | w)$.

For the difference of the first two terms in the right-hand side of (29), it can be bounded by using the result of [35] Lemma 9 (described below). Before that, let us first bound this difference as follows:

$$h(y^n_1 | s^n_{22}) - h(\tilde{y}^n_2 | s^n_{22})$$

$$\leq h(y^n_1 | s^n_{22}) - h(\tilde{y}^n_2 | s^n_{22}, z^n_2)$$

$$= h(y^n_1 | s^n_{22}) - h(\tilde{y}^n_2 | s^n_{22}, z^n_2)$$

$$= h(y^n_1 | s^n_{22}) - h(\tilde{y}^n_2 | s^n_{22}, z^n_2)$$

$$= h(y^n_1 | s^n_{22}) - h(\tilde{y}^n_2 | s^n_{22})$$

$$= h(y^n_1 | s^n_{22}) - h(\tilde{y}^n_2 | s^n_{22})$$

$$= h(y^n_1 | s^n_{22}) - h(\tilde{y}^n_2 | s^n_{22})$$

$$= h(y^n_1 | s^n_{22}) - h(\tilde{y}^n_2 | s^n_{22})$$

where $\tilde{y}^n_2(t)$ and $s^n_{22}(t)$ are defined in (18) and (14), respectively; (30) uses the fact that conditioning reduces differential entropy; (31) follows from the fact that $z^n_2$ is independent of $\sqrt{P_{\phi_3}} h_{21}x_1(t) + \sqrt{P_{\phi_3}} h_{22}x_2(t) + \tilde{z}_2(t)$; in (32) we replace $\tilde{z}_2(t)$ with a new noise random variable $z^n_2(t) \sim \mathcal{N}(0,1)$ that is independent of the other noise random variables and transmitted signals $\{x_1(t), x_2(t)\}_t$; note that replacing $\tilde{z}_2(t) \sim \mathcal{N}(0,1)$ with $z^n_2(t) \sim \mathcal{N}(0,1)$
will not change the differential entropies in (31), due to the fact that differential entropy depends on distributions. To bound the right-hand side of (32), we will use the result of [35] Lemma 9 that is described below.

**Lemma 2.** [35] Lemma 9] Let \( y_1(t) = \sqrt{P^{\alpha_{11}}}h_{11}x_1(t) + \sqrt{P^{\alpha_{12}}}h_{12}x_2(t) + z_1(t) \) and \( y_2(t) = \sqrt{P^{\alpha_{21}}}h_{21}x_1(t) + \sqrt{P^{\alpha_{22}}}h_{22}x_2(t) + z_2(t) \), as defined in (1). Consider a random variable (or a set of random variables), \( \tilde{w}_1 \), that is independent of \( \{ x_2^n, z_1^n, z_2^n, z_3^n, z_4^n \} \); and consider another random variable (or another set of random variables), \( \tilde{w}_2 \), that is independent of \( \{ x_1^n, z_1^n, z_2^n, z_3^n, z_4^n \} \). Then, we have

\[
\begin{align*}
  h(y^n_2|\tilde{w}_1) - h(y^n_1|\tilde{w}_1) &\leq \frac{n}{2} \log \left( 1 + P^{\alpha_{22} - \alpha_{12}} \cdot \frac{|h_{22}|^2}{|h_{12}|^2} + P^{\alpha_{21} - (\alpha_{11} - \alpha_{12})} \cdot \frac{|h_{21}|^2}{|h_{11}|^2} \right) + \frac{n}{2} \log 10 \quad (33) \\
  h(y^n_1|\tilde{w}_2) - h(y^n_2|\tilde{w}_2) &\leq \frac{n}{2} \log \left( 1 + P^{\alpha_{11} - \alpha_{12}} \cdot \frac{|h_{11}|^2}{|h_{21}|^2} + P^{\alpha_{12} - (\alpha_{22} - \alpha_{21})} \cdot \frac{|h_{12}|^2}{|h_{22}|^2} \right) + \frac{n}{2} \log 10. \quad (34)
\end{align*}
\]

Note that the result in (34) holds true when \( \tilde{w}_2 \) is set as \( \tilde{w}_2 \triangleq \{ \sqrt{P^{(\alpha_{22} - \alpha_{12})}h_{22}x_2(t) + z'_2(t)} \}_{i=1}^n \). Let us define \( \alpha'_{21} \triangleq \phi_3, \alpha'_{22} \triangleq \alpha_{22} - (\alpha_{21} - \phi_3) \) and \( y_2(t)' \triangleq \sqrt{P^{\alpha_{21}}h_{21}x_1(t) + \sqrt{P^{\alpha_{22}}}h_{22}x_2(t) + z_2(t)} \). Then, by incorporating the result of (34) into (32), we have

\[
\begin{align*}
  h(y^n_1|s^n_{22}) - h(y^n_1|\tilde{w}_2) &\leq \frac{n}{2} \log \left( 1 + P^{\alpha_{11} - \alpha_{21}} \cdot \frac{|h_{11}|^2}{|h_{21}|^2} + P^{\alpha_{12} - (\alpha_{22} - \alpha_{12})} \cdot \frac{|h_{12}|^2}{|h_{22}|^2} \right) + \frac{n}{2} \log 10 \quad (35) \\
  h(y^n_2|s^n_{22}) - h(y^n_2|\tilde{w}_2) &\leq \frac{n}{2} \log \left( 1 + P^{\alpha_{11} - \alpha_{21}} \cdot \frac{|h_{11}|^2}{|h_{21}|^2} + P^{\alpha_{12} - (\alpha_{22} - \alpha_{12})} \cdot \frac{|h_{12}|^2}{|h_{22}|^2} \right) + \frac{n}{2} \log 10. \quad (36)
\end{align*}
\]

where (35) is from (32); and (36) follows from (34).

For the difference of the last two terms in (29), we have an upper bound that is stated in the following lemma.

**Lemma 3.** For \( y_2(t) \) defined in (1), and \( s_{22}(t) \) defined in (14), the following inequality holds true

\[
h(y^n_2, s^n_{22}|w) - h(y^n_1, s^n_{22}|w) \leq \frac{n}{2} \log \left( 1 + P^{\phi_3 - \phi_1} |h_{22}|^2 \right) + \frac{n}{2} \log 168 \quad (38)
\]

where \( \phi_3 \triangleq \min \{ \alpha_{21}, \alpha_{12}, \phi_2 \}, \phi_2 \triangleq (\alpha_{11} - \phi_1)^+, \phi_1 \triangleq (\alpha_{12} - (\alpha_{22} - \alpha_{21})^+) \).

**Proof.** The proof of this lemma is provided in Appendix A.

Finally, by incorporating (38) and (37) into (29), then the secure rate is bounded by

\[
R \leq \frac{1}{2} \log \left( 1 + P^{\alpha_{11} - \phi_3} \cdot \frac{|h_{11}|^2}{|h_{21}|^2} + P^{\alpha_{12} - (\alpha_{22} - \alpha_{21})^+} \cdot \frac{|h_{12}|^2}{|h_{22}|^2} \right) + \frac{1}{2} \log \left( 1 + P^{\phi_3 - \phi_1} |h_{22}|^2 \right) + 7.3 + \epsilon_{1,n} + \epsilon.
\]

Letting \( n \to \infty \), \( \epsilon_{1,n} \to 0 \), \( \epsilon_{2,n} \to 0 \) and \( \epsilon \to 0 \), we get the desired bound (6).

**B. Proof of bound (7)**

Let us now prove bound (7). The proof follows from the proof of the second bound in [35] Lemma 8, with some modifications. Let \( \tilde{x}_k(t) \triangleq \sqrt{P^{\max(\alpha_{kk}, \alpha_{kl})}}x_k(t) + \tilde{z}_k(t) \)

and \( \tilde{x}_{k}^n \triangleq \{ \tilde{x}_k(t) \}_{i=1}^n \) for \( k, \ell \in \{ 1, 2 \}, k \neq \ell \), where \( \tilde{z}_k(t) \sim \mathcal{N}(0, 1) \) is a virtual noise that is independent of the other noise and transmitted signals. Recall that

\[
s_{lk}(t) \triangleq \sqrt{P^{\alpha_{lk}}h_{lk}x_k(t) + z_\ell(t)}
\]
for \( k, \ell \in \{ 1, 2 \}, k \neq \ell \) (cf. (15)). Beginning with Fano’s inequality, the secure rate is bounded as:

\[
nR - n\epsilon_{1,n} \leq I(w; y^n_t) \leq I(w; y^n_t) - I(w; y^n) + n\epsilon \tag{39}
\]

\[
\leq I(w; y^n_t, \tilde{x}^n_1, \tilde{x}^n_2) - I(w; y^n) + n\epsilon \tag{40}
\]

\[
= h(\tilde{x}^n_1, \tilde{x}^n_2) - h(y^n) + h(y^n_t, y^n | \tilde{x}^n_1, \tilde{x}^n_2) - h(y^n_t, \tilde{x}^n_1, \tilde{x}^n_2 | y^n, w) + n\epsilon \tag{41}
\]

where (39) results from a secrecy constraint (cf. (3)); (40) stems from the fact that adding information does not decrease the mutual information; (41) follows from the derivation that \( h(y^n_t) \geq h(y^n_t | x^n_1) = h(s^n_{21}) \).

Note that \( y_2(t) = \sqrt{P_{\alpha_22}}h_{22}x_2(t) + s_{21}(t) \). On the other hand, we have

\[
nR \leq I(x^n_1; y^n_1) + n\epsilon_{1,n} \tag{42}
\]

\[
= h(y^n_1) - h(s^n_{12} | x^n_1) + n\epsilon_{1,n} \tag{43}
\]

\[
= h(y^n_1) - h(s^n_{12}) + n\epsilon_{1,n} \tag{44}
\]

where (42) follows from the Markov chain of \( w \to x^n_1 \to y^n_1 \); (43) results from the fact that \( y_1(t) = \sqrt{P_{\alpha_{11}}}h_{11}x_1(t) + s_{12}(t) \); (44) follows from the independence between \( x^n_1 \) and \( s^n_{12} \). Finally, by combining (41) and (44), it gives

\[
2nR - 2n\epsilon_{1,n} - n\epsilon \leq h(\tilde{x}^n_1) - h(s^n_{21}) + h(\tilde{x}^n_2) - h(s^n_{12}) + h(y^n) + h(y^n_t, y^n | \tilde{x}^n_1, \tilde{x}^n_2) - h(y^n_t, \tilde{x}^n_1, \tilde{x}^n_2 | y^n, w). \tag{45}
\]

At this point, by following the steps from (171)-(176) in [35], we then have

\[
2R + 2\epsilon_{1,n} - \epsilon \leq \frac{1}{2} \log(1 + \frac{P^{(\alpha_{11} - \alpha_{21})^+}}{|h_{21}|^2}) + \frac{1}{2} \log(1 + \frac{P^{(\alpha_{22} - \alpha_{12})^+}}{|h_{12}|^2}) + \frac{1}{2} \log(1 + P^{\alpha_{11}|h_{11}|^2} + P^{\alpha_{12}|h_{12}|^2}) + \log 9.
\]

By setting \( n \to \infty \), \( \epsilon_{1,n} \to 0 \) and \( \epsilon \to 0 \), it gives bound (7).

C. Proof of bound (8)

Bound (8) is directly from [35, Lemma 8].

V. ACHIEVABILITY

This section focuses on the symmetric Gaussian wiretap channel with a helper defined in Section II. For this channel, we will provide a cooperative jamming scheme to achieve the optimal secure GDoF expressed in Theorem 1. The proposed scheme will use the pulse amplitude modulation (PAM) and signal alignment. The details of the scheme are described as follows.

1) Codebook: At transmitter 1, a codebook is generated as

\[
\mathcal{B} \triangleq \left\{ v^n(w, w_0) : w \in \{ 1, 2, \cdots , 2^nR \}, w_0 \in \{ 1, 2, \cdots , 2^nR_0 \} \right\} \tag{46}
\]

with \( v^n \) being the codewords. All the codewords’ elements are independent and identically generated according to a specific distribution. \( R \) and \( R_0 \) are the rates of the confidential message \( w \) and the confusion message \( w_0 \), respectively. The purpose of using the confusion message is to guarantee the security of the confidential message. The message will be mapped to a codeword under the following two steps. First, given the message \( w \), a sub-codebook \( \mathcal{B}(w) \) is selected, where \( \mathcal{B}(w) \) is defined as

\[
\mathcal{B}(w) \triangleq \left\{ v^n(w, w_0) : w_0 \in \{ 1, 2, \cdots , 2^nR_0 \} \right\}.
\]

Second, transmitter 1 randomly selects a codeword from the selected sub-codebook based on a uniform distribution. Then, the channel input is mapped from selected codeword \( v^n \) such that

\[
x_t(t) = h_{22}v(t) \tag{47}
\]

for \( t = 1, 2, \cdots , n \), where \( v(t) \) denotes the \( t \)th element of \( v^n \).
2) Constellation and alignment: In the proposed scheme, each codeword $v^n$ is generated such that each element takes the following form

$$v(t) = \sqrt{P^{-\beta_c}} \cdot v_c(t) + \sqrt{P^{-\beta_m}} \cdot v_m(t) + \sqrt{P^{-\beta_p}} \cdot v_p(t)$$

(48)

which suggests that the input $x_1$ in (47) can be described as

$$x_1 = \sqrt{P^{-\beta_c}} h_{22} v_c + \sqrt{P^{-\beta_m}} h_{22} v_m + \sqrt{P^{-\beta_p}} h_{22} v_p$$

(49)

without the time index for simplicity (same for the next signal descriptions). For transmitter 2 (the helper), the transmitted signal is a cooperative jamming signal designed as

$$x_2 = \sqrt{P^{\alpha-1-\beta_c}} h_{21} u_c + \sqrt{P^{\alpha-1-\beta_m}} h_{21} u_p.$$  

(50)

For the above transmitted signals, the random variables $v_c, v_m, v_p, u_c$ and $u_p$ are independently (cross symbols and times) and uniformly drawn from the corresponding PAM constellation sets

$$v_c, u_c \in \Omega(\xi = \frac{6\gamma}{Q}, \text{ } Q = P^{\frac{\lambda_c}{2}})$$

(51)

$$v_m, u_p \in \Omega(\xi = \frac{2\gamma}{Q}, \text{ } Q = P^{\frac{\lambda_m}{2}})$$

(52)

$$v_p \in \Omega(\xi = \frac{\gamma}{Q}, \text{ } Q = P^{\frac{\lambda_p}{2}})$$

(53)

where $\Omega(\xi, Q) \triangleq \{\xi \cdot a: a \in \mathbb{Z} \cap [-Q, Q]\}$ denotes the PAM constellation set, and $\gamma$ is a finite constant such that

$$\gamma \in (0, 1/20].$$

(54)

In Table I we provide the parameters $\{\beta_c, \beta_m, \beta_p, \lambda_c, \lambda_m, \lambda_p\}$ under different cases of $\alpha$. If the parameters are set as $\beta_p = \infty$ and $\lambda_p = 0$, we will treat $v_p$ as an empty term in the transmitted signal. Similar implication is applied to $\{v_c, u_c, v_m, u_p\}$. Given our signal design, the power constraints $\mathbb{E}|x_1|^2 \leq 1$ and $\mathbb{E}|x_2|^2 \leq 1$ are satisfied. Focusing on the first transmitter, we have

$$\mathbb{E}|v_c|^2 \leq \frac{72\gamma^2}{3}, \quad \mathbb{E}|v_m|^2 \leq \frac{8\gamma^2}{3}, \quad \mathbb{E}|v_p|^2 \leq \frac{2\gamma^2}{3}$$

(55)

which suggests that

$$\mathbb{E}|x_1|^2 \leq 3 \times 4 \times \left(\frac{72\gamma^2}{3} + \frac{8\gamma^2}{3} + \frac{2\gamma^2}{3}\right) = 328\gamma^2 \leq 328 \times \frac{1}{400} < 1.$$  

(56)

Similarly, we have $\mathbb{E}|x_2|^2 \leq 1$. Note that, with our parameter design it holds true that $\beta_c \geq \alpha - 1$ and $\beta_m \geq 2\alpha - 1$, which controls the average power of the transmitted signal $x_2$ to satisfy $\mathbb{E}|x_2|^2 \leq 1$.

The above signal design then implies the following forms of the received signals

$$y_1 = \sqrt{P_1^{-\beta_c}} h_{12} h_{22} v_c + \sqrt{P_1^{-\beta_m}} h_{12} h_{22} v_m + \sqrt{P_1^{-\beta_p}} h_{12} h_{22} v_p$$

$$+ \sqrt{P_2^{-\beta_c}} h_{21} u_c + \sqrt{P_2^{-\beta_m}} h_{21} u_p + z_1$$

$$y_2 = h_{21} h_{22} (\sqrt{P^{-\beta_m}} (v_c + u_c) + \sqrt{P^{-\beta_m}} (v_m + u_p)) + \sqrt{P^{-\beta_p}} h_{21} h_{22} v_p + z_2.$$  

(57)

(58)

As we can see, at the eavesdropper, the jamming signal $u_c$ (resp. $u_p$) is aligned at a specific power level and direction with the signal $v_c$ (resp. $v_m$). In this way, it will minimize the penalty in GDoF incurred by the secrecy constraint, which can be seen later. Note that, with the above parameter design, the power of signal term with $v_p$ is under the noise level at receiver 2, while the power of signal term with $u_p$ is under the noise level at receiver 1.
TABLE I
DESIGNED PARAMETERS FOR DIFFERENT CASES, FOR SOME $\epsilon > 0$.

| $0 \leq \alpha \leq \frac{1}{2}$ | $\frac{1}{2} \leq \alpha \leq \frac{3}{4}$ | $\frac{3}{4} \leq \alpha \leq 1$ | $1 \leq \alpha \leq \frac{4}{3}$ | $\frac{4}{3} \leq \alpha \leq 2$ |
|-------------------------------|---------------------------------|---------------------------------|---------------------------------|---------------------------------|
| $\beta_c$                    | 0                               | $\infty$                        | 0                               | $\alpha - 1$                     |
| $\beta_m$                    | $\infty$                        | $2\alpha - 1$                   | $2\alpha - 1$                   | $\infty$                        |
| $\beta_p$                    | $\alpha$                        | $\alpha$                        | $\alpha$                        | $\infty$                        |
| $\lambda_c$                  | $\alpha - \epsilon$             | 0                               | $4\alpha - 3 - \epsilon$        | $\alpha - 1/2 - \epsilon$       |
| $\lambda_m$                  | 0                               | $1 - \alpha - \epsilon$         | $1 - \alpha - \epsilon$         | 0                               |
| $\lambda_p$                  | $1 - \alpha - \epsilon$         | $1 - \alpha - \epsilon$         | $1 - \alpha - \epsilon$         | 0                               |

3) Secure rate analysis: For $\epsilon > 0$, let us define the two rates as

$$R \triangleq \mathbb{I}(v; y_1) - \mathbb{I}(v; y_2) - \epsilon$$

(59)

$$R' \triangleq \mathbb{I}(v; y_2) - \epsilon.$$  (60)

By using the above codebook and signal design, the result of [3] reveals that the rate $R$ defined in (59) is achievable and message $w$ is secure, i.e., $\mathbb{I}(w; y_2) \leq n\epsilon$. Note that the wiretap channel with a helper can be considered as a specific case of the two-user interference channel with confidential messages, by removing the message of the second transmitter. Therefore, the result of [26, Theorem 2] (or [12, Theorem 2]) also reveals that the rate $R$ defined in (59) is achievable and the massage $w$ is secure. In the following, we will analyze the secure rate for different cases of $\alpha$.

A. Rate analysis when $0 \leq \alpha \leq 1/2$

For the first case with $0 \leq \alpha \leq 1/2$, the parameter design in Table I gives the following forms of the transmitted signals

$$x_1 = h_{22}v_c + \sqrt{P^{-\alpha}}h_{22}v_p$$

(61)

$$x_2 = \sqrt{P^{\alpha-1}}h_{21}u_c.$$  (62)

Then, the received signals become

$$y_1 = \sqrt{P}h_{11}h_{22}v_c + \sqrt{P^{1-\alpha}}h_{11}h_{22}v_p + \sqrt{P^{2\alpha-1}}h_{12}h_{21}u_c + z_1$$

(63)

$$y_2 = \sqrt{P^\alpha}h_{21}h_{22}(v_c + u_c) + h_{21}h_{22}v_p + z_2.$$  (64)

Let us now analyze the achievable secure rate expressed in (59), i.e.,

$$R = \mathbb{I}(v; y_1) - \mathbb{I}(v; y_2)$$

(65)

by setting the $\epsilon \to 0$. In what follows we will bound the secure rate $R$. To do so, we will begin with the first term in the right-hand side of (65). With our signal design, $v$ is now expressed as $v = v_c + \sqrt{P^{-\alpha}}v_p$. In this case, the two random variables $v_c$ and $v_p$ can be estimated from $y_1$, with error probability denoted by $\Pr\{\{v_c \neq \hat{v}_c\} \cup \{v_p \neq \hat{v}_p\}]$. For the first term in the right-hand side of (65), we have the following bound

$$\mathbb{I}(v; y_1) \geq \mathbb{I}(v; \hat{v}_c, \hat{v}_p)$$

(66)

$$= \mathbb{H}(v) - \mathbb{H}(v|\hat{v}_c, \hat{v}_p)$$

$$\geq \mathbb{H}(v) - (1 + \Pr\{\{v_c \neq \hat{v}_c\} \cup \{v_p \neq \hat{v}_p\}] \cdot \mathbb{H}(v))$$

(67)

$$= (1 - \Pr\{\{v_c \neq \hat{v}_c\} \cup \{v_p \neq \hat{v}_p\}] \cdot \mathbb{H}(v) - 1$$

(68)
where the step in (66) uses the Markov property of \( v \to y_1 \to \{v_c, \hat{v}_p\} \); and the step in (67) follows from Fano’s inequality. The entropy \( \mathbb{H}(v) \) in (68) can be computed as

\[
\mathbb{H}(v) = \mathbb{H}(v_c) + \mathbb{H}(v_p)
\]

\[
= \log(2 \cdot P^\frac{\alpha}{2} + 1) + \log(2 \cdot P^\frac{1-\alpha}{2} + 1)
\]

\[
= \frac{1 - 2\epsilon}{2} \log P + o(\log P)
\]

(69)

using the facts that \( v_c \in \Omega(\xi = 6\gamma \cdot \frac{1}{Q}, \ Q = P^\frac{\alpha}{2}) \) and \( v_p \in \Omega(\xi = \gamma \cdot \frac{1}{Q}, \ Q = P^\frac{1-\alpha}{2}) \), and that \( \{v_p, v_c\} \) can be reconstructed from \( v \), and vice versa. For the error probability appeared in (68), we have the following result.

**Lemma 4.** Consider the case with \( 0 \leq \alpha \leq 1/2 \), and consider the signal design in (49)-(54) and Table 7. Then, the error probability of the estimation of \( \{v_c, v_p\} \) from \( y_1 \) is

\[
Pr[\{v_c \neq \hat{v}_c\} \cup \{v_p \neq \hat{v}_p\}] \to 0 \quad \text{as} \quad P \to \infty.
\]

(70)

**Proof.** The proof is described in Appendix B. In the proof, a successive decoding method is used in the estimation of \( \{v_c, v_p\} \) from \( y_1 \).

By combining the results of (68), (69) and (70), it produces the following bound

\[
\mathbb{I}(v; y_1) \geq \frac{1 - 2\epsilon}{2} \log P + o(\log P).
\]

(71)

Note that the term \( \mathbb{I}(v; y_2) \) in the right-hand side of (65) can be considered as a penalty term in the secure rate, incurred by the secrecy constraint. We will show that, with our scheme design using signal alignment, this penalty will be minimized to a small value that can be ignored in terms of GDoF. It can be seen from the received signal of the eavesdropper that, the jamming signal is aligned at a specific power level and direction with the signal sent from transmitter 1 (see (58)). Let us now bound the penalty term \( \mathbb{I}(v; y_2) \) as follows:

\[
\mathbb{I}(v; y_2) \leq \mathbb{I}(v; y_2, v_c + u_c) = \mathbb{I}(v; v_c + u_c) + \mathbb{I}(v; h_2^1h_2^2y_2 + z_2|v_c + u_c) = \mathbb{H}(v_c + u_c) - \mathbb{H}(u_c) + h(h_2^1h_2^2y_2 + z_2) - h(z_2) \leq \log(4 \cdot P^\frac{\alpha}{2} + 1) - \log(2 \cdot P^\frac{1-\alpha}{2} + 1) + \frac{1}{2} \log(2\pi e([h_2^1]^2[h_2^2]^2 + 1)) - \frac{1}{2} \log(2\pi e) \leq \log(2\sqrt{17})
\]

(72)

(73)

where (72) results from the identity that Gaussian input maximizes the differential entropy and the fact that \( v_c + u_c \in \Omega(\xi = 6\gamma \cdot P^\frac{\alpha}{2}, \ Q = 2P^\frac{\alpha}{2}) \). At the final step, we incorporate the results of (71) and (73) into (65) and then get the following bound on the secure rate

\[
R \geq \frac{1 - 2\epsilon}{2} \log P + o(\log P).
\]

(74)

It implies that the secure GDoF \( d = 1 \) is achievable for this case with \( 0 \leq \alpha \leq 1/2 \).
B. Rate analysis when $1/2 \leq \alpha \leq 3/4$

Given the parameter design in Table I in this case the transmitted signals are simplified as
\[
\begin{align*}
x_1 &= \sqrt{P^{-(2\alpha - 1)}} h_{22} v_m + \sqrt{P^{-\alpha}} h_{22} v_p \\
x_2 &= \sqrt{P^{-\alpha}} h_{21} u_p
\end{align*}
\]
which gives the following forms of the received signals
\[
\begin{align*}
y_1 &= \sqrt{P^{2-2\alpha}} h_{11} h_{22} v_m + \sqrt{P^{1-\alpha}} h_{11} h_{22} v_p + h_{12} h_{21} u_p + z_1 \\
y_2 &= \sqrt{P^{1-\alpha}} h_{21} h_{22} (v_m + u_p) + h_{21} h_{22} v_p + z_2.
\end{align*}
\]

In this case, we can prove that the secure rate $R \geq \frac{2-2\alpha-2\epsilon}{2} \log P + o(\log P)$ is achievable. The rate analysis for this case follows from the steps in the previous case (cf. (65)-(74)). To avoid the repetition, we will just provide the outline of the proof for this case. In the first step, it can be proved that
\[
\mathbb{I}(v; y_1) \geq \frac{2 - 2\alpha - 2\epsilon}{2} \log P + o(\log P)
\]
by following the derivations in (65)-(71). In this case $v = \sqrt{P^{-(2\alpha - 1)}} v_m + \sqrt{P^{-\alpha}} v_p$ and $\mathbb{H}(v) = \mathbb{H}(v_m) + \mathbb{H}(v_p) = \frac{2-2\alpha-2\epsilon}{2} \log P + o(\log P)$. Similarly to the conclusion in Lemma 4 for the previous case, in this case it is also true that the error probability of the estimation of $\{v_m, v_p\}$ from $y_1$ vanishes as $P \to \infty$. A successive decoding method is also used in this estimation. In the second step, by following the derivations related to (72) and (73), it can be proved that
\[
\mathbb{I}(v; y_2) \leq o(\log P)
\]
which, together with (79), gives the lower bound on the secure rate $R = \mathbb{I}(v; y_1) - \mathbb{I}(v; y_2) \geq \frac{2-2\alpha-2\epsilon}{2} \log P + o(\log P)$. It implies that the secure GDoF $d = 2 - \alpha$ is achievable for this case.

C. Rate analysis when $3/4 \leq \alpha \leq 5/6$

Given the parameter design in Table I in this case the transmitted signals are simplified as
\[
\begin{align*}
x_1 &= h_{22} v_c + \sqrt{P^{-(2\alpha - 1)}} h_{22} v_m + \sqrt{P^{-\alpha}} h_{22} v_p \\
x_2 &= \sqrt{P^{\alpha - 1}} h_{21} u_c + \sqrt{P^{-\alpha}} h_{21} u_p
\end{align*}
\]
In this case we have the received signals given as
\[
\begin{align*}
y_1 &= \sqrt{P} h_{11} h_{22} v_c + \sqrt{P^{2\alpha - 1}} h_{12} h_{21} u_c + \sqrt{P^{2-2\alpha}} h_{11} h_{22} v_m + \sqrt{P^{1-\alpha}} h_{11} h_{22} v_p + h_{12} h_{21} u_p + z_1 \\
y_2 &= h_{21} h_{22}(\sqrt{P^\alpha} (v_c + u_c) + \sqrt{P^{1-\alpha}} (v_m + u_p)) + h_{21} h_{22} v_p + z_2.
\end{align*}
\]
The rate analysis also follows from the steps in the first case (cf. (65)-(74)). In this case, we can prove that the secure rate $R \geq \frac{2\alpha - 1 - 3\epsilon}{2} \log P + o(\log P)$ is achievable. Again, to avoid the repetition we will just provide the outline of the proof for this case. In the first step, it can be proved that
\[
\mathbb{I}(v; y_1) \geq \frac{2\alpha - 1 - 3\epsilon}{2} \log P + o(\log P)
\]
by following the derivations in (65)-(71). In this case $v = \sqrt{P^{-(2\alpha - 1)}} v_m + \sqrt{P^{-\alpha}} v_p$ and $\mathbb{H}(v) = \mathbb{H}(v_c) + \mathbb{H}(v_m) + \mathbb{H}(v_p) = \frac{2\alpha - 1 - 3\epsilon}{2} \log P + o(\log P)$. It is true that the error probability of the estimation of $\{v_c, v_m, v_p\}$ from $y_1$ vanishes as $P \to \infty$. A successive decoding method is also used in this estimation. In the second step, by following the derivations related to (72) and (73), it can be proved that
\[
\mathbb{I}(v; y_2) \leq o(\log P).
\]
Therefore, it gives the lower bound on the secure rate $R = \mathbb{I}(v; y_1) - \mathbb{I}(v; y_2) \geq \frac{2\alpha - 1 - 3\epsilon}{2} \log P + o(\log P)$. The secure GDoF $d = 2\alpha - 1$ is achievable for this case.
D. Rate analysis when $5/6 \leq \alpha \leq 1$

In this case, the transmitted signals take the same forms as in (81) and (82), and the received signals are expressed as in (83) and (84). However, in the rate analysis, the estimation approaches of noise removal and signal separation will be used in this case. By following the previous derivations in (66)-(68), we have the following bound

$$ I(v;y_1) \geq (1 - \Pr[\{v_c \neq \hat{v}_c\} \cup \{v_m \neq \hat{v}_m\} \cup \{v_p \neq \hat{v}_p\}]) \cdot H(v) - 1 $$

(87)

where the entropy $H(v)$ in (87) can be computed as

$$ H(v) = H(v_c) + H(v_m) + H(v_p) = \frac{3/2 - \alpha - 3\epsilon}{2} \log P + o(\log P). $$

(88)

The probability $\Pr[\{v_c \neq \hat{v}_c\} \cup \{v_m \neq \hat{v}_m\} \cup \{v_p \neq \hat{v}_p\}]$ in (87) is the error probability of the estimation of $\{v_c, v_m, v_p\}$ from $y_1$, which vanishes as $P \to \infty$. The following lemma provides the result on this probability.

**Lemma 5.** Consider the case with $5/6 \leq \alpha \leq 1$, and consider the signal design in (49)-(54) and Table I. Then, for almost all the channel realizations $\{h_{kt}\} \in (1,2]^{2 \times 2}$, the error probability of the estimation of $\{v_c, v_m, v_p\}$ from $y_1$ is

$$ Pr[\{v_c \neq \hat{v}_c\} \cup \{v_m \neq \hat{v}_m\} \cup \{v_p \neq \hat{v}_p\}] \to 0 \quad \text{as} \quad P \to \infty. $$

(89)

**Proof.** The proof is described in Section VI. In the proof, noise removal and signal separation are used in the estimation of $\{v_c, v_m, v_p\}$ from $y_1$. \qed

The results of (87), (88) and (89) imply that the following bound

$$ I(v;y_1) \geq \frac{3/2 - \alpha - 3\epsilon}{2} \log P + o(\log P) $$

(90)

holds true for almost all the channel realizations $\{h_{kt}\} \in (1,2]^{2 \times 2}$. On the other hand, by following the derivations related to (72) and (73), it can be proved that

$$ I(v;y_2) \leq o(\log P). $$

(91)

Finally, the results of (90) and (91) reveal that $R = I(v;y_1) - I(v;y_2) \geq \frac{3/2 - \alpha - 3\epsilon}{2} \log P + o(\log P)$ and that the secure GDoF $d = 3/2 - \alpha$ is achievable in this case, for almost all the channel realizations.

E. Rate analysis when $1 \leq \alpha \leq 4/3$

In this case, the transmitted signals are simplified as

$$ x_1 = \sqrt{P-(\alpha-1)} h_{22} v_c $$

(92)

$$ x_2 = h_{21} u_c $$

(93)

and the received signals are expressed as

$$ y_1 = \sqrt{P^2-\alpha} h_{11} h_{22} v_c + \sqrt{P^2} h_{12} h_{21} u_c + z_1 $$

(94)

$$ y_2 = \sqrt{P} h_{21} h_{22} (v_c + u_c) + z_2. $$

(95)

As in the previous case, the estimation approaches of noise removal and signal separation are also used in the rate analysis in this case. In this case, the entropy $H(v)$ is computed as $H(v) = H(v_c) = \frac{\alpha/2 - \epsilon}{2} \log P + o(\log P)$. By following the previous derivations in (66)-(68), we have the following bound

$$ I(v;y_1) \geq (1 - \Pr[\{v_c \neq \hat{v}_c\}]) \cdot H(v) - 1 $$

$$ = (1 - \Pr[\{v_c \neq \hat{v}_c\}]) \cdot \frac{\alpha/2 - \epsilon}{2} \log P + o(\log P) $$

(96)
The following lemma provides the result on the error probability $\Pr[c \neq \hat{c}]$.

**Lemma 6.** Consider the case with $1 \leq \alpha \leq 4/3$, and consider the signal design in (49)-(54) and Table I. Then, for almost all the channel realizations \{\(h_{kt}\)\} \(\in (1, 2)^{2 \times 2}\), the error probability of the estimation of \(c\) from \(y_1\) is

$$\Pr[\hat{c} \neq c] \to 0 \quad \text{as} \quad P \to \infty.$$  \hspace{0.8cm} (97)

**Proof.** The proof is described in Appendix C. In the proof, noise removal and signal separation are used in the estimation of \(c\) from \(y_1\). □

The results of (96) and (97) implies that the following bound

$$I(v; y_1) \geq \alpha/2 - \epsilon \log P + o(\log P)$$  \hspace{0.8cm} (98)

holds true for almost all the channel realizations \{\(h_{kt}\)\} \(\in (1, 2)^{2 \times 2}\). One the other hand, it can be proved that

$$I(v; y_2) \leq o(\log P).$$  \hspace{0.8cm} (99)

The results of (99) and (98) reveal that $R = I(v; y_1) - I(v; y_2) \geq \alpha/2 - \epsilon \log P + o(\log P)$ and that the secure GDoF $d = \alpha/2$ is achievable in this case, for almost all the channel realizations.

**F. Rate analysis when $4/3 \leq \alpha \leq 2$**

In this case, the transmitted signals take the same forms as in (92) and (93), and the received signals are expressed as in (94) and (95). In this case, the entropy $H(v)$ is computed as $H(v) = H(c) = 2 - \frac{\alpha - \epsilon}{2} \log P + o(\log P)$. As in the previous case, the following bound holds true

$$I(v; y_1) \geq (1 - \Pr[c \neq \hat{c}]) \cdot \frac{2 - \alpha - \epsilon}{2} \log P + o(\log P)$$  \hspace{0.8cm} (100)

(cf. (96)). The probability $\Pr[c \neq \hat{c}]$ in (100) is the error probability of the estimation of \(c\) from \(y_1\). In this case, it can be proved that \(u_c\) and \(v_c\) can be estimated from \(y_1\) in a successive way and the error probability of this estimation vanishes as \(P \to \infty\). The proof of this step is similar to that of Lemma 4, and hence it is omitted here to avoid the repetition. Then, we have

$$I(v; y_1) \geq \frac{2 - \alpha - \epsilon}{2} \log P + o(\log P).$$  \hspace{0.8cm} (101)

As in the previous cases, it can be proved that $I(v; y_2) \leq o(\log P)$ in this case. Finally we have a lower bound on the secure rate $R \geq \frac{2 - \alpha - \epsilon}{2} \log P + o(\log P)$, which implies that the secure GDoF $d = 2 - \alpha$ is achievable in this case.

**VI. PROOF OF LEMMA 5**

Given the observation \(y_1\) in (83), and with $5/6 \leq \alpha \leq 1$, we will show that \(v_c, u_c, v_m\) and \(v_p\) can be estimated with vanishing error probability, for almost all the channel realizations. Our focus is to prove that \(v_c, u_c\) and \(v_m\) can be estimated from \(y_1\) simultaneously with vanishing error probability, for almost all the channel realizations. This proof is motivated by the proof of [35, Lemma 4], in which the noise removal and signal separation techniques will be used. Once \(v_c, u_c\) and \(v_m\) are estimated correctly from \(y_1\), we can remove \(v_c, u_c\) and \(v_m\) from \(y_1\) and then estimate \(v_p\) with vanishing error probability.
Recall that \( v_c, u_c \in \Omega (\xi = \frac{6\gamma}{Q^2}, Q = P^{\frac{1}{2} - \gamma}) \), \( v_m, u_p \in \Omega (\xi = \frac{2\gamma}{Q^2}, Q = P^{\frac{1}{2} - \gamma}) \), \( v_p \in \Omega (\xi = \frac{\gamma}{Q^2}, Q = P^{1 - \frac{1}{2} - \gamma}) \), for some parameters \( \gamma \in (0, 1/20] \) and \( \epsilon \to 0 \). Let us describe \( y_1 \) in the following form

\[
y_1 = \sqrt{P} h_{11} h_{22} v_c + \sqrt{P} h_1 h_{22} u_c + \sqrt{P} h_{11} h_{22} v_m + \sqrt{P} h_{11} h_{22} u_p + z_1
\]

\[
= \sqrt{P^{1-\alpha-\epsilon}} \cdot 2 \gamma (3 \sqrt{P^{1/2}} g_2 q_2 + 3 \sqrt{P^{2\alpha-3/2}} g_1 q_1 + g_0 q_0) + \sqrt{P^{1-\alpha}} (h_{11} h_{22} v_p + P h_{11} h_{21} u_p) + z_1
\]

\[
= \sqrt{P^{1-\alpha-\epsilon}} \cdot 2 \gamma s + \sqrt{P^{1-\alpha}} e + z_1
\]

(102)

where \( g_2 \triangleq g_0 \triangleq h_{11} h_{22}, \ g_1 \triangleq h_{11} h_{21}, \ \bar{e} \triangleq h_{11} h_{22} u_p, \ \gamma \triangleq h_{11} h_{22} v_p + \frac{1}{\sqrt{P^{1-\alpha}}} h_{11} h_{21} u_p, \ \bar{s} \triangleq g_0 q_0 + 3 \sqrt{P^{2\alpha-3/2}} g_1 q_1 + 3 \sqrt{P^{1/2}} g_2 q_2 \) and

\[
q_2 \triangleq \frac{Q_2}{6\gamma}, \ q_1 \triangleq \frac{Q_1}{6\gamma}, \ v_c, \ q_0 \triangleq \frac{Q_0}{2\gamma}, \ v_m, \ Q_2 \triangleq Q_1 \triangleq P^{\frac{1}{2} - \gamma}, \ Q_0 \triangleq P^{1-\alpha-\epsilon}.
\]

In this scenario, the following conditions are always satisfied: \( q_k \in Z \) and \( |q_k| \leq Q_k \) for \( k = 0, 1, 2 \). Let

\[
A_2 \triangleq 3 \sqrt{P^{1/2}}, \ A_1 \triangleq 3 \sqrt{P^{2\alpha-3/2}}, \ A_0 \triangleq 1.
\]

In this scenario with \( 5/6 \leq \alpha \leq 1 \), without loss of generality we will consider the case that \( Q_0, Q_1, Q_2, A_1, A_2 \in Z^+ \).

For the observation \( y_1 \) in (102), the goal is to estimate the sum \( \bar{s} = g_0 q_0 + 3 \sqrt{P^{1/2}} q_2 + 3 \sqrt{P^{2\alpha-3/2}} g_1 q_1 \) by considering the other signals as noise (noise removal). After decoding \( \bar{s} \) correctly, the three symbols \( q_0, q_1, q_2 \) can be estimated, based on the fact that \( \{g_0, q_1\} \) are rationally independent (signal separation, cf. [42]), as well as the fact that \( g_0 \) and \( q_2 \) can be reconstructed from \( q_0 + 3 \sqrt{P^{1/2}} q_2 \). Note that the minimum of \( 3 \sqrt{P^{1/2}} q_2 \) is no less than the maximum of \( 2q_0 \). To estimate \( \bar{s} \) from \( y_1 \), we will show that the minimum distance of \( \bar{s} \) is sufficiently large, in order to make the error probability vanishing. Let us define the minimum distance of \( \bar{s} \) as

\[
d_{\min}(g_0, q_1, g_2) \triangleq \min_{q_0, q_0, q_0 \in Z, q_1-q_0, q_2} |g_0(q_0 - \bar{q}_0) + 3 \sqrt{P^{2\alpha-3/2}} g_1(q_1 - \bar{q}_1) + 3 \sqrt{P^{1/2}} g_2(q_2 - \bar{q}_2)|.
\]

(103)

The following lemma provides a result on the minimum distance.

**Lemma 7.** For the case with \( 5/6 \leq \alpha \leq 1 \), and for some constants \( \delta \in (0, 1] \) and \( \epsilon > 0 \), the following bound on the minimum distance \( d_{\min} \) holds true

\[
d_{\min} \geq \delta
\]

(104)

for all the channel realizations \( \{h_{11}, h_{12}, h_{22}, h_2\} \in (1, 2)^{2 \times 2} \setminus \mathcal{H}_{\text{out}} \) where \( \mathcal{H}_{\text{out}} \subseteq (1, 2)^{2 \times 2} \) is an outage set whose Lebesgue measure, denoted by \( \mathcal{L}(\mathcal{H}_{\text{out}}) \), has the following bound

\[
\mathcal{L}(\mathcal{H}_{\text{out}}) \leq 12096 \delta \cdot P^{-\frac{1}{2}}
\]

(105)

**Proof.** For \( \beta \triangleq \delta \in (0, 1] \), we define an event as

\[
B(q_2, q_1, q_0) \triangleq \{(g_2, g_1, g_0) \in (1, 4)^3 : |A_2 g_2 q_2 + A_1 g_1 q_1 + g_0 q_0| < \beta\}
\]

(106)

The result of Lemma 5 still holds for the case when any of \{\( Q_0, Q_1, Q_2, A_1, A_2 \)\} is not integer. The proof just needs some minor modifications. For example, when \( A_2 \) is not an integer, we can modify \( v_c \) and \( u_c \) as \( v_c = \eta_v v_c' \) and \( u_c = \eta_u u_c' \), where \( v_c', u_c' \in \Omega (\xi = \frac{6\gamma}{Q^2}, Q = P^{\frac{1}{2} - \gamma}) \), and \( \eta_v \) is a selected parameter such that \( 0 < \eta_v < 1 \) and \( A_2 \eta_v \) is an integer. For another example, when \( Q_2 = \sqrt{P^{\frac{1}{2} - \gamma}} \) is not an integer, we can slightly modify \( \epsilon \) such that \( Q_2 \) is an integer and \( \epsilon \) is still very small, for the regime with large \( P \).
and define
\[ B \triangleq \bigcup_{q_0, q_1, q_2 \in \mathbb{Z}; \quad |q_k| \leq 2Q_k \quad \forall k} \{q_0, q_1, q_2\} \backslash \{q_0, q_1, q_2\} \neq \emptyset \] (107)

For \( 5/6 \leq \alpha \leq 1 \), by [43, Lemma 14] we have a bound on the Lebesgue measure of \( B \), given as
\[
\mathcal{L}(B) \leq 504\beta \cdot 4 \left( 2 \min \left\{ \frac{Q_0}{A_2}, Q_2 \right\} + \tilde{Q}_2 \cdot \min \{Q_1, \frac{Q_0}{A_1}, \frac{A_2 \tilde{Q}_2}{A_1} \} \right. \\
+ 2 \min \left\{ \frac{Q_0}{A_1}, Q_1 \right\} + \tilde{Q}_1 \cdot \min \left\{ Q_2, \frac{Q_0}{A_2}, \frac{A_1 \tilde{Q}_1}{A_2} \right\} \right) \\
\leq 504\beta \cdot 4 \left( \frac{2Q_0}{A_2} + \tilde{Q}_2 \cdot \frac{Q_0}{A_1} + \frac{2Q_0}{A_1} + \tilde{Q}_1 \cdot \frac{Q_0}{A_2} \right) \\
\leq 504\beta \cdot 4 \left( Q_1 \cdot \frac{9Q_0}{A_2} + \frac{4Q_0}{A_1} \right) \\
\leq 504\beta \cdot 8Q_0 \max \left\{ \frac{9Q_1}{A_2}, \frac{4}{A_1} \right\} \\
\leq 504\beta \cdot 8Q_0 \cdot 3P^{\frac{\alpha-1}{2}} \\
= 12096\delta \cdot P^{-\frac{\alpha}{2}} \tag{108}
\]

where \( \tilde{Q}_1 = \min \{Q_1, 8\max \{Q_0, A_2 Q_2\} \} = Q_1 \) and \( \tilde{Q}_2 = \min \{Q_2, 8\max \{Q_0, A_1 Q_1\} \} = Q_1 \cdot \min \left\{ 1, \frac{8A_1}{A_2} \right\} \). In this scenario, we can treat \( B \) as an outage set. When \( (g_0, g_1, g_2) \notin B \), by definition we have \( d_{\min}(g_0, g_1, g_2) \geq \delta \).

Recall that \( g_2 \triangleq g_0 \triangleq h_{11}h_{22} \) and \( g_1 \triangleq h_{12}h_{21} \). At this point, we define a new set \( \mathcal{H}_{\text{out}} \) as
\[
\mathcal{H}_{\text{out}} \triangleq \{(h_{11}, h_{22}, h_{12}, h_{21}) \in (1, 2]^2 : (g_2 = g_0, g_1, g_0) \in B \}. 
\]

We define \( \mathbb{1}_{\mathcal{H}_{\text{out}}}(h_{11}, h_{22}, h_{12}, h_{21}) = 1 \) if \( (h_{11}, h_{22}, h_{12}, h_{21}) \in \mathcal{H}_{\text{out}} \), else \( \mathbb{1}_{\mathcal{H}_{\text{out}}}(h_{11}, h_{22}, h_{12}, h_{21}) = 0 \). Similarly, we define \( \mathbb{1}_B(g_1, g_0) = 1 \) if \( (g_2 = g_0, g_1, g_0) \in B \), else \( \mathbb{1}_B(g_1, g_0) = 0 \). Then we can bound the Lebesgue measure of \( \mathcal{H}_{\text{out}} \) as
\[
\mathcal{L}(\mathcal{H}_{\text{out}}) = \int_{h_{11}=1}^{2} \int_{h_{12}=1}^{2} \int_{h_{21}=1}^{2} \int_{h_{11}=1}^{2} \mathbb{1}_{\mathcal{H}_{\text{out}}}(h_{11}, h_{22}, h_{12}, h_{21}) dh_{22} dh_{21} dh_{12} dh_{11} \\
= \int_{h_{11}=1}^{2} \int_{h_{12}=1}^{2} \int_{h_{21}=1}^{2} \int_{h_{11}=1}^{2} \mathbb{1}_B(h_{12}h_{21}, h_{11}h_{22}) dh_{22} dh_{21} dh_{12} dh_{11} \\
\leq \int_{h_{11}=1}^{2} \int_{h_{12}=1}^{2} \int_{g_1=1}^{4} \mathbb{1}_B(g_1, g_0) h_{11}^{-1} h_{12}^{-1} dg_1 dh_{12} dh_{11} \\
\leq \int_{h_{11}=1}^{2} \int_{h_{12}=1}^{2} \mathcal{L}(B) dh_{12} dh_{11} \\
\leq 12096\delta \cdot P^{-\frac{\alpha}{2}} \tag{109}
\]

where the last step uses the result in (108).

In the rest of this section, we will consider the channel realizations \( (h_{11}, h_{22}, h_{12}, h_{21}) \in (1, 2]^2 \) that are not in the outage set \( \mathcal{H}_{\text{out}} \). The result of Lemma 7 reveals that
\[
\mathcal{L}(\mathcal{H}_{\text{out}}) \rightarrow 0, \quad \text{for} \quad P \rightarrow \infty.
\]

When the channel realizations satisfy the condition \( (h_{11}, h_{22}, h_{12}, h_{21}) \notin \mathcal{H}_{\text{out}} \), we have the following property on the minimum distance defined in (103): \( d_{\min} \geq \delta \) for a given constant \( \delta \in (0, 1] \). With
this result, we can estimate \( \hat{s} \) from \( y_1 \) expressed in (102). For the random variable \( \hat{c} = h_{11} h_{22} v_p + \frac{1}{\sqrt{P^{1-\alpha}}} h_{12} h_{21} u_p \) appeared in (102), it is true that

\[
|\hat{c}| \leq \hat{c}_{\text{max}} \triangleq \frac{3}{5} \quad \forall \hat{c}.
\]

At this point, we have the following bound on the error probability of the estimation of \( \hat{s} \) from \( y_1 \)

\[
\Pr[\hat{s} \neq \hat{s}] \leq \Pr\left[ |z_1 + \sqrt{P^{1-\alpha} \hat{c}}| > \sqrt{P^{1-\alpha+\epsilon} \cdot 2\gamma \cdot d_{\text{min}}/2} \right] \\
\leq 2 \cdot Q\left( \frac{P^{1-\alpha+\epsilon} \cdot 2\gamma \cdot d_{\text{min}}/2 - P^{1-\alpha} \hat{c}_{\text{max}}}{\sqrt{2}} \right) \\
\leq 2 \cdot Q\left( \frac{P^{1-\alpha} (\gamma \delta P^{\frac{1}{2}} - 3/5)}{\sqrt{2}} \right)
\]

(110)

where \( \hat{s} \) denotes the estimate of \( s \); \( Q(\tau) \triangleq \frac{1}{\sqrt{2\pi}} \int_{\tau}^{\infty} \exp(-z^2/2)dz \); the last step stems from the result that \( d_{\text{min}} \geq \delta \). By following the fact that \( Q(\tau) \leq \frac{1}{2} \exp(-\tau^2/2) \), \( \forall \tau \geq 0 \), the result in (110) implies the following conclusion

\[
\Pr[\hat{s} \neq \hat{s}] \to 0 \quad \text{for} \quad P \to \infty.
\]

(111)

After decoding \( \hat{s} = g_0(q_0 + 3\sqrt{P^{1/2}q_2}) + 3\sqrt{P^{2\alpha-3/2}}g_1q_1 \) correctly, the three symbols \( q_0, q_1, q_2 \) can be recovered, based on the fact that \( \{g_0, g_1\} \) are rationally independent, and the fact that \( q_0 \) and \( q_2 \) can be reconstructed from \( q_0 + 3\sqrt{P^{1/2}q_2} \).

In the following step, by removing the decoded \( \hat{s} \) from \( y_1 \), the symbol \( v_p \) can be estimated from the following observation

\[
y_1 - \sqrt{P^{1-\alpha+\epsilon} \cdot 2\gamma \hat{s}} = \sqrt{P^{1-\alpha}} h_{11} h_{22} v_p + h_{12} h_{21} u_p + z_1.
\]

(112)

Since the interference term \( h_{12} h_{21} u_p \) in (112) is under the noise level, i.e., \( h_{12} h_{21} u_p \leq 8\gamma \leq 2/5 \), one can easily prove that the the error probability for decoding \( v_p \) from the observation in (112) is

\[
\Pr[v_p \neq \hat{v}_p] \to 0 \quad \text{for} \quad P \to \infty.
\]

(113)

Therefore, from the results in (111) and (113), it reveals that the error probability of the estimation of \( \{v_c, v_m, v_p\} \) from \( y_1 \) is

\[
\Pr[\{v_c \neq \hat{v}_c\} \cup \{v_m \neq \hat{v}_m\} \cup \{v_p \neq \hat{v}_p\}] \to 0 \quad \text{as} \quad P \to \infty
\]

for almost all the channel realizations \( (h_{11}, h_{22}, h_{12}, h_{21}) \in (1, 2)^{2 \times 2} \), in the regime of large \( P \).

VII. Conclusion

In this work, we characterized the optimal secure GDoF of a symmetric Gaussian wiretap channel with a helper. The result reveals that, adding a helper can significantly increase the secure GDoF of the wiretap channel. A new converse and a new scheme are provided in this work. The converse derived in this work holds for the symmetric and asymmetric channels. In the proposed scheme, the helper sends a cooperative jamming signal at a specific power level and direction, which allows to minimize the penalty in GDoF incurred by the secrecy constraint. In the secure rate analysis, the techniques of noise removal and signal separation are used. The optimal secure GDoF result is described in different expressions for different interference regimes. For the regimes of \( 0 \leq \alpha \leq 5/6 \) and \( 4/3 \leq \alpha \leq 2 \), the achievable secure GDoF result holds for all the channel realizations under our channel model. For the regime of \( 5/6 < \alpha < 4/3 \), the achievable secure GDoF result holds for almost all the channel realizations when \( P \) is large, under our channel model. In the future work, we will generalize our secure GDoF result to understand the constant-gap secure capacity.
In this section we provide the proof of Lemma 3. Recall that $s_2(t)$, $s_{22}(t)$, $x_1(t)$ and $x_2(t)$ are defined in (1), (14), (16), and (17), respectively. In this setting, we have

$$h(y^n_1, s^n_{22}, x^n_1, w) = h(y^n_1, s^n_{22}, x^n_1, w) + h(x^n_1, w) + h(y^n_1, s^n_{22}, x^n_1, w) - h(y^n_1, s^n_{22}, x^n_1, w) + J_{11}$$

$$= h(y^n_1, s^n_{22}, x^n_1, w) + h(y^n_1, s^n_{22}, x^n_1, w) + h(x^n_1, w) - h(y^n_1, s^n_{22}, x^n_1, w) + J_{11}$$

$$= h(y^n_1, s^n_{22}, x^n_1, w) - h(y^n_1, s^n_{22}, x^n_1, w) + h(x^n_1, w) + J_{11} - J_{22} + J_{33}$$

$$= h(y^n_1, s^n_{22}, x^n_1, w) - h(y^n_1, s^n_{22}, x^n_1, w) + h(x^n_1, w) + J_{11} - J_{22} + J_{33}$$

by using the independence between $s^n_{22}, s^n_{12}$ and $x^n_1, w, x^n_1$, as well as the identity that $y_1(t) = \sqrt{P_{\alpha_1} h_{11} x_1(t)} + s_1(t)$. To complete this proof, we will use the results in the following lemma.

**Lemma 8.** For $J_{11} \triangleq h(y^n_1, s^n_{22}, x^n_1, w)$, $J_{22} \triangleq h(s^n_{12}, x^n_1, w, y^n_2, s^n_{22})$, $J_{33} \triangleq h(y^n_2, s^n_{22}, s^n_{12}, x^n_2, x^n_1)$ and $J_{44} \triangleq h(x^n_2, s^n_{22}, s^n_{12}, x^n_1, w)$, we have

$$J_{11} \leq \frac{n}{2} \log(42\pi e)$$

$$J_{22} \geq \frac{3n}{2} \log(2\pi e)$$

$$J_{33} \leq \frac{n}{2} \log(16\pi e)$$

$$J_{44} \leq \frac{n}{2} \log(2\pi e (1 + P_{\phi_3 - \phi_1} |h_{22}|^2))$$

where $\phi_3 \triangleq \min\{\alpha_{21}, \alpha_{12}, (\alpha_{11} - \phi_1)^+\}$ and $\phi_1 \triangleq (\alpha_{12} - (\alpha_{22} - \alpha_{21})^+)^+$. 

**APPENDIX A**

**PROOF OF LEMMA 3**

Recall that $y_2(t), s_2(t), x_1(t)$ and $x_2(t)$ are defined in (1), (14), (16), and (17), respectively. In this setting, we have

$$J_{11} \triangleq h(y^n_2, s^n_{22}, x^n_1, w)$$

$$J_{12} \triangleq h(y^n_2, s^n_{22}, x^n_1, w) - h(y^n_1, s^n_{22}, x^n_1, w) + h(x^n_1, w)$$

$$J_{22} \triangleq h(y^n_2, s^n_{22}, x^n_1, w) - h(y^n_1, s^n_{22}, x^n_1, w) + J_{11}$$

by using the independence between $s^n_{22}, s^n_{12}$ and $x^n_1, w, x^n_1$, as well as the identity that $y_1(t) = \sqrt{P_{\alpha_1} h_{11} x_1(t)} + s_1(t)$. To complete this proof, we will use the results in the following lemma.
The proof of Lemma 8 is given in the following subsection. By incorporating the results of Lemma 8 into (115), we have

\[
\log(1 + P^{\phi_3 - \phi_1} |h_{22}|^2) + \frac{n}{2} \log 168.
\]

At this point, we complete the proof of Lemma 3.

A. Proof of Lemma 8

Recall that

\[
s_{11}(t) = \sqrt{P_{\alpha_{11} - \alpha_{12}}} h_{11} x_1(t) + \tilde{z}_1(t), \quad s_{22}(t) = \sqrt{P_{\alpha_{22} - \alpha_{21}}} h_{22} x_2(t) + \tilde{z}_2(t),
\]

\[
s_{12}(t) = \sqrt{P_{\alpha_{11} - \alpha_{12}}} h_{12} x_1(t) + z_1(t), \quad \bar{x}_1(t) \triangleq \sqrt{P_{\min(\alpha_{21}, \alpha_{12}, \alpha_{11} - \phi_1)}} h_{21} x_1(t) + z_3(t), \quad \bar{x}_2(t) \triangleq \sqrt{P_{\phi_3}} \tilde{z}_2(t) + \tilde{z}_4(t), \quad \bar{y}_2(t) \triangleq \sqrt{P_{-(\alpha_{21} - \phi_3)}} y_2(t) + \tilde{z}_2(t), \quad \phi_3 \triangleq \min(\alpha_{21}, \alpha_{12}, \phi_2), \quad \phi_2 \triangleq (\alpha_{11} - \phi_1)^+ \text{ and } \phi_1 \triangleq (\alpha_{12} - (\alpha_{22} - \alpha_{21})^+)\].

At first we focus on the bound of $J_{11}$:

\[
J_{11} = h(\bar{x}_1^n | w, y_1^n, s_{22}^n)
\]

\[
\leq \sum_{t=1}^n h(\bar{x}_1(t) | y_1(t), s_{22}(t))
\]

\[
= \sum_{t=1}^n h(\bar{x}_1(t) - \sqrt{P_{\min(\alpha_{21}, \alpha_{12}, \alpha_{11} - \phi_1) - \alpha_{11}}} h_{21} y_1(t) - \sqrt{P_{\alpha_{12} - (\alpha_{22} - \alpha_{21})}} \frac{h_{12}}{h_{22}} s_{22}(t) | y_1(t), s_{22}(t))
\]

\[
\leq \frac{n}{2} \log (2\pi e \left(1 + \sum_{\alpha_{11} \leq 1} \frac{|h_{21}|^2}{|h_{11}|^2} + \sum_{\alpha_{11} + \alpha_{12} - (\alpha_{22} - \alpha_{21}) \leq 1} \frac{|h_{21}|^2 |h_{12}|^2}{|h_{11}|^2 |h_{22}|^2} \right))
\]

\[
\leq \frac{n}{2} \log (42\pi e)
\]

where (122) follows from chain rule and the fact that conditioning reduces differential entropy; (123) uses the fact that $h(a|b) = h(a - \beta b|b)$ for a constant $\beta$ and two continuous random variables $a$ and $b$; (124) follows from the fact that Gaussian input maximizes the differential entropy and that conditioning reduces differential entropy; (125) uses the identities $\min(\alpha_{21}, \alpha_{12}, \alpha_{11} - \phi_1) - \alpha_{11} \leq 0$ and $\min(\alpha_{21}, \alpha_{12}, \alpha_{11} - \phi_1) - \alpha_{11} + \alpha_{12} - (\alpha_{22} - \alpha_{21})^+ \leq 0$, where $\phi_1 = (\alpha_{12} - (\alpha_{22} - \alpha_{21})^+)\].

For $J_{22}$, it can be bounded by

\[
J_{22} = h(s_{12}^n, \bar{x}_2^n, \bar{z}_1^n | w, \bar{y}_2^n, s_{22}^n)
\]

\[
\geq h(s_{12}^n, \bar{x}_2^n, \bar{z}_1^n | w, \bar{y}_2^n, s_{22}^n, x_2^n, \tilde{z}_1^n) = h(s_{12}^n, \bar{z}_1^n, \bar{z}_2^n)
\]

\[
= \frac{3n}{2} \log(2\pi e).
\]

where (126) follows from the fact that conditioning reduces differential entropy.
For \( J_{33} \), we have the following bound:

\[
J_{33} = h(y^n_2|w, s^n_{22}, s^n_{12}, \bar{x}_2^n, \bar{x}_1^n) \\
\leq \sum_{t=1}^{n} h(\bar{y}_2(t)|s_{22}(t), \bar{x}_2(t), \bar{x}_1(t)) \\
= \sum_{t=1}^{n} h(\bar{y}_2(t) - \bar{x}_1(t) - \sqrt{P^{-(\alpha_{22} - \alpha_{21})^+ + (\alpha_{22} - \alpha_{21})}}(\sqrt{P^{\phi_3}}s_{22}(t) - \bar{x}_2(t))|s_{22}(t), \bar{x}_2(t), \bar{x}_1(t)) \\
= \sum_{t=1}^{n} h((\sqrt{P^{\phi_3}} - \sqrt{P^{\min\{\alpha_{21},\alpha_{12},\alpha_{11} - \phi_1\}}})h_{21}x_1(t) + \bar{z}_2(t)) + \sqrt{P^{\phi_3 - \alpha_{21}}}z_2(t) - \bar{z}_3(t) \\
+ \sqrt{P^{-(\alpha_{22} - \alpha_{21})^+ + (\alpha_{22} - \alpha_{21})}}\bar{z}_4(t)|s_{22}(t), \bar{x}_2(t), \bar{x}_1(t)) \\
\leq \frac{n}{2} \log(2\pi e ((\sqrt{P^{\phi_3}} - \sqrt{P^{\min\{\alpha_{21},\alpha_{12},\alpha_{11} - \phi_1\}}})^2|h_{21}|^2 + 1 + P^{\phi_3 - \alpha_{21}} + 1 + P^{-(\alpha_{22} - \alpha_{21})^+ + (\alpha_{22} - \alpha_{21})}) \leq 1 \\
\leq \frac{n}{2} \log(16\pi e) \tag{130}
\]

where (128) results from chain rule and the fact that conditioning reduces differential entropy; (129) follows from the fact that Gaussian input maximizes the differential entropy and that conditioning reduces differential entropy; (130) uses the identity that \((\sqrt{P^{\min\{\alpha_{21},\alpha_{12},\alpha_{11} - \phi_1\}}})^2 \leq 1 \) and the definition that \( \phi_3 \triangleq \min\{\alpha_{21}, \alpha_{12}, \phi_2\} \).

For the term \( J_{44} \), we have two different bounds. One bound is given as

\[
J_{44} = h(\bar{x}_2^n|s_{22}^n, s_{12}^n, \bar{x}_1^n, w) \\
\leq \sum_{t=1}^{n} h(\bar{x}_2(t)|s_{22}(t), s_{12}(t)) \\
= \sum_{t=1}^{n} h(\bar{x}_2(t) - \sqrt{P^{\phi_3}}(s_{22}(t) - \sqrt{P^{-\alpha_{12} + (\alpha_{22} - \alpha_{21})^+}}\frac{h_{22}}{h_{12}}s_{12}(t))|s_{22}(t), s_{12}(t)) \\
= \sum_{t=1}^{n} h(\bar{z}_4(t) + \sqrt{P^{\phi_3 - \alpha_{12} + (\alpha_{22} - \alpha_{21})^+}}\frac{h_{22}}{h_{12}}z_1(t)|s_{22}(t), s_{12}(t)) \\
\leq \frac{n}{2} \log(2\pi e (1 + P^{\phi_3 - \alpha_{12} + (\alpha_{22} - \alpha_{21})^+} \cdot \frac{|h_{22}|^2}{|h_{12}|^2})) \tag{132}
\]

where (131) results from chain rule and the fact that conditioning reduces differential entropy; (132) follows from the fact that Gaussian input maximizes the differential entropy and that conditioning reduces differential entropy. The other bound is given as

\[
J_{44} \leq \sum_{t=1}^{n} h(\bar{x}_2(t)) \\
= \frac{n}{2} \log(2\pi e (1 + P^{\phi_3})) \tag{133}
\]
where (133) uses the fact that conditioning reduces differential entropy. By combining the bounds in (132) and (134), we finally have
\[
J_{44} \leq \frac{n}{2} \log \left( 2\pi e \left( 1 + \min \left\{ P_{\phi_3}, P_{\phi_3-(a_{12}-(a_{22}+a_{21})^+)}, \frac{|h_{22}|^2}{|h_{12}|^2} \right\} \right) \right)
\leq \frac{n}{2} \log \left( 2\pi e \left( 1 + \min \left\{ P_{\phi_3}|h_{22}|^2, P_{\phi_3-(a_{12}-(a_{22}+a_{21})^+)}|h_{22}|^2 \right\} \right) \right)
= \frac{n}{2} \log \left( 2\pi e \left( 1 + P_{\phi_3-(a_{12}-(a_{22}+a_{21})^+)}|h_{22}|^2 \right) \right).
\]
(135)

At this point we complete the proof of Lemma 8.

**APPENDIX B**

**PROOF OF LEMMA 9**

Before showing the proof of Lemma 8, we will describe the result of [35, Lemma 1] below, which will be used in our proof.

**Lemma 9.** [35, Lemma 1] Let \( y' = \sqrt{P^{\alpha_1}}hx + \sqrt{P^{\alpha_2}}e + z \), with three random variables \( z \sim N(0, \sigma^2) \), \( x \in \Omega(\xi, Q) \), and \( e \in S_e \), for a given discrete set \( S_e \), under the condition of
\[
|e| \leq e_{\text{max}}, \quad \forall e \in S_e.
\]

In this model, \( e_{\text{max}}, h, \sigma, \alpha_1 \) and \( \alpha_2 \) are positive constants independent of \( P \), with a constraint that \( \alpha_1 > \alpha_2 \). Let \( \gamma' > 0 \) be a finite constant independent of \( P \). If the parameters \( Q \) and \( \xi \) are set as
\[
Q = \frac{P^{\alpha_2}}{2e_{\text{max}}} h_{\gamma'}, \quad \xi = \gamma' \cdot \frac{1}{Q}, \quad \text{for} \quad 0 < \alpha' < \alpha_1 - \alpha_2
\]
then the error probability of the estimation of \( x \) from \( y' \) is
\[
\Pr(e) \to 0 \quad \text{as} \quad P \to \infty.
\]

Let us now prove Lemma 9. Given the observation \( y_1 \) expressed in (63), we will show that \( v_c \) and \( v_p \) can be estimated from \( y_1 \) with vanishing error probability. In this case, \( y_1 \) can be described as
\[
y_1 = \sqrt{P_{h_{11}h_{22}v_c + \sqrt{P^{1-\alpha}e'+ \xi}} + z_1}
\]
where \( e' = h_{11}h_{22}v_c + \sqrt{P^{3\alpha-2}}h_{12}h_{21}u_c \). In this scenario with \( 0 \leq \alpha \leq 1/2 \), we have
\[
|e'| \leq 7/5
\]
for any realizations of \( e' \). Note that, \( v_c, u_c \in \Omega(\xi = \frac{\gamma}{Q}, Q = P^{\alpha_1}) \) and \( v_p \in \Omega(\xi = \frac{\gamma}{Q}, Q = P^{1-\alpha'-\frac{1}{2}}) \), for some parameters \( \gamma \in (0, 1/20) \) and \( \epsilon \to 0 \). Then, by Lemma 9, it holds true that the error probability of the estimation of \( v_c \) from \( y_1 \) is
\[
\Pr[v_c \neq \hat{v}_c] \to 0, \quad \text{as} \quad P \to \infty.
\]
(136)

In the next step, we remove \( v_c \) from \( y_1 \) and then estimate \( v_p \) from the following observation
\[
y_1' = \sqrt{P^{1-\alpha}h_{11}h_{22}v_p + \sqrt{P^{2\alpha-1}h_{12}h_{21}u_c + z_1}}.
\]
(137)
For the second term in the right-hand side of (137), the following condition is always satisfied
\[
|h_{12}h_{21}u_c| \leq 4 \times 6\gamma \leq 6/5.
\]
Therefore, by Lemma 9 it is also true that the error probability of the estimation of \( v_p \) from \( y_1' \) expressed in (137) is
\[
\Pr[v_p \neq \hat{v}_p|v_c = \hat{v}_c] \to 0, \quad \text{as} \quad P \to \infty.
\]
(138)
At this point, by combining the results of (136) and (138), it gives
\[
\Pr[\{v_c \neq \hat{v}_c\} \cup \{v_p \neq \hat{v}_p\}] \to 0 \quad \text{as} \quad P \to \infty.
\]
Given the case with $1 \leq \alpha \leq 4/3$, we will show that $v_c$ and $u_c$ can be estimated from $y_1$ with vanishing error probability, for almost all the channel realizations. Recall that $v_c, u_c \in \Omega(\xi = \frac{6\gamma}{Q}, Q = P^{\frac{\alpha-2}{2}-\epsilon})$, for some parameters $\gamma \in (0, 1/20]$ and $\epsilon \rightarrow 0$. Let us describe $y_1$ in the following form

$$
y_1 = \sqrt{P^{2-\alpha}h_{11}h_{22}v_c} + \sqrt{P^{\alpha}h_{12}h_{21}}u_c + z_1
$$

$$
= 6\gamma P^{\epsilon/2} (A'_0 g'_0 q_0' + A'_1 g'_1 q_1') + z_1
$$

$$
= 6\gamma P^{\epsilon/2} s' + z_1
$$

where $g'_0 \triangleq h_{11}h_{22}, g'_1 \triangleq h_{12}h_{21}, A'_0 \triangleq \sqrt{P^{2-3\alpha/2}}, A'_1 \triangleq \sqrt{P^{\alpha/2}}, s' \triangleq A'_0 g'_0 q'_0 + A'_1 g'_1 q'_1$ and

$$
q'_0 \triangleq \frac{Q_0}{6\gamma}, q'_1 \triangleq \frac{Q_1}{6\gamma}, Q'_0 \triangleq Q_0 \triangleq P^{\frac{\alpha-2}{2}-\epsilon}.
$$

In this scenario, the following conditions are always satisfied: $q'_0, q'_1 \in \mathbb{Z}, |q'_0| \leq Q'_0$ and $|q'_1| \leq Q'_0$. Again, without loss of generality we will consider the case that $Q'_0, A'_0, A'_1 \in \mathbb{Z}^+$. For the observation $y_1$ in (139), our focus is to estimate the sum $s' = A'_0 g'_0 q'_0 + A'_1 g'_1 q'_1$. After decoding $s'$ correctly, $q'_0$ and $q'_1$ can be recovered, because $\{g'_0, g'_1\}$ are rationally independent. We define the minimum distance of $s'$ as

$$
d'_{\min}(g'_0, g'_1) \triangleq \min_{q'_0, q'_1, q'_0 \neq \tilde{q}_0, q'_1 \in \mathbb{Z}^{+}: \left|q'_0 q'_1\right|} |A'_0 g'_0 (q'_0 - \tilde{q}_0) + A'_1 g'_1 (q'_1 - \tilde{q}_1)|.
$$

The following lemma provides a result on the minimum distance.

**Lemma 10.** For the case with $1 \leq \alpha \leq 4/3$, and for some constants $\delta \in (0, 1]$ and $\epsilon > 0$, the following bound on the minimum distance $d'_{\min}$ defined in (140) holds true

$$
d'_{\min} \geq \delta
$$

for all the channel realizations $\{h_{11}, h_{12}, h_{22}, h_{21}\} \in (1, 2)^{2 \times 2} \setminus \mathcal{H}'_{\text{out}}$, where $\mathcal{H}'_{\text{out}} \subseteq (1, 2)^{2 \times 2}$ is an outage set whose Lebesgue measure, denoted by $\mathcal{L}(\mathcal{H}'_{\text{out}})$, has the following bound

$$
\mathcal{L}(\mathcal{H}'_{\text{out}}) \leq 192\delta \cdot P^{-\frac{\epsilon}{2}}.
$$

**Proof.** For $\beta \triangleq \delta \in (0, 1]$, we define an event as

$$
B'(q'_1, q'_0) \triangleq \{(g'_1, g'_0) \in (1, 4)^2 : |A'_1 g'_1 q'_1 + A'_0 g'_0 q'_0| < \beta\}
$$

and define

$$
B' \triangleq \bigcup_{q'_0, q'_1 \in \mathbb{Z}^{+}: \left|q'_0 q'_1\right| \leq 2Q'_0 \forall k \left(q'_0 q'_1\right) \neq 0} B'(q'_1, q'_0).
$$

For this case with $1 \leq \alpha \leq 4/3$, by Lemma 1] we have a bound on the Lebesgue measure of $B'$, given as

$$
\mathcal{L}(B') \leq 24\beta \min\left\{\frac{4Q'_0 Q'_1}{A'_1}, \frac{4Q'_0 Q'_1}{A'_0}, \frac{8Q'_0}{A'_1}, \frac{8Q'_0}{A'_0}\right\}
$$

$$
\leq 24\beta \cdot \frac{8Q'_0}{A'_1}
$$

$$
= 192\delta \cdot P^{-\frac{\epsilon}{2}}.
$$
At this point, we define a new set \( \mathcal{H}'_{\text{out}} \) as
\[
\mathcal{H}'_{\text{out}} \triangleq \{ (h_{11}, h_{22}, h_{12}, h_{21}) \in (1, 2)^{2 \times 2} : (g'_1, g'_0) \in B' \}.
\]
By following the steps related to (109), we have the following bound on the Lebesgue measure of \( \mathcal{H}'_{\text{out}} \)
\[
\mathcal{L}(\mathcal{H}'_{\text{out}}) \leq \mathcal{L}(B') \leq 192\delta \cdot P^{-\frac{1}{2}}.
\] (146)

Lemma 10 reveals that the Lebesgue measure of the outage set \( \mathcal{H}'_{\text{out}} \) is vanishing when \( P \) is large, i.e.,
\[
\mathcal{L}(\mathcal{H}'_{\text{out}}) \to 0, \text{ for } P \to \infty.
\]

Let us now consider the channel condition that \( (h_{11}, h_{22}, h_{12}, h_{21}) \notin \mathcal{H}'_{\text{out}} \), in which the minimum distance of \( \tilde{s}' \), defined in (103), satisfies the inequality of \( d_{\min}' \geq \delta \) (see (139)). With this result, we can conclude that the error probability for decoding \( \tilde{s}' \) from \( y_1 = 6\gamma P^{\epsilon/2} \tilde{s}' + z_1 \) (see (139)), denoted by \( \Pr[\tilde{s}' \neq \hat{s}] \), is
\[
\Pr[\tilde{s}' \neq \hat{s}] \to 0 \text{ for } P \to \infty
\]
for almost all the channel realizations in the regime of large \( P \). After decoding \( \tilde{s}' \) correctly, \( q'_0 \) and \( q'_1 \) can be recovered, based on the fact that \( \{ q'_0, q'_1 \} \) are rationally independent. Then, we complete the proof.

APPENDIX D

SECURE GDoF OF THE GAUSSIAN WIRETAP CHANNEL without A HELPER

This section focuses on the wiretap channel without a helper (removing transmitter 2). For this channel, the secure capacity, denoted by \( C_{\text{no}} \), is given by:
\[
C_{\text{no}} = \max_{v \rightarrow x_1 \rightarrow y_1, y_2} \mathbb{I}(v; y_1) - \mathbb{I}(v; y_2)
\] (147)
(cf. [3]), where the maximum is computed over all random variables \( v, x_1, y_1, y_2 \) such that \( v \rightarrow x_1 \rightarrow y_1, y_2 \) forms a Markov chain, and \( y_k = \sqrt{P^{\alpha_{k1}}} h_{k1} x_1 + z_k \) for \( k = 1, 2 \). Let us focus on the upper bound on the following difference:
\[
\mathbb{I}(v; y_1) - \mathbb{I}(v; y_2)
\leq \mathbb{I}(v; y_1, y_2) - \mathbb{I}(v; y_2)
= h(y_1|y_2) - h(y_1|y_2, v)
\leq h(y_1|y_2) - h(y_1|y_2, v, x_1)
\]
\[
= h(y_1|y_2) - \frac{1}{2} \log(2\pi e)
\] (148)
\[
= h(y_1 - \sqrt{P^{\alpha_{11}} - \alpha_{21}} \frac{h_{11}}{h_{21}} y_2|y_2) - \frac{1}{2} \log(2\pi e)
\]
\[
= h(z_1 - \sqrt{P^{\alpha_{11}} - \alpha_{21}} \frac{h_{11}}{h_{21}} z_2|y_2) - \frac{1}{2} \log(2\pi e)
\]
\[
\leq h(z_1 - \sqrt{P^{\alpha_{11}} - \alpha_{21}} \frac{h_{11}}{h_{21}} z_2) - \frac{1}{2} \log(2\pi e)
\]
\[
= \frac{1}{2} \log(1 + P^{\alpha_{11} - \alpha_{21}} \frac{|h_{11}|^2}{|h_{21}|^2})
\] (150)

where (148) and (150) use the identity that conditioning reduces differential entropy; (149) results from the fact that \( h(y_1|y_2, v, x_1) = h(z_1) = \frac{1}{2} \log(2\pi e) \). By combining (147) and (151), the secure GDoF, denoted by \( d_{\text{no}} \), is upper bounded by
\[
d_{\text{no}} \leq (\alpha_{11} - \alpha_{21})^+. \] (152)
On the other hand, since the secure capacity is optimized over the random variables $v$ and $x_1$, by setting $x_1 = v \sim \mathcal{N}(0, 1)$ we have the lower bound on the secure capacity:

$$C_{no} \geq \mathbb{I}(v; y_1) - \mathbb{I}(v; y_2)$$

$$= h(\sqrt{P_{\alpha_{11}}h_{11}x_1 + z_1}) - h(z_1) - h(\sqrt{P_{\alpha_{21}}h_{21}x_1 + z_2}) + h(z_2)$$

$$= \frac{1}{2} \log(1 + P_{\alpha_{11}}|h_{11}|^2) - \frac{1}{2} \log(1 + P_{\alpha_{21}}|h_{21}|^2). \quad (153)$$

The bound in (153) reveals that the secure GDoF is lower bounded by

$$d_{no} \geq (\alpha_{11} - \alpha_{21})^+$$

which, together with (152), gives the optimal secure GDoF

$$d_{no} = (\alpha_{11} - \alpha_{21})^+. \quad (155)$$

For the symmetric case of notation with $\alpha_{11} = 1$ and $\alpha_{12} = \alpha$, this secure GDoF becomes

$$d_{no} = (1 - \alpha)^+ \quad \forall \alpha \in [0, \infty).$$

**APPENDIX E**

**PROOF OF COROLLARY 2**

For the symmetric setting with $\alpha_{11} = \alpha_{22} = 1, \alpha_{21} = \alpha_{12} = \alpha$, $\phi_1$ and $\phi_3$ take the following forms:

$$\phi_1 = (\alpha - (1 - \alpha)^+)^+$$

$$\phi_3 = \min\{\alpha, (1 - (\alpha - (1 - \alpha)^+)^+)^+\}.$$

In this symmetric case, the three bounds in Corollary 1 then become

$$d \leq \max\{\phi_1, (1 - \phi_3)^+\} + (\phi_3 - \phi_1)^+ \quad (156)$$

$$d \leq (1 - \alpha)^+ + \frac{\max\{1, \alpha\}}{2} \quad (157)$$

$$d \leq (2 - \alpha)^+. \quad (158)$$

When $0 \leq \alpha \leq 1/2$, it reveals that $\phi_1 = 0$ and $\phi_3 = \alpha$, and the bounds in (156)-(158) can be simplified as

$$d \leq 1$$

$$d \leq 3/2 - \alpha$$

$$d \leq 2 - \alpha$$

which implies that

$$d \leq \min\{1, 3/2 - \alpha, 2 - \alpha\} = 1, \quad \forall \alpha \in [0, 1/2].$$

When $1/2 \leq \alpha \leq 1$, it suggests that $\phi_1 = 2\alpha - 1$ and $\phi_3 = \min\{\alpha, 2(1 - \alpha)\}$. Then, the bounds in (156)-(158) can be simplified as

$$d \leq \max\{2\alpha - 1, 1 - \alpha\} + \min\{1 - \alpha, (3 - 4\alpha)^+\}$$

$$d \leq 3/2 - \alpha$$

$$d \leq 2 - \alpha.$$
From the above results, the GDoF $d$ can be bounded as
\[
d \leq \min\{2 - 2\alpha, 3/2 - \alpha, 2 - \alpha\} = 2 - 2\alpha, \quad \forall \alpha \in [1/2, 3/4] \\
d \leq \min\{2\alpha - 1, 3/2 - \alpha, 2 - \alpha\} = 2\alpha - 1, \quad \forall \alpha \in [3/4, 5/6] \\
d \leq \min\{2\alpha - 1, 3/2 - \alpha, 2 - \alpha\} = 3/2 - \alpha, \quad \forall \alpha \in [5/6, 1].
\]

When $1 \leq \alpha$, then $\phi_1 = (\alpha - (1 - \alpha)^+) = \alpha$ and $\phi_3 = 0$, and the bounds in (156)-(158) can be simplified as
\[
d \leq \alpha \\
d \leq \alpha/2 \\
d \leq (2 - \alpha)^+.
\]

The above results imply that
\[
d \leq \min\{(2 - \alpha)^+, \alpha/2\} = \alpha/2, \quad \forall \alpha \in [1, 4/3] \\
d \leq \min\{(2 - \alpha)^+, \alpha/2\} = 2 - \alpha, \quad \forall \alpha \in [4/3, 2] \\
d \leq \min\{(2 - \alpha)^+, \alpha/2\} = 0, \quad \forall \alpha \in [2, +\infty].
\]

At this point we complete the proof.

REFERENCES

[1] C. E. Shannon, “Communication theory of secrecy systems,” *Bell System Technical Journal*, vol. 28, no. 4, pp. 656 – 715, Oct. 1949.

[2] A. D. Wyner, “The wire-tap channel,” *Bell System Technical Journal*, vol. 54, no. 8, pp. 1355 – 1378, Jan. 1975.

[3] I. Csiszár and J. Körner, “Broadcast channels with confidential messages,” *IEEE Trans. Inf. Theory*, vol. 24, no. 3, pp. 339 – 348, May 1978.

[4] S. K. Leung-Yan-Cheong and M. E. Hellman, “Gaussian wiretap channel,” *IEEE Trans. Inf. Theory*, vol. 24, no. 4, pp. 451 – 456, Jul. 1978.

[5] 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, Jun. 2008.

[6] ——, “The Gaussian multiple access wire-tap channel,” *IEEE Trans. Inf. Theory*, vol. 54, no. 12, pp. 5747 – 5755, Dec. 2008.

[7] Y. Liang and H. V. Poor, “Multiple access channels with confidential messages,” *IEEE Trans. Inf. Theory*, vol. 54, no. 3, pp. 976 – 1002, Mar. 2008.

[8] R. Liu, Y. Liang, and H. V. Poor, “Fading cognitive multiple-access channels with confidential messages,” *IEEE Trans. Inf. Theory*, vol. 57, no. 8, pp. 4992 – 5005, Aug. 2011.

[9] X. He, A. Khisti, and A. Yener, “MIMO multiple access channel with an arbitrarily varying eavesdropper: Secrecy degrees of freedom,” *IEEE Trans. Inf. Theory*, vol. 59, no. 8, pp. 4733 – 4745, Aug. 2013.

[10] S. Karmakar and A. Ghosh, “Approximate secrecy capacity region of an asymmetric MAC wiretap channel within 1/2 bits,” in *IEEE 14th Canadian Workshop on Information Theory*, Jul. 2015.

[11] P. Babaeiheidarian, S. Salimi, and P. Papadimitratos, “Finite-SNR regime analysis of the Gaussian wiretap multiple-access channel,” in *Proc. Allerton Conf. Communication, Control and Computing*, Sep. 2015.

[12] R. Liu, I. Maric, P. Spasojevic, and R. D. Yates, “Discrete memoryless interference and broadcast channel with confidential messages: secrecy rate regions,” *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2493 – 2507, Jun. 2008.

[13] A. Khisti, A. Tchamkerten, and G. W. Wornell, “Secure broadcasting over fading channels,” *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2453 – 2469, Jun. 2008.

[14] J. Xu, Y. Cao, and B. Chen, “Capacity bounds for broadcast channels with confidential messages,” *IEEE Trans. Inf. Theory*, vol. 55, no. 10, pp. 4529 – 4542, Oct. 2009.

[15] R. Liu, T. Liu, H. V. Poor, and S. Shamai, “Multiple-input multiple-output Gaussian broadcast channels with confidential messages,” *IEEE Trans. Inf. Theory*, vol. 56, no. 9, pp. 4215 – 4227, Sep. 2010.

[16] Y. K. Chia and A. El Gamal, “Three-receiver broadcast channels with common and confidential messages,” *IEEE Trans. Inf. Theory*, vol. 58, no. 5, pp. 2748 – 2765, May 2012.

[17] Y. Liang, A. Somekh-Baruch, H. V. Poor, S. Shamai, and S. Verdú, “Capacity of cognitive interference channels with and without secrecy,” *IEEE Trans. Inf. Theory*, vol. 55, no. 2, pp. 604 – 619, Feb. 2009.

[18] Z. Li, R. D. Yates, and W. Trappe, “Secrecy capacity region of a class of one-sided interference channel,” in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Jul. 2008.

[19] R. D. Yates, D. Tse, and Z. Li, “Secret communication on interference channels,” in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Jul. 2008.

[20] X. He and A. Yener, “A new outer bound for the Gaussian interference channel with confidential messages,” in *Proc. 43rd Annu. Conf. Inf. Sci. Syst.*, Mar. 2009.
[21] E. Perron, S. Diggavi, and E. Telatar, “On noise insertion strategies for wireless network secrecy,” in Proc. Inf. Theory and App. Workshop (ITA), Feb. 2009.

[22] O. O. Koyluoglu, H. El Gamal, L. Lai, and H. V. Poor, “Interference alignment for secrecy,” IEEE Trans. Inf. Theory, vol. 57, no. 6, pp. 3323 – 3332, Jun. 2011.

[23] J. Xie and S. Ulukus, “Secure degrees of freedom of one-hop wireless networks,” IEEE Trans. Inf. Theory, vol. 60, no. 6, pp. 3359 – 3378, Jun. 2014.

[24] A. Mukherjee, S. A. Fakoorian, and A. L. S. J. Huang, “Principles of physical layer security in multiuser wireless networks: A survey,” IEEE Communications Surveys & Tutorials, vol. 16, no. 3, pp. 1550 – 1573, Aug. 2014.

[25] P. Mohapatra and C. R. Murthy, “Outer bounds on the secrecy rate of the 2-user symmetric deterministic interference channel with transmitter cooperation,” in Proc. 20th National Conference on Communications (NCC), 2014.

[26] J. Xie and S. Ulukus, “Secure degrees of freedom of $K$-user Gaussian interference channels: A unified view,” IEEE Trans. Inf. Theory, vol. 61, no. 5, pp. 2647 – 2661, May 2015.

[27] C. Geng, R. Tandon, and S. A. Jafar, “On the symmetric 2-user deterministic interference channel with confidential messages,” in Proc. IEEE Global Conf. Communications (GLOBECOM), Dec. 2015.

[28] C. Geng and S. A. Jafar, “Secure GDoF of $K$-user Gaussian interference channels: When secrecy incurs no penalty,” IEEE Communications Letters, vol. 19, no. 8, pp. 1287 – 1290, Aug. 2015.

[29] P. Mohapatra and C. R. Murthy, “On the capacity of the two-user symmetric interference channel with transmitter cooperation and secrecy constraints,” IEEE Trans. Inf. Theory, vol. 62, no. 10, pp. 5664 – 5689, Oct. 2016.

[30] J. Chen, “New results on the secure capacity of symmetric two-user interference channels,” in Proc. Allerton Conf. Communication, Control and Computing, Sep. 2016.

[31] P. Mukherjee and S. Ulukus, “MIMO one hop networks with no eve CSIT,” in Proc. Allerton Conf. Communication, Control and Computing, Sep. 2016.

[32] R. Fritschek and G. Wunder, “Towards a constant-gap sum-capacity result for the Gaussian wiretap channel with a helper,” in Proc. IEEE Int. Symp. Inf. Theory (ISIT), Jul. 2016, pp. 2978 – 2982.

[33] P. Mukherjee, J. Xie, and S. Ulukus, “Secure degrees of freedom of one-hop wireless networks with no eavesdropper CSIT,” IEEE Trans. Inf. Theory, vol. 63, no. 3, pp. 1898 – 1922, Mar. 2017.

[34] J. Chen, “Secure communication over interference channel: To jam or not to jam?” in Proc. Allerton Conf. Communication, Control and Computing, Oct. 2018.

[35] ———, “Secure communication over interference channel: To jam or not to jam?” Oct. 2018, available on ArXiv: https://arxiv.org/pdf/1810.13256.pdf.

[36] ———, “On the optimality of secure communication without using cooperative jamming,” Jun. 2017, available on ArXiv: https://arxiv.org/pdf/1706.06220.pdf.

[37] J. Chen and F. Li, “Adding a helper can totally remove the secrecy constraints in interference channel,” Dec. 2018, available on ArXiv: [http://arxiv.org/pdf/1812.00550.pdf](http://arxiv.org/pdf/1812.00550.pdf).

[38] J. Xie and S. Ulukus, “Secure degrees of freedom of the Gaussian wiretap channel with helpers,” in Proc. Allerton Conf. Communication, Control and Computing, Oct. 2012.

[39] ———, “Secure degrees of freedom of the Gaussian wiretap channel with helpers and no eavesdropper CSI: Blind cooperative jamming,” in 47th Annual Conference on Information Sciences and Systems (CISS), Mar. 2013.

[40] M. Nafea and A. Yener, “Degrees of freedom of the single antenna Gaussian wiretap channel with a helper irrespective of the number of antennas at the eavesdropper,” in 2013 IEEE Global Conference on Signal and Information Processing, Dec. 2013.

[41] R. H. Etkin, D. N. C. Tse, and H. Wang, “Gaussian interference channel capacity to within one bit,” IEEE Trans. Inf. Theory, vol. 54, no. 12, pp. 5534 – 5562, Dec. 2008.

[42] A. S. Motahari, S. O. Gharan, M. A. Maddah-Ali, and A. K. Khandani, “Real interference alignment: Exploiting the potential of single antenna systems,” IEEE Trans. Inf. Theory, vol. 60, no. 8, pp. 4799 – 4810, Aug. 2014.

[43] U. Niesen and M. A. Maddah-Ali, “Interference alignment: From degrees of freedom to constant-gap capacity approximations,” IEEE Trans. Inf. Theory, vol. 59, no. 8, pp. 4855 – 4888, Aug. 2013.