Secrecy Capacity Achieving with Physical Layer Security Approach in MIMO Two-Way Relay Channels

Qiao Liu *†, Guang Gong†, *Fellow, IEEE*, Yong Wang* and Hui Li* *The State Key Lab of ISN, Xidian University, Xi'an, Shaanxi, China †Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, Canada
Emails: {qiao.liu, ggong}@uwaterloo.ca, {wangyong, lihui}@mail.xidian.edu.cn

Abstract

In this paper, we propose a novel secure transmission scheme for MIMO Two-Way Relay Channels. By exploiting the properties of the transmission medium in the physical layer, our proposed scheme could achieve a high transmission efficiency as well as security. Two different approaches has been introduced including Information Theoretical approach and Physical Layer Encryption approach. Direction Rotation Alignment technique is the backbone of our scheme that is used to support high efficiency and security. We show our scheme is secure under three different adversarial models: 1) Untrusted relay attack model; 2) Trusted relay with eavesdropper attack model; 3) Untrusted relay with eavesdroppers attack model. Using the two different approaches, the secrecy capacities of our proposed scheme have been developed under these three models. Finally, simulation results are conducted to demonstrate that compared to the existing schemes, our proposed scheme could achieve a better performance in both transmission efficiency and security.

I. Introduction

As two key techniques in LTE-Advanced, cooperation relaying and MIMO are playing more and more important roles in wireless networks. To meet the high rates requirement in a cost efficient way, these two techniques are used in LTE-Advanced to provide more possibility of heterogeneous network planning as well as spectral efficiency increasing. So the MIMO Two-Way Relay Channels (TWRC), as an integration of these two key techniques, have certainly attracted increasing attentions in the recent years. It has been shown in a lot of works [1–7] that MIMO TWRC channels can drastically improve the transmission performance. At the same time, using the physical layer approach is one of the most promising techniques to secure this type of channel. Consequently, finding a physical layer transmission scheme with high transmission efficiency would undoubtedly be of theoretical and practical interests.

Along with the pioneered study by Wyner [8], physical layer security problems were first introduced into MIMO case by Hero [9] utilizing space–time code at the transmitter to enhance information security and hiding capabilities. After that the research of multiple antennas are mainly focus on MISO (Multi-input Single-output) [10] or SIMO (Single-input Multi-output) [11] until Khisti *et al.* analyzed the MIMO wiretap channel secrecy capacity in [12], and they give an upper bound for secrecy capacity under the situation that the transmitter know the instantaneous channel state information (CSI) about the eavesdropper. After that, a lot of researchers are aimed at giving a secrecy capacity bound by different approaches and different constraints [13–15].

The physical layer security in cooperation relaying was first considered in [16]. Depending on the relay adversarial model, the security problems in cooperation relaying system are divided into two parts in [17]: 1) Untrusted relay model; 2) Trusted relay model.

For the untrusted relay model, the relay itself acts as an untrusted node which may attempt to illegitimately recover the information messages from the users. This is a common case in the Ad-hoc network, since many potential unfriendly devices exist in the Ad-hoc network and some of them are eager to wiretap to the messages by providing the fake assistance. In [18], the authors give a joint source and relay secure beamforming design for the one-way MIMO untrusted relay model. Transmitting jamming signals by friendly jammers in [19] is a secure method for TWRC channels, but the selection of friendly jammers will be difficult to realize in practice. The authors in [20] give an approach to achieve secrecy capacity in MIMO two-way untrusted relay channels based on the signal alignment precoding. However, this scheme is power inefficient especially in the bad channel condition. So the optimization of signal alignment is critical in improving the secrecy capacity.

For the trusted relay model, the relay assists the legitimate users to achieve secure transmission. A lot of works have focused on the single antenna system. Securing the trusted relay model for MIMO systems was first introduced in [21], which uses artificial noise alignment to jam the eavesdropper. The authors in [22] present a physical layer network coding design with secure precoding for Two-Way MIMO trusted relay channels.

After reviewing these existing solutions in the literature, we feel considerable improvements can be made in terms of transmission efficiency and security for MIMO TWRC channels. Two approaches has been introduced based on different performance requirement including information theoretical approach and physical layer encryption approach.

Motivated by [5], we use *Direction Rotation Alignment* as the key to our information theoretical approach. From the transmission efficiency aspects, Direction Rotation Alignment can overcome the power loss in signal alignment scheme. From the physical layer security aspects, the alignment of the two separated signals causes the received signal to be a signal sum in the view of the intended receivers, relay and eavesdroppers. However, only the intended receivers can directly decode the information symbols from their communication partners with their self-information serving as the private key. While the relay or eavesdroppers can obtain partial information with the sum signal. Therefore, by finding the ideal transmission rate, the system can achieve information theoretical security.

On the other hand, encryption vector has been nested into precoding matrix in physical layer encryption approach. After physical layer encryption, signal directions of each user will be distorted. So these will certainly bring enough confusion to the adversaries. With such encryption, the system can achieve computational security.

The main contribution and results of this paper are listed below:

- A new information theoretical security approach is introduced with key technique Direction Rotation Alignment. This technique can eliminate the power loss caused by signal alignment. At the same time, this technique can conceal user message to achieve information theoretical security.
- Following information theoretical approach, physical layer encryption approach is presented to achieve better transmission efficiency and security performance.
- We show that our proposed scheme is secure under three different adversary models: Untrusted relay attack model; 2) Trusted relay with eavesdropper attack model; 3) Untrusted relay with eavesdroppers attack model. To the best of our knowledge, our scheme is the first secure

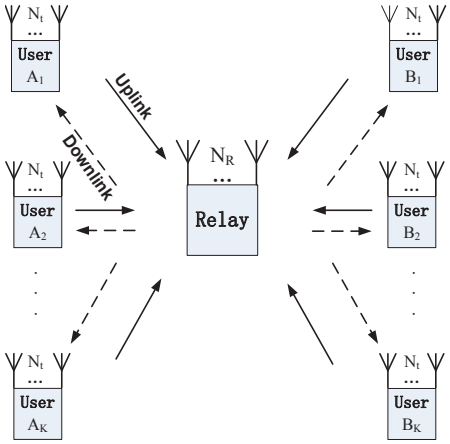

Fig. 1. The Channel Model of Multi-Users MIMO Two-Way Relay Channels

method in all these adversary models

- We analyze the secrecy capacities of the two approaches under each adversary model. With such analysis, ideal transmission rate could be found.

The paper is organized as follows. In Section II, we introduce the system and adversarial models. Section III presents information theoretical approach as well as the capacity analysis under different adversarial models. And the physical layer encryption approach with its capacity analysis is been discussed in Section IV. In Section V, we demonstrate simulation results on our proposed scheme. Finally, we give conclusions and extensions in Section V.

Notations: $\mathrm{Tr}(\cdot)$, $\varepsilon(\cdot)$, $(\cdot)^{-1}$ and $\det(\cdot)$ denote the trace, expectation, inverse or pseudo-inverse and determinant of matrix, respectively. And $[x]^+$ denotes the max $(0, x)$.

II. System Model

A. Transmission Model

1) Channel Model: In this subsection, we will describe the TWRC channels system. This is depicted in Fig. 1. *K* communication pairs exchange their information with a relay. The users on the left side in Fig. 1 are denoted as A_k $(k \in \kappa\{\kappa = 1, 2, \cdots K\})$ and the users on the right side are denoted as B_k. Furthermore, we assume each user is equipped with n_T antennas, and the relay is equipped with n_R antennas.

Both the relay and users work in half-duplex mode and there is no direct link between each pair. We assume all the channels experience the flat-fading and the channel coefficient between user $m\,(m \in \{A_k, B_k\})$ and relay is $\mathbf{H}_m$ which is an $n_R * n_T$ matrix. The channel coefficient between relay and user *m* is $\mathbf{G}_m$ with the size of $n_T * n_R$. Since all channels experience flat fading, both $\mathbf{H}_m$ and $\mathbf{G}_m$ are kept constant in each round of information exchange. Finally, the channel state information (CSI) is available for the users and relay.

The proposed transmission protocol consists of two time slots to accomplish one round of information exchange. In the first time slot, all users transmit their information to the relay simultaneously. Because the users act as a source node in the first time slot, this time slot is called up-link phase or multiple access (MAC) phase. Upon receiving the message, the relay broadcasts its signal in the second time slot with the name of down-link or broadcast phase (BC). Now we introduce the two phases separately.

2) Up-link Phase: In the Up-link Phase (MAC), the relay receives the converging signals from all the user nodes as:

$$\mathbf{Y}_R = \sum_{k=1}^{K} (\mathbf{H}_{A_k}\mathbf{X}_{A_k} + \mathbf{H}_{B_k}\mathbf{X}_{B_k}) + \mathbf{Z}_R, \tag{1}$$

where $\mathbf{X}_{A_k}$ is an $n_T * 1$ column vector represents the transmitted signal vector of user A_k containing the information message $\mathbf{c}_{A_k}$; $\mathbf{X}_{B_k}$ represents the transmitted signal of user B_k; $\mathbf{Y}_R$ denotes the received signal vector by relay, which is an $n_R * 1$ column vector; and $\mathbf{Z}_R$ is an $n_R * 1$ zero mean circularly symmetric complex Gaussian noise vector at the relay node modelled by $\mathbf{Z}_R \sim \mathcal{CN}(\mathbf{0}, \mathbf{I})$.

We denote the covariances of the channel inputs in user m is $\mathbf{Q}_m = \varepsilon\left(\mathbf{X}_m\mathbf{X}_m^H\right)$. Then we have the power constraint in up-link phase like:

$$\mathrm{Tr}\left\{\sum_{k=1}^{K} (\mathbf{Q}_{A_k} + \mathbf{Q}_{B_k})\right\} \leq P_T. \tag{2}$$

3) Down-link Phase: In the Down-link phase (BC), the relay broadcasts its signal $\mathbf{X}_R$ to all users, and each user recovers the information message from its communication partner.

The relay is set up as Amplify-and-Forward (AF) model in the proposed scheme. Thus, the transmitted signal $\mathbf{X}_R$ of relay is just the same as the received signal $\mathbf{Y}_R$.

Then we consider the situation in user A_m as a case. In A_m, we have the observer as

$$\mathbf{Y}_{A_m} = \mathbf{G}_{A_m}\mathbf{X}_R + \mathbf{Z}_{A_m}, \tag{3}$$

where $\mathbf{Z}_{A_m}$ is the zero mean circularly symmetric complex Gaussian noise vector at the user A_m modelled by $\mathbf{Z}_{A_m} \sim \mathcal{CN}(\mathbf{0}, \mathbf{I})$. The user A_m then decodes the partner's message $\mathbf{c}_{B_m}$ with the help of its self-information and detection vector.

B. Adversary Model

In this subsection, we will discuss the system security model for MIMO TWRC channels. We divide the system security model into untrusted relay attack model and trusted relay with eavesdropper attack model two cases.

1) Untrusted Relay Adversary Model: With a pessimistic consideration, we assume the relay itself is an untrusted node. Under such assumption, the relay acts as an eavesdropper to wiretap message from the communication pairs illegitimately. In order to exchange information, each user regulates its transmission rate to guarantee the successful transmission and to resist the untrusted relay attack. In doing so, we could obtain the achievable secrecy channel capacity C_{TR}^s as:

$$C_s^{UR} = \left[\sum_{k=1}^{K} \left(R_{A_k}^{UR} + R_{B_k}^{UR}\right) - R_R^{UR}\right]^+, \tag{4}$$

where $R_{A_k}^{UR}$ and $R_{B_k}^{UR}$ are the achievable maximum information rate from user A_k and B_k to their respective partners as:

$$R_{A_k}^{UR} = \frac{1}{2} I\left(\mathbf{Y}_{B_k}; \mathbf{X}_{A_k} \mid \mathbf{Y}_R, \mathbf{X}_R\right), \tag{5}$$

$$R_{B_k}^{UR} = \frac{1}{2} I\left(\mathbf{Y}_{A_k}; \mathbf{X}_{B_k} \mid \mathbf{Y}_R, \mathbf{X}_R\right). \tag{6}$$

And R_R^{UR} denotes the achievable information rate at the untrusted relay as:

$$R_R^{UR} = \frac{1}{2} I(\mathbf{Y}_R; \mathbf{X}_{A_1}, \mathbf{X}_{A_2}, \cdots, \mathbf{X}_{A_k}, \mathbf{X}_{B_1}, \cdots, \mathbf{X}_{B_k}). \tag{7}$$

Note here that the achievable secrecy channel capacity above is a general result independent of the transmission scheme. One of our goals in this paper is developing a novel scheme to achieve high capacity in an untrusted relay attack model scenario.

2) Trusted Relay with Eavesdropper Adversary Model: In this subsection we consider the situation where the communication pair exchanges their information message via a trusted relay in the presence of the eavesdroppers. We assume there exists an eavesdropper E_m in between users A_m and B_m. In addition, the eavesdropper has the complete knowledge of the channel information and transmission protocol. Furthermore, let the channel coefficient between user and eavesdropper be $\mathbf{H}_{A_m}^E$ and $\mathbf{H}_{B_m}^E$ respectively, then the received signal by the eavesdropper Y_{E_m} is:

$$\mathbf{Y}_{E_m} = \mathbf{H}_{A_m}^E \mathbf{X}_{A_m} + \mathbf{H}_{B_m}^E \mathbf{X}_{B_m} + \mathbf{Z}_{E_m}, \tag{8}$$

where $\mathbf{Z}_{E_m}$ is the noise at eavesdropper E_m. And upon receiving the $\mathbf{Y}_{E_m}$, the eavesdropper tries to recover the information messages $\mathbf{c}_{A_m}$ and $\mathbf{c}_{B_m}$.

The MIMO wiretap channel introduced by [23] can be considered as multiple and parallel single sub wiretap channels, each sub channel contains the communication user pair and the potential eavesdroppers. In doing so, we obtain the achievable secrecy channel capacity C_s^{TR} for trusted relay with eavesdropper attack model as:

$$C_s^{TR} = \left[\sum_{k=1}^{K} \left(R_{A_k}^{TR} + R_{B_k}^{TR} - R_{E_k}^{TR} \right) \right]^+, \tag{9}$$

where $R_{A_k}^{TR}$ and $R_{A_k}^{TR}$ are the secrecy information rate between users A_k and B_k respectively. They have the identical analysis as (5) and (6):

$$R_{A_k}^{TR} = \frac{1}{2} \left[I \left(\mathbf{Y}_{B_k}; \mathbf{X}_{A_k} \mid \mathbf{Y}_R, \mathbf{X}_R \right) \right], \tag{10}$$

$$R_{B_k}^{TR} = \frac{1}{2} \left[I \left(\mathbf{Y}_{A_k}; \mathbf{X}_{B_k} \mid \mathbf{Y}_R, \mathbf{X}_R \right) \right]. \tag{11}$$

And $R_{E_k}^{TR}$ is the information rate at the eavesdropper as:

$$R_{E_k}^{TR} = \frac{1}{2} \left[I \left(\mathbf{Y}_{E_k}; \mathbf{X}_{A_k}, \mathbf{X}_{B_k} \right) \right]. \tag{12}$$

The secrecy channel capacity here is also a general result.

3) Untrusted Relay with Eavesdropper Adversary Model: In the worst case, the relay itself is an unfriendly node, meanwhile there exists a considerable number of eavesdroppers between each communication pair. We hold the same assumption as the above two subsection, then we can obtain the achievable secrecy capacity C_s in such scenario as:

$$C_s^{UE} = \left[\sum_{k=1}^{K} \left(R_{A_k}^{UE} + R_{B_k}^{UE} - R_{E_k}^{UE} \right) - R_R^{UE} \right]^+, \tag{13}$$

where $R_{A_k}^{UE}$ and $R_{B_k}^{UE}$ are the secrecy information rate between users A_k and B_k respectively, and they still have the identical analysis as (5) and (6):

$$R_{A_k}^{UE} = \frac{1}{2} \left[I \left(\mathbf{Y}_{B_k}; \mathbf{X}_{A_k} | \mathbf{Y}_R, \mathbf{X}_R \right) \right], \tag{14}$$

$$R_{B_k}^{UE} = \frac{1}{2} \left[I \left(\mathbf{Y}_{A_k}; \mathbf{X}_{B_k} | \mathbf{Y}_R, \mathbf{X}_R \right) \right]. \tag{15}$$

And $R_{E_k}^{UE}$ and R_R^{UE} are the information rate at the eavesdropper and untrusted relay respectively as:

$$R_{E_k}^{UE} = \frac{1}{2}\left[I\left(\mathbf{Y}_{E_k}; \mathbf{X}_{A_k}, \mathbf{X}_{B_k}\right)\right]. \tag{16}$$

$$R_R^{UE} = \frac{1}{2} I(\mathbf{Y}_R; \mathbf{X}_{A_1}, \mathbf{X}_{A_2}, \cdots, \mathbf{X}_{A_k}, \mathbf{X}_{B_1}, \cdots, \mathbf{X}_{B_k}). \tag{17}$$

We will discuss the capacity analysis of our proposed scheme in the following section.

III. Achievable Secrecy Transmission Scheme with Information Theoretical Approach

In this section, we will present an achievable secrecy transmission scheme using the information theoretical approach for the all three adversary models.

A. The Transmission Scheme Based on Direction Rotation Alignment

This scheme is composed of two transmission phases and one relay operation phase. The details are shown below.

1) Multiple Access Phase: The information symbols $\mathbf{c}_{A_k}$ (*or* $\mathbf{c}_{B_k}$) are modified by a precoding matrix prior to the transmission. The precoding matrix is used to construct equivalent parallel sub-channels for different communication pairs. The scenario is identical on either user side A_k or B_k, so we only present the design for A_k. The precoding matrix on user A_k is denoted as $\mathbf{F}_{A_k}$. Then the transmitted signal could be rewritten as: $\mathbf{X}_{A_k} = \mathbf{F}_{A_k} \cdot \mathbf{c}_{A_k}$.

We now move on to investigate the design of precoding matrix $\mathbf{F}_{A_k}$. Using the singular value decomposition (SVD), the channel matrix $\mathbf{H}_{A_k}$ could be represented as follows:

$$\mathbf{H}_{A_k} = \mathbf{U}_{A_k} \mathbf{\Sigma}_{A_k} \mathbf{V}_{A_k}^H, \tag{18}$$

where $\mathbf{U}_{A_k}$ and $\mathbf{V}_{A_k}$ are unitary matrices and $\mathbf{\Sigma}_{A_k}$ is a diagonal matrix with positive diagonal elements. So we define the $\mathbf{F}_{A_k}$ in the following form:

$$\mathbf{F}_{A_k} = \mathbf{V}_{A_k} \mathbf{\Sigma}_{A_k}^{-1} \mathbf{U}_{A_k}^H \mathbf{R} \mathbf{\Psi}_{A_k} \mathbf{L}_k, \tag{19}$$

where $\mathbf{R}$ is an $n_R * n_R$ unitary matrix called *Direction Rotation matrix* and $\mathbf{\Sigma}_{A_k}^{-1}$ denotes the pseudo-inverse of $\mathbf{\Sigma}_{A_k}$. $\mathbf{\Psi}_{A_k}$ represents the allocated transmission power for user A_k. In addition, we assume it is identical for all users in this work. The $\mathbf{L}_k$ is called *channel allocation matrix* to guarantee multi-pair users communicate simultaneously. $\mathbf{L}_k$ allocates the constructed equivalent parallel sub-channels to corresponding users.The design and optimization of $\mathbf{R}$ and $\mathbf{L}_k$ will affect the transmission efficiency of proposed scheme. Then we will introduce the design of $\mathbf{R}$ and $\mathbf{L}_k$ respectively.

Design of *Direction Rotation matrix*: The authors in [5] have given an approximate design of Direction Rotation matrix for One-pair TWRC channels. Along with their work, we extend their results into Multi-pair TWRC channels.

Before design $\mathbf{R}$, we first define a new matrix $\mathbf{G}$ as:

$$\mathbf{G} \triangleq \sum_{k=1}^{K} \left\{ \mathbf{U}_{A_k} \mathbf{\Sigma}_{A_k}^{-2} \mathbf{U}_{A_k}^H + \mathbf{U}_{B_k} \mathbf{\Sigma}_{B_k}^{-2} \mathbf{U}_{B_k}^H \right\}. \tag{20}$$

Using Eigen-decompose, the $\mathbf{G}$ could be represented as:

$$\mathbf{G} = \mathbf{U}_g \mathbf{\Lambda}_g \mathbf{U}_g^H, \tag{21}$$

where $\mathbf{U_g}$ is an unitary matrix and $\mathbf{\Lambda}_g$ is a diagonal matrix whose non-zero elements are the Eigen-values of $\mathbf{G}$ arranged in the ascending order. Then we choose $\mathbf{R}$ as:

$$\mathbf{R} = \mathbf{U_g}. \tag{22}$$

Design of *channel allocation matrix*: Before designing $\mathbf{L}_k$, we first define two varieties d_k and D_k. d_k is the independent signal streams of the kth communicate pair, and D_k is the sum independent signal streams of the 1th communicate pair to the kth as:$D_k = \sum_{i=1}^{k-1} d_i$. In order to align the signals from the same communication pair to the same directions, we define $\mathbf{L}_{A_k} = \mathbf{L}_{B_k} = \mathbf{L_k}$. And the $\mathbf{L_k}$ is designed by collecting the $D_k + 1$ to $D_k + d_k$ column vector from the $n_R * n_R$ unit matrix, so the $\mathbf{L}_k$ is in the size of $n_R * d_k$. The $\mathbf{L}_k$ is showed as follow:

$$\mathbf{L}_k = \begin{bmatrix} & \overbrace{\quad}^{d_k} \\ D_k \begin{cases} 00...0 \\ 00...0 \\ ... \\ 00...0 \end{cases} \\ d_k \begin{cases} 10...0 \\ 01...0 \\ ... \\ 00...1 \end{cases} \\ 00...0 \\ ... \\ 00...0 \end{bmatrix}. \tag{23}$$

2) Relay's Operation: After the precoding operation, the users transmit their coded signal to the relay. Then the received signal in relay is:

$$\mathbf{Y}_R = \sum_{k=1}^{K} (\mathbf{H}_{A_k}\mathbf{F}_{A_k}\mathbf{c}_{A_k} + \mathbf{H}_{B_k}\mathbf{F}_{B_k}\mathbf{c}_{B_k}) + \mathbf{Z}_R. \tag{24}$$

For $k \in \{A_k, B_k\}$, we have

$$\begin{aligned} \mathbf{H}_k\mathbf{F}_k =& \mathbf{U}_k\Sigma_k\mathbf{V}_k^H\mathbf{V}_k\mathbf{\Sigma}_k^{-1}\mathbf{U}_k^H\mathbf{R}\mathbf{L}_k \\ =& \mathbf{R}\mathbf{L}_k, \end{aligned} \tag{25}$$

so the received signal $\mathbf{Y}_R$ could be rewritten as

$$\begin{aligned} \mathbf{Y}_R =& \mathbf{R}\sum_{k=1}^{K} \mathbf{A}_k (\mathbf{c}_{A_k} + \mathbf{c}_{B_k}) + \mathbf{Z}_R \\ =& \mathbf{R} \begin{bmatrix} \mathbf{c}_{A_1} + \mathbf{c}_{B_1} \\ \mathbf{c}_{A_2} + \mathbf{c}_{B_2} \\ \cdots \\ \mathbf{c}_{A_K} + \mathbf{c}_{B_K} \end{bmatrix} + \mathbf{Z}_R \end{aligned} \tag{26}$$

As shown in (26), the signals from the same communication pairs have been aligned into the same directions.

Upon receiving $\mathbf{Y}_R$, the relay generates its transmitting signal $\mathbf{X}_R$. In the amplify-forward (AF) agreements, the relationship between $\mathbf{X}_R$ and $\mathbf{Y}_R$ is simply written as $\mathbf{X}_R = \mathbf{Y}_R$.

3) Broadcast Phase: In the BC phase, each user receives the broadcast signal from the relay. By considering the received signal at user B_m, we can obtain:

$$\begin{aligned}\mathbf{Y}_{B_m} &= \mathbf{G}_{B_m}\mathbf{X}_R + \mathbf{Z}_{B_m} \\ &= \mathbf{G}_{B_m}\sum_{k=1}^{K}\left(\mathbf{H}_{A_k}\mathbf{F}_{A_k}\mathbf{c}_{A_k} + \mathbf{H}_{B_k}\mathbf{F}_{B_k}\mathbf{c}_{B_k}\right) \\ &\quad + \mathbf{G}_{B_m}\mathbf{Z}_R + \mathbf{Z}_{B_k}.\end{aligned} \tag{27}$$

Subtracting the self-interference and the co-channel interference from other communication pairs, the user B_m could obtain the equivalent receiving signal $\tilde{\mathbf{Y}}_{B_k}$ as:

$$\tilde{\mathbf{Y}}_{B_m} = \mathbf{G}_{B_m}\mathbf{H}_{A_m}\mathbf{F}_{A_m}\mathbf{c}_{A_m} + \mathbf{G}_{B_m}\mathbf{Z}_R + \mathbf{Z}_{A_m}. \tag{28}$$

The interference cancellation will be accomplished by the detection vector $\mathbf{D}_{A_m}$. $\mathbf{D}_{A_m}$ is depend on $\mathbf{G}_{A_m}$. Consider the case where $\mathbf{G}_{A_m}$ is simply the transpose of $\mathbf{H}_{A_m}$. Then the $\mathbf{D}_{A_m}$ is designed such that $\mathbf{D}_{B_m} = \mathbf{L}_m^H\mathbf{R}^H\mathbf{U}_{B_m}\left(\Sigma_{B_m}^H\right)^{-1}\mathbf{V}_{B_m}^H$. Consequently, the received signal will be:

$$\begin{aligned}\tilde{\mathbf{Y}}_{B_m} &= \mathbf{D}_{B_m}\mathbf{Y}_{B_m} \\ &= \mathbf{D}_{B_m}\left(\mathbf{H}_{B_m}^H\mathbf{X}_R + \mathbf{Z}_{B_m}\right) \\ &= \mathbf{L}_m^H\mathbf{R}^H\mathbf{U}_{B_m}\left(\Sigma_{B_m}^H\right)^{-1}\mathbf{V}_{B_m}^H\mathbf{V}_{B_m}\Sigma_{B_m}^H\mathbf{U}_{B_m}^H\mathbf{R} \\ &\quad \cdot\sum_{k=1}^{K}\mathbf{L}_m\left(\mathbf{c}_{A_m} + \mathbf{c}_{B_m}\right) + \mathbf{D}_{B_m}\mathbf{Z}_R + \mathbf{Z}_{B_m} \\ &= \left(\mathbf{c}_{A_m} + \mathbf{c}_{B_m}\right) + \mathbf{Z}_{B_m}^{'},\end{aligned} \tag{29}$$

where $\mathbf{Z}_{B_m}^{'}$ denotes the sum of noise in user B_m.

From (29), we can clearly see that the user B_m could recover the information symbols $\mathbf{c}_{A_m}$ by the XOR operation with its self-information symbols $\mathbf{c}_{B_m}$. Exactly alike, the user A_m could recover the information symbols from B_m in the same way. Thus one round of information exchange is completed.

B. The Achievable Secrecy Channel Capacity Analysis for Untrusted Relay Model

In this subsection, we discuss the achievable secrecy channel capacity of our proposed scheme for the untrusted relay model based on the analysis given in the previous section. From (4), we can see that the capacity is affected by R_R^{UR} and $\left\{R_{A_1}^{UR}, R_{A_2}^{UR}, \cdots, R_{A_K}^{UR}, R_{B_1}^{UR}, \cdots R_{A_K}^{UR}\right\}$. We now discuss the impact of these components and obtain the achievable secrecy channel capacity C_s^{UR}.

After one round of transmission, the received equivalent information at user B_m is shown in (29). The information rate from A_m to B_m is:

$$\begin{aligned}R_{A_m}^{UR} &= \frac{1}{2}\text{logdet}\left(\mathbf{I} + \mathbf{F}_{A_m}^H\mathbf{H}_{A_m}^H\mathbf{G}_{B_m}^H\mathbf{K}_{A_m}^{-1}\mathbf{G}_{B_m}\mathbf{H}_{A_m}\mathbf{F}_{A_m}\right) \\ &= \frac{1}{2}\log\det\left(\mathbf{I} + \mathbf{L}_m^H\mathbf{R}\mathbf{G}_{B_m}^H\mathbf{K}_{A_m}^{-1}\mathbf{G}_{B_m}\mathbf{R}\mathbf{L}_m\right),\end{aligned} \tag{30}$$

where $\mathbf{K}_{A_m} = \mathbf{G}_{B_m}\mathbf{G}_{B_m}^H + \mathbf{I}$.

Similarly, the information rate from B_m to A_m is:

$$R_{B_m}^{UR} = \frac{1}{2}\log\det\left(\mathbf{I} + \mathbf{L}_m^H\mathbf{R}\mathbf{G}_{A_m}^H\mathbf{K}_{B_m}^{-1}\mathbf{G}_{A_m}\mathbf{R}\mathbf{L}_m\right). \tag{31}$$

For the untrusted relay model, the adversary tries to recover the message symbols from all the users node. So the achievable information rate equals to the maximum sum rate of the up-link multi-user MAC channel:

$$R_R^{UR} = \frac{1}{2}\log\det\left[\mathbf{I} + \sum_{k=1}^{K}\left(\mathbf{H}_{A_k}\mathbf{F}_{A_k}\mathbf{F}_{A_k}^H\mathbf{H}_{A_k}^H + \mathbf{H}_{B_k}\mathbf{F}_{B_k}\mathbf{F}_{B_k}^H\mathbf{H}_{B_k}^H\right)\right]. \tag{32}$$

From (30), (31) and (32), the achievable secrecy channel capacity for the untrusted relay model can be obtained with matrix operation [24] as:

$$C_s^{UR} = \frac{1}{2}\log\det\left[\frac{\prod_{k=1}^{K}\left(\mathbf{I} + \mathbf{L}_k^H\mathbf{R}\mathbf{G}_{B_k}^H\mathbf{K}_{A_k}^{-1}\mathbf{G}_{B_k}\mathbf{R}\mathbf{L}_k\right)\left(\mathbf{I} + \mathbf{L}_k^H\mathbf{R}\mathbf{G}_{A_k}^H\mathbf{K}_{B_k}^{-1}\mathbf{G}_{A_k}\mathbf{R}\mathbf{L}_k\right)}{\mathbf{I} + \sum_{k=1}^{K}\left(\mathbf{H}_{A_k}\mathbf{F}_{A_k}\mathbf{F}_{A_k}^H\mathbf{H}_{A_k}^H + \mathbf{H}_{B_k}\mathbf{F}_{B_k}\mathbf{F}_{B_k}^H\mathbf{H}_{B_k}^H\right)}\right] \tag{33}$$

C. The Achievable Secrecy Channel Capacity Analysis for Trusted Relay with Eavesdropper Model

In this subsection, we will discuss the achievable secrecy channel capacity of our proposed scheme for the trusted relay with eavesdropper model. Before discussing the capacity, we first consider the received signal by eavesdropper E_m between the users A_m and B_m.

The received signal in general case is shown in (8), and for the proposed scheme we have:

$$\mathbf{Y}_{E_m} = \mathbf{H}_{A_m}^E\mathbf{F}_{A_m}\mathbf{c}_{A_m} + \mathbf{H}_{B_m}^E\mathbf{F}_{B_m}\mathbf{c}_{B_m} + \mathbf{Z}_{E_m}, \tag{34}$$

where the $\mathbf{Z}_{E_m}$ is noise at eavesdropper E_m. Consequently, we have the achievable information rate as:

$$R_{E_m}^{TR} = \frac{1}{2}\text{logdet}\left[\mathbf{I} + \mathbf{H}_{A_m}^E\mathbf{F}_{A_m}\mathbf{F}_{A_m}^H\left(\mathbf{H}_{A_m}^E\right)^H + \mathbf{H}_{B_m}^E\mathbf{F}_{B_m}\mathbf{F}_{B_m}^H\left(\mathbf{H}_{B_m}^E\right)^H\right]. \tag{35}$$

Meanwhile, the information rate $R_{A_m}^{TR}$ and $R_{B_m}^{TR}$ are identical to the untrusted relay model, namely:

$$R_{A_m}^{TR} = \frac{1}{2}\log\det\left(\mathbf{I} + \mathbf{L}_m^H\mathbf{R}\mathbf{G}_{B_m}^H\mathbf{K}_{A_m}^{-1}\mathbf{G}_{B_m}\mathbf{R}\mathbf{L}_m\right), \tag{36}$$

$$R_{B_m}^{TR} = \frac{1}{2}\log\det\left(\mathbf{I} + \mathbf{L}_m^H\mathbf{R}\mathbf{G}_{A_m}^H\mathbf{K}_{B_m}^{-1}\mathbf{G}_{A_m}\mathbf{R}\mathbf{L}_m\right). \tag{37}$$

As a result, we obtain the achievable secrecy channel capacity as:

$$C_s^{TR} = \frac{1}{2}\log\det\left[\sum_{k=1}^{K}\frac{\left(\mathbf{I} + \mathbf{L}_k^H\mathbf{R}\mathbf{G}_{B_k}^H\mathbf{K}_{A_k}^{-1}\mathbf{G}_{B_k}\mathbf{R}\mathbf{L}_k\right)\left(\mathbf{I} + \mathbf{L}_k^H\mathbf{R}\mathbf{G}_{A_k}^H\mathbf{K}_{B_k}^{-1}\mathbf{G}_{A_k}\mathbf{R}\mathbf{L}_k\right)}{\mathbf{I} + \mathbf{H}_{A_k}^E\mathbf{F}_{A_k}\mathbf{F}_{A_k}^H\left(\mathbf{H}_{A_k}^E\right)^H + \mathbf{H}_{B_k}^E\mathbf{F}_{B_k}\mathbf{F}_{B_k}^H\left(\mathbf{H}_{B_k}^E\right)^H}\right] \tag{38}$$

D. The Secrecy Channel Capacity Analysis for Untrusted Relay with Eavesdropper Model

We will discuss the secrecy channel capacity for the worst case: the relay itself is an unfriendly node, meanwhile there exists a considerable number of eavesdroppers between each communication pair. The situation under this case is just like a combination of the former two case, and the general capacity analysis of this model is given by (13). So we first give the all components based on the former two subsection, and then give the achievable secrecy channel capacity.

The information rate $R_{A_m}^{UE}$ and $R_{B_m}^{UE}$ are given as:

$$R_{A_m}^{UE} = \frac{1}{2}\log\det\left(\mathbf{I} + \mathbf{L}_m^H\mathbf{R}\mathbf{G}_{B_m}^H\mathbf{K}_{A_m}^{-1}\mathbf{G}_{B_m}\mathbf{R}\mathbf{L}_m\right), \tag{39}$$

$$R_{B_m}^{UE} = \frac{1}{2}\log\det\left(\mathbf{I} + \mathbf{L}_m^H\mathbf{R}\mathbf{G}_{A_m}^H\mathbf{K}_{B_m}^{-1}\mathbf{G}_{A_m}\mathbf{R}\mathbf{L}_m\right). \tag{40}$$

And the achievable information rate at the untrusted relay is given as:

$$R_R^{UE} = \frac{1}{2}\log\det\left[\mathbf{I} + \sum_{k=1}^{K}\left(\mathbf{H}_{A_k}\mathbf{F}_{A_k}\mathbf{F}_{A_k}^H\mathbf{H}_{A_k}^H + \mathbf{H}_{B_k}\mathbf{F}_{B_k}\mathbf{F}_{B_k}^H\mathbf{H}_{B_k}^H\right)\right]. \tag{41}$$

And the achievable information rate at eavesdropper is given as:

$$R_{E_m}^{UE} = \frac{1}{2}\text{logdet}\left[\mathbf{I} + \mathbf{H}_{A_m}^E\mathbf{F}_{A_m}\mathbf{F}_{A_m}^H\left(\mathbf{H}_{A_m}^E\right)^H + \mathbf{H}_{B_m}^E\mathbf{F}_{B_m}\mathbf{F}_{B_m}^H\left(\mathbf{H}_{B_m}^E\right)^H\right]. \tag{42}$$

With (39), (40), (41) and (42), we obtain the achievable secrecy channel capacity as:

$$C_s^{UE} = \frac{1}{2}\log\det\left\{\frac{\sum_{k=1}^{K}\frac{\left(\mathbf{I}+\mathbf{L}_k^H\mathbf{R}\mathbf{G}_{B_k}^H\mathbf{K}_{A_k}^{-1}\mathbf{G}_{B_k}\mathbf{R}\mathbf{L}_k\right)\left(\mathbf{I}+\mathbf{L}_k^H\mathbf{R}\mathbf{G}_{A_k}^H\mathbf{K}_{B_k}^{-1}\mathbf{G}_{A_k}\mathbf{R}\mathbf{L}_k\right)}{\mathbf{I}+\mathbf{H}_{A_k}^E\mathbf{F}_{A_k}\mathbf{F}_{A_k}^H\left(\mathbf{H}_{A_k}^E\right)^H+\mathbf{H}_{B_k}^E\mathbf{F}_{B_k}\mathbf{F}_{B_k}^H\left(\mathbf{H}_{B_k}^E\right)^H}}{\mathbf{I}+\sum_{k=1}^{K}\left(\mathbf{H}_{A_k}\mathbf{F}_{A_k}\mathbf{F}_{A_k}^H\mathbf{H}_{A_k}^H + \mathbf{H}_{B_k}\mathbf{F}_{B_k}\mathbf{F}_{B_k}^H\mathbf{H}_{B_k}^H\right)}\right\} \tag{43}$$

Note here that C_s^{UE} has great probability equaling to zero, and it is a common case independent with transmission scheme. So immediately we have this question: how to optimize the proposed scheme to secrecy transmission even under the worst case. For this reason, we optimize the precoding nested physical layer encryption. The design details will be presented in the following section.

IV. Secrecy Transmission Scheme with Physical Layer Encryption Approach

In above section, we have discussed the secrecy transmission scheme based information theoretical analysis. However, the traditional information theoretical approach achieve secrecy by sacrificing the transmission efficiency. And all the schemes including our proposed information theoretical approach are not constantly valid for the worst case.

Under this motivation, we design a encryption vector nested into the precoding matrix to accomplish the message encryption in the physical layer. With this physical layer encryption, the system security will only depend on the security of the shared secret key rather than the mutual information in eavesdropper or untrusted relay. So the channel could achieve full capacity instead of part of it. In this section, we will first present the physical layer encryption scheme in MIMO TWRC channels, then present the capacity analysis for physical layer encryption.

A. Physical Layer Encryption Scheme

In order to accomplish the encryption, we redesign the precoding matrix as $\mathbf{P}_{A_m}$ and $\mathbf{P}_{B_m}$ for user A_m and B_m. We consider the situation in A_m as a case. Containing two function parts, the $\mathbf{P}_{A_m}$ can be artificially divide into two parts as:

$$\mathbf{P}_{A_m} = \mathbf{F}_{A_m}\mathbf{S}_{A_m} \tag{44}$$

where the $\mathbf{F}_{A_m}$ is designed as same as the above discussion, and the $\mathbf{S}_{A_m}$ is designed for physical layer encryption. Note that although we artificially separate the precoding matrix into transmission and security matrix, the precoding matrix affects in its entirety.

The encryption precoding matrix $\mathbf{S}_{A_m}$ or $\mathbf{S}_{B_m}$ is generated from a key stream $\mathbf{s}_m$ where $s_m(i) \in \{1, -1\}$. The generation of $\mathbf{S}_{A_m}$ and $\mathbf{S}_{B_m}$ will depend on the security level of the system. For low security level, the $\mathbf{S}_{A_m}$ and $\mathbf{S}_{B_m}$ will just be equal to $\mathbf{s}_m$ as $\mathbf{S}_{A_m} = \mathbf{S}_{B_m} = \mathbf{s}_m$. For high level security, the $\mathbf{S}_{A_m}$ and $\mathbf{S}_{B_m}$ will be different by dividing the $\mathbf{s}_m$ into two parts. Note here that

the key stream must be pre-shared between user A_m and B_m before the transmission, and $\mathbf{s}_m$ is produced by pseudorandom sequence generators(PRSG).

With $\mathbf{S}_{A_m}$ and $\mathbf{S}_{B_m}$, each user could encrypt its information symbols bit by bit. And in the next part, we will explore how the proposed encryption scheme to promote the security performance under both untrusted and trusted model.

B. Attack Analysis for Physical Layer Encryption Scheme

We first consider the untrusted relay model. Because the untrusted relay could be viewed as the most powerful eavesdropper, so if the proposed scheme is secure under untrusted relay adversary model, it will certainly be secure under the all adverasary models.

We now begin to discuss the attack analysis under untrusted relay adversary model. With the new precoding matrix, the received signal in relay now will be:

$$\begin{aligned}\mathbf{Y}_R^{Enc} =&\mathbf{R}\sum_{k=1}^{K}\mathbf{A}_k\left(\mathbf{S}_{A_k}\mathbf{c}_{A_k}+\mathbf{S}_{B_k}\mathbf{c}_{B_k}\right)+\mathbf{Z}_R\\ =&\mathbf{R}\begin{bmatrix}\mathbf{S}_{A_1}\mathbf{c}_{A_1}+\mathbf{S}_{B_1}\mathbf{c}_{B_1}\\ \mathbf{S}_{A_2}\mathbf{c}_{A_2}+\mathbf{S}_{B_2}\mathbf{c}_{B_2}\\ \cdots\\ \mathbf{S}_{A_K}\mathbf{c}_{A_K}+\mathbf{S}_{B_K}\mathbf{c}_{B_K}\end{bmatrix}+\mathbf{Z}_R\end{aligned} \tag{45}$$

By comparison, we also consider the relay receiving signal for information theoretical approach as (26). Considering BPSK modulation as a case, and we assume the untrusted relay could get the Direction Rotation matrix $\mathbf{R}$. Then we obtain the data patterns for the two different approaches as follow tables:

TABLE I
BPSK DATA PATTERNS OF USER TRANSMITTING SIGNALS AND RELAY RECEIVING SIGNAL FOR PHYSICAL LAYER ENCRYPTION APPROACH

X_{A_k}	S_{A_k}	X_{B_k}	S_{B_k}	Y_R^{Enc}
1	1	1	1	2
1	1	1	-1	0
1	1	-1	1	0
1	1	-1	-1	2
1	-1	1	1	0
1	-1	1	-1	-2
1	-1	-1	1	-2
1	-1	-1	-1	0
-1	1	1	1	0
-1	1	1	-1	-2
-1	1	-1	1	-2
-1	1	-1	-1	0
-1	-1	1	1	2
-1	-1	1	-1	0
-1	-1	1	-1	0
-1	-1	-1	-1	2

With Table. II we can see that, the untrusted relay could directly recover some characteristic bit like all 1 or all 0. For this reason, the difficulty degree of message recover for untrusted relay is significantly reduced. However, as Table. I, the characteristics will be distorted by the encryption. For example, if $Y_R = 2$, the relay could easily recover the transmitting message pair is $X_{A_k} = 1$

TABLE II
BPSK DATA PATTERNS OF USER TRANSMITTING SIGNALS AND RELAY RECEIVING SIGNAL FOR INFORMATION THEORETICAL APPROACH

X_{A_k}	X_{B_k}	Y_R
1	1	2
1	-1	0
-1	1	0
-1	-1	-2

and $X_{B_k} = 1$. However, if $Y_R^{Enc} = 2$, the transmitting message pair could be all the four cases. So with the physical layer encryption, the untrusted relay have no better way rather than guessing each bit of the messages or the keys.

The attack analysis is identical for the eavesdropper, So we will have no specific explanation. With this analysis, we conclude that our proposed physical layer encryption scheme is secure under all three adversary models.

C. The Achievable Secrecy Channel Capacity Analysis for Physical Layer Encryption Scheme

In this subsection we will investigate the achievable secrecy channel capacity for physical layer encryption scheme. The capacity is presented by theorem:

Theorem 1 *With physical layer encryption, the achievable secrecy channel capacity for MIMO TWRC channels is given by:*

$$C_{Enc} = \left[\sum_{k=1}^{K} (R_{A_k} + R_{B_k}) \right]^+ . \tag{46}$$

where R_{A_k} and R_{B_k} are the secrecy information rate between users A_k and B_k.

The proof of Theorem 1 is given in Appendix.

By comparing (46) with (33), (38) and (43), we can have the following result: because the *log function* is an increasing function, the proposed physical layer encryption scheme evidently increase the sum capacity of the system. However, due to the complexity of key preshare, there will be an apparent trade-off between transmission performance and key preshare complexity. Depending on different performance requirement, the user could choose physical layer encryption approach with better transmission performance or information theoretical approach with lower system complexity.

V. SIMULATION RESULTS

In this section, we present three simulations for our proposed scheme using MATLAB. First, we show our proposed scheme outperforms some of the well-known existing schemes in terms of transmission quality. In the second simulation, we respectively show our proposed scheme has good security by comparing the bit error rate (BER) between the intended receiver and the untrusted relay and the BER between the receiver and the eavesdropper. In the last simulation, we show the capacity of our proposed scheme under the three different adversary models. We assume four pairs of users communicate at the same time via a relay, and the users, relay and eavesdroppers are all equipped with four antennas, i.e., $n_R = n_T = n_E = 4$. Note that all of these results are obtained by averaging over 10,000 realizations.

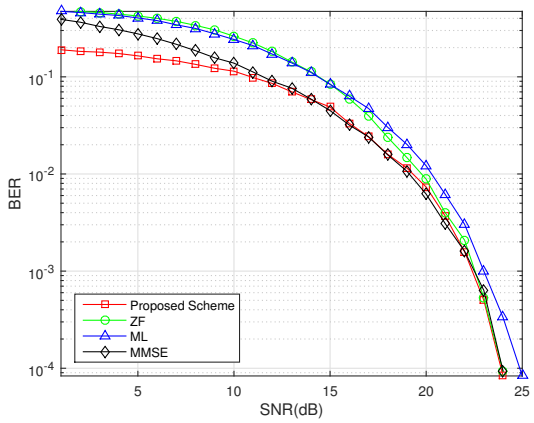

Fig. 2. Transmission Performance Comparison between Proposed Scheme and Existing Schemes

A. Transmission Performance Evaluation between Different Schemes in MIMO TWRC channels

To test the transmission performance of our proposed scheme, we first compare our scheme with some existing well known schemes in MIMO TWRC channels like Zero-Forcing (ZF), Minimum Mean Square Error (MMSE) and Maximum Likelihood (ML). From the simulation results in Fig. 2 we can clearly see that the proposed scheme can achieve a better BER performance especially under low SNR condition. This is because the proposed scheme can effectively avoid the power loss caused by the direction alignment.

B. Security Performance Evaluation of Information Theoretical Approach and Physical Layer Encryption Approach

We then test the security performance of our proposed scheme by comparing the BER of the intended receiver, the untrusted relay and the eavesdropper. The BER comparison between the intended receiver and the untrusted relay is shown in Fig. 3. We assume a stronger adversarial model where the relay can obtain all channel information including the Direction Rotation matrix R. From Fig. 3 we can see that the BER at the intended receiver will decrease with SNR by a large proportion, however the BER at the untrusted relay will stay in the high magnitude constantly. Meanwhile, we can also see that the proposed physical layer encryption will reduce the correct decoding probability at the untrusted relay.

Similar with the untrusted relay adversary model, we compare the BER between the intended receiver and the eavesdropper. The results is shown in Fig. 4. To test different adversarial level, we classify four cases to simulate: information theoretical approach with known Direction Rotation matrix; information theoretical approach without known Direction Rotation matrix; physical layer encryption approach with known Direction Rotation matrix, and physical layer encryption without known Direction Rotation matrix. From Fig. 4 we can see that the eavesdropper gives strongest attack under the first case: information theoretical approach with known Direction Rotation matrix. And if the eavesdropper fails to get the Direction Rotation matrix, the eavesdropper will suffer a worse decoding error ratio which is shown as the second case. However, the security performance of information theoretical approach is not as good as the physical layer encryption approach. From the results of the third and forth cases, we can see that the decoding error bit ratios of these two cases almost the same which is identical to the error ratio of random guessing.

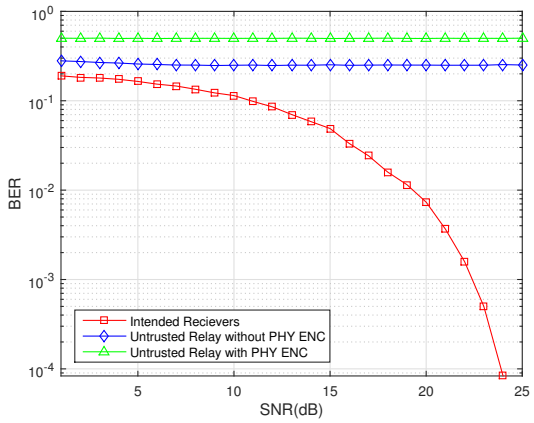

Fig. 3. Security Performance Comparison between the Intended Receiver and the Untrusted Relay

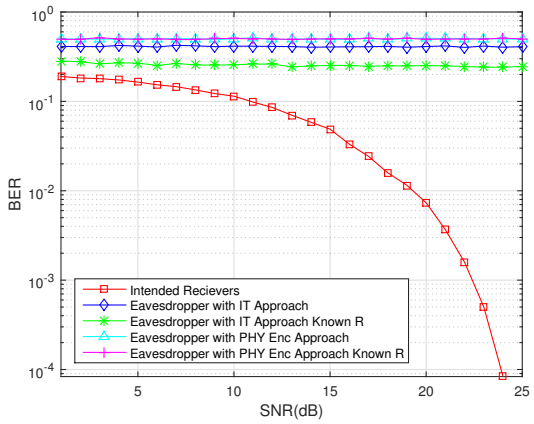

Fig. 4. Security Performance Comparison between the Intended Receiver and the Eavesdropper

C. Secure Channel Capacity Analysis Evaluation between Under Different Adversary Models

In this subsection, we will give the secure channel capacity analysis of under the three different adversary models. The results are shown in Figs. 5 to 7.

We compare the secure capacities of information theoretical approach and physical layer encryption approach under untrusted relay adversary model in Fig. 5. From the comparison we can see, with the SNR increasing, the physical layer security encryption approach almost achieve twice than the information theoretical approach. And the simulation result is in accord with 33 and 46.

We then compare the secure capacities of information theoretical approach and physical layer encryption approach under trusted relay with eavesdroppers adversary model in Fig. 6. We test one eavesdropper, two eavesdroppers and four eavesdroppers cases. And from Fig. 6 we can see that the capacity of information theoretical approach suffers a remarkable decline with the increasing of the eavesdroppers.

The secure capacities comprsion between information theoretical approach and physical layer encryption approach under untrusted relay with eavesdroppers adversary model is shown in Fig. 7. From Fig. 7 we can see that the capacity of physical layer encryption approach shows no change

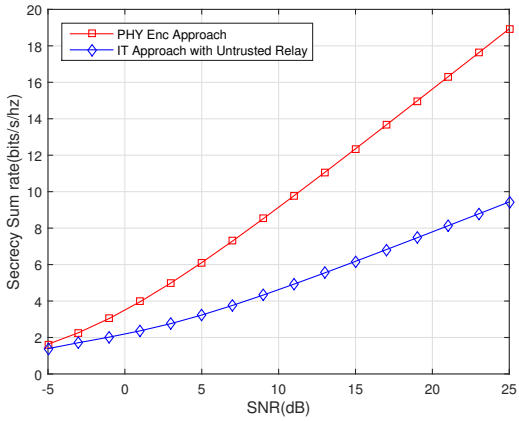

Fig. 5. Capacity Comparison between Physical Layer Encryption Approach and Information Theoretical Approach under Untrusted Relay Adversary Model

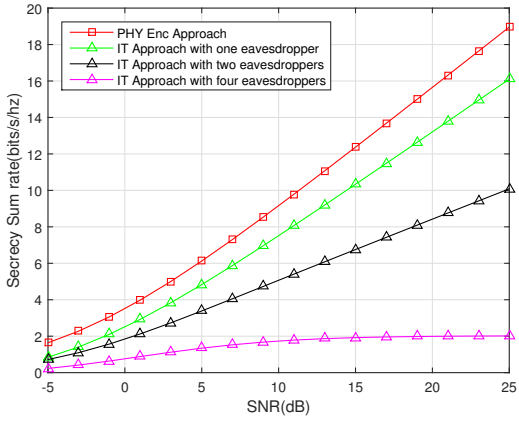

Fig. 6. Capacity Comparison between Physical Layer Encryption Approach and Information Theoretical Approach under Trusted Relay with Eavesdroppers Model

with the increase of the eavesdroppers. However, the information theoretical approach can hardly resist the attack under such scenario, for the capacity has enormous probability equal to zero when there exists more than two eavesdroppers.

VI. Conclusion

In this paper, a novel transmission scheme has been introduced for MIMO TWRC channels. We consider three general attack models: Untrusted relay adversarial model, trusted relay with eavesdropper adversarial model and untrusted relay adversarial model. Two different approaches including information theoretical approach and physical layer encryption approach have been proposed to achieve transmission efficiency as well as computational security. The key techniques of the proposed scheme lie in Direction Rotation Alignment and physical layer encryption. With alignment, signals from the same communication pair is aligned into the same signal direction. The direction rotation can avoid power loss in bad channel condition. And with the physical layer

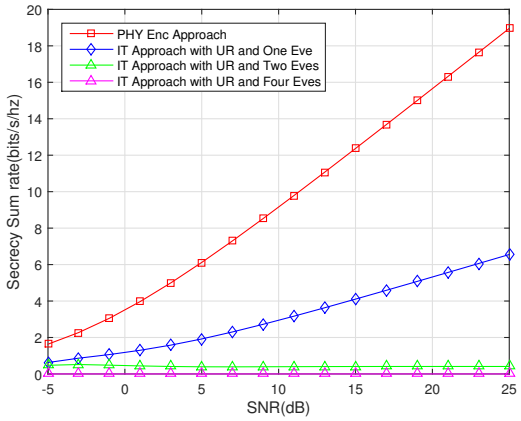

Fig. 7. Capacity Comparison between Physical Layer Encryption Approach and Information Theoretical Approach under Untrusted Relay with Eavesdroppers Model

encryption, the security of the system only depends on the security of the pre-shared key rather than the mutual information. Secrecy capacities of our proposed scheme are given for all the three models. Finally, simulation results show our proposed scheme can achieve better performance in both transmission rate and security.

Comparing the two different approaches, we find that the physical layer encryption approach can get a better performance in transmission and security. However, such performance improvement is obtained by sacrificing the system complexity because the pre-shared key is needed. So how to balance the trade-off between the system complexity and performance will be the future work.

APPENDIX

We consider the worst adversary model that untrusted relay with eavesdroppers model. For if the physical layer encryption approach can achieve the proposed secrecy capacity like (46) in the worst case, it would certainly achieve the same capacity in other two adversary models.

The the achievable secrecy capacity under untrusted relay with eavesdroppers model has been shown in (13). By comparing (46) and (13) we can see that if we proof $R_R = 0$ and $R_{E_k} = 0$, we can proof (46). And R_R and R_{E_k} are:

$$R_R = \frac{1}{2} I(\mathbf{Y}_R; \mathbf{X}_{A_1}, \mathbf{X}_{A_2}, \cdots, \mathbf{X}_{A_k}, \mathbf{X}_{B_1}, \cdots, \mathbf{X}_{B_k}). \tag{47}$$

$$R_{E_k} = \frac{1}{2} \left[I\left(\mathbf{Y}_{E_k}; \mathbf{X}_{A_k}, \mathbf{X}_{B_k} \right) \right]. \tag{48}$$

We now start to prove $R_R = 0$. With (47), we have:

$$\begin{aligned} R_R &= \frac{1}{2} I(\mathbf{Y}_R; \mathbf{X}_{A_1}, \mathbf{X}_{A_2}, \cdots, \mathbf{X}_{A_k}, \mathbf{X}_{B_1}, \cdots, \mathbf{X}_{B_k}) \\ &\overset{(a)}{=} \frac{1}{2} I(\mathbf{X}_{A_1}, \mathbf{X}_{A_2}, \cdots, \mathbf{X}_{A_k}, \mathbf{X}_{B_1}, \cdots, \mathbf{X}_{B_k}; \mathbf{Y}_R) \\ &\overset{(b)}{=} \frac{1}{2} \sum_{k=1}^{K} \Big[I\left(\mathbf{X}_{A_k}; \mathbf{Y}_R | \mathbf{X}_{A_{k-1}}, \cdots, \mathbf{X}_{A_1}, \mathbf{X}_{B_K}, \cdots, \mathbf{X}_{B_1}\right) + \\ &\qquad + I\left(\mathbf{X}_{B_k}; \mathbf{Y}_R | \mathbf{X}_{B_{k-1}}, \cdots, \mathbf{X}_{B_1}\right) \Big] \\ &\overset{(c)}{=} \frac{1}{2} \sum_{k=1}^{K} \left[I\left(\mathbf{X}_{A_k}; \mathbf{Y}_R\right) + I\left(\mathbf{X}_{B_k}; \mathbf{Y}_R\right) \right]. \end{aligned} \tag{49}$$

where (a) is from the basic theorem that $I(A;B) = I(B;A)$, (b) is from the chain rule for mutual information, and (c) is from that all the transmitting signals are independent.

With (49) we can see that if we could show each mutual information part $I(\mathbf{X}_{A_k}; \mathbf{Y}_R)$ or $I(\mathbf{X}_{B_k}; \mathbf{Y}_R)$ is zero, the proposition will be permit.

So we move on to the proof of $I(\mathbf{X}_{A_k}; \mathbf{Y}_R) = 0$. We consider the BPSK modulation as a case. So the transmitting signal in A_k and B_k will be 1 with probability $\frac{1}{2}$, and -1 with probability $\frac{1}{2}$. And the Key streams S_{A_k} and S_{B_k} will also be 1 with probability $\frac{1}{2}$, and -1 with probability $\frac{1}{2}$.

We have shown the signal pattern for BPSK in Table I. With Table I, we can compute the probability distributions of Y_R as:

TABLE III
PROBABILITY DISTRIBUTIONS OF Y_R

Y_R	2	0	-2
p	$\frac{1}{4}$	$\frac{1}{2}$	$\frac{1}{4}$

And we can also compute the joint probability distributions of X_{A_k} and Y_R as:

TABLE IV
JOINT PROBABILITY DISTRIBUTIONS OF X_{A_k} AND Y_R

Y_R \ X_{A_k}	1	-1
2	$\frac{1}{8}$	$\frac{1}{8}$
0	$\frac{1}{4}$	$\frac{1}{4}$
-2	$\frac{1}{8}$	$\frac{1}{8}$

So we can get the conditional probability distribution between Y_R and X_{A_k} as:

TABLE V
CONDITIONAL PROBABILITY DISTRIBUTION BETWEEN Y_R AND X_{A_k}

Y_R	2	0	-2
$P(Y_R \mid X_{A_k} = 1)$	$\frac{1}{4}$	$\frac{1}{2}$	$\frac{1}{4}$
$P(Y_R \mid X_{A_k} = -1)$	$\frac{1}{4}$	$\frac{1}{2}$	$\frac{1}{4}$

With Table III, Table IV and Table V, we can compute $H\left(Y_R\right)$ and $H\left(Y_R|X_{A_k}\right)$ as:

$$\begin{aligned} H\left(Y_R\right) &= H\left(\frac{1}{4},\frac{1}{2},\frac{1}{4}\right) \\ &= \frac{1}{4}log_2 4 + \frac{1}{2}log_2 2 + \frac{1}{4}log_2 4 \\ &= \frac{3}{2}bit. \end{aligned} \tag{50}$$

$$\begin{aligned} H\left(Y_R|X_{A_k}\right) &= \sum_{x_{A_k}\in\{1,-1\}} p\left(x_{A_k}\right) H\left(Y_R|X_{A_k}=x_{A_k}\right) \\ &= \frac{1}{2}H\left(\frac{1}{4},\frac{1}{2},\frac{1}{4}\right) + \frac{1}{2}H\left(\frac{1}{4},\frac{1}{2},\frac{1}{4}\right) \\ &= H\left(\frac{1}{4},\frac{1}{2},\frac{1}{4}\right) \\ &= \frac{3}{2}bit. \end{aligned} \tag{51}$$

So we can compute the mutual information $I\left(Y_R;X_{A_k}\right)$ as:

$$\begin{aligned} I\left(Y_R;X_{A_k}\right) &= H\left(Y_R\right) - H\left(Y_R|X_{A_k}\right) \\ &= \frac{3}{2} - \frac{3}{2} \\ &= 0bit. \end{aligned} \tag{52}$$

Exactly alike, the mutual information analysis is identical for the eavesdroppers model. So we can get the same result that:

$$I\left(Y_{E_k};X_{A_k}\right) = 0 \tag{53}$$

With (13), (52) and (52), we can proof (46).

The analysis of other modulation models are identical with BPSK models, so we omit the details.

REFERENCES

[1] R. Vaze and R. Heath, "Capacity scaling for mimo two-way relaying," in *Information Theory, 2007. ISIT 2007. IEEE International Symposium on*, pp. 1451–1455, June 2007.

[2] W. Nam, S.-Y. Chung, and Y. H. Lee, "Capacity of the gaussian two-way relay channel to within $\frac{1}{2}$ bit," *Information Theory, IEEE Transactions on*, vol. 56, pp. 5488–5494, Nov 2010.

[3] R. Vaze and R. Heath, "On the capacity and diversity-multiplexing tradeoff of the two-way relay channel," *Information Theory, IEEE Transactions on*, vol. 57, pp. 4219–4234, July 2011.

[4] H. J. Yang, J. Chun, and A. Paulraj, "Asymptotic capacity of the separated mimo two-way relay channel," *Information Theory, IEEE Transactions on*, vol. 57, pp. 7542–7554, Nov 2011.

[5] T. Yang, X. Yuan, L. Ping, I. Collings, and J. Yuan, "A new physical-layer network coding scheme with eigen-direction alignment precoding for mimo two-way relaying," *Communications, IEEE Transactions on*, vol. 61, pp. 973–986, March 2013.

[6] Z. Fang, X. Yuan, and X. Wang, "Towards the asymptotic sum capacity of the mimo cellular two-way relay channel," *Signal Processing, IEEE Transactions on*, vol. 62, pp. 4039–4051, Aug 2014.

[7] G. Zheng, "Joint beamforming optimization and power control for full-duplex mimo two-way relay channel," *Signal Processing, IEEE Transactions on*, vol. 63, pp. 555–566, Feb 2015.

[8] A. Wyner, "The wire-tap channel," *Bell System Technical Journal, The*, vol. 54, pp. 1355–1387, Oct 1975.

[9] A. O. HERo, "Secure space-time communication," *Information Theory, IEEE Transactions on*, vol. 49, no. 12, pp. 3235–3249, 2003.

[10] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas i: The misome wiretap channel," *Information Theory, IEEE Transactions on*, vol. 56, no. 7, pp. 3088–3104, 2010.

[11] P. Parada and R. Blahut, "Secrecy capacity of simo and slow fading channels," in *Information Theory, 2005. ISIT 2005. Proceedings. International Symposium on*, pp. 2152–2155, Sept 2005.

[12] A. Khisti, G. Wornell, A. Wiesel, and Y. Eldar, "On the gaussian mimo wiretap channel," in *Information Theory, 2007. ISIT 2007. IEEE International Symposium on*, pp. 2471–2475, June 2007.

[13] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas—part ii: The mimome wiretap channel," *Information Theory, IEEE Transactions on*, vol. 56, no. 11, pp. 5515–5532, 2010.

[14] F. Oggier and B. Hassibi, "The secrecy capacity of the mimo wiretap channel," *Information Theory, IEEE Transactions on*, vol. 57, no. 8, pp. 4961–4972, 2011.

[15] T. Liu and S. Shamai, "A note on the secrecy capacity of the multiple-antenna wiretap channel," *Information Theory, IEEE Transactions on*, vol. 55, no. 6, pp. 2547–2553, 2009.

[16] Y. Oohama, "Capacity theorems for relay channels with confidential messages," in *Information Theory, 2007. ISIT 2007. IEEE International Symposium on*, pp. 926–930, June 2007.

[17] A. Mukherjee, S. Fakoorian, J. Huang, and A. Swindlehurst, "Principles of physical layer security in multiuser wireless networks: A survey," *Communications Surveys Tutorials, IEEE*, vol. 16, pp. 1550–1573, Third 2014.

[18] C. Jeong, I.-M. Kim, and D. I. Kim, "Joint secure beamforming design at the source and the relay for an amplify-and-forward mimo untrusted relay system," *Signal Processing, IEEE Transactions on*, vol. 60, pp. 310–325, Jan 2012.

[19] R. Zhang, L. Song, Z. Han, and B. Jiao, "Physical layer security for two-way untrusted relaying with friendly jammers," *Vehicular Technology, IEEE Transactions on*, vol. 61, pp. 3693–3704, Oct 2012.

[20] J. Mo, M. Tao, Y. Liu, and R. Wang, "Secure beamforming for mimo two-way communications with an untrusted relay," *Signal Processing, IEEE Transactions on*, vol. 62, pp. 2185–2199, May 2014.

[21] Z. Ding, M. Peng, and H.-H. Chen, "A general relaying transmission protocol for mimo secrecy communications," *Communications, IEEE Transactions on*, vol. 60, pp. 3461–3471, November 2012.

[22] K. Jayasinghe, P. Jayasinghe, N. Rajatheva, and M. Latva-Aho, "Secure beamforming design for physical layer network coding based mimo two-way relaying," *Communications Letters, IEEE*, vol. 18, pp. 1270–1273, July 2014.

[23] F. Oggier and B. Hassibi, "The secrecy capacity of the mimo wiretap channel," *Information Theory, IEEE Transactions on*, vol. 57, pp. 4961–4972, Aug 2011.

[24] G. H. Golub and C. F. Van Loan, *Matrix computations*, vol. 3. JHU Press, 2012.