Progress In Electromagnetics Research C, Vol. 43, 187–199, 2013

GENERALIZED TRANSMISSION SCHEME FOR MIMO Y CHANNEL

Yong Wang[1, *], Qiao Liu[1], Hui Li[1], and Fengrong Li[2]

[1]State Key Laboratory of Integrated Service Networks, Xidian University, Xi'an, Shanxi 710071, China

[2]Key Laboratory of Wireless Sensor Network & Communication, Shanghai Institute of Microsystem and Information Technology, Chinese Academy of Sciences, 865 Changning Road, Shanghai 200050, China

Abstract—This paper proposes a novel scheme for a multi-way communication where users combine bi-directional multi-pair messages exchange with multi-directional multi-pair exchange. Particularly, we focus on the system where multiple users have multiple antennas exchange both private and common messages with each other. In this scheme, we can use simple zero forcing combined with successive network code decoding enables all user to decipher the encryption message from the relay despite the fact that they all have different self-information which they use as a key.

1. INTRODUCTION

Several kinds of signaling scheme have been used to successfully handle the interference problem and enhance the network transmission rates performance at the same time and frequency. Recently, increasing attention has been paid to interference alignment (IA) and network coding. IA has become an active area of interest because of its efficiency in interference suppression at high signal to noise ratios (SNR) and a superior capability for increasing the throughput of multi-user wireless communications systems. Cadambe and Jafar introduced IA in [1], and by using it in a K-user single antenna interference channel, $K/2$ spatial degrees of freedom could be obtained, contrary to the previously

Received 13 July 2013, Accepted 2 September 2013, Scheduled 6 September 2013

* Corresponding author: Yong Wang (xd.wangyong@gmail.com).

common belief that an interference channel with any number of users has only one degrees of freedom (DoF).

The two-way relay channel has drawn more attention because of its attractive application to cellular networks. It has been recently generalized to include multiple links. The authors in [2] studied the relay-aided multi-pair communication network, where a relay node facilitates the communication between multiple pairs of users. Multi-user and multi-way relay communications were considered in [3, 4], where multiple users intend to exchange information with a shared relay terminal. Particularly in [4], a multiple-input multiple output (MIMO) Gaussian Y channel with one relay and three users was introduced. An efficient signal space alignment for network coding scheme exploiting the concepts of interference alignment [5–7] and network coding [8, 9] is proposed to manage interference signals in the multi-user bi-directional system. The extension of the MIMO Y channel to the case where a general number of users simultaneously exchange messages with each other was investigated in [10].

From the successful results of network coding in the context of a wired network, the idea of network coding can be also considered as an efficient approach to solve the interference problem in wireless networks since it provides a new perspective about interference, which is interference utilization. Through this new view about interference, it has been demonstrated that physical-layer network coding (PNC) [11, 12] and analog-network coding (ANC) [13, 14] can significantly improve the transmission rate of the two-way relay channel [15–17]. ANC and PNC allow simultaneous transmission of two nodes to the relay node over the same frequency for the multiple access phase. If the relay detects two messages independently, this transmission causes interference at the relay. However, the relay jointly detects and decodes the sum of two independent signals that interfere with each other. This implies that the relay exploits the interfering signal to obtain meaningful information, so that each end terminal can remove the interference during the broadcasting phase by using side information which is transmitted during the multiple access phases.

In this paper, we consider a message exchange scenario in combining bi-directional multi-pair message exchange with multi-directional multi-pair exchange communication systems, where K users having multiple antennas exchange both private and common messages with each other. This communication scenario is similar with [19], while the proposed algorithm required fewer nodes antennas in keeping DoF under the same users' number. It has great benefits for practical engineering applications.

2. SYSTEM MODEL

The MIMO Gaussian K-user MIMO Y channel is considered in this section. K users have M multiple antennas, and a relay has N multiple antennas. Each user tries to send both private and common messages to the other users in the multiple access channel (MAC) phase and wishes to decode both of them in the broadcast channel (BC) phase. We denote $W_p^{[j,i]}$ as the private message sent by user i to user j and $W_c^{[i]}$ as the common message transmitted by user i to all other users.

In the MAC phase, all messages $W_p^{[j,i]}$ and $W_c^{[i]}$ are sent by user i using the symbols $s_p^{[j,i]}$ and $s_c^{[i]}$. When the messages are transmitted, user i employs the precoding vectors $\mathbf{v}_p^{[j,i]}$ and $\mathbf{v}_c^{[i]}$ for $s_p^{[j,i]}$ and $s_c^{[i]}$, respectively. Thus, the transmit signal for user i is expressed as $\mathbf{x}^{[i]} = \sum_{j\neq i} \mathbf{v}_p^{[j,i]} s_p^{[j,i]} + \mathbf{v}_c^{[i]} s_c^{[i]}$. Then, the received signal at the relay is given by

$$\mathbf{y}^{[R]} = \sum_{i=1}^{K} \mathbf{H}^{[R,i]}\mathbf{x}^{[i]}+\mathbf{n}^{[R]} \tag{1}$$

where $\mathbf{H}^{[R,i]}$ represents the $N \times M$ channel matrix from user i to the relay, and $\mathbf{n}^{[R]}$ indicates the additive white Gaussian noise (AWGN) vector with zero mean and unit variance. The relay subsequently generates the transmit signal $\mathbf{x}^{[R]} = \mathbf{U}^{-1}\mathbf{y}^{[R]}$, where $\mathbf{U}$ is designed as the beamforming precoding matrix.

In the BC phase, the relay broadcasts $\mathbf{x}^{[R]}$ to all users. Then, user j receives the signal as

$$\mathbf{y}^{[j]} = \sum_{i=1}^{K} \mathbf{H}^{[j,R]}\mathbf{x}^{[R]}+\mathbf{n}^{[j]} \tag{2}$$

where $\mathbf{H}^{[j,R]}$ represents the $M \times N$ channel matrix from the relay to user j, and $\mathbf{n}^{[j]}$ is AWGN vector at user j. Additionally, it is assumed that all users and the relay operate in full-duplex mode. The channel is assumed to be known perfectly at all users and the relay in both the transmitting and receiving modes.

3. NOVEL SIGNALING FOR THE MIMO Y CHANNEL

In this section, we investigate the DoF that can be achieved according to transmit scheme for the K-user MIMO Y channel. The following theorem is the main result of this paper.

Theorem 1: For the private and common messages setting of K-user Y channels where each user wishes to obtain the DoF of 1 for each message, the total DoF of K^2 is achieved if the relay has $N = \max(\frac{1}{2}(K-1)(K+2), 2M-1)$ antennas and each user has $M = 2(K-1)+1$ antennas.

Proof: Let us first consider $K = 4$, $N = 13$, $M = 7$ case to explain the basic idea of an achievable scheme. Then, we will generalize this construction to more general number of users later.

3.1. Four User Case ($K = 4$)

During the MAC phase, each user sends three private and two common messages to the relay (copies of the same common message), but user 1 and user 4 send only one common message. The relay receives a total of eighteen independent messages which consist of twelve private messages and four common messages. Since the relay has $N = 13$ antennas, each user cooperatively transmits those messages so that they maximize the utility of the signal dimensions at the relay, as described in Fig. 1. By using the notion of SSA-NC [18], each user designs the beamforming direction so that two desired signals are aligned within the same spatial dimension, i.e., $span(\mathbf{H}^{[R,i]}\mathbf{v}_p^{[j,i]}) = span(\mathbf{H}^{[R,j]}\mathbf{v}_p^{[i,j]})$. Specifically, we first choose the six signal dimensions for the private messages as $\mathbf{U}_p = [\ \mathbf{u}_p^{\pi(1,2)}\ \ \mathbf{u}_p^{\pi(1,3)}\ \ \mathbf{u}_p^{\pi(1,4)}\ \ \mathbf{u}_p^{\pi(2,3)}\ \ \mathbf{u}_p^{\pi(2,4)}\ \ \mathbf{u}_p^{\pi(3,4)}\ ]$, where $\mathbf{u}_p^{\pi(i,j)}$ is unit vector in the intersection subspace between the channel of user i and user j with the index $\pi(i,j)$.

Then, by solving the following linear equation

$$\begin{bmatrix} \mathbf{I}_N & -\mathbf{H}^{[R,i]} & \mathbf{0} \\ \mathbf{I}_N & \mathbf{0} & -\mathbf{H}^{[R,j]} \end{bmatrix} \begin{bmatrix} \mathbf{u}_p^{\pi(i,j)} \\ \mathbf{v}_p^{[j,i]} \\ \mathbf{v}_p^{[i,j]} \end{bmatrix} = \mathbf{0} \tag{3}$$

For the common messages, user 1 and user 4 send symbols.

$\mathbf{s}_c^{[1]}$ and $\mathbf{s}_c^{[4]}$ along with precoding vectors $\mathbf{v}_{c,1}^{[1]}$ and $\mathbf{v}_{c,1}^{[4]}$, as expressed by $\mathbf{x}_c^{[1]} = \mathbf{v}_{c,1}^{[1]} s_c^{[1]}$, $\mathbf{x}_c^{[4]} = \mathbf{v}_{c,1}^{[4]} s_c^{[4]}$. While user 2 and user 3 transmit message send symbols $\mathbf{s}_c^{[2]}$ and $\mathbf{s}_c^{[3]}$ along with precoding vectors $\mathbf{v}_{c,1}^{[i]}$ and $\mathbf{v}_{c,2}^{[i]}$, as expressed by $\mathbf{x}_c^{[i]} = \mathbf{v}_{c,1}^{[i]} s_c^{[i]} + \mathbf{v}_{c,2}^{[i]} s_c^{[i]}$, $i = \{2,3\}$[16].

The proposed common messages precoding strategy is aiming at obtaining three network coding messages with chain property, $W_c^{[1]} \oplus W_c^{[2]}$, $W_c^{[2]} \oplus W_c^{[3]}$, $W_c^{[3]} \oplus W_c^{[4]}$ at the relay. All users carefully choose the precoding vectors in order to satisfy the conditions of signal

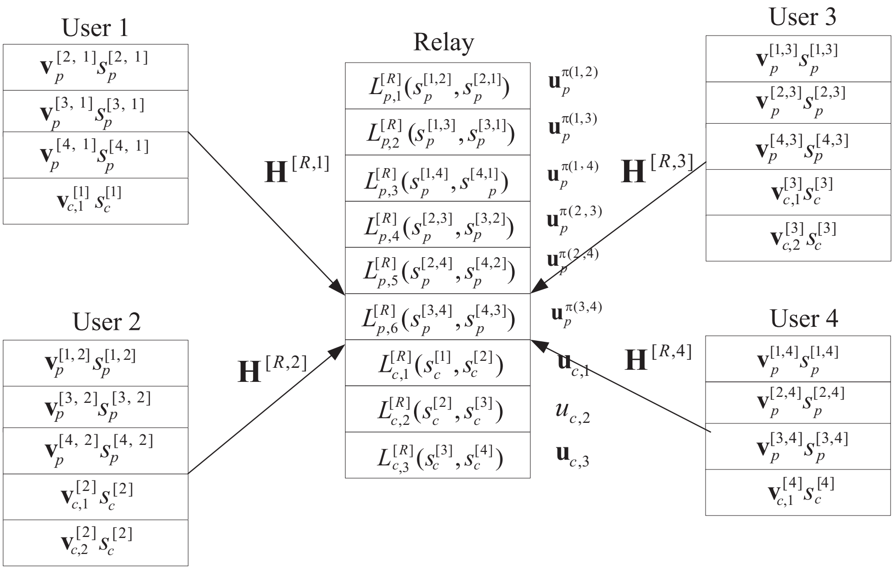

Figure 1. Signaling alignment for network coding for $K = 4$.

space alignment for an encryption message. These are given by:

$$\begin{aligned} span\left(\mathbf{H}^{[R,1]}\mathbf{v}_{c,1}^{[1]}\right) &= span\left(\mathbf{H}^{[R,2]}\mathbf{v}_{c,1}^{[2]}\right) \\ span\left(\mathbf{H}^{[R,2]}\mathbf{v}_{c,2}^{[2]}\right) &= span\left(\mathbf{H}^{[R,3]}\mathbf{v}_{c,1}^{[3]}\right) \\ span\left(\mathbf{H}^{[R,3]}\mathbf{v}_{c,2}^{[3]}\right) &= span\left(\mathbf{H}^{[R,4]}\mathbf{v}_{c,1}^{[4]}\right) \end{aligned} \tag{4}$$

We choose the three signal dimensions for the common messages as $\mathbf{U}_c = [\mathbf{u}_{c,1} \quad \mathbf{u}_{c,2} \quad \mathbf{u}_{c,3}]$.

The received signal at the relay is given by

$$\begin{aligned} \mathbf{y}^{[R]} &= \sum_{i=1}^{4}\mathbf{H}^{[R,i]}\left(\sum_{j\neq i}\mathbf{v}_p^{[j,i]}s_p^{[j,i]} + \mathbf{v}_{c,1}^{[i]}s_c^{[i]} + \mathbf{v}_{c,2}^{[i]}s_c^{[i]}\right) + \mathbf{n}^{[R]} \\ &= [\mathbf{U}_p \quad \mathbf{U}_c]\begin{bmatrix}\mathbf{s}_p^{[R]} \\ \mathbf{s}_c^{[R]}\end{bmatrix} + \mathbf{n}^{[R]} \end{aligned} \tag{5}$$

where $\mathbf{v}_{c,2}^{[1]} = \mathbf{v}_{c,2}^{[4]} = \mathbf{0}_{M\times 1}$. We define $\mathbf{s}_p^{[R]} = [L_{p,1}^{[R]}(s_p^{[1,2]}, s_p^{[2,1]})$, $L_{p,2}^{[R]}(s_p^{[1,3]}, s_p^{[3,1]})$, $L_{p,3}^{[R]}(s_p^{[1,4]}, s_p^{[4,1]})$, $L_{p,4}^{[R]}(s_p^{[2,3]}, s_p^{[3,2]})$, $L_{p,5}^{[R]}(s_p^{[2,4]}, s_p^{[4,2]})$, $L_{p,6}^{[R]}(s_p^{[3,4]}, s_p^{[4,3]})]^T$, $\mathbf{s}_c^{[R]} = [L_{c,1}^{[R]}(s_c^{[1]}, s_c^{[2]})$, $L_{c,2}^{[R]}(s_c^{[2]}, s_c^{[3]})$, $L_{c,3}^{[R]}(s_c^{[3]}, s_c^{[4]})]^T$

and $\mathbf{U} = [\ \mathbf{U}_p \quad \mathbf{U}_c\ ]$, $L^{[R]}_{p,m}$ and $L^{[R]}_{c,m}$ are the m-th linear combination of the transmitted symbols at the relay.

Because all channel elements are independently drawn from a continuous distribution, the rank of the null space of matrix becomes 9. The each column of $\mathbf{U}$ is linearly independent with probability one [18], i.e., $\Pr[\det(\mathbf{U}) = 0] = 0$. Employing the SSA-NC, each user is able to contain two independent private data symbols into one signal dimension for network coding and common data symbols into network code chain structure at the relay.

Therefore, $\mathbf{s}^{[R]}$ can be obtained by elimination the inter-signal space interference using a zero-forcing (ZF) decoder, which is $\mathbf{s}^{[R]} = \mathbf{U}^{-1}\mathbf{y}^{[R]} + \mathbf{U}^{-1}\mathbf{n}^{[R]}$. The nine network coded messages $\hat{W}^{[R]}_{p,\pi(1,2)} = W^{[1,2]}_p \oplus W^{[2,1]}_p$, $\hat{W}^{[R]}_{p,\pi(1,3)} = W^{[1,3]}_p \oplus W^{[3,1]}_p$, $\hat{W}^{[R]}_{p,\pi(1,4)} = W^{[1,4]}_p \oplus W^{[4,1]}_p$, $\hat{W}^{[R]}_{p,\pi(2,3)} = W^{[2,3]}_p \oplus W^{[3,2]}_p$, $\hat{W}^{[R]}_{p,\pi(2,4)} = W^{[2,4]}_p \oplus W^{[4,2]}_p$, $\hat{W}^{[R]}_{p,\pi(3,4)} = W^{[3,4]}_p \oplus W^{[4,3]}_p$, $\hat{W}^{[R]}_{c,\pi(1,2)} = W^{[1]}_c \oplus W^{[2]}_c$, $\hat{W}^{[R]}_{c,\pi(2,3)} = W^{[2]}_c \oplus W^{[3]}_c$, $\hat{W}^{[R]}_{c,\pi(3,4)} = W^{[3]}_c \oplus W^{[4]}_c$ are then obtained by applying the physical-layer network coding (PNC) modulation-demodulation mapping principle into each symbol $s^{[R]}_i$ via a signal dimension.

During the BC phase, relay broadcasts nine information $\hat{W}^{[R]}_{p,\pi(1,2)}$, $\hat{W}^{[R]}_{p,\pi(1,3)}$, $\hat{W}^{[R]}_{p,\pi(1,4)}$, $\hat{W}^{[R]}_{p,\pi(2,3)}$, $\hat{W}^{[R]}_{p,\pi(2,4)}$, $\hat{W}^{[R]}_{p,\pi(3,4)}$, $\hat{W}^{[R]}_{c,\pi(1,2)}$, $\hat{W}^{[R]}_{c,\pi(2,3)}$, $\hat{W}^{[R]}_{c,\pi(3,4)}$ to all users using nine encoded symbols $\mathbf{s}_R = [s^1_{R,p}, s^2_{R,p}, s^3_{R,p}, s^4_{R,p}, s^5_{R,p}, s^6_{R,p}, s^1_{R,c}, s^2_{R,c}, s^3_{R,c}]^T$ along beamforming vectors $\mathbf{V}_R = [\mathbf{v}^1_{R,p}, \mathbf{v}^2_{R,p}, \mathbf{v}^3_{R,p}, \mathbf{v}^4_{R,p}, \mathbf{v}^5_{R,p}, \mathbf{v}^6_{R,p}, \mathbf{v}^1_{R,c}, \mathbf{v}^2_{R,c}, \mathbf{v}^3_{R,c}]$.

Let us consider the receiver of user1. Since the signal $\hat{W}^{[R]}_{p,\pi(2,3)}$, $\hat{W}^{[R]}_{p,\pi(2,4)}$, $\hat{W}^{[R]}_{p,\pi(3,4)}$ causes interference to the user 1, the beamforming vectors $\mathbf{v}^4_{R,p}$, $\mathbf{v}^5_{R,p}$ and $\mathbf{v}^6_{R,p}$ should be designed to lie in the null space of $\mathbf{H}^{[1,R]}$ to remove this interference. At the same time, the beamforming vectors $\mathbf{v}^2_{R,p}$, $\mathbf{v}^3_{R,p}$ and $\mathbf{v}^6_{R,p}$ should be designed to lie in the null space of $\mathbf{H}^{[2,R]}$ to remove interference for user 2. The beamforming vectors $\mathbf{v}^1_{R,p}$, $\mathbf{v}^3_{R,p}$ and $\mathbf{v}^5_{R,p}$ should be designed to lie in the null space of $\mathbf{H}^{[3,R]}$ to remove interference for user 3. The beamforming vectors $\mathbf{v}^1_{R,p}$, $\mathbf{v}^2_{R,p}$ and $\mathbf{v}^4_{R,p}$ should be designed to lie in the null space of $\mathbf{H}^{[4,R]}$ to remove interference for user 4. It claims that $\mathbf{H}^{[1,R]}$ has 6-dimensional null space so $\mathbf{v}^6_{R,p}$ can be designed to be in this null space. This condition can be satisfied, however, the resulting $\mathbf{v}^6_{R,p}$ cannot be chosen to be in the null space of both $\mathbf{H}^{[1,R]}$

and $\mathbf{H}^{[2,R]}$. Because of the dimensionality constraint, i.e., $N \prec 2M$, beamforming vector $\mathbf{v}_{R,p}^{6}$ should generally not be constructed so that $\mathbf{v}_{R,p}^{6} \in null(\mathbf{H}^{[1,R]}) \cap null(\mathbf{H}^{[2,R]})$. Thus, we consider an antenna selection scheme to solve this dimensionality constraint problem. Each user chooses $\hat{M} = 6$ antennas to receive signals coming from the relay among the $M = 7$ total antennas they have. Then, the size of the effective channel matrices $\hat{\mathbf{H}}^{[i,R]}$ from the relay to user i becomes 6×13. Now, we can design the relay beamforming vectors $\mathbf{v}_{R,p}^{6}$ to remove interference, i.e., $\mathbf{v}_{R,p}^{6} \in null(\hat{\mathbf{H}}^{[1,R]}) \cap null(\hat{\mathbf{H}}^{[2,R]})$. In the similar way, we can design beamforming vectors for the relay, which are represented as follows:

$$\begin{array}{ll} \begin{bmatrix} \hat{\mathbf{H}}^{[3,R]} \\ \hat{\mathbf{H}}^{[4,R]} \end{bmatrix} \mathbf{v}_{R,p}^{1} = 0, & \begin{bmatrix} \hat{\mathbf{H}}^{[2,R]} \\ \hat{\mathbf{H}}^{[4,R]} \end{bmatrix} \mathbf{v}_{R,p}^{2} = 0 \\ \begin{bmatrix} \hat{\mathbf{H}}^{[2,R]} \\ \hat{\mathbf{H}}^{[3,R]} \end{bmatrix} \mathbf{v}_{R,p}^{3} = 0, & \begin{bmatrix} \hat{\mathbf{H}}^{[1,R]} \\ \hat{\mathbf{H}}^{[4,R]} \end{bmatrix} \mathbf{v}_{R,p}^{4} = 0 \\ \begin{bmatrix} \hat{\mathbf{H}}^{[1,R]} \\ \hat{\mathbf{H}}^{[3,R]} \end{bmatrix} \mathbf{v}_{R,p}^{5} = 0, & \begin{bmatrix} \hat{\mathbf{H}}^{[1,R]} \\ \hat{\mathbf{H}}^{[2,R]} \end{bmatrix} \mathbf{v}_{R,p}^{6} = 0 \end{array} \tag{6}$$

The received signal at user 1 can be expressed as

$$\begin{aligned} \hat{\mathbf{y}}^{[1]} &= \hat{\mathbf{H}}^{[1,R]} \left(\sum_{m=1}^{6} \mathbf{v}_{R,p}^{m} s_{R,p}^{m} + \sum_{n=1}^{3} \mathbf{v}_{R,c}^{n} s_{R,c}^{n} \right) + \hat{\mathbf{n}}^{[1]} \\ &= \hat{\mathbf{Q}}^{[1,R]} \begin{bmatrix} s_{R,p}^{1} & s_{R,p}^{2} & s_{R,p}^{3} & s_{R,c}^{1} & s_{R,c}^{2} & s_{R,c}^{3} \end{bmatrix}^{T} + \hat{\mathbf{n}}^{[1]} \end{aligned} \tag{7}$$

where $\mathbf{Q}^{[1,R]}$ denotes the effective channel from the relay to use 1 and is invertible with high probability. Therefore, the conclusion is that all users are able to detect symbols by ZF detection, which nulls out the inter-signal space interference. For user 1, the detected signal is

$$\mathbf{s}_{R,1} = \hat{\mathbf{Q}}^{[1,R]^{-1}} \hat{\mathbf{y}}^{[1]} + \hat{\mathbf{Q}}^{[1,R]^{-1}} \hat{\mathbf{n}}^{[1]} \tag{8}$$

After self-interference cancellation, user 1 gets the three desired private messages coming from user 2, user 3 and user 4, i.e., $s_p^{[1,2]}$, $s_p^{[1,3]}$ and $s_p^{[1,4]}$, and the three encrypted common messages. The decryption procedure is performed by successive network code decoding scheme. By exploiting self-information $W_c^{[1]}$ as a key, user 1 first extracts $\hat{W}_c^{[2]}$ from message $\hat{W}_{c,\pi(1,2)}^{[R]} = W_c^{[1]} \oplus W_c^{[2]}$, as follows:

$$\hat{W}_c^{[2]} = \hat{W}_{c,\pi(1,2)}^{[R]} \oplus W_c^{[1]} \tag{9}$$

Subsequently, user 1 successively decodes $W_c^{[3]}$ from message $\hat{W}_{c,\pi(2,3)}^{[R]} = W_c^{[2]} \oplus W_c^{[3]}$ using message $\hat{W}_c^{[2]}$ as another key; this is decoded message from the previous step. In this consecutive approach, user 1 untangles the network code chain successively. Eventually, user 1 is able to obtain all common messages from the other users. In the same manner, other all users can decode three private messages and three common messages. It lead to achieve the total DoF $\eta_{sum}(4) = 16$ when $K = 4$, $M = 7$ and $N = 13$.

In the BC phase, the relay transmits the encrypted common massages with the network code chain structure. Assuming that an eavesdropper having M antennas wants to decode the messages during the BC phase, the question arises as to how many messages the eavesdropper can reliably decode. The proposed coding strategy only allows the users who participate in the message exchange via relay to decipher the messages, as the users who take part have the key to crack the network code chain. Therefore, due to the absence of knowledge regarding a certain key, the eavesdropper cannot decode any message. It indicates that the proposed scheme is robust in terms of the message security.

3.2. Extension to the General K-user Case

In this section, we generalize the proposed scheme to the general K-user case, assuming that each user achieves the DoF of 1 for each message. Since each user transmits total $K - 1$ private messages and one common message with two branches, the relay receives $(K - 1 + 1) \times K = K^2$ messages for K users during the MAC phase. The user can transmit $K - 1$ private messages and two branches of one common message properly if

$$M \geq (K + 1) \tag{10}$$

As explained in the previous subsection, each user transmits total $K - 1$ private messages and K users can transmit $K(K - 1)$ private messages. After SSA-NC, the relay needs $\frac{1}{2}K(K-1)$ dimensional signal space for containing the private messages and $K-1$ dimensional signal space for the common messages, which requires

$$N \geq \frac{1}{2}K(K - 1) + (K - 1) = \frac{1}{2}(K - 1)(K + 2) \tag{11}$$

for the relay to properly contain the K^2 messages during the MAC phase.

In order to properly align intersection subspace for private and common messages, the beamforming vectors $\mathbf{v}_p^{[j,i]}$ and $\mathbf{v}_c^{[i]}$ should be designed by satisfying the condition

$$\begin{bmatrix} \mathbf{I}_N & -\mathbf{H}^{[R,i]} & \mathbf{0} \\ \mathbf{I}_N & \mathbf{0} & -\mathbf{H}^{[R,j]} \end{bmatrix}_{2N\times(N+2M)} \begin{bmatrix} \mathbf{u}_p^{\pi(i,j)} \\ \mathbf{v}_p^{[j,i]} \\ \mathbf{v}_p^{[i,j]} \end{bmatrix}_{(N+2M)\times 1} = \mathbf{0}_{2N\times 1} \quad (12)$$

Since the size of matrix in (12) is $2N\times(N+2M)$ and its entries are independently drawn from a continuous distribution, a solution of (12) exists if

$$2M > N \quad (13)$$

There exists intersection subspace constituted by the column space of channel matrices for each user pair.

Recall that while $K-1$ common message symbols are the desired signals for all users, the private message pairs excluding the desired $K-1$ private messages among $\frac{1}{2}K(K-1)$ private message pairs become $\frac{1}{2}K(K-1)-(K-1)=\frac{1}{2}(K-1)(K-2)$ interference signals. The receiver can decode the desired signals successfully if the antennas of each user meet

$$M > (K-1)+(K-1) \quad (14)$$

when receiver has removed $\frac{1}{2}(K-1)(K-2)$ interference signals.

The main idea of the relay beamforming is to eliminate inter-user interference signals. According to (6), a solution exists if $N > 2M$, which is contradict to (13). To accomplish this, we use antenna selection scheme ($\hat{M}=M-1$) to solve this dimensionality constraint problem, i.e.,

$$N > 2\hat{M} = 2(M-1) \quad (15)$$

which generates null space in (6). Since there are $\frac{1}{2}(K-1)(K-2)$ nullity in the downlink effective channel, the relay selects $\frac{1}{2}(K-1)(K-2)$ private message pairs which are interference to user i and designs their beamforming vectors just like Equation (6) so that each user does not receive $\frac{1}{2}(K-1)(K-2)$ interference symbols among a total of $\frac{1}{2}K(K-1)$ private message pairs.

From (10) and (14), we can obtain

$$\left.\begin{matrix} M \geq (K+1) \\ M > (K-1)+(K-1) \end{matrix}\right\} \Rightarrow M \geq 2(K-1)+1$$

From (11) and (15), we can obtain

$$N = \max\left(\frac{1}{2}(K-1)(K+2), 2M-1\right)$$

As a result, all users achieve the DoF of 1 for each message, as they are able to transmit $K-1$ private messages and one common message to the desired users without any interference. Thus, the proposed signaling method achieves the DoF of $\eta = K^2$ with the antenna configuration of $M = 2(K-1)+1$ and $N = \max(\frac{1}{2}(K-1)(K+2), 2M-1)$.

4. SIMULATION AND DISCUSSION

We provide the simulation results to evaluate the sum rate performance of the proposed scheme. From the simulation results, we will confirm the feasibility condition in Theorem 1. Each user allocates equal power to each beamforming vector.

As size and cost constraints, it is hard to configure more antennas for user nodes. Fewer antennas configure, more conducive to engineering application. Table 1 illustrates the proposed scheme require fewer the number of user antennas than [19]. With the number

Table 1. Compare the number of antennas of different scheme.

K	**4**		**5**		**6**	
scheme	**Proposed scheme**	**Ref. [19]**	**Proposed scheme**	**Ref. [19]**	**Proposed scheme**	**Ref. [19]**
M	7	8	9	12	11	18
N	13	9	17	14	21	20

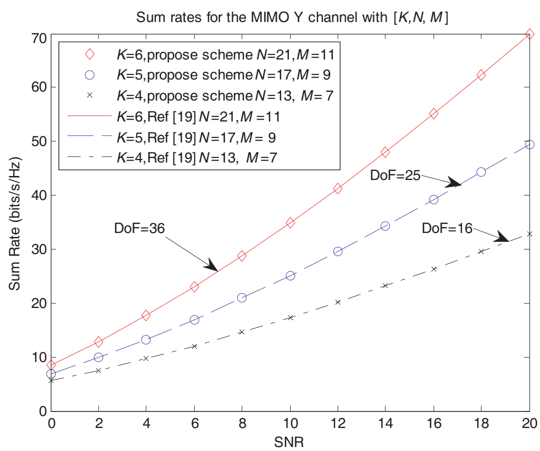

Figure 2. Sum rate performance of $K = 4$, 5 and 6.

of users increases, the number of user antennas can approximate to [19].

(We have modified the Sum Rate unit as "bits/s/Hz" in Fig. 2 according to reviewer's comment. At the same time, we change the DoF of $K = 4$ from 14 to 16 in Fig. 2 since we make a slip in writing.)

Figure 2 exhibits the sum rate performance of $K = 4$, 5 and 6 with respect to SNR. The slope of the sum rate curves indicates the achievable DoF. It is shown from the Fig. 2 that the proposed scheme has the same DoF as [19] while all users' antennas not more than those in [19]. At the same time, the relay transmits the encrypted common messages with the network code chain structure. The proposed coding strategy only allows the users who participate in the message exchange via relay to decipher the messages, as the users who take part have the key to crack the network code chain. It indicates that the proposed scheme is robust in terms of the message security.

5. CONCLUSIONS

In this paper, we consider multi-pair messages exchange scenario in multi-way communication systems where K users having multiple antennas exchange both private and common messages with each other. They are able to transmit $K - 1$ private messages and one common message to the desired users without any interference. Thus, the proposed signaling method achieves the DoF of $\eta = K^2$.

ACKNOWLEDGMENT

The Project Supported by the National Natural Science Foundation of China (No. 61101147), National Basic Research Program of China (973 Program, No. 2012CB316100), Specialized Research Fund for the Doctoral Program of Higher Education (No. 20110203120004), Science Research Plan in Shaanxi Province of China (Program No. 2013K06-15), Science and Technology Projects in Xi'an of China (Program No. CX1251(4)), Open Project of Key Laboratory of Wireless Sensor Network & Communication, Shanghai Institute of Microsystem and Information Technology, Chinese Academy of Sciences (No. 2012004), The Fundamental of Research Funds for the Central Universities (No. K5051301006), The 111 Project (No. B08038).

REFERENCES

1. Cadambe, V. R. and S. A. Jafar, "Interference alignment and degrees of freedom for the K user interference channel," *IEEE Trans. Inform. Theory*, No. 54, No. 8, 3425–3441, 2008.

2. Avestimehr, S., M. A. Khajehnejad, A. Sezgin, and B. Hassibi, "Capacity region of the deterministic multi-pair bi-directional relay network," *Proc. IEEE ITW*, 57–61, Jun. 2009.
3. Gündüz, D., A. Yener, A. Goldsmith, and H. V. Poor, "The multiway relay channel," *Proc. IEEE ISIT*, Vol. 59, No. 1, 51–63, Jun. 2009.
4. Lee, N., J.-B. Lim, and H. Chun, "Degrees of freedom of the MIMO Y channel: Signal space alignment for network coding," *IEEE Trans. Inform. Theory*, Vol. 56, No. 7, 3332–3342, Jul. 2010.
5. Emadi, M., K. H. Sadeghi, A. Jafargholi, and F. Marvasti, "Combined beamforming with Alamouti coding using double antenna array group for multiuser interference cancellation," *Progress In Electromagnetics Research*, Vol. 88, 213–226, 2008.
6. Jafar, S. A. and S. Shamai, "Degrees of freedom for the MIMO X channel," *IEEE Trans. Inform. Theory*, Vol. 54, No. 1, 151–170, Jan. 2008.
7. Lin, M., K. An, J. Ouyang, Y. Huang, and M. Li, "Effect of beamforming on multi-antenna two hop asymmetric fading channels with fixed gain relays," *Progress In Electromagnetics Research*, Vol. 133, 367–390, 2013.
8. Ahlswede, R., N. Cai, S.-Y. R. Li, and R. W. Yeung, "Network information flow," *IEEE Trans. Inform. Theory*, Vol. 46, No. 4, 1204–1216, Jul. 2000.
9. Ho, T., M. Médard, R. Koetter, D. Karger, M. Effros, J. Shi, and B. Leong, "A random linear network coding approach to multicast," *IEEE Trans. Inform. Theory*, Vol. 52, No. 10, 4413–4430, Oct. 2006.
10. Lee, K., N. Lee, and I. Lee, "Feasibility conditions of signal space alignment for network coding on K-user MIMO Y channels," *Proc. IEEE ICC*, 1–5, Jun. 2011.
11. Zhang, S., S.-C. Liew, and P. P. Lam, "Physical layer network coding," *ACM Mobicom 2006*, 2006.
12. Zhang, S., S.-C. Liew, and L. Lu, "Physical layer network coding schemes over finite and infinite fields," *Global Telecommunications Conference, IEEE GLOBECOM*, 1–6, 2008.
13. Katti, S., S. Gollakota, and D. Katabi, "Embracing wireless interference: Analog network coding," *Comput. Sci. Artif. Intell. Lab. Tech. Rep.*, MIT-CSAIL-TR-2007-012, Cambridge, MA, 2007.
14. Katti, S., H. Rahul, W. Hu, D. Katabi, M. Medard, and J. Crowcroft, "XORs in the air: Practical wireless network

coding," *Proc. ACM Special Interest Group Data Commun.*, 243–254, Pisa, Italy, Sep. 11–15, 2006.

15. Rankov, B. and A. Wittneben, "Spectral efficient protocols for half-duplex fading relay channels," *IEEE J. Sel. Areas Commun.*, Vol. 25, No. 2, 379–389, Feb. 2007.
16. Lee, N. and J. Chun, "Signal space alignment for an encryption message and successive network code decoding on the MIMO K-way relay channel," *IEEE ICC 2011*, 1–5, Kyoto, Japan, Jun. 2011.
17. Hausl, C. and J. Hagenauer, "Iterative network and channel decoding for the two-way relay channel," *Proc. IEEE Int. Conf. Commun.*, Vol. 4, 1568–1573, Jun. 2006.
18. Lee, N., J.-B. Lim, and J. Chun, "Degrees of the freedom of the MIMO Y channel: Signal space alignment for network coding," *IEEE Trans. Inf. Theory*, Vol. 56, 3332–3342, Jul. 2010.
19. Lee, K., N. Lee, and I. Lee, "Achievable degree of freedom on K-user Y channels with heterogeneous messages," *IEEE Communications Letters*, Vol. 17, No. 2, 333–336, Feb. 2013.