Artificial-Noise Alignment for Secure Multicast using Multiple Antennas

Ashish Khisti and Dongye Zhang

***Abstract*—We propose an artificial-noise alignment scheme for multicasting a common-confidential message to a group of legitimate receivers. Our scheme transmits a superposition of information and noise symbols. At each legitimate receiver, the noise symbols are aligned in such a way that the information symbols can be decoded with high probability. In contrast, the noise symbols completely mask the information symbols at the eavesdroppers. Our proposed scheme does not use the knowledge of the eavesdropper's channel gains at the transmitter for alignment, yet it achieves the best-known lower bound on the secure degrees of freedom. The knowledge of the eavesdropper's channel gains is still necessary when selecting the rate of the wiretap code. Our scheme is also a natural generalization of the approach of transmitting artificial noise in the null-space of the legitimate receiver's channel, previously proposed in the literature.**

I. Introduction

Multiple antennas provide a promising approach for enhancing confidentiality of messages at the physical layer. A natural technique using multiple antennas is artificial-noise transmission [1]. We transmit an information message by beamforming in the direction of the legitimate receiver and superimpose a noise signal in a direction orthogonal to the legitimate receiver. This way any eavesdropper, whose channel vector has a component along the noise vector gets jammed by the noise signal. Unfortunately, such an approach does not scale when we need to multicast a common message to a large number of legitimate receivers. If the number of receivers is larger than the number of transmit antennas, we cannot find a vector that is simultaneously in the null space of all receivers. In this note we show how real-interference alignment [4], [5], can be used to to *align* the noise symbols at each legitimate receiver so that together they occupy only $\frac{1}{M}$ degrees of freedom at each desired user and yet mask the information symbols completely at each undesired user.

In related works, the multi-antenna compound wiretap channel was introduced in [2] where a common message needs to be transmitted to a group of legitimate receivers and needs to be kept confidential from a group of eavesdroppers. An interference alignment scheme for this setup was proposed in [3]. The interference alignment scheme in [3] however uses the knowledge of the eavesdropper channel gains for interference alignment. Using the real-interference alignment approach [4], [5], it aligns the information symbols at each eavesdropping receiver, so that they only occupy $\frac{1}{M}$ degrees of freedom. This results in $1-\frac{1}{M}$ secure degrees of freedom being achievable, which is the best known lower bound. In this note we show that a noise-alignment scheme that only requires the channel gains of the legitimate receivers for alignment can also attain the same lower bound. Unfortunately the knowledge of the eavesdropper channel gains appears necessary for selecting the rate of the wiretap codebook and thus the scheme is not completely blind to the eavesdropper's knowledge.

II. Channel Model

We consider a compound multi-antenna wiretap channel that consists of one transmitter with M antennas, a group of J_1 legitimate receivers, each with one antenna, and a group of J_2 eavesdroppers each with one antenna. The resulting channel model can be expressed as

$$\begin{aligned} y_j &= \mathbf{h}_j^T\mathbf{x} + v_j, \qquad j = 1,\dots,J_1 \\ z_k &= \mathbf{g}_k^T\mathbf{x} + w_k, \qquad k = 1,\dots,J_2, \end{aligned} \tag{1}$$

where the transmitted signal vector $\mathbf{x}\in\mathbb{R}^M$ is required to satisfy the average power constraint $E[||\mathbf{x}||^2]\le P$, and the additive noise variables v_j and w_k are independent identically distributed (i.i.d) AWGN noise variables, distributed $\mathcal{N}(0,1)$. In our model we assume that all the elements of the vectors $\mathbf{h}_j, \mathbf{g}_k \in \mathbb{R}^M$ are rationally independent; such a condition is satisfied with probability 1 if the channel gains are sampled independently from any continuous valued distribution. We will assume that the channel gains $\mathbf{h}_j$ and $\mathbf{g}_k$ are known to the transmitter. However the knowledge of the channel gains $\mathbf{g}_k$ is only used in selecting the rate of the wiretap code, as will become apparent from our analysis. Furthermore, we only consider the case that the channel coefficients remain fixed for the entire duration of communication.

We transmit a single common message m to all the J_1 legitimate receivers. A rate R is achievable if there exists a sequence of length n wiretap codes such that

This work was supported by an NSERC Discovery Grant

A. Khisti and D. Zhang are with the Dept. Electrical and Computer Engineering, University of Toronto, ON, Canada M5S 3G4. (Email addresses: akhisti@comm.utoronto.ca; dongye.zhang@mail.utoronto.ca).

the error probability at each legitimate receiver goes to zero as $n \to \infty$ and the leakage rate $\frac{1}{n} I(m; z_k^n)$ also approaches zero as $n \to \infty$ for each $k = 1, \ldots, J_2$. Of particular interest is the achievable degrees of freedom i.e., $d = \lim_{P \to \infty} \frac{R}{\frac{1}{2}\log_2 P}$. As remarked earlier, the result in [3] assumes a complete knowledge of channel gains of the eavesdroppers and proposes a signal alignment scheme that achieves $d = 1 - \frac{1}{M}$.

Our main result is that the same degrees of freedom can be achieved using a noise alignment scheme that aligns artificial-noise in the direction of legitimate receivers. Such a scheme has the advantage that it does not need any information about the eavesdropper's channel in the alignment process. In the rest of this letter, we outline the proposed noise alignment scheme in section III and present the secrecy-rate analysis in section IV. Conclusions are provide in section V.

III. Artificial-Noise Alignment

Our transmission scheme consists of sending fictitious (noise) messages in addition to the information message. Through an appropriate choice of a precoder, we align the noise symbols at each legitimate receiver while the noise symbols do not get aligned at any eavesdropper. This enables the legitimate receiver to decode the information message while they are completely masked by the fictitious messages at the eavesdroppers.

We begin by defining the precoding sets as follows. Let N be a sufficiently large integer and let

$$\mathcal{T} = \left\{ \prod_{j=1}^{J_1} \prod_{i=1}^{M} h_{ji}^{\alpha_{ji}} \,\middle|\, \alpha_{ji} \in \{0, \ldots, N-1\} \right\}, \quad (2)$$

$$\mathcal{A} = \left\{ \prod_{j=1}^{J_1} \prod_{i=1}^{M} h_{ji}^{\alpha_{ji}} \,\middle|\, \alpha_{ji} \in \{0, \ldots, N\} \right\}, \quad (3)$$

where h_{ji} denotes the channel gain between the i-th transmitter antenna and the j-th legitimate receiver. Note that each selection of the tuple $\{\alpha_{ji}\} \in \{0, \ldots, N-1\}^{MJ_1}$ results in a different element of $\mathcal{T}$. There are a total of $L = N^{MJ_1}$ elements in $\mathcal{T}$, and $L' = (N+1)^{MJ_1}$ elements in $\mathcal{A}$. Let $\mathbf{v} \in \mathbb{R}^L$ consists of all elements in the set $\mathcal{T}$, and let

$$V = \begin{bmatrix} \mathbf{v}^T & 0 & \cdots & 0 \\ 0 & \mathbf{v}^T & \cdots & 0 \\ \vdots & & \ddots & \vdots \\ 0 & 0 & \cdots & \mathbf{v}^T \end{bmatrix} \in \mathbb{R}^{M \times ML}. \quad (4)$$

We let our signal constellation be

$$\mathcal{C} = a \{-Q, -Q+1, \ldots, Q-1, Q\} \quad (5)$$

where a is the scaling constant and $Q \in \mathbb{Z}$ denotes the size of the constellation, whose values will be defined in the sequel. We let the transmit vector be given as

$$\mathbf{x} = \mathbf{u}(\boldsymbol{\alpha}^T \mathbf{b}_1) + V \mathbf{b}_2 \quad (6)$$

where $\mathbf{b}_1 \in \mathcal{C}^{KL}$ is the vector of information symbols and $\mathbf{b}_2 \in \mathcal{C}^{ML}$ is the vector of fictitious noise symbols. All the symbols are uniformly distributed over $\mathcal{C}$. Furthermore $\mathbf{u} \in \mathbb{R}^M$ and $\boldsymbol{\alpha} \in \mathbb{R}^{KL}$ are vectors whose elements are mutually independent and also independent of all the elements in h_{ji}. The output at each legitimate receiver can be expressed as

$$y_j = \mathbf{h}_j^T \mathbf{u} \boldsymbol{\alpha}^T \mathbf{b}_1 + \mathbf{h}_j^T V \mathbf{b}_2 + v_j, \qquad j = 1, \ldots, J_1. \quad (7)$$

Let $\hat{\mathbf{h}}_j = \left(\mathbf{h}_j^T \mathbf{u} \boldsymbol{\alpha}^T\right)^T$, so that $\hat{\mathbf{h}}_j \in \mathbb{R}^{KL}$. Notice that the elements of $\hat{\mathbf{h}}_j$ are rationally independent and independent of the elements in $\mathcal{A}$. We let

$$\tilde{\mathbf{h}}_j^T = \mathbf{h}_j^T V = \left[h_{j1} \mathbf{v}^T, \ldots, h_{jM} \mathbf{v}^T \right]. \quad (8)$$

Thus, $\tilde{\mathbf{h}}_j$ is a length ML vector whose elements belong to the set $\mathcal{A}$ in (3). Since all elements of $\tilde{\mathbf{h}}_j$ belong to $\mathcal{A}$ we can also express it as [3, Lemma 2]

$$\tilde{\mathbf{h}}_j^T = \tilde{\mathbf{h}}^T T_j, \quad (9)$$

where $\tilde{\mathbf{h}} \in \mathbb{R}^{L'}$ is a vector consisting of all the elements in $\mathcal{A}$ and $T_j \in \mathbb{R}^{L' \times ML}$ is a matrix for which every column has exactly one element that equals 1, and the remaining elements are zero. Furthermore it follows from (8) that no more than M entries in each row of T_j are non-zero. The output at each legitimate receiver can be simplified as

$$y_j = \hat{\mathbf{h}}_j^T \mathbf{b}_1 + \tilde{\mathbf{h}}^T T_j \mathbf{b}_2 + v_j, \qquad j = 1, \ldots, J_1 \quad (10)$$

Note that the elements of $\hat{\mathbf{h}}_j$ and $\tilde{\mathbf{h}}$ are rationally independent. The output at each eavesdropper can be expressed as

$$z_k = (\mathbf{g}_k^T \mathbf{u}) \boldsymbol{\alpha}^T \mathbf{b}_1 + \mathbf{g}_k^T V \mathbf{b}_2 + w_k, \qquad k = 1, \ldots, J_2. \quad (11)$$

We let

$$\tilde{\mathbf{g}}_k^T = \mathbf{g}_k^T V = \left[g_{k1} \mathbf{v}^T, \ldots, g_{kM} \mathbf{v}^T \right] \quad (12)$$

and note that Eq. (11) reduces to

$$z_k = \hat{\mathbf{g}}_k^T \mathbf{b}_1 + \tilde{\mathbf{g}}_k^T \mathbf{b}_2 + w_k, \qquad k = 1, \ldots, J_2. \quad (13)$$

where $\hat{\mathbf{g}}_k = \left(\mathbf{g}_k^T \mathbf{u} \boldsymbol{\alpha}^T\right)^T \in \mathbb{R}^{KL}$.

Since the elements of $\mathbf{u}$, $\boldsymbol{\alpha}$, $\mathbf{h}_j$ and $\mathbf{g}_k$ are rationally independent, it follows that all the elements of $\hat{\mathbf{g}}_k$ and $\tilde{\mathbf{g}}_k$ are rationally independent. Eq. (10) and (11) complete the noise alignment procedure. In the next section, we propose the suitable choice of constellation parameters and the the corresponding expression for an achievable rate.

IV. Secrecy Rate Analysis

Our analysis is based on the Khintchine-Grovshev type theorem on manifolds in $\mathbb{R}^n$.

Proposition 1: (Motahari et. al [5]) Let $v_1, v_2, \ldots, v_m$ be a collection of m analytic functions in $\mathbb{R}^n$ for some $m < n$ and let $\{1, v_1, v_2, \ldots, v_m\}$ be linearly independent. Then for all vectors $\mathbf{f} \in \mathbb{R}^n$, except a set of measure zero, and every $\varepsilon > 0$ there exists a constant $\kappa = \kappa(\mathbf{f}, \varepsilon)$ such that for all integers $p, q_1, \ldots, q_m \in \mathbb{Z}$ with $q_i \neq 0$ for at-least some $1 \leq i \leq m$, we have that

$$|p + q_1 v_1(\mathbf{f}) + \ldots + q_m v_m(\mathbf{f})| > \frac{\kappa}{\max_{1\leq i \leq m} |q_i|^{m+\varepsilon}} \tag{14}$$

is satisfied. □

Recall that by construction, the entries in the vectors $\hat{\mathbf{h}}_j \in \mathbb{R}^{KL}$ and $\tilde{\mathbf{h}} \in \mathbb{R}^{L'}$ in (10) are rationally independent. We can express a signal constellation point at receiver j in (10) as

$$\hat{\mathbf{h}}_j^T \mathbf{b}_1 + \tilde{\mathbf{h}}^T T_j \mathbf{b}_2 = a \left(\sum_{k=1}^{KL} \hat{h}_{jk} q_k + \sum_{l=1}^{L'} \tilde{h}_l p_{jl} \right) \tag{15}$$

where we have that $q_k \in \{-Q, \ldots, Q\}$ and $p_{jl} \in \{-MQ, \ldots, MQ\}$, a and Q are the constellation parameters (5), and $\{\hat{h}_{jk}\}\{$ and $\{\tilde{h}_l\}$ are the entries of $\hat{\mathbf{h}}_j$ and $\tilde{\mathbf{h}}$ respectively. Using (14) it follows that the minimum distance d_0 in the received signal constellation across all the legitimate receivers is

$$d_0 \geq \frac{\kappa_0 a}{(2MQ)^{KL+L'-1+\varepsilon}} \tag{16}$$

where we let $\kappa_0 = \min_{1 \leq j \leq J_1} \kappa(\hat{\mathbf{h}}_j, \tilde{\mathbf{h}}, \varepsilon)$.

Following [5], we select the following values of Q and a in order to attain the optimal degrees of freedom:

$$Q = P^{\frac{1-\varepsilon}{2(KL+L'+\varepsilon)}}, \qquad a = \gamma \frac{P^{\frac{1}{2}}}{Q} \tag{17}$$

where γ is a normalizing constant in order to satisfy the average power constraint. Recall from (6) that

$$x_i = u_i(\boldsymbol{\alpha}^T \mathbf{b}_1) + \mathbf{v}^T \mathbf{b}_{2,i} \tag{18}$$

where $\mathbf{b}_{2,i} \in \mathbb{R}^L$ is the noise vector from antenna i. It follows that

$$E[x_i^2] \leq u_i^2 E[(\boldsymbol{\alpha}^T \mathbf{b}_1)^2] + E[(\mathbf{v}^T \mathbf{b}_{2,i})^2] \tag{19}$$

$$= u_i^2 \sum_{j=1}^{KL} \alpha_j^2 E[b_{1,j}^2] + \sum_{j=1}^{L} v_j^2 E[b_{2,i,j}^2] \tag{20}$$

$$\leq u_i^2 a^2 Q^2 ||\boldsymbol{\alpha}||^2 + a^2 Q^2 ||\mathbf{v}||^2 \tag{21}$$

$$\leq u_i^2 \gamma^2 P ||\boldsymbol{\alpha}||^2 + \gamma^2 P ||\mathbf{v}||^2 \tag{22}$$

where (20) follows from the fact that all the input symbols in $\mathbf{b}_1$ and $\mathbf{b}_{2,i}$ are sampled independently, (21) follows since each constellation point is uniformly distributed in $\mathcal{C}$ in (5) and the last step (22) follows by substituting (17). By selecting

$$\gamma^2 = \frac{1}{M(||\boldsymbol{\alpha}||^2 + ||\mathbf{v}||^2)}, \quad |u_i| \leq 1 \tag{23}$$

it follows that $E[x_i]^2 \leq \frac{P}{M}$ and thus $E[||\mathbf{x}||^2] \leq P$. Furthermore substituting (17) into (16) we have that

$$d_0^2 \geq \frac{\kappa_0^2}{(2M)^{(2(KL+L'-1+\varepsilon))}} \frac{a^2}{Q^{2(KL+L'-1+\varepsilon)}} \tag{24}$$

$$= \frac{\kappa_0^2 \gamma^2}{(2M)^{2(KL+L'-1+\varepsilon)}} \frac{P}{Q^{2(KL+L'+\varepsilon)}} \tag{25}$$

$$= \frac{\kappa_0^2 \gamma^2}{(2M)^{2(KL+L'-1+\varepsilon)}} P^{\varepsilon} \triangleq \eta \cdot P^{\varepsilon} \tag{26}$$

where the constant η depends on the channel gains $\mathbf{h}_j$ but not on P. Thus for *fixed* channel gains and K, N (c.f. (3)) and ε, if we take $P \to \infty$ we have that $|d_0| \to \infty$ and the error probability at receiver j

$$\Pr(e_j) \leq \exp(-d_0^2/4) \leq \exp(-\eta P^{\varepsilon}/4) = o_P(1;\eta) \tag{27}$$

approaches 0 as $P \to \infty$.

An achievable secrecy rate for the compound wiretap channel model is [2]

$$R = \max_{p_{\mathbf{b}_1, \mathbf{x}}} \left\{ \min_j I(\mathbf{b}_1; y_j) - \max_k I(\mathbf{b}_1; z_k) \right\}. \tag{28}$$

To compute (28) we note that

$$I(\mathbf{b}_1; y_j) - I(\mathbf{b}_1; z_k) = H(\mathbf{b}_1) - H(\mathbf{b}_1|y_j) - I(\mathbf{b}_1; z_k) \tag{29}$$

and bound each of the three terms. Since all elements of $\mathbf{b}_1 \in \mathbb{R}^{KL}$ are uniformly distributed over the constellation $\mathcal{C}$ it follows that

$$H(\mathbf{b}_1) = KL \log_2(2Q+1) \geq \frac{1}{2} \frac{KL(1-\varepsilon)}{KL + L' + \varepsilon} \log_2 P \tag{30}$$

Next using Fano's inequality we have,

$$H(\mathbf{b}_1|y_j) \leq 1 + \Pr(e_j) H(\mathbf{b}_1)$$

$$= 1 + \Pr(e_j) KL \log_2(2Q+1)$$

$$= 1 + o_P(1;\eta) \log_2 P. \tag{31}$$

where we substitute (27) for $\Pr(e_j)$ and observe that for fixed K and L as $P \to \infty$ we have that $KL \cdot o_P(1;\eta)$ also vanishes with P but depends on η for any fixed P.

We next compute $I(\mathbf{b}_1; z_k)$. We first express

$$I(\mathbf{b}_1; z_k) = I(\mathbf{b}_1, \mathbf{b}_2; z_k) - I(\mathbf{b}_2; z_k|\mathbf{b}_1)$$

$$= I(\mathbf{x}; z_k) - H(\mathbf{b}_2) + H(\mathbf{b}_2|z_k, \mathbf{b}_1) \tag{32}$$

$$\leq \frac{1}{2} \log(1 + ||\mathbf{g}_k||^2 P) - H(\mathbf{b}_2) + H(\mathbf{b}_2|z_k, \mathbf{b}_1) \tag{33}$$

where we use the fact that $\mathbf{x}$ is a function of $(\mathbf{b}_1, \mathbf{b}_2)$ in (32) and the fact that a Gaussian input maximizes the mutual information in (33).

Since the elements of $\mathbf{b}_2 \in \mathcal{C}^{ML}$ are uniformly distributed in $\mathcal{C}$ it follows that

$$H(\mathbf{b}_2) = ML \log(2Q+1) \tag{34}$$

$$\leq ML + \frac{ML}{2(KL + L' + \varepsilon)} \log_2 P \tag{35}$$

To compute the final term in (33) we consider revealing $\mathbf{b}_1$ to each eavesdropper. For (11) it follows that the effective channel at the eavesdropper is now given by $\tilde{z}_k = \tilde{\mathbf{g}}_k \mathbf{b}_2 + w_k$ where the entries in $\tilde{\mathbf{g}}_k$ are rationally independent. We next propose a condition under which the term $H(\mathbf{b}_2|z_k, \mathbf{b}_1)$ is small. Note that the received signal constellation point at receiver k can be expressed as $a\left(\sum_{j=1}^{ML} \tilde{g}_{kj} b_{2,j}\right)$. Therefore using (14) it follows that for all channel gains $\tilde{\mathbf{g}}_k$, except a set of measure zero, we have that the minimum distance in the received constellation satisfies

$$d_e \geq \frac{\kappa_e a}{(2Q)^{ML-1+\varepsilon}} \tag{36}$$

where κ_e depends on the vectors $\tilde{\mathbf{g}}_k$. Substituting the values of Q and a from (17) and by imposing

$$KL + L' \geq ML \tag{37}$$

we have that

$$d_e^2 \geq \frac{\kappa_e^2 \gamma^2}{2^{2(KL+L'-1+\varepsilon)}} P^{\varepsilon} \tag{38}$$

which increases as $P \to \infty$. Thus the error probability associated with the eavesdropper is given by

$$\begin{aligned} \Pr(e_k) &= \Pr(\mathbf{b}_2 \neq \hat{\mathbf{b}}_{2,k}) \\ &\leq \exp(-\eta_e P^{\varepsilon}/4) = o_P(1;\eta_e) \end{aligned} \tag{39}$$

It thus follows that

$$H(\mathbf{b}_2|\mathbf{b}_1, z_k) \leq H(\mathbf{b}_2|\tilde{z}_k) \leq 1 + o_P(1;\eta_e)\log_2 P \tag{40}$$

where $o_P(1;\eta_e)$ decreases to zero as $P \to \infty$, but depends on η_e for any fixed P. Substituting (35) and (40) into (33) we have that

$$\begin{aligned} I(\mathbf{b}_1; z_k) &\leq \frac{1}{2}\log_2(cP+1) \\ &- \frac{1}{2}\frac{ML(1-\varepsilon)}{KL+L'+\varepsilon}\log_2 P - o_P(1;\eta_e)\log_2 P - 1 \end{aligned} \tag{41}$$

where we have introduced $c = \max_{1\leq k\leq J_2} ||\mathbf{g}_k||^2$.

Substitute (30), (31) and (41) into (29), we can achieve the lower bound on the secrecy rate

$$\begin{aligned} R &= I(\mathbf{b}_1; y_j) - I(\mathbf{b}_1; z_k) \\ &= H(\mathbf{b}_1) - H(\mathbf{b}_1|y_j) - I(\mathbf{b}_1; z_k) \\ &\geq \frac{1}{2}\frac{KL(1-\varepsilon)}{KL+L'+\varepsilon}\log_2 P - (1 + o_P(1)\log_2 P) - \\ &\left(\frac{1}{2}\log_2(cP+1) - \frac{1}{2}\frac{ML(1-\varepsilon)}{KL+L'+\varepsilon}\log_2 P + o_P(1;\eta_e)\log_2 P\right) \\ &\geq \frac{1}{2}\left(\frac{(K+M)L(1-\varepsilon)}{KL+L'+\varepsilon} - 1 - o_P(1;\eta_e,\eta)\right)\log_2 P \end{aligned} \tag{42}$$

Remark 1: We note that for any fixed P the rate of the wiretap codebook depends on the channel gains of the eavesdropper. Indeed both the constant c as well as the constant η_e in the above expressions depend on the channel gains of the eavesdropper. An interesting question for further study is whether there exists a class of channels for which the error probability (39) decays to zero *uniformly* for all eavesdropper channels in that class. Such a bound will enable us to obtain a coding scheme that is oblivious to the eavesdropper channel gains.

Using (42) we have the secure degree of freedom (s.d.o.f) is

$$d = \lim_{P\to\infty} \frac{R}{\frac{1}{2}\log P} = \frac{(K+M)L(1-\varepsilon)}{KL+L'+\varepsilon} - 1 \tag{43}$$

We need to select K to maximize d given the constraint in (37). We select

$$K = M - \frac{L'}{L} = M - \frac{(N+1)^{MJ_1}}{N^{MJ_1}} \tag{44}$$

By selecting N sufficiently large, $K \to M-1$ and ε can be selected to be sufficiently close to zero, the secure d.o.f in (43) can be made arbitrarily close to $1 - \frac{1}{M}$.

V. Conclusion

We propose the use of artificial-noise alignment for transmitting a confidential message using a multi-antenna transmitter. The proposed scheme transmits a superposition of information and noise symbols. It simultaneously aligns the noise symbols at all intended users so that the message symbols can be decoded by these receivers. In contrast, the message symbols are completely masked by noise symbols at the eavesdroppers. As future work it will be of interest to see whether one can obtain suitable non-asymptotic versions of the Khintchine-Grovshev theorem in Prop. 1 which would enable uniform bounds on the equivocation for a class of eavesdropper channels. This will relax the need of having eavesdropper's channel gains at the transmitter when selecting the rate of the wiretap codebook.

In other directions, the result could potentially be extended to the case when the eavesdropper has multiple antennas, perhaps using a recent approach in [6]. It will also be interesting to consider the impact of imperfect and outdated CSI, finite SNR and the cost of acquiring CSI at the transmitter. Indeed such directions remain a fertile area of research in the literature of interference alignment.

Acknowledgement

Xiang He provided useful feedback on an earlier draft of the paper.

References

[1] S. Goel and R. Negi, "Guaranteeing Secrecy using Artificial Noise," *IEEE Transactions on Wireless Communications*, vol. 7, no. 6, pp. 2180-2189, June 2008

[2] Y. Liang, G. Kramer, H. V. Poor, and S. S. (Shitz), "Compound wire-tap channels," *EURASIP Journal on Wireless Communications and Networking, Special Issue on Wireless Physical Layer Security*, 2010

[3] A. Khisti, "Interference Alignment for the Multi-Antenna Compound Wiretap Channel," *IEEE Trans. Inform. Theory*, vol. 57, no. 5, pp. 2967–2993, May, 2011.

[4] A. S. Motahari, S. O. Gharan, and A. K. Khandani, "Real interference alignment with real numbers," *Submitted to IEEE Trans. Inform. Theory, http://arxiv.org/abs/0908.1208*, 2009.

[5] A. S. Motahari, S. O. Gharan, M. Maddah-Ali, and A. K. Khandani, "Real interference alignment: Exploiting the potential of single antenna systems," *Submitted to IEEE Trans. Inform. Theory, http://arxiv.org/abs/0908.2282*, 2009.

[6] M. Zamanighomi and Z. Wang, "Multiple-Antenna Interference Channel with Receive Antenna Joint Processing and Real Interference Alignment," CoRR abs/1301.6315 (2013)