Sensors & Transducers, Vol. 166, Issue 3, March 2014, pp. 135-144

www.sensorsportal.com

Sensors & Transducers

http://www.sensorsportal.com

Secure Degrees of Freedom of the Gaussian Z Channel with Single Antenna

Xianzhong XIE, Xiujuan ZHANG, Bin MA, Weijia LEI
Chongqing Key Lab of Mobile Communications Technology, Institute of Personal Communications, Chongqing University of Posts and Telecommunications, Chongqing, China
Tel.: 18883862996
E-mail: zhangxjcqupt@163.com

Received: /Accepted: 28 February 2014 /Published: 31 March 2014

Abstract: This paper presents the secrecy capacity and the secure degrees of freedom of Gaussian Z channel with single antenna and confidential information. Firstly, we analysis the secrecy capacity and the upper bound of secure degrees of freedom of this channel in theory. Then, we respectively discuss the security pre-coding scheme for real Gaussian channel model and frequency selection channel model. Under the first model, through real interference alignment and cooperative jamming, we obtain the secrecy capacity and secure degrees of freedom, proving that it can reach the upper bound of secure degrees of freedom in theory. While, under the second one, a strong security pre-coding algorithm is proposed, which is based on the fact that sparse matrix has strong hash property. Next, we arrange interference with interference alignment and the receivers process their received signal through zero forcing algorithm. At last, the messages are reconstructed with maximum likelihood decoding, where it shows that the algorithm can asymptotically achieve the optimal secrecy capacity.

Keywords: Z channel, Interference alignment, Hash property, Cooperative jamming, Secrecy capacity.

1. Introduction

Wireless transmissions have the potential of eavesdropping for its broadcast property. To combat this problem, initial security measures were above the physical layer with methods such as encryption. While, recent information-theoretic researches on secure communication have focused on implementing security measures at the physical layer. This problem was first considered by Wyner in wiretap channel in [1]. After that, secure communication was widely studied in a variety of channels [2-13], where interference alignment technology and cooperative jamming scheme are widely used in [2-9] and a different strategy for secrecy based on hash property that is proved to achieve the optimal secrecy capacity is proposed in [10-13].

However, the secure degrees of freedom (SDOF) and secrecy capacity of Gaussian Z channel have not been systematically studied. To solve the problem, in section 3, we prove the upper bound of SDOF on this channel at first and then prove that the upper bound can be achieved with cooperative jamming and real interference alignment which reveals the accurate upper bound of SDOF in this channel.

In section 4, the security pre-coding based on hash property in Z channel is addressed. While, this channel is different from wiretap channel in [10], in which interference cannot be ignored. So it should be considered how to deal with interference. Whereas, unlike the method in [11], a low-complexity linear pre-coding is introduced in the second coding scheme to combat interference. Moreover, receivers obtain their corresponding messages by zero forcing the

interference, which can enable us to decode the messages in relatively shorter length of data compared with that in [11], which can further reduce the complexity.

The rest of the paper is organized as follows. The system model and definitions are presented in section 2. The SDOF of Gaussian Z channel with single antenna in theory is studied at first and then the achievable scheme of the real Gaussian Z channel is introduced in section 3. As a result, the accurate upper bound of SDOF is also derived. While, in section 4, we introduce a different security pre-coding scheme which is based on hash property in frequency selection Gaussian Z channel with single antenna. In section 5, we conclude this paper. And finally, we give the proof of the theorem in Appendix A.

2. System Model and Definitions

2.1. System Model

The Gaussian Z channel with single antenna is shown in Fig. 1, where $Y_i(i=1,2)$ is the channel output of the legitimate receiver, X_i is the channel input of the legitimate transmitter, $h_{ji}(i,j=1,2)$ is the channel gain of the i[th] transmitter to the j[th] receiver and $\{N_1,N_2\}$ are mutually independent zero-mean unit-variance Gaussian random variables. The message W_i is sent by transmitter $i(i=1,2)$ to receiver i.

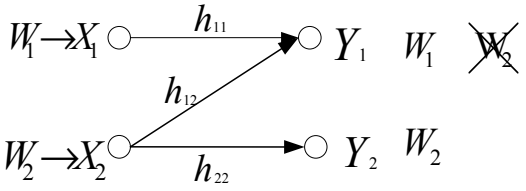

Fig. 1. Gaussian Z channel with one antenna.

Throughout this paper, we also use the following definitions and notations. The cardinality of a set $\mathcal{U}$ is denoted by $|\mathcal{U}|$, and $\mathcal{U}\backslash V \equiv \mathcal{U}\cap V^c$ denotes the set difference, where V^c denotes the complement of V. Column vectors and sequences are denoted in boldface. Let $A\mathbf{u}$ denote a value taken by a function $A: u^n \to \bar{u}$ at $\mathbf{u}=(u_1,u_2,...,u_n)\in u^n$, where u^n is a domain of the function. When A is a linear function, it can be expressed by a $l\times n$ matrix. For a set $\boldsymbol{A}$, let $\mathrm{Im}\,\boldsymbol{A}$ be defined as

$$\mathrm{Im}\,\boldsymbol{A} \equiv \bigcup_{A\in\boldsymbol{A}} \{A\mathbf{u} : \mathbf{u}\in U^n\}$$

And we define sets $C_A(\mathbf{a})$ and $C_{AB}(\mathbf{a},\mathbf{b})$ as

$$C_A(\mathbf{a}) \equiv \{\mathbf{u} : A\mathbf{u}=\mathbf{a}\} \quad C_{AB}(\mathbf{a},\mathbf{b}) \equiv \{\mathbf{u} : A\mathbf{u}=\mathbf{a}, B\mathbf{u}=\mathbf{b}\}$$

In the context of linear codes, $C_A(\mathbf{a})$ is called a coset determined by $\mathbf{a}$. The random variables of a function A and a vector $\mathbf{a}$ are denoted by letters A and a, respectively. On the other hand, the random variable of a vector $\mathbf{u}$ is denoted by letter U when it is not used to represent a matrix.

Let μ_{UV} be the joint probability distribution of random variables U and V. Let μ_U and μ_V be the respective marginal distributions and $\mu_{U|V}$ be the conditional probability distribution. Let $H(U)$ and $H(U|V)$ be the entropy and the conditional entropy, respectively. A set of typical sequences $T_{U,\gamma}$ and a set of conditionally typical sequences $T_{U|V,\gamma}(\mathbf{v})$ are defined as

$$T_{U,\gamma} \equiv \{\mathbf{u} : D(v_{\mathbf{u}} \| \mu_U) < \gamma\}$$
$$T_{U|V,\gamma}(\mathbf{v}) \equiv \{\mathbf{u} : D(v_{\mathbf{u}|\mathbf{v}} \| \mu_{U|V} | v_{\mathbf{v}}) < \gamma\},$$

where $D(v_{\mathbf{u}} \| \mu_U)$ and $D(v_{\mathbf{u}|\mathbf{v}} \| \mu_{U|V} | v_{\mathbf{v}})$ are divergence and the conditional divergence. Moreover, $v_{\mathbf{u}}$ and $v_{\mathbf{u}|\mathbf{v}}$ are the empirical distribution of $\mathbf{u}$ and the conditional empirical distribution of $\mathbf{u}$ for a given $\mathbf{v}$, respectively.

In addition, we define $\chi(.)$ as follows

$$\chi(a\neq b) \equiv \begin{cases} 1 & \text{if } a\neq b \\ 0 & \text{if } a=b \end{cases}$$

For $\gamma,\gamma' > 0$, we defined

$$\lambda_U \equiv \frac{|U|\log[n+1]}{n}$$

$$\zeta_U(\gamma) \equiv \gamma - \sqrt{2\gamma}\log\frac{\sqrt{2\gamma}}{|U|} + \sqrt{2\gamma}\log|U|$$

$$\zeta_{U|V}(\gamma' | \gamma) \equiv \gamma' - \sqrt{2\gamma'}\log\frac{\sqrt{2\gamma'}}{|U||V|} + \sqrt{2\gamma}\log|U|$$

$$\eta_U(\gamma) \equiv -\sqrt{2\gamma}\log\frac{\sqrt{2\gamma}}{|U|} + \frac{|U|\log[n+1]}{n}$$

$$\eta_{U|V}(\gamma' | \gamma) \equiv -\sqrt{2\gamma'}\log\frac{\sqrt{2\gamma'}}{|U||V|} + \sqrt{2\gamma}\log|U| + \frac{|U||V|\log[n+1]}{n}$$

2.1. Strong Hash Property

In the following, we will briefly discuss the strong hash property for an ensemble of functions

which will be used later. It is introduced in [12] and requires stronger conditions than those introduced in [13].

Definition 1: Let $\boldsymbol{A} \equiv \{A_n\}_{n=1}^{\infty}$ be a sequence of sets such that A_n is a set of functions $A : \mathcal{U}^n \to \overline{\mathcal{U}}_{A_n}$ satisfying

$$\lim_{n\to\infty} \frac{\log(|\overline{\mathcal{U}}_{A_n}| / |\mathrm{Im}\, A_n|)}{n} = 0 \tag{1}$$

For a probability distribution $p_{A,n}$ on A_n, we call a sequence $(\boldsymbol{A}, \mathbf{p}_A) \equiv \{(A_n, p_{A,n})\}_{n=1}^{\infty}$ an ensemble. Then $(\boldsymbol{A}, \mathbf{p}_A)$ has a strong $(\alpha_A, \beta_A)-$hash property if there are two sequences $\alpha_A \equiv \{\alpha_A(n)\}_{n=1}^{\infty}$ and $\beta_A \equiv \{\beta_A(n)\}_{n=1}^{\infty}$ such that

$$\lim_{n\to\infty} \alpha_A(n) = 1, \tag{2}$$

$$\lim_{n\to\infty} \beta_A(n) = 0, \tag{3}$$

and

$$\sum_{\substack{\mathbf{u}' \in \mathcal{U}^n \setminus \{\mathbf{u}\} \\ p_{A,n}(\{A : A\mathbf{u} = A\mathbf{u}'\}) > \frac{\alpha_A(n)}{|\mathrm{Im}\, A_n|}}} p_{A,n}(\{A : A\mathbf{u} = A\mathbf{u}'\}) \le \beta_A(n) \tag{4}$$

for any $\mathbf{u} \in \mathcal{U}^n$. Throughout this paper, we omit the dependence of A, p_A, α_A, β_A on n.

Note that the conditions (1)-(4) require that the collision probability of the event is far greater than $1/|\mathrm{Im}\, A_n|$ vanishes as the block length goes to infinity.

We have the following related lemmas.

Lemma 1: If $(\boldsymbol{A}, \mathbf{p}_A)$ has a strong $(\alpha_A, \beta_A)-$hash property, then for any $T, T' \in \mathcal{U}^n$, we have

$$\sum_{\substack{\mathbf{u}' \in T' \\ \mathbf{u} \in T}} p_A(\{A : A\mathbf{u} = A\mathbf{u}'\}) \le |T \cap T'| + \frac{|T||T'|\alpha_A}{|\mathrm{Im}\, A|} + \min\{|T|, |T'|\}\beta_A, \tag{5}$$

We review the following lemma that is called the collision-resistant property, that is, if the number of bins is greater than the number of items then there is an assignment such that every bin contains at most one item.

Lemma 2: If $(\boldsymbol{A}, \mathbf{p}_A)$ satisfies (5), then for any $\mathfrak{g} \in \mathcal{U}^n$ and $\mathbf{u} \in \mathcal{U}^n$, we have

$$p_A(\{A : [\mathfrak{g} \setminus \{\mathbf{u}\}] \cap C_A(A\mathbf{u} \ne \varnothing)\}) \le \frac{|\mathfrak{g}|\alpha_A}{|\mathrm{Im}\, A|} + \beta_A,$$

where $\mathfrak{g}$ is the function satisfying

$$\mathfrak{g} \equiv \{\mathbf{u}' : \mu(\mathbf{u}') \ge \mu(\mathbf{u}), \mathbf{u}' \ne \mathbf{u}\}$$

Lemma 3: If $(\boldsymbol{A}, \mathbf{p}_A)$ satisfies (5), then

$$p_{A\mathbf{a}}(\{(A, \mathbf{a}) : T \cap C_A(\mathbf{a}) \ne \varnothing\}) \le \alpha_A - 1 + \frac{|\mathrm{Im}\, A|[\beta_A + 1]}{|T|}$$

Next, we will consider the combination of two ensembles, where functions have the same domain. Note that the assumption of a strong hash property makes it unnecessary to assume a function be linear.

Lemma 4: Assume that an ensemble $(\boldsymbol{A}, \mathbf{p}_A)$ has a strong $(\alpha_A, \beta_A)-$hash property and $(\boldsymbol{B}, \mathbf{p}_B)$ has a strong $(\alpha_B, \beta_B)-$hash property. Then, let p_{AB} be the joint distribution on $\boldsymbol{A} \times \boldsymbol{B}$ defined as

$$p_{AB}(A, B) = p_A(A) p_B(B)$$

for each $A \in \boldsymbol{A}$ and $B \in \boldsymbol{B}$. And $(\alpha_{AB}, \beta_{AB})$ is defined as

$$\alpha_{AB} = \alpha_A \times \alpha_B$$
$$\beta_{AB} = \beta_A + \beta_B$$

Then the ensemble $(\boldsymbol{A} \times \boldsymbol{B}, \mathbf{p}_{AB})$ can be defined as $(A, B)\mathbf{u} = (A\mathbf{u}, B\mathbf{u})$ for each $(A, B) \in \boldsymbol{A} \times \boldsymbol{B}$ and $\mathbf{u} \in \mathcal{U}^n$, which has a strong $(\alpha_{AB}, \beta_{AB})-$hash property.

Lemma 5: If $(\boldsymbol{A}, \mathbf{p}_A)$ satisfies (4), then for any function $f : \mathcal{U}^n \to [0, \infty]$, and $T \subset \mathcal{U}^n$, we have

$$E_A\left[\sum_{\mathbf{c}} \left| \frac{f(C_A(\mathbf{c})) \cap T}{f(T)} - \frac{1}{|\mathrm{Im}\, A|} \right|\right] \le \sqrt{\alpha_A - 1 + \frac{[\beta_A + 1]|\mathrm{Im}\, A| \max_{\mathbf{u} \in T} f(\mathbf{u})}{f(T)}},$$

where

$$f(T) \equiv \sum_{\mathbf{u} \in T} f(\mathbf{u})$$

3. Secrecy Capacity and Secure Degrees of Freedom of Z channel

In this section, we will derive the secrecy capacity and SDOF of Z channel with single antenna based on the idea of real interference alignment and cooperative jamming. We have the following theorem which will be proved in this section.

Theorem 1: The accurate sum SDOF of the Z channel with single antenna and confidential message is 1.

In this channel, each transmitter i intends to send a message W_i, uniformly chosen from a set $\mathcal{W}_i$, to receiver i. The rate of message is $R_i = \log|\mathcal{W}_i|/n$, where n presents the number of channel uses. Transmitter i uses a stochastic function $\phi_i : \mathcal{W}_i \rightarrow \mathbf{X}_i$ to encode the message, where $\mathbf{X}_i \triangleq X_i^n$ is the n-length channel input of user $i(i=1,2)$. We use boldface letters to denote n-length vector signals, e.g., $\mathbf{X}_i \triangleq X_i^n, \mathbf{Y}_i \triangleq Y_i^n$, etc. The legitimate receiver j decodes the message $\overline{W}_j$ based on its observation $\mathbf{Y}_j$. The rate (R_1, R_2) is said to be achievable if for any $\varepsilon > 0$ there exist joint n-length codes such that each receiver j can decode the corresponding message reliably, i.e., the probability of decoding error is less than ε as

$$P_r(W_i \neq \overline{W}_j) \leq \varepsilon \tag{6}$$

$$\frac{1}{n}H(W_2 \mid \mathbf{Y}_1) \geq \frac{1}{n}H(W_2) - \varepsilon \tag{7}$$

Then the sum SDOF is defined as

$$D_{s\Sigma} = \lim_{n\to\infty}\frac{C_s}{\frac{1}{2}\log P} = \lim_{n\to\infty}\frac{R_{s1}+R_{s1}}{\frac{1}{2}\log P}, \tag{8}$$

In the following, we will prove the theorem 1. Firstly, we will prove secrecy capacity and the upper bound of sum SDOF in theory. From the Lemma 1 in [9], the secrecy rate R_2 of the confidential message W_2 can be bounded by

$$\begin{aligned} nR_2 = H(W_2) &\leq h(\overline{\mathbf{X}}_2) = h(\mathbf{X}_2 + \overline{\mathbf{N}}_2) \\ &\leq h(\mathbf{Y}_1) - H(W_1) + nc_1 \end{aligned}, \tag{9}$$

By noting that $H(W_1) = nR_1$ and $H(\mathbf{Y}_1) = \frac{n}{2}\log P$ and c_1 is independent of P in (9), we have

$$R_1 + R_2 \leq \frac{1}{2}\log P + c_1 \tag{10}$$

Then, from the definition of secrecy capacity, we have

$$D_{s\Sigma} = \lim_{n\to\infty}\left[(R_1+R_2)/(\frac{1}{2}\log P)\right] \leq 1 \tag{11}$$

In the following, we discuss an achievable scheme for real Gaussian Z channel. Before the messages are encoded, the channel output can be wrote as

$$Y_1 = h_{11}X_1 + h_{12}X_2 + N_1 \quad Y_2 = h_{22}X_2 + N_2, \tag{12}$$

where the corresponding parameters are defined as the previous.

Let $\{V_1, U_1, U_2\}$ be mutually independent discrete random variables. Each of them is uniformly and independently drawn from the same constellation $C(a, Q)$, where a and Q will be specified later. Here, the role of U_i is to carry message W_i, and the role of V_1 is the cooperative jamming signal to help the transmitter-receiver pair 2. We choose the input signals of the transmitters as:

$$X_1 = U_1 + \frac{h_{12}}{h_{11}}V_1 \qquad X_2 = U_2$$

With these input signal selections, observations of the receivers are

$$Y_1 = h_{11}U_1 + h_{12}(U_2 + V_1) + N_1, \tag{13}$$

$$Y_2 = h_{22}U_2 + N_2, \tag{14}$$

Since, for V_1 and U_1 are not in the same dimension at receiver 1, we align V_1 in the dimension of U_2 such that U_2 is secure and U_1 can occupy a larger space, which is illustrated in Fig. 2.

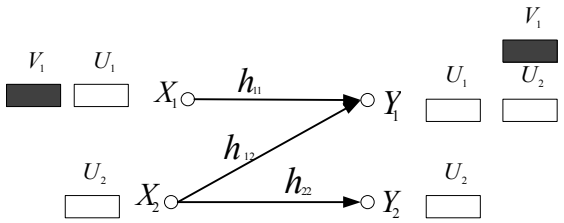

Fig. 2. Real interference alignment for real Gaussian Z channel.

By related theorem, we know that the following secrecy rate pair is achievable.

$$R_{s1} \geq I(U_1; Y_1), \tag{15}$$

$$R_{s2} \geq I(U_2; Y_2) - I(U_2; Y_1 \mid U_1), \tag{16}$$

The space observed at receiver 1 consists of $(2Q+1)(4Q+1)$ signal points. By using the Khintchine-Groshev theorem of Diophantine approximation in number theory, we can limit the

minimum distance $d_{\min}$ between points in the 1th receiver constellation as follow: For any δ>0, there exists a constant k_δ such that

$$d_{\min} \geq (k_\delta a / ((2Q)^{1+\delta})), \quad (17)$$

for almost all rationally independent $\{h_{11}, h_{12}\}$, except for a set of Lebesgue message zero. Then, we can upper bound the probability of decoding error of such a PAM scheme by considering the additive Gaussian noise at receiver 1 as follows,

$$\Pr(U_1 \neq \overline{U}_1) \leq \exp(-\frac{d_{\min}^2}{8}) \leq \exp(-\frac{k_\delta^2 a^2}{8(2Q)^{2(1+\delta)}}), \quad (18)$$

where $\overline{U}_1$ is the estimate for U_1 obtained by choosing the closest point in the constellation based on observation Y_1. For any δ>0, if we choose $Q = P^{(1-\delta)/(2(2+\delta))}$ and $a = \gamma P^{1/2} / Q$, where γ is a constant which is independent of P, then

$$\Pr(U_1 \neq \overline{U}_1) \leq \exp(-\frac{k_\delta^2 a^2}{8(2Q)^{2(1+\delta)}}) = \exp(-\frac{k_\delta^2 \gamma^2 P^\delta}{2^{2\delta+5}}), \quad (19)$$

From (19), we can have $\Pr(U_1 \neq \overline{U}_1) \to 0$ as $P \to \infty$. To satisfy the power constraint at the transmitters, we can simply choose $\gamma < \min\{1, 1/\sqrt{1+(h_{12}/h_{11})^2}\}$. By Fano's inequality and the Markov chain $U_1 \to Y_1 \to \overline{U}_1$, we know that

$$\begin{aligned} H(U_1 \mid Y_1) &\leq H(U_1 \mid \overline{U}_1) \\ &\leq 1 + \exp(-\frac{k_\delta^2 \gamma^2 P^\delta}{2^{2\delta+5}}) \log(2Q+1) \end{aligned}, \quad (20)$$

this means that

$$\begin{aligned} I(U_1; Y_1) &= H(U_1) - H(U_1 \mid Y_1) \geq H(U_1) - H(U_1 \mid \overline{U}_1) \\ &\geq [1 - \exp(-(k_\delta^2 \gamma^2 P^\delta))] \log(2Q+1) + o(\log P) \end{aligned}, \quad (21)$$

Combining (15) and (21), we obtain

$$R_{s1} \geq \frac{1-\delta}{2+\delta}(\frac{1}{2}\log P) + o(\log P), \quad (22)$$

By applying this same analysis to rate R_{s2}, we can also have $\Pr(U_2 \neq \overline{U}_2) \to 0$ as $P \to \infty$ and

$$\begin{aligned} R_{s2} &\geq I(U_2; \mathbf{Y}_2) - I(U_2; \mathbf{Y}_1 \mid U_1) \\ &\geq \frac{1-\delta}{2+\delta}(\frac{1}{2}\log P) + o(\frac{1}{2}\log P) \end{aligned}, \quad (23)$$

Then, by choosing δ arbitrarily small, we can achieve that

$$D_{s\Sigma} = \lim_{n\to\infty} \frac{C_s}{\frac{1}{2}\log P} = \lim_{n\to\infty} \frac{R_{s1} + R_{s2}}{\frac{1}{2}\log P} \geq 1 \quad (24)$$

By combining (11) and (24), we can derive that the accurate upper bound of sum SDOF of Gaussian Z channel with single antenna is 1. Then we completely prove the theorem 1.

4. Secure Pre-coding Scheme Based on Strong Hash Property for Gaussian Z Channel

In the scenario of two-user frequency selection Gaussian Z channel, each of two transmitters has an independent message for each receiver. The channel output at the jth receiver over the fth slot and the tth time slot is described as follows:

$$\begin{aligned} Y_1(f,t) &= h_{11}(f)X_1(f,t) + h_{12}(f)X_2(f,t) + N_1(f,t) \\ Y_2(f,t) &= h_{22}(f)X_2(f,t) + N_2(f,t) \end{aligned}$$

where $X_i(f,t)$ is the input signal at transmitter i, $h_{ji}(f)$ is the channel coefficient from transmitter i to receiver j and $N_i(f,t)$ represents the additive white Gaussian noise (AWGN) at receiver i. We assume that channel coefficients vary across frequency slots but remain constant in time and are drawn from a continuous distribution. We assume all channel coefficients are known to all transmitters and receivers. Using the symbol extension channel, the input-output relationship is characterized as follows:

$$\overline{\mathbf{Y}}_1(t) = \overline{\mathbf{H}}_{11}\overline{\mathbf{X}}_1(t) + \overline{\mathbf{H}}_{12}\overline{\mathbf{X}}_2(t) + \overline{\mathbf{N}}_1(t), \quad (25)$$

$$\overline{\mathbf{Y}}_2(t) = \overline{\mathbf{H}}_{22}\overline{\mathbf{X}}_2(t) + \overline{\mathbf{N}}_2(t), \quad (26)$$

where $\overline{\mathbf{X}}_i(t)$ is the $F \times 1$ column vector representing the $F = 2n$ symbol extension of the transmitted symbol $X_i(t)$, i.e., $\overline{\mathbf{X}}_i(t) = [X_i(1,t), ..., X_i(F,t)]^T$. Similarly, $\overline{\mathbf{Y}}_j(t)$ and $\overline{\mathbf{N}}_j(t)$ represent symbol extension of Y_j and N_j, respectively. $\overline{\mathbf{H}}_{ji}$ is the $F \times F$ diagonal matrix representing the extension of the channel, i.e.,

$$\overline{\mathbf{H}}_{ji} = \begin{pmatrix} h_{ji}(1) & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & h_{ji}(F) \end{pmatrix}_{F\times F}$$

Over the F symbol extension channel, message W_i is encoded at transmitter i into $m_i = n$ independent streams $\mathbf{X}_i(t)$, which is a $n \times 1$ vector. It should be noted that the following coding scheme introduces randomness to ensure the secrecy. Then

transmitter i employs the interference alignment scheme mapping $\mathbf{X}_i(t)$ into $\overline{\mathbf{X}}_i(t)=\mathbf{V}_i(t)\mathbf{X}_i(t)$ where $\mathbf{V}_i(t)$ is the $F\times m_i$ matrix. At last, transmitter i sends the signal into the channel. While how to choose the pre-coding matrices will be discussed later.

So that the desired signal vectors span a signal space which is disjoint with the space spanned by the interference vectors at each receiver. Therefore, each receiver can decode its desired data streams by zero forcing the interference.

In the following, we will address how to choose pre-coding matrices. To make transmitter 1 can send the message W_1 with the optimal sub-channels, $\mathbf{V}_1(t)$ is formed from the maximum n right singular vectors of the matrix $\overline{H}_{11}$. In addition, to enhance the sum secrecy capacity of this system, we make joint generalized singular value decomposition on channel matrixes of $\overline{H}_{12}$ and $\overline{H}_{22}$ as follows

$$\overline{\mathbf{H}}_{22}\mathbf{A}_2=\mathbf{E}_{r2}\mathbf{C}, \tag{27}$$

$$\overline{\mathbf{H}}_{12}\mathbf{A}_2=\mathbf{E}_{e2}\mathbf{D}, \tag{1}$$

to return them into unitary matrices $\mathbf{E}_{r2}\in\mathbb{C}^{F\times F}$ and $\mathbf{E}_{e2}\in\mathbb{C}^{F\times F}$, where $\mathbf{A}_2$ is a matrix such that $\mathbf{A}_2\in\mathbb{C}^{n\times n}$. Moreover, the nonzero elements of $\mathbf{C}$ are in ascending order while the nonzero elements of $\mathbf{D}$ are in decreasing order, and $\mathbf{C}^T\mathbf{C}+\mathbf{D}^T\mathbf{D}=\mathbf{I}$. Letting c_i and d_i represent the ith diagonal elements of $\mathbf{C}^T\mathbf{C}$ and $\mathbf{D}^T\mathbf{D}$, respectively. We see that from the viewpoint of maximizing secrecy capacity, it is clear that only those sub-channels for which $c_i>d_i$ should be used to carry the confidential information, since for these sub-channels, the information of transmitter 1 which is a potential eavesdropper is degraded compared with the desired recipient. To this end, we choose the matrix $\mathbf{V}_2(t)$ as n column vectors of the matrix $\mathbf{A}_2$, where these vectors should satisfy $c_i>d_i$. At last, receiver i obtain corresponding signal $\mathbf{X}_i(t)$ and then recover related message from it.

In the following, we will focus on how to achieve secrecy pre-coding for this system, that is, how to generate signal $\mathbf{X}_i(t)$ at transmitter i.

Transmitter i has the message W_i intended for receiver i, which results a total of two independent messages. An (M_1,M_2,N,F,P_e) code for the Z channel consists of the following:

1) Two independent message sets $\mathcal{W}_i=\{1,2,...,M_i\}$;

2) Two encoding functions $\varphi_i:\mathbf{m}_i\to\overline{\mathbf{X}}_i^N$, where $\overline{\mathbf{X}}_i^N=[\mathbf{X}_i(1),...,\mathbf{X}_i(N)]$, which map the message $w_i\in\mathbf{m}_i$ to transmitted symbols. Each transmitter has a power constraint, e.g., $\frac{1}{NF}\sum_{f=1}^{F}\sum_{t=1}^{N}\left|X_i(f,t)\right|^2\le P, i\in\{1,2\}$;

3) two decoding functions $\psi_i:\overline{\mathbf{Y}}_i^N\to\mathcal{W}_i$, which map the received sequence $\overline{\mathbf{Y}}_i^N$ to the decoded message $\overline{w}_i\in\mathbf{m}_i$. The average probability of decoding error $P_{e,i}$ for receiver i is defined as $P_{e,i}=\frac{1}{M_i}\sum_{w_i\in\mathbf{m}_i}\Pr(\phi_i(\mathbf{Y}_i\neq w_i\mid w_i \text{ is sent}))$.

We define two types of secrecy measure. The first is the variation distance $d(p_{M_2Y_1^n},p_{M_2}\times p_{Y_1^n})$, where $p_{M_2}\times p_{Y_1^n}(m_2,\mathbf{Y}_1)\equiv p_{M_2}(m_2)p_{Y_1^n}(\mathbf{Y}_1)$. The second is the mutual information $I(M_2;\mathbf{Y}_1^n)$ We call the coding scheme asymptotically perfectly secure with respect to the variation distance or the mutual information if any one of them goes to zero as the block length n goes to infinity.

In the following, we will illustrate how to generate codeword in detail, which can be illustrated as in Fig. 3. We will focus on secrecy pre-coding scheme for the two transmitters to generate encoded signal $X_i(t)$. To be simple, we omit time slot when it not be explained specifically.

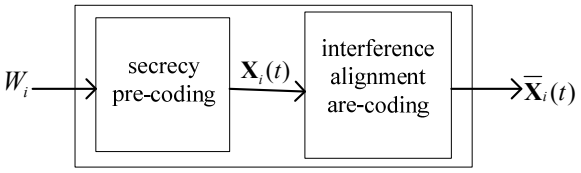

Fig. 3. Coding scheme for transmitters.

First, security pre-coding is made on transmitter 1 to achieve optimal capacity. We assume that $\mu_{\mathbf{X}_1}$ is given. Let $A_1\in\mathcal{A}_1$ and $B_1\in\mathcal{B}_1$ be functions $A_1:\chi^n\to\chi^{l_{A_1}}$ and $B_1:\chi^n\to\chi^{l_{B_1}}$, where l_{A_1} and l_{B_1} are defined as

$$l_{A_1}\equiv\frac{n[H(\mathbf{X}_1\mid\mathbf{Y}_1)+\varepsilon_{A_1}]}{\log|\chi|}$$

$$l_{B_1}\equiv\frac{n[I(\mathbf{X}_1;\mathbf{Y}_1)-\varepsilon_{B_1}]}{\log|\chi|}$$

For a given vector $\mathbf{a}\in\chi^{l_{A_1}}$, let $\mathcal{W}_{\mathbf{X}_1,\gamma}(A_1,B_1,\mathbf{a},\mathbf{m}_1)$ be the set $\left\{0,...,\left|T_{\mathbf{X}_1,\gamma}\cap C_{A_1B_1}(\mathbf{a},\mathbf{m}_1)-1\right|\right\}$ and we define:

$g_{A_1B_1}(\mathbf{a},\mathbf{m}_1,.):\mathcal{W}_{\mathbf{X}_1,\gamma}(A_1,B_1,\mathbf{a},\mathbf{m}_1)\to T_{\mathbf{X}_1,\gamma}\cap C_{A_1B_1}(\mathbf{a},\mathbf{m}_1)$. In addition, let W_1 be the random variable corresponding to the message $\mathbf{m}_1$, where the probability $p_{M_1}(\mathbf{m}_1)$ is uniform distribution on $\mathrm{Im}\,\mathcal{B}_1$. We construct a stochastic encoder by using a random number $W_1\in\mathcal{W}_{\mathbf{X}_1,\gamma}(A_1,B_1,\mathbf{a},\mathbf{m}_1)$ generated from the distribution $p_{W_1|M_1}(.|\mathbf{m}_1)$ for each $\mathbf{m}_1\in\mathrm{Im}\,\mathcal{B}_1$. We define the stochastic encoder $\phi_1:\chi^{l_{B_1}}\to\chi^n$ and the decoder $\psi_1:y^n\to\chi^{l_{B_1}}$ as

$$\phi_1(\mathbf{m}_1)\equiv g_{A_1B_1}(\mathbf{a},\mathbf{m}_1)$$
$$\psi_1(\mathbf{m}_1)\equiv B_1 g_{A_1}(\mathbf{a}\,|\,\mathbf{Y}_1)$$

where

$$g_{A_1B_1}(\mathbf{a},\mathbf{m}_1)\equiv\arg\min_{\mathbf{X}_1'\in C_{A_1B_1}(\mathbf{a},\mathbf{m}_1)}\mu_{\mathbf{X}_1}(\mathbf{X}_1')$$
$$g_{A_1}(\mathbf{a}\,|\,\mathbf{Y}_1)\equiv\arg\min_{\mathbf{X}_1'\in C_{A_1}(\mathbf{a})}\mu_{\mathbf{X}_1Y_1}(\mathbf{X}_1'\,|\,\mathbf{Y}_1)$$

Then rate R_1 of this secure pre-coding is given by $R_1\equiv|\mathrm{Im}\,\mathcal{B}_1|/n$ and the decoding error of probability is as follows

$$\Pr_{Y_1|X_1}(A_1,B_1,\mathbf{a})\equiv\sum_{\mathbf{m}_1,\mathbf{Y}_1}[p_M(\mathbf{m}_1)\mu_{Y_1|X_1}(\mathbf{Y}_1\,|\,\psi_1(\mathbf{m}_1))\times\chi(\psi_1(\mathbf{Y}_1)\neq\mathbf{m}_1)]$$

What's more, we provide an intuitive interpretation of the construction of the code, which is illustrated in Fig. 4.

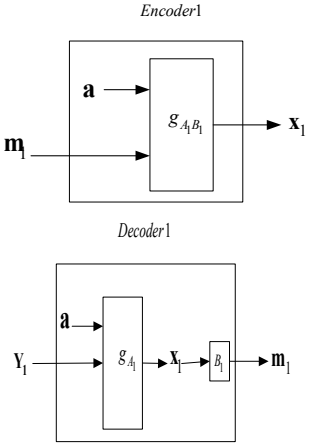

Fig. 4. Security pre- coding scheme for Transmitter 1.

We assume that $\mathbf{a}$ is shared by the encoder and the decoder 1. For $\mathbf{a}$ and a message $\mathbf{m}_1$, the function $g_{A_1B_1}$ generates a typical sequence $\mathbf{X_1}\in T_{X_1,\gamma}$ as a channel input. The decoder reproduces the channel input $\mathbf{X_1}$ by using g_{A_1} from $\mathbf{a}$ and a channel output $\mathbf{Y}_1$. Since $(\mathbf{X_1},\mathbf{Y_1})$ is jointly typical and $B_1\mathbf{X}_1=\mathbf{m}_1$, the decoding will succeed if the amount of information of $\mathbf{a}$ is greater than $H(\mathbf{X}_1\,|\,\mathbf{Y}_1)$ to satisfy the collision-resistant property. On the other hand, the total rate of $\mathbf{a}$ and $\mathbf{m}_1$ should be less than $H(\mathbf{X}_1)$ to satisfy the saturating property. Then, we can set the encoding rate of $\mathbf{m}_1$ be close to $I(\mathbf{X}_1;\mathbf{Y}_1)$. Here we describe the channel secure coding in Lemma 6 for transmitter 1 as follows.

Lemma 6: Let $\mu_{Y_1|X_1}$ be the conditional probability distribution of transmitter 1. For given $\varepsilon_{A_1},\varepsilon_{B_1}>0$ satisfying $\zeta_{y|\chi}(3[\varepsilon_{B_1}-\varepsilon_{A_1}]\,|\,3[\varepsilon_{B_1}-\varepsilon_{A_1}])<\varepsilon_{A_1}<\varepsilon_{B_1}$. We assume that $(\boldsymbol{A},\mathbf{p}_A)$ and $(\boldsymbol{A}\times\boldsymbol{B},\mathbf{p}_{A_1B_1})$ have hash property.

Then, for all $\delta>0$ and sufficiently large n, there are functions (sparse matrices) $A_1\in\mathcal{A}_1$, $B_1\in\mathcal{B}_1$ and a vector $\mathbf{a}\in\mathrm{Im}\,\mathcal{A}_1$ such that

$$R_1\geq I(\mathbf{X}_1;\mathbf{Y}_1)-\varepsilon_{B_1}-\delta, \tag{29}$$

$$\Pr_{Y_1|X_1}(A_1,B_1,\mathbf{a})<\delta, \tag{30}$$

This lemma can be similarly proved as theorem 3 in [13]. Then form it, the rate of the proposed code is close to the capacity of transmitter-receiver 1 as $\varepsilon_{B_1},\delta\to0$.

Next, we analysis the security pre-coding scheme for transmitter 2 to enhance secrecy capacity. In the following, we assume that for a given $\mu_{Y_1Y_2|X_2}$ there is μ_{X_2} such that

$$I(\mathbf{X}_2;\mathbf{Y}_2)>I(\mathbf{X}_2;\mathbf{Y}_1\,|\,\mathbf{X}_1), \tag{31}$$

Let $A_2\in\mathcal{A}_2$ and $B_2\in\mathcal{B}_2$ be functions $A_2:\chi^n\to\chi^{l_{A_2}}$ and $B_2:\chi^n\to\chi^{l_{B_2}}$, where l_{A_2} and l_{B_2} are defined as

$$l_{A_2}\equiv\frac{n[H(\mathbf{X}_2\,|\,\mathbf{Y}_2)+\varepsilon_{A_2}]}{\log|\chi|}$$
$$l_{B_2}\equiv\frac{n[I(\mathbf{X}_2;\mathbf{Y}_2)-I(\mathbf{X}_2;\mathbf{Y}_1\,|\,\mathbf{X}_1)-\varepsilon_{B_2}]}{\log|\chi|}$$

For a given $\mathbf{b}\in\mathrm{Im}\,\mathcal{A}_2$ and $\mathbf{m}_2\in\mathrm{Im}\,\mathcal{B}_2$, let $\mathcal{W}_{X_2,\gamma}(A_2,B_2,\mathbf{b},\mathbf{m}_2)\equiv\{0,...,|T_{X_2,\gamma}\cap C_{A_2B_2}(\mathbf{b},\mathbf{m}_2)|-1\}$ and $g_{A_2B_2}(\mathbf{b},\mathbf{m}_2):\mathcal{W}_{X_2,\gamma}(A_2,B_2,\mathbf{b},\mathbf{m}_2)\to T_{X_2,\gamma}\cap C_{A_2B_2}(\mathbf{b},\mathbf{m}_2)$ be a bijection. Let $p_{M_2}(\mathbf{m}_2)$ be uniformly distribution on $\mathrm{Im}\,\mathcal{B}_2$. For a given $\mathbf{b}\in\mathrm{Im}\,\mathcal{A}_2$ and $\mathbf{m}_2\in\mathrm{Im}\,\mathcal{B}_2$, let $p_{W_2|M_2}(.|\mathbf{m}_2)$ be uniformly distribution on $\mathcal{W}_{X_2,\gamma}(A_2,B_2,\mathbf{b},\mathbf{m}_2)$ for each $\mathbf{m}_2\in\mathrm{Im}\,\mathcal{B}_2$.

We then similarly construct a stochastic encoder and decoder for transmitter 2 as $\phi_2 : \chi^{l_{B_2}} \to \chi^n$ and $\psi_2 : y^n \to \chi^{l_{B_2}}$ as

$$\phi_2(\mathbf{m}_2) \equiv g_{A_2B_2}(\mathbf{b}, \mathbf{m}_2, W_2) \quad \psi_2(\mathbf{m}_2) \equiv B_2 g_{A_2}(\mathbf{b} \mid \mathbf{Y}_2)$$

Here, we omit how to encode and decode the message W_2 since it is similar to the previous. So we can have the rate of this code as $R_2 \equiv \left|\mathrm{Im}\, B_2\right| / n$. Moreover, by assuming (31), the rate goes to $I(\mathbf{X}_2;\mathbf{Y}_2) - I(\mathbf{X}_2;\mathbf{Y}_1 \mid \mathbf{X}_1) - \varepsilon_{B_2}$ as $n \to \infty$. We then have the following theorem.

Theorem 2: Let $\mu_{Y_1Y_2|X_2}$ be the conditional probability distribution of this channel and assume that μ_{X_2} and $\mu_{Y_1Y_2|X_2}$ satisfy (31). Assume that ensembles $\left(\boldsymbol{A}_2, \mathbf{p}_{A_2}\right)$ and $\left(\boldsymbol{A}_2 \times \boldsymbol{B}_2, \mathbf{p}_{A_2B_2}\right)$ have strong hash property when positive parameters ε_{A_2} and ε_{B_2} are given. Then for any $\delta > 0$ and all sufficiently large n, there are $\varepsilon_{B_2} > \varepsilon_{A_2} > 0$, functions (sparse matrices) $A_2 \in \mathcal{A}_2$, $B_2 \in \mathcal{B}_2$ and a vector $\mathbf{b} \in \mathrm{Im}\, A_2$ such that

$$R_2 \equiv \left[\left|\mathrm{Im}\, B_2\right| / n\right] \geq I(\mathbf{X}_2;\mathbf{Y}_2) - I(\mathbf{X}_2;\mathbf{Y}_1 \mid \mathbf{X}_1) - \varepsilon_{B_2} - \delta \quad (32)$$

$$\Pr(\psi_2(\mathbf{Y}_2^n) \neq M_2) < \delta \quad (33)$$

$$d(p_{M_2Y_1^n}, p_{M_2} \times p_{Y_1^n}) < \delta \quad (34)$$

Furthermore, if

$$\max\left\{\sqrt{\alpha_{A_2B_2} - 1}, \beta_{A_2}\right\} = o(\frac{1}{n}), \quad (35)$$

then

$$I(M_2;\mathbf{Y}_1^n) \to 0, \quad (36)$$

for any $\delta > 0$ and sufficiently large n.

It is shown in theorem 2 that when time slot $N \to \infty$ and number of channel use $2n \to \infty$, by choosing sufficient small δ the proposed scheme can achieve secrecy capacity for transmitter 2. Based on the definition between capacity and secure degrees of freedom, the achievable rate for each message is as follows

$$R_{s1} = \frac{1}{F} I(\mathbf{X}_1;\overline{\mathbf{Y}}_1) = \frac{1}{2}(\log P) + o(\log P) = \frac{1}{2}(\log P) \quad (37)$$

$$\begin{aligned} R_{s2} &= \frac{1}{F} I(\mathbf{X}_2;\overline{\mathbf{Y}}_2) - \frac{1}{2F} I(\mathbf{X}_2;\overline{\mathbf{Y}}_1 \mid \mathbf{X}_1) \\ &= \frac{1}{2}(\log P) + o(\log P) \end{aligned} \quad (38)$$

Then, the corresponding SDOF can be shown as

$$D_{s\Sigma} = \lim_{n\to\infty} \frac{R_{s1} + R_{s2}}{\frac{1}{2}\log P} \geq 1 \quad (39)$$

It is shown that the proposed scheme can achieve the upper bound of SDOF by combining (39) and theorem 1.

5. Conclusion

In this paper, we study secure communication of Gaussian Z channel with single antenna. We make two contributions. The first one is that we give specific proof for SDOF of Gaussian Z channel in theory, propose an achievable scheme for real Gaussian Z channel with single antenna through cooperative jamming and real interference alignment and then obtain accurate SDOF of Gaussian Z channel with single antenna. And the other one is that we propose a security pre-coding scheme based on hash property for frequency selection Gaussian Z channel with single antenna. At the same time, we then use interference alignment technology to address interference, choose the optimal sub-channels and reduce complexity for receivers. In future work, we will focus on secrecy capacity and SDOF of MIMO Gaussian Z channel.

Appendix A

Applying Lemma 5 by letting $f(\mathbf{X}_2)$ be the uniform distribution on $T_{\mathbf{X}_2,\gamma}$, we have

$$\begin{aligned} &E_{A_2B_2}\left[\sum_{\mathbf{b},\mathbf{m}_2}\left|\frac{\left|T_{\mathbf{X}_2,\gamma} \cap C_{A_2B_2}(\mathbf{b},\mathbf{m}_2)\right|}{\left|T_{\mathbf{X}_2,\gamma}\right|} - \frac{1}{\left|\mathrm{Im}\, A_2\right|\left|\mathrm{Im}\, B_2\right|}\right|\right] \\ &\leq \sqrt{\alpha_{A_2B_2} - 1 + \frac{\left[\beta_{A_2B_2} + 1\right]\left|\mathrm{Im}\, A_2\right|\left|\mathrm{Im}\, B_2\right|}{\left|T_{\mathbf{X}_2,\gamma}\right|}} \end{aligned} \quad (40)$$

It implies that there is a pair (A_2, B_2) of functions that is the balanced coloring function of $T_{\mathbf{X}_2,\gamma}$. Then we focus on the proving of theorem 2. First, we have

$$\begin{aligned} &E_{A_2B_2\mathbf{b}}\left[\Pr(\psi_2(\mathbf{Y}_2^n) \neq M_2)\right] \leq 2^{-n[\gamma - \lambda_{\chi y}]} + \\ &E_{A_2B_2}\left[\sum_{\mathbf{b},\mathbf{m}_2}\left|\frac{\left|T_{\mathbf{X}_2,\gamma} \cap C_{A_2B_2}(\mathbf{b},\mathbf{m}_2)\right|}{\left|T_{\mathbf{X}_2,\gamma}\right|} - \frac{1}{\left|\mathrm{Im}\, A_2\right|\left|\mathrm{Im}\, B_2\right|}\right|\right] \\ &+ \frac{\left|\left\{\mathbf{X}_2' : \mu_{X_2|Y_2X_1}(\mathbf{X}_2' \mid \mathbf{Y}_2\mathbf{X}_1) \geq 2^{-n[H(\mathbf{X}_2|\mathbf{Y}_2\mathbf{X}_1)] + \zeta_{\chi|y}(2\gamma|2\gamma)}\right\}\right|\alpha_{A_2}}{\left|\mathrm{Im}\, A_2\right|} \\ &+ \beta_{A_2} \end{aligned} \quad (41)$$

Then, we evaluate $E_{A_2B_2\mathbf{b}}[d(p_{M_2Y_1^n}, p_{M_2}\times p_{Y_1^n})]$. At first, the joint distribution $p_{M_2Y_1^n}(\mathbf{m}_2,\mathbf{Y}_1)$ is given as

$$p_{M_2Y_1^n}(\mathbf{m}_2,\mathbf{Y}_1)=\sum_{\mathbf{w}_2}\frac{\mu_{Y_1|X_1,X_2}(\mathbf{Y}_1\mid g_{A_2B_2}(\mathbf{b},\mathbf{m}_2,\mathbf{w}_2))}{|\mathrm{Im}\,B_2|\left|T_{\mathbf{X}_2,\gamma}\cap C_{A_2B_2}(\mathbf{b},\mathbf{m}_2)\right|},$$
$$=\sum_{\mathbf{X}_2\in T_{\mathbf{X}_2,\gamma}\cap C_{A_2B_2}(\mathbf{b},\mathbf{m}_2)}\frac{\mu_{Y_2|X_1,X_2}(\mathbf{Y}_1\mid\mathbf{X}_2,\mathbf{X}_1)}{|\mathrm{Im}\,B_2|\left|T_{\mathbf{X}_2,\gamma}\cap C_{A_2B_2}(\mathbf{b},\mathbf{m}_2)\right|} \quad (42)$$

where the second equality comes from the fact that $g_{A_2B_2}(\mathbf{b},\mathbf{m}_2,.)$ is bijective. The marginal distribution $p_{\mathbf{Y}_1^n}$ is given as

$$p_{\mathbf{Y}_1^n}(\mathbf{Y}_1)\equiv\sum_{\mathbf{m}_2,\mathbf{X}_2\in T_{\mathbf{X}_2,\gamma_1}\cap C_{A_2B_2}(\mathbf{b},\mathbf{m}_2)}\frac{\mu_{Y_1|X_1,X_2}(\mathbf{Y}_1\mid\mathbf{X}_1,\mathbf{X}_2)}{\left|T_{\mathbf{X}_2,\gamma}\cap C_{A_2B_2}(\mathbf{b},\mathbf{m}_2)\right||\mathrm{Im}\,B_2|}$$

Let

$$p_{\overline{Y}_1^n}(\mathbf{Y}_1)\equiv\sum_{\mathbf{X}_2\in T_{\mathbf{X}_2,\gamma}}\frac{\mu_{Y_1|X_1,X_2}(\mathbf{Y}_1\mid\mathbf{X}_1,\mathbf{X}_2)}{\left|T_{\mathbf{X}_2,\gamma}\right|}$$

$$p_{\mathbf{Y}_1^n((A_2,B_2,\mathbf{b},\mathbf{m}_2))}(\mathbf{Y}_1)\equiv\sum_{\mathbf{X}_2\in T_{\mathbf{X}_2,\gamma}\cap C_{A_2B_2}(\mathbf{b},\mathbf{m}_2)}\frac{\mu_{Y_1|X_1,X_2}(\mathbf{Y}_1\mid\mathbf{X}_1,\mathbf{X}_2)}{\left|T_{\mathbf{X}_2,\gamma}\cap C_{A_2B_2}(\mathbf{b},\mathbf{m}_2)\right|}$$

$$p_{\overline{\mathbf{Y}}_1^n((A_2,B_2,\mathbf{b},\mathbf{m}_2))}(\mathbf{Y}_1)\equiv\sum_{\mathbf{X}_2\in T_{\mathbf{X}_2,\gamma}\cap C_{A_2B_2}(\mathbf{b},\mathbf{m}_2)}\Big[|\mathrm{Im}\,A_2||\mathrm{Im}\,B_2|\times\mu_{Y_1|X_1,X_2}(\mathbf{Y}_1\mid\mathbf{X}_1,\mathbf{X}_2))/\left|T_{\mathbf{X}_2,\gamma}\right|\Big]$$

Then we have

$$d(p_{M_2Y_1^n},p_{M_2}\times p_{Y_1^n})=\sum_{\mathbf{m}_2,\mathbf{Y}_1}\left(\frac{1}{|\mathrm{Im}\,B_2|}\left|p_{Y_1^n((A_2,B_2,\mathbf{b},\mathbf{m}_2))}(\mathbf{Y}_1)-p_{Y_1^n}(\mathbf{Y}_1)\right|\right)$$
$$\le\sum_{\mathbf{m}_2,\mathbf{Y}_1}\frac{1}{|\mathrm{Im}\,B_2|}\left|p_{Y_1^n((A_2,B_2,\mathbf{b},\mathbf{m}_2))}(\mathbf{Y}_1)-p_{\overline{Y}_1^n}(\mathbf{Y}_1)\right|+\sum_{\mathbf{Y}_1}\left|p_{\overline{Y}_1^n}(\mathbf{Y}_1)-p_{Y_1^n}(\mathbf{Y}_1)\right| \quad (43)$$
$$\le 2\sum_{\mathbf{m}_2,\mathbf{Y}_1}\frac{1}{|\mathrm{Im}\,B_2|}\left|p_{Y_1^n(A_2,B_2,\mathbf{b},\mathbf{m}_2)}(\mathbf{Y}_1)-p_{\overline{Y}_1^n}(\mathbf{Y}_1)\right|$$
$$\le 2\sum_{\mathbf{m}_2,\mathbf{Y}_1}\frac{1}{|\mathrm{Im}\,B_2|}\left|p_{\mathbf{Y}_1^n((A_2,B_2,\mathbf{b},\mathbf{m}_2))}(\mathbf{Y}_1)-p_{\overline{\mathbf{Y}}_1^n((A_2,B_2,\mathbf{b},\mathbf{m}_2))}(\mathbf{Y}_1)\right|$$
$$+2\sum_{\mathbf{m}_2,\mathbf{Y}_1}\frac{1}{|\mathrm{Im}\,B_2|}\left|p_{\overline{\mathbf{Y}}_1^n((A_2,B_2,\mathbf{b},\mathbf{m}_2))}(\mathbf{Y}_1)-p_{\overline{\mathbf{Y}}_1^n}(\mathbf{Y}_1)\right|$$

In the following, we evaluate the average of the first term in (43) as

$$E_{A_2B_2\mathbf{b}}\left[\sum_{\mathbf{m}_2,\mathbf{Y}_1}\frac{1}{|\mathrm{Im}\,B_2|}\left|p_{\mathbf{Y}_1^n((A_2,B_2,\mathbf{b},\mathbf{m}_2))}(\mathbf{Y}_1)-p_{\overline{\mathbf{Y}}_1^n((A_2,B_2,\mathbf{b},\mathbf{m}_2))}(\mathbf{Y}_1)\right|\right]$$
$$\le E_{A_2B_2}\left[\sum_{\mathbf{b},\mathbf{m}_2,\mathbf{Y}_1}\sum_{\mathbf{X}_2\in T_{\mathbf{X}_2,\gamma}\cap C_{A_2B_2}(\mathbf{b},\mathbf{m}_2)}\left(\frac{\mu_{Y_1|X_1,X_2}(\mathbf{Y}_1\mid\mathbf{X}_1,\mathbf{X}_2)}{|\mathrm{Im}\,A_2||\mathrm{Im}\,B_2|}\times\left|\frac{1}{\left|T_{\mathbf{X}_2,\gamma}\cap C_{A_2B_2}(\mathbf{b},\mathbf{m}_2)\right|}-\frac{|\mathrm{Im}\,A_2||\mathrm{Im}\,B_2|}{\left|T_{\mathbf{X}_2,\gamma}\right|}\right|\right)\right] \quad (44)$$
$$=E_{A_2B_2}\left[\sum_{\mathbf{b},\mathbf{m}_2}\left|\frac{\left|T_{\mathbf{X}_2,\gamma}\cap C_{A_2B_2}(\mathbf{b},\mathbf{m}_2)\right|}{\left|T_{\mathbf{X}_2,\gamma}\right|}-\frac{1}{|\mathrm{Im}\,A_2||\mathrm{Im}\,B_2|}\right|\right]$$

We define the following function

$$f(\mathbf{X}_2\mid\mathbf{Y}_1)\equiv\begin{cases}\dfrac{\mu_{Y_1|X_1,X_2}(\mathbf{Y}_1\mid\mathbf{X}_1,\mathbf{X}_2)}{\left|T_{\mathbf{X}_2,\gamma}\right|p_{\overline{\mathbf{Y}}_1^n}(\mathbf{Y}_1)}, & \text{if } \mathbf{X}_2\in T_{\mathbf{X}_2,\gamma}\\ 0 & \text{if } \mathbf{X}_2\notin T_{\mathbf{X}_2,\gamma}\end{cases}$$
$$T(\mathbf{Y}_1)\equiv\left\{\mathbf{X}_2\in T_{\mathbf{X}_2,\gamma}:\mathbf{Y}_1\in T_{Y_1|X_2,X_1,\gamma}(\mathbf{X}_2)\right\}$$

By applying Lemma 25 in [12], we have

$$E_{\overline{Y}_1^n}\left[f([T(\overline{Y}_1^n)]^c\cap T_{\mathbf{X}_2,\gamma}\mid\overline{Y}_1^n)\right]$$
$$\le\sum_{\mathbf{X}_2\in T_{\mathbf{X}_2,\gamma}}\sum_{\mathbf{Y}_1\notin T_{Y_1|X_1X_2}\gamma(\mathbf{X}_2)}\frac{\mu_{Y_1|X_1,X_2}(\mathbf{Y}_1\mid\mathbf{X}_1,\mathbf{X}_2)}{\left|T_{\mathbf{X}_2,\gamma}\right|} \quad (45)$$
$$\le 2^{-n\left[\gamma-\lambda_{\chi\gamma_1}\right]}$$

Then we evaluate the second term in (43) as

$$E_{A_2B_2\mathbf{b}}\left[\sum_{\mathbf{m}_2,\mathbf{Y}_1}\frac{1}{|\mathrm{Im}\,B_2|}\left|p_{\overline{Y}_1^n((A_2,B_2,\mathbf{b},\mathbf{m}_2))}(\mathbf{Y}_1)-p_{\overline{Y}_1^n}(\mathbf{Y}_1)\right|\right]$$
$$=E_{A_2B_2\overline{Y}_1^n}[\sum_{\mathbf{b},\mathbf{m}_2}\left|f(T_{\mathbf{X}_2,\gamma}\cap C_{A_2B_2}(\mathbf{b},\mathbf{m}_2)\mid\overline{Y}_1^n)-\frac{1}{|\mathrm{Im}\,A_2||\mathrm{Im}\,B_2|}\right|]$$
$$\le E_{A_2B_2\overline{Y}_1^n}\left[\sum_{\mathbf{b},\mathbf{m}_2}\left|f(T(\overline{Y}_1^n)\cap C_{A_2B_2}(\mathbf{b},\mathbf{m}_2)\mid\overline{Y}_1^n)-\frac{f\left(T(\overline{Y}_1^n)\mid\overline{Y}_1^n\right)}{|\mathrm{Im}\,A_2||\mathrm{Im}\,B_2|}\right|\right] \quad (46)$$
$$+2E_{\overline{Y}_1^n}\left[g([T(\overline{Y}_1^n)]^c\cap T_{\mathbf{X}_2,\gamma}\mid\overline{Y}_1^n)\right]$$

From Lemma 5, we then have the equality as

$$E_{A_2B_2\overline{Y}_1^n}\left[\sum_{\mathbf{b},\mathbf{m}_2}\left|f(T(\overline{Y}_1^n)\cap C_{A_2B_2}(\mathbf{b},\mathbf{m}_2)\mid\overline{Y}_1^n)-\frac{f(T(\overline{Y}_1^n)\mid\overline{Y}_1^n)}{|\mathrm{Im}\,A_2||\mathrm{Im}\,B_2|}\right|\right]$$
$$=\sum_{\mathbf{Y}_1:T(\mathbf{Y}_1)\neq\varnothing}p_{\overline{Y}_1^n}(\mathbf{Y}_1)f(T(\mathbf{Y}_1)\mid\mathbf{Y}_1)\times E_{A_2B_2}\left[\sum_{\mathbf{b},\mathbf{m}_2}\left|\frac{f(T(\mathbf{Y}_1)\cap C_{A_2B_2}(\mathbf{b},\mathbf{m}_2)\mid\mathbf{Y}_1)}{f(T(\mathbf{Y}_1)\mid\mathbf{Y}_1)}-\frac{1}{|\mathrm{Im}\,A_2||\mathrm{Im}\,B_2|}\right|\right] \quad (47)$$
$$\le\sum_{\mathbf{Y}_1:T(\mathbf{Y}_1)\neq\varnothing}p_{\overline{Y}_1^n}(\mathbf{Y}_1)f(T(\mathbf{Y}_1)\mid\mathbf{Y}_1)\times\sqrt{\alpha_{A_2B_2}-1+\frac{\left[\beta_{A_2B_2}+1\right]|\mathrm{Im}\,A_2||\mathrm{Im}\,B_2|\max_{\mathbf{X}_2\in T(\mathbf{Y}_1)}f(\mathbf{X}_2\mid\mathbf{Y}_1,\mathbf{X}_1)]}{f(T(\mathbf{Y}_1)\mid\mathbf{Y}_1)}}$$
$$\le\sqrt{\alpha_{A_2B_2}-1+\left[\beta_{A_2B_2}+1\right]|\mathrm{Im}\,A_2||\mathrm{Im}\,B_2||\overline{f}}$$

where

$$\begin{aligned}\overline{f} &\equiv \max_{\mathbf{Y}_1:T(\mathbf{Y}_1)\neq\varnothing}\max_{\mathbf{X}_2\in T(\mathbf{Y}_1)} f(\mathbf{X}_2\mid\mathbf{Y}_1)\\ &= \max_{\mathbf{Y}_1:T(\mathbf{Y}_1)\neq\varnothing}\frac{\max\limits_{\mathbf{X}_2\in T(\mathbf{Y}_1)}\mu_{Y_1|X_1,X_2}(\mathbf{Y}_1\mid\mathbf{X}_1,\mathbf{X}_2)}{\sum\limits_{\mathbf{X}_2\in T_{\mathbf{X}_2,\gamma_1}}\mu_{Y_1|X_1,X_2}(\mathbf{Y}_1\mid\mathbf{X}_1,\mathbf{X}_2)}\\ &\le \max_{\mathbf{Y}_1:T(\mathbf{Y}_1)\neq\varnothing}\frac{2^{-n[H(\mathbf{Y}_1|\mathbf{X}_1,\mathbf{X}_2)]-\zeta_{y_1|\chi}(\gamma|\gamma)}}{\sum\limits_{\mathbf{X}_2\in T(y_1)}\mu_{Y_1|X_1,X_2}(\mathbf{Y}_1\mid\mathbf{X}_1,\mathbf{X}_2)}\\ &\le \max_{\mathbf{Y}_1:T(\mathbf{Y}_1)\neq\varnothing}\frac{2^{-n[H(\mathbf{Y}_1|\mathbf{X}_1,\mathbf{X}_2)]-\zeta_{y_1|\chi}(\gamma|\gamma)]}}{\sum\limits_{\mathbf{X}_2\in T(\mathbf{Y}_1)}2^{-n[H(\mathbf{Y}_1|\mathbf{X}_1,\mathbf{X}_2)+\zeta_{y_1|\chi}(\gamma|\gamma)]}}\\ &= \max_{\mathbf{Y}_1:T(\mathbf{Y}_1)\neq\varnothing}\frac{2^{2n\zeta_{y_1|\chi}(\gamma|\gamma)}}{\left|T(\mathbf{Y}_1)\right|}\end{aligned}$$

According to the inequalities (40)-(47), and the fact that $T_{\mathbf{X}_2,\gamma_1}\ge\left|T(\mathbf{Y}_1)\right|\ge 2^{-n[H(\mathbf{X}_2|\mathbf{X}_1,\mathbf{Y}_1)]-\eta_{\chi|y_1}(2\gamma|2\gamma)}$ for every $\mathbf{Y}_1$ which satisfies $T(\mathbf{Y}_1)\neq\varnothing$, then we have the fact that there are $A_2\in\mathcal{A}_2$, $B_2\in\mathcal{B}_2$ and $\mathbf{b}\in\mathrm{Im}\,A_2$ such that

$$\begin{aligned}&\Pr(\psi_2(\mathbf{Y}_2^n)\neq M_2))+d(p_{M_2Y_1^n},p_{M_2}\times p_{Y_1^n})\\ &\le 2^{-n[\gamma-\lambda_{\chi|y}]}+4\times 2^{-n\left[\gamma-\gamma-\lambda_{\chi|y_1}\right]}+\frac{2^{n[H(\mathbf{X}_2|\mathbf{Y}_1,\mathbf{X}_1)]}+\zeta_{\chi|y}(2\gamma\mid 2\gamma)\alpha_{A_2}}{\left|\mathrm{Im}\,A_2\right|}\\ &\quad+\beta_{A_2}+3\sqrt{\alpha_{A_2B_2}-1+\frac{[\beta_{A_2B_2}+1]\left|\mathrm{Im}\,A_2\right|\left|\mathrm{Im}\,B_2\right|}{2^{n[H(\mathbf{X}_2)-\eta_\chi(\gamma)]}}}\\ &\quad+2\sqrt{\alpha_{A_2B_2}-1+\frac{[\beta_{A_2B_2}+1]\left|\mathrm{Im}\,A_2\right|\left|\mathrm{Im}\,B_2\right|}{2^{n[H(\mathbf{X}_2|\mathbf{Y}_1,\mathbf{X}_1)-2n\zeta_{y_1|\chi}(\gamma|\gamma)]-\eta_{\chi|y_1}(2\gamma|2\gamma)}}}\end{aligned}$$

By assuming

$$\frac{l_{A_2}\log|\chi|}{n}>H(\mathbf{X}_2\mid\mathbf{Y}_2)+\zeta_{\chi|y}(2\gamma\mid 2\gamma)+\frac{\log(\left|\chi^{l_{A_2}}\right|/\left|\mathrm{Im}\,A_2\right|)}{n}$$

$$\frac{[l_{A_2}+l_{B_2}]\log|\chi|}{n}>H(\mathbf{X}_2\mid\mathbf{Y}_1,\mathbf{X}_1)+\zeta_{y_1|\chi}(\gamma\mid\gamma)-\eta_{\chi|y_1}(2\gamma\mid 2\gamma)$$

we have the inequalities (32) and (33) for all $\delta>0$ and sufficiently large n. In addition, we have $d(p_{M_2Y_1^n},p_{M_2}\times p_{Y_1^n})<o(\frac{1}{n})$ and $I(M_2;Y_1^n)<o(1)$ if (34) is satisfied.

Acknowledgements

This work was supported by the National Nature Science Foundation of China Grant #61271259 and 61301123, the project of Chongqing Municipal Education Commission Grant #Kjzh11206, the Chongqing Nature Science Foundation Grant #CTSC2011jjA40006, the Research Project of Chongqing Education Commission Grant #KJ120501, KJ120502 and KJ130536 and the special fund of Chongqing key laboratory (CSTC).

References

[1]. A. D. Wyner, The wiretap channel, *Bell Systems Technical Journal*, Vol. 54, No. 8, January 1975, pp. 1355–1387.

[2]. J. W. Xie and S. Ulukus, Secure degrees of freedom of the Gaussian multiple access wiretap channel, in *Proceedings of the IEEE International Symposium on Information Theory Proceedings (ISIT)*, Istanbul, Turkey, 7-12 July 2013.

[3]. J. W. Xie and S. Ulukus, Unified secure DoF analysis of K-user Gaussian interference channels, in *Proceedings of the IEEE International Symposium on Information Theory Proceedings (ISIT)*, Istanbul, Turkey, 7-12 July 2013.

[4]. J. W. Xie and S. Ulukus, Sum secure degrees of freedom of two-unicast layered wireless networks, *IEEE Journal on Selected Areas in Communications*, Vol. 31, Issue 9, 2013, 1931-1943.

[5]. C. Wang, H. Farhadi, and M. Skoglund, Achieving the degrees of freedom of wireless multi-user relay networks, *IEEE Transactions on Communications*, Vol. 60, No. 9, June 2012, pp. 2612-2622.

[6]. A. Mukherjee and A. L. Swindlehurst, Robust beamforming for security in MIMO wiretap channels with imperfect CSI, *IEEE Transactions on Signal Processing*, Vol. 59, Issue 1, 2010, pp. 351-361.

[7]. S. Yang, M. Kobayashi, P. Piantanida, and S. Shamai, Secrecy degrees of freedom of MIMO broadcast channels with delayed CSIT, *IEEE Transactions on Information Theory*, Vol. 59, Issue 9, 2013, pp. 5244-5256.

[8]. L. Chen, Cooperation with an untrusted relay in broadcast channels, in *Proceedings of the IEEE International Symposium on Information Theory (ISIT)*, Istanbul, Turkey, 7-12, July 2013.

[9]. J. W. Xie and S. Ulukus, Secure degrees of freedom of one-hop wireless networks, submitted to *IEEE Transactions on Information Theory*, September 2012, in press.

[10]. J. Muramatsu and S. Miyake, Construction of strongly secure wiretap channel code based on hash property, in *Proceedings of the IEEE International Symposium on Information Theory Proceedings (ISIT)*, St. Petersburg, Russia, July 31 – August 5, 2011.

[11]. J. Muramatsu and S. Miyake, Construction of broadcast channel code based on hash property, in *Proceedings of the IEEE International Symposium on Information Theory Proceedings (ISIT)*, Austin, Texas, USA, 13-18 June 2010.

[12]. J. Muramatsu and S. Miyake, Construction of Slepian-Wolf source code and broadcast channel code based on hash property, submitted to *IEEE Transactions on Information Theory*, 2010, in press.

[13]. J. Muramatsu and S. Miyake, Hash property and coding theorems for sparse matrices and maximal-likelihood coding, *IEEE Transaction on Information Theory*, Vol. 56, Issue 5, May 2010, pp. 2143–2167.