Degrees of Freedom of the Single Antenna Gaussian Wiretap Channel with a Helper Irrespective of the Number of Antennas at the Eavesdropper

Mohamed Nafea Aylin Yener
Wireless Communications and Networking Laboratory (WCAN)
Electrical Engineering Department
The Pennsylvania State University, University Park, PA 16802.
msn139@psu.edu *yener@engr.psu.edu*

***Abstract*—A Gaussian wiretap channel with a helper, i.e., a cooperative jammer, is considered and its secure degrees of freedom (s.d.o.f.) is computed. Previous work showed that the s.d.o.f. is upper bounded by $\frac{1}{2}$ in this model when all parties are equipped with one antenna each. In this paper, the more challenging scenario where the eavesdropper has multiple antennas is tackled. Relying on structured signaling and cooperative jamming, specifically, by real interference alignment, it is shown that s.d.o.f. of $\frac{1}{2}$ is achievable irrespective of the number of antennas the eavesdropper may have as long as the cooperative jammer has the same number of antennas as the eavesdropper. The design insight revealed is that the price to pay for the increase in the number of antennas at the eavesdropper is an equivalent increase in the number of antennas at the cooperative jammer in order to maintain the same s.d.o.f.**

I. Introduction

The wiretap channel model in [1] provides the foundation for exploiting noisy communication channels to secure information at the physical layer. Specifically, Wyner in [1] has established the secrecy capacity for a channel with one sender, one receiver, and one eavesdropper assuming that the received signal at the eavesdropper is a degraded version of what is received by the legitimate receiver. This result has been extended to more general discrete memoryless channels in [2]. Secrecy capacity of the Gaussian wiretap channel has been found in [3]. The wiretap channel model has since been extended to an abundance of multi-terminal models, see for example [4]–[11].

In reference [8], *cooperative jamming* is proposed in the multiple access wiretap channel. A transmitter that is not capable of achieving positive secrecy rate for its own, rather than staying silent, can transmit a jamming signal that hurts the eavesdropper more than the legitimate receiver. Equivalently, in a single user wiretap scenario, an external cooperative jammer may be incorporated to improve the achievable secrecy rate of the system [12]. While cooperative jamming is useful in improving the secrecy rate for finite signal to noise ratio (SNR) values in these models, it is known that using Gaussian signaling and jamming achieves zero secure degrees of freedom (s.d.o.f.) [13]. Recently, it has been shown that using structured signaling both for transmission and for cooperative jamming can remedy this shortcoming and achieve positive s.d.o.f. [12].

More recently, an upper bound of $\frac{1}{2}$ on the s.d.o.f. of Gaussian wiretap channel with a cooperative jammer with one antenna at each node has been derived in [14], tightening the earlier bound of $\frac{2}{3}$ [15]. One justification of the tight upper bound in [14] is that the optimal jamming signal that completely covers the received information signal at the eavesdropper, can never occupy less than half of received dimensions at the legitimate receiver. Building on this intuition, in this paper, we answer the question whether it is possible to find jamming signals that completely cover the information signal at an eavesdropper with multiple antennas, while occupying only half of received dimensions at the legitimate receiver. In other words, whether the s.d.o.f. of $\frac{1}{2}$ is achievable even if the eavesdropper has multiple antennas. The answer turns out to be affirmative as long as the cooperative jammer has the same number of antennas as the eavesdropper as shown in this paper.

The key for the achievability lies in the fact that a cooperative jammer with the same number of antennas as the eavesdropper can transmit a scaled copy of the same jamming signal from each antenna so that the received copies of this jamming signal at each antenna of the eavesdropper completely cover the received information signal at this antenna. On the other hand, the legitimate receiver receives the information signal and multiple copies of the same jamming signal which enables achieving s.d.o.f. of $\frac{1}{2}$.

The remainder of the paper is organized as follows. In section II, we introduce the channel model. Section III describes the achievable scheme. We conclude the paper in section IV. *Notation:* The set of integers $\{-Q, -Q+1, \cdots, Q-1, Q\}$, where Q is an integer, is denoted by $C(Q)$. The set $\{\alpha\mathcal{A}\}$ is the set of all elements that belong to the set $\mathcal{A}$ each is scaled by the factor α. We denote the random variables with upper case letters and the random vectors with bold upper case letters. Matrices are also denoted by bold upper case letters. The distinction between random vectors and matrices is clear from the context.

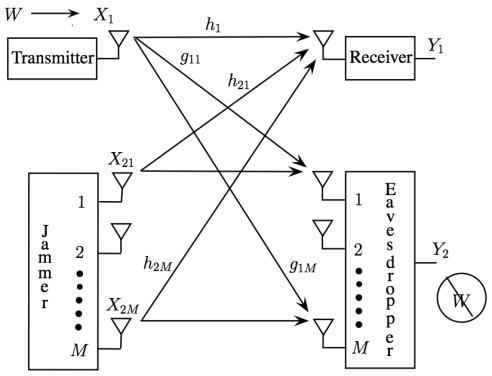

Fig. 1: Gaussian wiretap channel with one antenna at the transmitter and receiver, and M antennas at the cooperative jammer and eavesdropper.

II. Channel Model and Definitions

We consider a Gaussian wiretap channel composed of a legitimate transmitter-receiver pair, an external eavesdropper, and an external cooperative jammer as depicted in Fig. 1. The transmitter and receiver are equipped with one antenna each. The eavesdropper and the cooperative jammer, on the other hand, have $M \geq 2$ antennas each.

The received signals at the receiver and the eavesdropper can be expressed as

$$\begin{aligned} Y_1 &= h_1 X_1 + \mathbf{h}_2^T \mathbf{X}_2 + Z_1 \\ \mathbf{Y}_2 &= \mathbf{g}_1 X_1 + \mathbf{G}_2 \mathbf{X}_2 + \mathbf{Z}_2. \end{aligned} \tag{1}$$

X_1 and $\mathbf{X}_2 = [X_{21}\ X_{22}\ \cdots\ X_{2M}]^T$ are the transmitted signals from the transmitter and the cooperative jammer, respectively, where X_{2i} is the transmitted signal from the ith antenna of the cooperative jammer, $i = 1, 2, \cdots, M$. $Y_1 \in \mathbb{R}$ is the received signal at the legitimate receiver. The received signal vector at the eavesdropper is $\mathbf{Y}_2 = [Y_{21}\ Y_{22}\ \cdots\ Y_{2M}]^T$, where Y_{2i} is the received signal at ith antenna of the eavesdropper. $h_1 \in \mathbb{R}$ and $\mathbf{h}_2 \in \mathbb{R}^M$ are the channel gains from the transmitter and the cooperative jammer, respectively, to the legitimate receiver. The channel gains from the transmitter and the cooperative jammer to the eavesdropper are, respectively, $\mathbf{g}_1 \in \mathbb{R}^M$ and $\mathbf{G}_2 \in \mathbb{R}^{M \times M}$. We assume that all channel gains are constant, real valued, and known at all terminals. It is also assumed that all channel gains are drawn from a continuous distribution. Z_1 and $\mathbf{Z}_2 = [Z_{21}\ Z_{22}\ \cdots\ Z_{2M}]$ are additive Gaussian noises at the legitimate receiver and the eavesdropper, respectively, where Z_1, Z_{21}, $\cdots$, and Z_{2M} are assumed to be independent and identically distributed (i.i.d.) Gaussian random variables with zero mean and unit variance. The power constraints on the transmitted signals are $E\left[X_1^2\right] \leq P$ and $E\left[X_{2i}^2\right] \leq P$, for all $i = 1, 2, \cdots, M$.

The legitimate transmitter wishes to send a message W to the legitimate receiver and keep it secret from the external eavesdropper. The transmitter uses a stochastic encoder $f : \mathcal{W} \to \mathcal{X}_1^n$ to encode its message into a length-n channel input sequence, $X_1^n \in \mathcal{X}_1^n$. The legitimate receiver decodes its received sequence, $Y_1^n \in \mathcal{Y}_1^n$, into an estimate of the transmitted message, $\hat{W}$.

Secrecy rate R_s is said to be achievable if, for any $\sigma > 0$, there exists a length-n channel code $(2^{nR_s}, n)$ such that the probability of decoding error $P_e = \Pr\{\hat{\mathrm{W}} \neq \mathrm{W}\} \leq \sigma$, and that the uncertainty of the transmitted message W at the eavesdropper given its observation, $\mathbf{Y}_2^n$, is almost equal to the uncertainty of the message W without this observation[1], i.e., $\frac{1}{n}H(W|\mathbf{Y}_2^n) \geq \frac{1}{n}H(W) - \sigma$. The secrecy capacity of a channel, C_s, is defined as the closure (supremum) of all achievable secrecy rates for this channel. For a channel with real valued coefficients, the achievable secure degrees of freedom (s.d.o.f.), is defined as $D_s = \lim_{P\to\infty} \frac{R_s}{\frac{1}{2}\log P}$.

The cooperative jammer transmits M sequences, $X_{2i}^n \in \mathcal{X}_2^n$, $i = 1, 2, \cdots, M$, in order to jam the eavesdropper and put it at a disadvantage with respect to the legitimate receiver. However, this friendly interference from the cooperative jammer affects the legitimate receiver as well. Thus, we need to design information and jamming signals such that the jamming signals cause the most harm to the reception capability of the eavesdropper, while causing the least possible harm at the legitimate receiver. Coordinated jamming signals at the M antennas of the cooperative jammer accomplish the task of completely confusing the eavesdropper with M antennas about the information message, while at the same time occupying half of received dimensions at the legitimate receiver at the high SNR regime, as shown next.

III. Achievable Scheme

In this section, we show that we can achieve s.d.o.f. of $\frac{1}{2}$ for the channel in (1) irrespective of the number of antennas at the eavesdropper as long as the cooperative jammer has the same number of antennas as the eavesdropper.

A. Encoding Scheme

Following the real interference alignment technique in [14], [16], we express the transmitted signals from the transmitter and the cooperative jammer as

$$X_1 = \alpha U \tag{2}$$

$$\mathbf{X}_2 = \alpha \mathbf{c} V, \tag{3}$$

where U and V are i.i.d. uniform over the set $C(Q)$, where Q is an integer which will be chosen in Section III-B. The length-n sequence of i.i.d. U's carries the message W. On the other hand, V is the jamming signal transmitted from the cooperative jammer. The jamming precoder $\mathbf{c} = [c_1\ c_2\ \cdots\ c_M]^T$, where c_i is a scaling for the jamming signal V at the ith antenna of the cooperative jammer, for $i = 1, 2, \cdots, M$. Specifically, the jamming precoder $\mathbf{c}$ is chosen to align the jamming signal V over the information signal U at each antenna of the eavesdropper. The constant α simply normalizes the transmission power to satisfy the power constraints at the transmitter and the M antennas of the cooperative jammer.

[1]We consider weak secrecy throughout this paper.

By encoding the transmitted signals from the transmitter and the cooperative jammer as in (2) and (3), respectively, the received signals at the legitimate receiver and the eavesdropper are given by

$$Y_1 = \alpha\left(h_1 U + \mathbf{h}_2^T \mathbf{c} V\right) + Z_1 \tag{4}$$

$$\mathbf{Y}_2 = \alpha\left(\mathbf{g}_1 U + \mathbf{G}_2 \mathbf{c} V\right) + \mathbf{Z}_2. \tag{5}$$

In order to perfectly align the jamming signal V over the information U at each antenna of the eavesdropper, the jamming precoder $\mathbf{c}$ has to satisfy the condition

$$\mathbf{g}_1 = \mathbf{G}_2 \mathbf{c}, \tag{6}$$

where the $(M \times M)$ matrix $\mathbf{G}_2$ is almost surely full rank since the channel gains are all assumed to be drawn from a continuous distribution. When the cooperative jammer has the same number of antennas as the eavesdropper, the jamming precoder $\mathbf{c}$ is given by

$$\mathbf{c} = \mathbf{G}_2^{-1} \mathbf{g}_1. \tag{7}$$

Therefore, the received signals at the legitimate receiver and the eavesdropper can be rewritten as

$$Y_1 = \alpha\left(h_1 U + \mathbf{h}_2^T \mathbf{G}_2^{-1} \mathbf{g}_1 V\right) + Z_1 \tag{8}$$

$$\mathbf{Y}_2 = \alpha \mathbf{g}_1 (U + V) + \mathbf{Z}_2. \tag{9}$$

Note that the number of antennas at the cooperative jammer has to be greater than or equal to the number of antennas at the eavesdropper so that (6) has a solution for $\mathbf{c}$.

Since X_1 and X_2 are independent and the channel is memoryless, the secrecy rate

$$R_s = I(X_1; Y_1) - I(X_1; \mathbf{Y}_2), \tag{10}$$

is achievable [2]. Computing the exact value of this expression is challenging. In Section III-C, we will instead compute a lower bound for this achievable rate which will be sufficient to show our main result.

B. Decoding Scheme

The legitimate receiver employs a hard decision decoder which maps the received signal to the nearest point in the received constellation. From (8), it is easy to see that the received constellation points at the legitimate receiver belong to the set $\mathcal{Y}_1 = \alpha\left\{h_1 \mathcal{U} + \mathbf{h}_2^T \mathbf{G}_2^{-1} \mathbf{g}_1 \mathcal{V}\right\}$, where $\mathcal{U}$ and $\mathcal{V}$ are the transmit constellations at the transmitter and the cooperative jammer, respectively. Since h_1 and $\mathbf{h}_2^T \mathbf{G}_2^{-1} \mathbf{g}_1$ are almost surely rationally independent, there exists a many to one mapping from the received constellation $\mathcal{Y}_1$ to the transmit constellation $\mathcal{U}$ [16]. Therefore, the legitimate receiver passes the output of the hard decoder through this many to one mapping from $\mathcal{Y}_1$ to $\mathcal{U}$ in order to decode the signal U. Then, after n channel uses, the legitimate receiver can use a typical set decoder to decode the message W from the decoded length-n sequence of U's.

Notice that the only source of error in decoding the signal U from the received signal Y_1 is the additive Gaussian noise. Therefore, if the estimated signal at the legitimate receiver is $\hat{U}$, the probability of decoding error at the legitimate receiver $P_e = \Pr\left(\hat{\mathrm{U}} \neq \mathrm{U}\right)$ can be bounded as

$$P_e \leq Q\left(\frac{d_{\min}}{2}\right) \leq \exp\left(-\frac{d_{\min}^2}{8}\right), \tag{11}$$

where $d_{\min}$ is the minimum distance between received constellation points at the legitimate receiver. Bounding the performance of the decoder, i.e., the probability of decoding error P_e, is used to bound the achievable secrecy rate of the proposed scheme.

From (11), in order to bound P_e, we need to calculate $d_{\min}$ first. The distances between the points in the received constellation are irregular and calculating the exact minimum distance is difficult. However, we can use the Khintchine-Groshev Theorem in number theory to lower bound $d_{\min}$. The distance d between any two points Y_1 and Y_1' in the received constellation $\mathcal{Y}_1$ can be expressed as

$$d = \alpha h_1 \left| (U - U') + \frac{\mathbf{h}_2^T \mathbf{G}_2^{-1} \mathbf{g}_1}{h_1} (V - V') \right|. \tag{12}$$

Applying Khintchine-Groshev theorem, we have

$$d_{\min} > \frac{k h_1 \alpha}{(2Q)^{1+\epsilon}}, \tag{13}$$

where for each $\epsilon > 0$, there exists a constant k such that the above equation holds for almost all channel gains. Thus, we have the probability of error P_e is bounded by

$$P_e \leq \exp\left(\frac{-k^2 h_1^2 \alpha^2}{8(2Q)^{2(1+\epsilon)}}\right). \tag{14}$$

We choose $\alpha = \frac{P^{\frac{1}{2}}}{\lambda Q}$ to satisfy the power constraint P at the transmitter and the M antennas of the cooperative jammer, where $\lambda^2 = \max\left\{1, c_1^2, c_2^2\right\}$ [16]. Choose Q such that

$$Q = \eta\left(P^{\frac{1-\epsilon}{2(2+\epsilon)}} - \varsigma\right), \tag{15}$$

where η and ς are constants that do not depend on the power P. The constant ς is used to set Q to an integer. Thus, we have

$$P_e \leq \exp(-\mu P^{\epsilon}), \tag{16}$$

where μ is a constant which does not depend on power. As a result, we have that the probability of error $P_e \to 0$ as $P \to \infty$.

C. Achievable Secrecy Rate

Recall that $R_s = I(X_1; Y_1) - I(X_1; \mathbf{Y}_2)$ is achievable. We will compute a lower bound for the right hand side, and thus also an achievable secrecy rate, as follows. First, the mutual information between the transmitter and the legitimate receiver is bounded as

$$I(X_1; Y_1) \geq I(U; \hat{U}) \tag{17}$$

$$= H(U) - H(U|\hat{U}) \tag{18}$$

$$\geq H(U) - 1 - P_e \log|\mathcal{U}| \tag{19}$$

$$= (1 - P_e)\log(2Q + 1) - 1, \tag{20}$$

where (17) follows from the Markov chain $(U \to X_1 \to Y_1 \to \hat{U})$, (19) follows from Fano's inequality, and (20) follows from the uniformity assumption of U over $\mathcal{U} = C(Q)$, where $|C(Q)| = 2Q + 1$.

Using the bound on the probability of decoding error, P_e, in (16), we have that

$$I(X_1; Y_1) \geq (1 - \exp(-\mu P^{\epsilon})) \log(2Q + 1) - 1. \quad (21)$$

Next, we find an upper bound for $I(X_1; \mathbf{Y}_2)$ as follows:

$$\begin{aligned} I(X_1; \mathbf{Y}_2) &\leq I(X_1; \mathbf{Y}_2 \mathbf{Z}_2) && (22)\\ &= I(X_1; \mathbf{Y}_2 | \mathbf{Z}_2) && (23)\\ &= I(X_1; \mathbf{Y}_2 - \mathbf{Z}_2) && (24)\\ &= H(\mathbf{Y}_2 - \mathbf{Z}_2) - H(\mathbf{Y}_2 - \mathbf{Z}_2 | X_1), && (25) \end{aligned}$$

where (23) follows since X_1 and $\mathbf{Z}_2$ are independent.

Using (9) and (25), we have

$$\begin{aligned} I(X_1; \mathbf{Y}_2) &\leq H(U + V) - H(V) && (26)\\ &\leq \log(4Q + 1) - \log(2Q + 1) && (27)\\ &= \log\left(\frac{4Q + 1}{2Q + 1}\right) && (28)\\ &\leq 1, && (29) \end{aligned}$$

where the inequality in (27) follows since the entropy of the uniform random variable over the set $\{-2Q, -2Q + 1, \cdots, 2Q - 1, 2Q\}$ is an upper bound to the entropy of $U + V$.

Using the lower bound in (21) and the upper bound in (29), we have the following achievable secrecy rate

$$\begin{aligned} R_s &= I(X_1; Y_1) - I(X_1; \mathbf{Y}_2) && (30)\\ &\geq (1 - \exp(-\mu P^{\epsilon})) \log(2Q + 1) - 2. && (31) \end{aligned}$$

D. Achievable Secure Degrees of Freedom

Using (31), we can compute the achievable s.d.o.f. as follows.

$$\begin{aligned} D_s &= \lim_{P \to \infty} \frac{R_s}{\frac{1}{2} \log P} && (32)\\ &\geq \lim_{P \to \infty} \frac{(1 - \exp(-\mu P^{\epsilon})) \log(2Q + 1) - 2}{\frac{1}{2} \log P} && (33)\\ &= \lim_{P \to \infty} \frac{\log\left(2\eta\left(P^{\frac{1-\epsilon}{2(2+\epsilon)}} - \varsigma\right) + 1\right) - 2}{\frac{1}{2} \log P} && (34)\\ &= \frac{1 - \epsilon}{2 + \epsilon}, && (35) \end{aligned}$$

where (34) follows from substituting (15) in (33). Since ϵ is a positive number that can be chosen arbitrarily small, we can achieve s.d.o.f. of $\frac{1}{2}$.

IV. Conclusion and Discussion

It has been previously shown that the secure degrees of freedom (s.d.o.f.) of a Gaussian wiretap channel with one transmitter, one receiver, an external eavesdropper, and an external cooperative jammer, is $\frac{1}{2}$ when all terminals are equipped with one antenna each. In addition, when M independent cooperative jammers, each is equipped with one antenna, are used for this channel, the s.d.o.f. increases to $\frac{M}{M+1}$ [14]. Thus, with increasing the number of cooperative jammers, the s.d.o.f. approaches to one which is an immediate upper bound for the s.d.o.f. of a single-antenna Gaussian wiretap channel. These earlier results have shown that the use of additional jamming resources boosts the s.d.o.f. of the channel. In this paper, we have considered a different use of additional jamming resources. Specifically, we have considered using a multiple-antenna cooperative jammer in order to maintain the achievable s.d.o.f. at $\frac{1}{2}$ when the eavesdropper is equipped with multiple antennas, while the legitimate terminals are still equipped with one antenna each. With the use of structured signaling and cooperative jamming, we have shown that a s.d.o.f. of $\frac{1}{2}$ is achievable for a Gaussian wiretap channel with one antenna at each of the transmitter and receiver, and multiple antennas at the eavesdropper, as long as the cooperative jammer has the same number of antennas as the eavesdropper. It remains open whether the s.d.o.f. can be further improved, and is of current interest.

References

[1] A. D. Wyner, "The wire-tap channel," *Bell System Technical Journal*, vol. 54, no. 8, pp. 1355–1387, 1975.

[2] I. Csiszar and J. Korner, "Broadcast channels with confidential messages," *IEEE Trans. Info. Theory*, vol. 24, no. 3, pp. 339–3487, 1978.

[3] S. Leung-Yan-Cheong and M. Hellman, "The Gaussian wire-tap channel," *IEEE Trans. Info. Theory*, vol. 24, no. 4, pp. 451–456, 1978.

[4] E. Tekin, S. Serbetli, and A. Yener, "On secure signaling for the Gaussian multiple access wire-tap channel," in *2005 Asilomar Conf. On Signals, Systems, and Computers*, Nov. 2005, pp. 1747–1751.

[5] R. Liu, I. Maric, P. Spasojevic, and R. D. Yates, "Discrete memoryless interference and broadcast channels with confidential messages: Secrecy rate regions," *IEEE Trans. Info. Theory*, vol. 54, no. 6, pp. 2493–2507, 2008.

[6] O. O. Koyluoglu, H. El Gamal, L. Lai, and H. V. Poor, "Interference alignment for secrecy," *IEEE Trans. Info. Theory*, vol. 57, no. 6, pp. 3323–3332, 2011.

[7] X. He and A. Yener, "A new outer bound for the Gaussian interference channel with confidential messages," in *43rd Annual Conference on Information Sciences and Systems. CISS*, 2009, pp. 318–323.

[8] E. Tekin and A. Yener, "Achievable rates for the general Gaussian multiple access wire-tap channel with collective secrecy," in *44th Annual Allerton Conf. On Communication, Control, and Computing*, Sep. 2006, pp. 809–816.

[9] ——, "The general Gaussian multiple-access and two-way wiretap channels: Achievable rates and cooperative jamming," *IEEE Trans. Info. Theory*, vol. 54, no. 6, pp. 2735–2751, 2008.

[10] E. Ekrem and S. Ulukus, "Secrecy in cooperative relay broadcast channels," *IEEE Trans. Info. Theory*, vol. 57, no. 1, pp. 137–155, 2011.

[11] X. He and A. Yener, "End-to-end secure multi-hop communication with untrusted relays," *IEEE Trans. Wireless Communications*, vol. 12, no. 1, pp. 1–11, 2013.

[12] ——, "Providing secrecy with structured codes: Tools and applications to two-user Gaussian channels," *arXiv preprint arXiv:0907.5388*, 2009.

[13] X. Tang, R. Liu, P. Spasojevic, and H. V. Poor, "The Gaussian wiretap channel with a helping interferer," in *IEEE International Symposium on Information Theory. ISIT*, 2008, pp. 389–393.

[14] J. Xie and S. Ulukus, "Secure degrees of freedom of one-hop wireless networks," *Submitted to IEEE Trans. Info. Theory*, 2012, arXiv preprint arXiv:1209.5370.

[15] X. He, "Cooperation and information theoretic security in wireless networks," PhD Dissertation, August 2010, available online at http://etda.libraries.psu.edu/theses/approved/WorldWideIndex/ETD-5342/index.html.

[16] A. S. Motahari, S. O. Gharan, and A. K. Khandani, "Real interference alignment with real numbers," *Submitted to IEEE Trans. Info. Theory*, 2009, arXiv preprint arXiv:0908.1208.