Hindawi
Mobile Information Systems
Volume 2017, Article ID 7843843, 12 pages
https://doi.org/10.1155/2017/7843843

Research Article

A Novel Secure Transmission Scheme in MIMO Two-Way Relay Channels with Physical Layer Approach

Qiao Liu,[1,2] Guang Gong,[2] Yong Wang,[1] and Hui Li[1]

[1]*State Key Lab of ISN, Xidian University, Xi'an, Shaanxi, China*
[2]*Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, ON, Canada*

Correspondence should be addressed to Qiao Liu; windachilles@gmail.com

Received 20 October 2016; Revised 24 December 2016; Accepted 29 December 2016; Published 2 March 2017

Academic Editor: Jing Zhao

Security issue has been considered as one of the most pivotal aspects for the fifth-generation mobile network (5G) due to the increasing demands of security service as well as the growing occurrence of security threat. In this paper, instead of focusing on the security architecture in the upper layer, we investigate the secure transmission for a basic channel model in a heterogeneous network, that is, two-way relay channels. By exploiting the properties of the transmission medium in the physical layer, we propose a novel secure scheme for the aforementioned channel mode. With precoding design, the proposed scheme is able to achieve a high transmission efficiency as well as security. Two different approaches have been introduced: information theoretical approach and physical layer encryption approach. We show that our scheme is secure under three different adversarial models: (1) untrusted relay attack model, (2) trusted relay with eavesdropper attack model, and (3) untrusted relay with eavesdroppers attack model. We also derive the secrecy capacity of the two different approaches under the three attacks. Finally, we conduct three simulations of our proposed scheme. The simulation results agree with the theoretical analysis illustrating that our proposed scheme could achieve a better performance than the existing schemes.

1. Introduction

As the next evolution of the mobile communication system, 5G (5th-generation mobile network) has become the hottest topic in the academia as well as industry. To meet the high rate requirement in a cost-efficient way, many techniques are designed to be employed into the 5G system, including heterogeneous network (HetNet), massive multiple inputs multiple outputs (Massive MIMO), Device-to-Device (D2D), and millimeter wave (mmWave) techniques.

Meanwhile, security issues have attracted much more attention compared to any other time in the past. Thus, research on 5G security would undoubtedly be of theoretical and practical interest. Besides focusing on the security strategy for the system level, it is also worth investigating security transmission in some basic channel model, especially relevant to the aforementioned key techniques for 5G. With such motivation, we consider the secure transmission in two-way relay channels, which are one of the most basic channel models in HetNet and D2D networks. In addition, the proposed scheme is designed for multiple antenna system. Although this scheme is not particularly designed for Massive MIMO, it can be easily transplanted into it.

The research on TWRC channel has continued for a long time; the early works on this type of channel model are concentrated on efficient transmission [1–8]. The results in these works show that MIMO TWRC channels can drastically improve the transmission performance. After that, some researchers began to think about the security of this type of channel model. Instead of following the upper layer encryption approach, the physical layer approach is believed to be a promising way which enjoys less system complexity compared with the traditional cryptography scheme.

Along with the pioneering study by Wyner [9], physical layer security problems were first introduced into MIMO case by Hero [10] utilizing space-time code at the transmitter to enhance information security and hiding capabilities. After that, the research of multiple antennas mainly focused on MISO (multiple input, single output) [11] or SIMO (single input, multiple output) [12] until Khisti et al. analyzed the

MIMO wiretap channel secrecy capacity in [13], and they gave an upper bound for secrecy capacity under the situation that the transmitter knows the instantaneous channel state information (CSI) about the eavesdropper. After that, a lot of researchers aimed at giving a secrecy capacity bound by different approaches and different constraints [14–16].

The physical layer security in cooperation relaying was first considered in [17]. Depending on the relay adversarial model, the security problems in cooperation relaying system are divided into two parts in [18]: (1) untrusted relay model and (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 HetNet network, since many potential unfriendly devices exist in the HetNet network and some of them are eager to wiretap to the messages by providing fake assistance. In [19], 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 [20] is a secure method for TWRC channels, but the selection of friendly jammers will be difficult to realize in practice. The authors in [21] 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 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 [22], which uses artificial noise alignment to jam the eavesdropper. The authors in [23] 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 that considerable improvements can be made in terms of transmission efficiency and security for MIMO TWRC channels. Two approaches have been introduced based on different performance requirements: 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, the signal direction of each user will be distorted. So, these will certainly bring about enough confusion for the adversaries. With such encryption, the system can achieve computational security.

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

(i) 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 the user message to achieve information theoretical security.

(ii) Following information theoretical approach, physical layer encryption approach is presented to achieve better transmission efficiency and security performance.

(iii) We show that our proposed scheme is secure under three different adversary models: untrusted relay attack model, (2) trusted relay with eavesdropper attack model, and (3) untrusted relay with eavesdroppers attack model. To the best of our knowledge, our scheme is the first secure method in all these adversary models

(iv) 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 2, we introduce the system and adversarial models. Section 3 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 discussed in Section 4. In Section 5, we demonstrate simulation results on our proposed scheme. Finally, we give conclusions and extensions in Section 5.

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

2. System Model

In this section, we will introduce the system model for the proposed scheme which is previously defined in [24].

2.1. Transmission Model

(1) Channel Model. In this subsection, we will describe the TWRC channels system. This is depicted in Figure 1. K communication pairs exchange their information with a relay. The users on the left side in Figure 1 are denoted as A_k ($k \in \kappa \{\kappa = 1, 2, \ldots, K\}$) 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 the users work in half-duplex mode and there is no direct link between each pair. We assume that 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

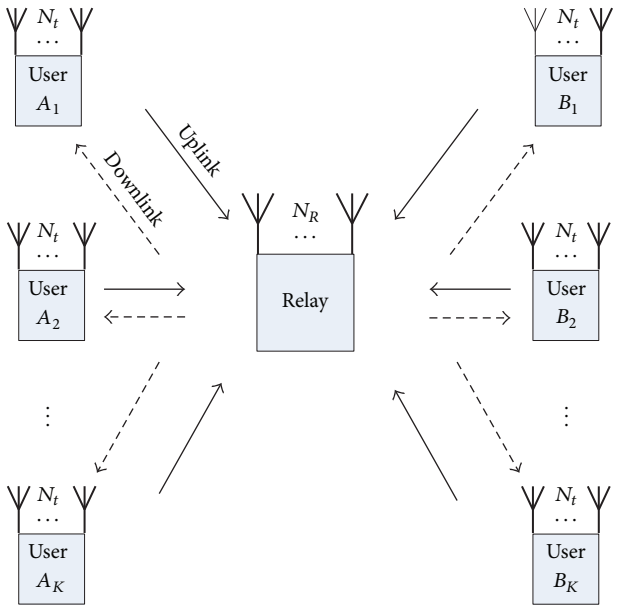

Figure 1: The channel model of multiusers MIMO two-way relay channels.

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, we assume that the channel state information (CSI) is available for the users and relay. The channel state information could be obtained by the channel estimation for the MIMO channel. There are already a lot of relative works focusing on the channel estimation. In [25], the CSI has been estimated with partial channel information. In addition, the authors propose a semiblind estimation method in [26]. Particularly, in [27], the authors consider using fine time synchronization in the estimation which is the most suitable method for our proposed scheme.

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 uplink phase or multiple access (MAC) phase. Upon receiving the message, the relay broadcasts its signal in the second time slot with the name of downlink or broadcast (BC) phase. Now, we introduce the two phases separately.

(2) Uplink Phase. In the uplink (MAC) phase, the relay receives the converging signals from all the user nodes as follows:

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

where $\mathbf{X}_{A_k}$ is an $n_T * 1$ column vector that 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 as $\mathbf{Q}_m = \varepsilon(\mathbf{X}_m \mathbf{X}_m^H)$. Then, we have the power constraint in uplink phase like

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

(3) Downlink Phase. In the downlink (BC) phase, 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 an Amplify-and-Forward (AF) model in the proposed scheme. Thus, the transmitted signal $\mathbf{X}_R$ of the 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.

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

(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_s^{UR} as follows:

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

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

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

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

$$R_R^{\mathrm{UR}} = \frac{1}{2} I\left(\mathbf{Y}_R; \mathbf{X}_{A_1}, \mathbf{X}_{A_2}, \ldots, \mathbf{X}_{A_k}, \mathbf{X}_{B_1}, \ldots, \mathbf{X}_{B_k} \right). \tag{6}$$

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 to develop 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 exchange 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 complete knowledge of the channel information and transmission protocol. Furthermore, let the channel coefficient between user and eavesdropper be $\mathbf{H}^E_{A_m}$ and $\mathbf{H}^E_{B_m}$, respectively; then, the received signal by the eavesdropper $\mathbf{Y}_{E_m}$ is

$$\mathbf{Y}_{E_m} = \mathbf{H}^E_{A_m}\mathbf{X}_{A_m} + \mathbf{H}^E_{B_m}\mathbf{X}_{B_m} + \mathbf{Z}_{E_m}, \tag{7}$$

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

The MIMO wiretap channel introduced by [15] can be considered as multiple and parallel single subwiretap channels; each subchannel 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

$$C_s^{\mathrm{TR}} = \left[\sum_{k=1}^{K}\left(R^{\mathrm{TR}}_{A_k} + R^{\mathrm{TR}}_{B_k} - R^{\mathrm{TR}}_{E_k}\right)\right]^+, \tag{8}$$

where $R^{\mathrm{TR}}_{A_k}$ and $R^{\mathrm{TR}}_{B_k}$ are the secrecy information rate between users A_k and B_k, respectively. They have identical analysis as (5):

$$\begin{aligned} R^{\mathrm{TR}}_{A_k} &= \frac{1}{2}\left[I\left(\mathbf{Y}_{B_k}; \mathbf{X}_{A_k} \mid \mathbf{Y}_R, \mathbf{X}_R\right)\right], \\ R^{\mathrm{TR}}_{B_k} &= \frac{1}{2}\left[I\left(\mathbf{Y}_{A_k}; \mathbf{X}_{B_k} \mid \mathbf{Y}_R, \mathbf{X}_R\right)\right]. \end{aligned} \tag{9}$$

And $R^{\mathrm{TR}}_{E_k}$ is the information rate at the eavesdropper as

$$R^{\mathrm{TR}}_{E_k} = \frac{1}{2}\left[I\left(\mathbf{Y}_{E_k}; \mathbf{X}_{A_k}, \mathbf{X}_{B_k}\right)\right]. \tag{10}$$

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 exist a considerable number of eavesdroppers between each communication pair. We hold the same assumption as the above two subsections, and then we can obtain the achievable secrecy capacity C_s in such scenario as

$$C_s^{\mathrm{UE}} = \left[\sum_{k=1}^{K}\left(R^{\mathrm{UE}}_{A_k} + R^{\mathrm{UE}}_{B_k} - R^{\mathrm{UE}}_{E_k}\right) - R^{\mathrm{UE}}_{R}\right]^+, \tag{11}$$

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

$$\begin{aligned} R^{\mathrm{UE}}_{A_k} &= \frac{1}{2}\left[I\left(\mathbf{Y}_{B_k}; \mathbf{X}_{A_k} \mid \mathbf{Y}_R, \mathbf{X}_R\right)\right], \\ R^{\mathrm{UE}}_{B_k} &= \frac{1}{2}\left[I\left(\mathbf{Y}_{A_k}; \mathbf{X}_{B_k} \mid \mathbf{Y}_R, \mathbf{X}_R\right)\right]. \end{aligned} \tag{12}$$

And $R^{\mathrm{UE}}_{E_k}$ and R^{UE}_{R} are the information rate at the eavesdropper and untrusted relay, respectively, as

$$\begin{aligned} R^{\mathrm{UE}}_{E_k} &= \frac{1}{2}\left[I\left(\mathbf{Y}_{E_k}; \mathbf{X}_{A_k}, \mathbf{X}_{B_k}\right)\right], \\ R^{\mathrm{UE}}_{R} &= \frac{1}{2} I\left(\mathbf{Y}_R; \mathbf{X}_{A_1}, \mathbf{X}_{A_2}, \ldots, \mathbf{X}_{A_k}, \mathbf{X}_{B_1}, \ldots, \mathbf{X}_{B_k}\right). \end{aligned} \tag{13}$$

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

3. 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.

3.1. 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 subchannels 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:

$$\mathbf{H}_{A_k} = \mathbf{U}_{A_k}\mathbf{\Sigma}_{A_k}\mathbf{V}^H_{A_k}, \tag{14}$$

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 $\mathbf{F}_{A_k}$ in the following form:

$$\mathbf{F}_{A_k} = \mathbf{V}_{A_k}\mathbf{\Sigma}^{-1}_{A_k}\mathbf{U}^H_{A_k}\mathbf{R}\mathbf{\Psi}_{A_k}\mathbf{L}_k, \tag{15}$$

where $\mathbf{R}$ is an $n_R * n_R$ unitary matrix called *Direction Rotation matrix* and $\mathbf{\Sigma}^{-1}_{A_k}$ denotes the pseudoinverse 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. $\mathbf{L}_k$ is called *channel allocation matrix* to guarantee that multipair users communicate simultaneously. $\mathbf{L}_k$ allocates the

constructed equivalent parallel subchannels to corresponding users. The design and optimization of $\mathbf{R}$ and $\mathbf{L}_k$ will affect the transmission efficiency of the 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 the Direction Rotation matrix for one-pair TWRC channels. Along with their work, we extend their results into multipair TWRC channels.

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

$$\mathbf{G} \triangleq \sum_{k=1}^{K} \left\{ \mathbf{U}_{A_k} \boldsymbol{\Sigma}_{A_k}^{-2} \mathbf{U}_{A_k}^{H} + \mathbf{U}_{B_k} \boldsymbol{\Sigma}_{B_k}^{-2} \mathbf{U}_{B_k}^{H} \right\}. \tag{16}$$

Using eigendecomposition, $\mathbf{G}$ could be represented as

$$\mathbf{G} = \mathbf{U}_g \boldsymbol{\Lambda}_g \mathbf{U}_g^{H}, \tag{17}$$

where $\mathbf{U}_g$ is a unitary matrix and $\boldsymbol{\Lambda}_g$ is a diagonal matrix whose nonzero elements are the eigenvalues of $\mathbf{G}$ arranged in the ascending order. Then, we choose $\mathbf{R}$ as

$$\mathbf{R} = \mathbf{U}_g. \tag{18}$$

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 communication pair, and D_k is the sum independent signal streams of the 1st communication pair to the kth pair 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 $\mathbf{L}_k$ is designed by collecting the $D_k + 1$ to $D_k + d_k$ column vector from the $n_R * n_R$ unit matrix, so $\mathbf{L}_k$ is in the size of $n_R * d_k$. $\mathbf{L}_k$ is shown as follows:

$$\mathbf{L}_k = \begin{bmatrix} & \overbrace{\quad}^{d_k} \\ D_k \begin{cases} \overbrace{00\cdots0} \\ 00\cdots0 \\ \vdots \\ 00\cdots0 \end{cases} \\ d_k \begin{cases} 10\cdots0 \\ 01\cdots0 \\ \vdots \\ 00\cdots1 \end{cases} \\ 00\cdots0 \\ \vdots \\ 00\cdots0 \end{bmatrix}. \tag{19}$$

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

$$\mathbf{Y}_R = \sum_{k=1}^{K} \left(\mathbf{H}_{A_k} \mathbf{F}_{A_k} \mathbf{c}_{A_k} + \mathbf{H}_{B_k} \mathbf{F}_{B_k} \mathbf{c}_{B_k} \right) + \mathbf{Z}_R. \tag{20}$$

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

$$\mathbf{H}_k \mathbf{F}_k = \mathbf{U}_k \Sigma_k \mathbf{V}_k^{H} \mathbf{V}_k \boldsymbol{\Sigma}_k^{-1} \mathbf{U}_k^{H} \mathbf{R} \mathbf{L}_k = \mathbf{R} \mathbf{L}_k, \tag{21}$$

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

$$\begin{aligned} \mathbf{Y}_R &= \mathbf{R} \sum_{k=1}^{K} \mathbf{L}_k \left(\mathbf{c}_{A_k} + \mathbf{c}_{B_k} \right) + \mathbf{Z}_R \\ &= \mathbf{R} \begin{bmatrix} \mathbf{c}_{A_1} + \mathbf{c}_{B_1} \\ \mathbf{c}_{A_2} + \mathbf{c}_{B_2} \\ \vdots \\ \mathbf{c}_{A_K} + \mathbf{c}_{B_K} \end{bmatrix} + \mathbf{Z}_R. \end{aligned} \tag{22}$$

As shown in (22), 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-and-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

$$\begin{aligned} \mathbf{Y}_{B_m} &= \mathbf{G}_{B_m} \mathbf{X}_R + \mathbf{Z}_{B_m} \\ &= \mathbf{G}_{B_m} \sum_{k=1}^{K} \left(\mathbf{H}_{A_k} \mathbf{F}_{A_k} \mathbf{c}_{A_k} + \mathbf{H}_{B_k} \mathbf{F}_{B_k} \mathbf{c}_{B_k} \right) + \mathbf{G}_{B_m} \mathbf{Z}_R \\ &\quad + \mathbf{Z}_{B_k}. \end{aligned} \tag{23}$$

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

$$\widetilde{\mathbf{Y}}_{B_m} = \mathbf{G}_{B_m} \mathbf{H}_{A_m} \mathbf{F}_{A_m} \mathbf{c}_{A_m} + \mathbf{G}_{B_m} \mathbf{Z}_R + \mathbf{Z}_{A_m}. \tag{24}$$

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

$$\begin{aligned} \widetilde{\mathbf{Y}}_{B_m} &= \mathbf{D}_{B_m} \mathbf{Y}_{B_m} = \mathbf{D}_{B_m} \left(\mathbf{H}_{B_m}^{H} \mathbf{X}_R + \mathbf{Z}_{B_m} \right) \\ &= \mathbf{L}_m^{H} \mathbf{R}^{H} \mathbf{U}_{B_m} \left(\Sigma_{B_m}^{H} \right)^{-1} \mathbf{V}_{B_m}^{H} \mathbf{V}_{B_m} \Sigma_{B_m}^{H} \mathbf{U}_{B_m}^{H} \mathbf{R} \\ &\quad \cdot \sum_{k=1}^{K} \mathbf{L}_m \left(\mathbf{c}_{A_m} + \mathbf{c}_{B_m} \right) + \mathbf{D}_{B_m} \mathbf{Z}_R + \mathbf{Z}_{B_m} \\ &= \left(\mathbf{c}_{A_m} + \mathbf{c}_{B_m} \right) + \mathbf{Z}'_{B_m}, \end{aligned} \tag{25}$$

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

From (25), 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.

3.2. 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 $\{R_{A_1}^{\mathrm{UR}}, R_{A_2}^{\mathrm{UR}}, \ldots, R_{A_K}^{\mathrm{UR}}, R_{B_1}^{\mathrm{UR}}, \ldots, R_{A_K}^{\mathrm{UR}}\}$. 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 (25). The information rate from A_m to B_m is

$$\begin{aligned} R_{A_m}^{\mathrm{UR}} &= \frac{1}{2}\log\det\left(\mathbf{I} + \mathbf{F}_{A_m}^H \mathbf{H}_{A_m}^H \mathbf{G}_{B_m}^H \mathbf{K}_{A_m}^{-1} \mathbf{G}_{B_m} \mathbf{H}_{A_m} \mathbf{F}_{A_m}\right) \\ &= \frac{1}{2}\log\det\left(\mathbf{I} + \mathbf{L}_m^H \mathbf{R} \mathbf{G}_{B_m}^H \mathbf{K}_{A_m}^{-1} \mathbf{G}_{B_m} \mathbf{R} \mathbf{L}_m\right), \end{aligned} \tag{26}$$

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

$$R_{B_m}^{\mathrm{UR}} = \frac{1}{2}\log\det\left(\mathbf{I} + \mathbf{L}_m^H \mathbf{R} \mathbf{G}_{A_m}^H \mathbf{K}_{B_m}^{-1} \mathbf{G}_{A_m} \mathbf{R} \mathbf{L}_m\right). \tag{27}$$

For the untrusted relay model, the adversary tries to recover the message symbols from all the users node. So, the achievable information rate is equal to the maximum sum rate of the uplink multiuser MAC channel:

$$\begin{aligned} R_R^{\mathrm{UR}} = \frac{1}{2}\log\det\Bigg[&\mathbf{I} \\ &+ \sum_{k=1}^{K}\left(\mathbf{H}_{A_k}\mathbf{F}_{A_k}\mathbf{F}_{A_k}^H\mathbf{H}_{A_k}^H + \mathbf{H}_{B_k}\mathbf{F}_{B_k}\mathbf{F}_{B_k}^H\mathbf{H}_{B_k}^H\right)\Bigg]. \end{aligned} \tag{28}$$

From (26), (27), and (28), the achievable secrecy channel capacity for the untrusted relay model can be obtained with matrix operation [28] as follows:

$$C_s^{\mathrm{UR}} = \frac{1}{2}\log\det\left[\frac{\prod_{k=1}^{K}\left(\mathbf{I} + \mathbf{L}_k^H \mathbf{R} \mathbf{G}_{B_k}^H \mathbf{K}_{A_k}^{-1} \mathbf{G}_{B_k} \mathbf{R} \mathbf{L}_k\right)\left(\mathbf{I} + \mathbf{L}_k^H \mathbf{R} \mathbf{G}_{A_k}^H \mathbf{K}_{B_k}^{-1} \mathbf{G}_{A_k} \mathbf{R} \mathbf{L}_k\right)}{\mathbf{I} + \sum_{k=1}^{K}\left(\mathbf{H}_{A_k}\mathbf{F}_{A_k}\mathbf{F}_{A_k}^H\mathbf{H}_{A_k}^H + \mathbf{H}_{B_k}\mathbf{F}_{B_k}\mathbf{F}_{B_k}^H\mathbf{H}_{B_k}^H\right)}\right]. \tag{29}$$

3.3. 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 (7), and for the proposed scheme we have

$$\mathbf{Y}_{E_m} = \mathbf{H}_{A_m}^E \mathbf{F}_{A_m} \mathbf{c}_{A_m} + \mathbf{H}_{B_m}^E \mathbf{F}_{B_m} \mathbf{c}_{B_m} + \mathbf{Z}_{E_m}, \tag{30}$$

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

$$\begin{aligned} R_{E_m}^{\mathrm{TR}} = \frac{1}{2}\log\det\Big[&\mathbf{I} + \mathbf{H}_{A_m}^E \mathbf{F}_{A_m} \mathbf{F}_{A_m}^H \left(\mathbf{H}_{A_m}^E\right)^H \\ &+ \mathbf{H}_{B_m}^E \mathbf{F}_{B_m} \mathbf{F}_{B_m}^H \left(\mathbf{H}_{B_m}^E\right)^H\Big]. \end{aligned} \tag{31}$$

Meanwhile, the information rates $R_{A_m}^{\mathrm{TR}}$ and $R_{B_m}^{\mathrm{TR}}$ are identical to the untrusted relay model; namely,

$$\begin{aligned} R_{A_m}^{\mathrm{TR}} &= \frac{1}{2}\log\det\left(\mathbf{I} + \mathbf{L}_m^H \mathbf{R} \mathbf{G}_{B_m}^H \mathbf{K}_{A_m}^{-1} \mathbf{G}_{B_m} \mathbf{R} \mathbf{L}_m\right), \\ R_{B_m}^{\mathrm{TR}} &= \frac{1}{2}\log\det\left(\mathbf{I} + \mathbf{L}_m^H \mathbf{R} \mathbf{G}_{A_m}^H \mathbf{K}_{B_m}^{-1} \mathbf{G}_{A_m} \mathbf{R} \mathbf{L}_m\right). \end{aligned} \tag{32}$$

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

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

3.4. 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 exist a considerable number of eavesdroppers between each communication pair. The situation under this case is just like a combination of the former two cases, and the general capacity analysis of this model is given by (11). So, we first give all the components based on the former two subsections and then give the achievable secrecy channel capacity.

The information rates $R_{A_m}^{\mathrm{UE}}$ and $R_{B_m}^{\mathrm{UE}}$ are given as

$$R_{A_m}^{\mathrm{UE}} = \frac{1}{2}\log\det\left(\mathbf{I} + \mathbf{L}_m^H \mathbf{R}\mathbf{G}_{B_m}^H \mathbf{K}_{A_m}^{-1}\mathbf{G}_{B_m}\mathbf{R}\mathbf{L}_m\right),$$
$$R_{B_m}^{\mathrm{UE}} = \frac{1}{2}\log\det\left(\mathbf{I} + \mathbf{L}_m^H \mathbf{R}\mathbf{G}_{A_m}^H \mathbf{K}_{B_m}^{-1}\mathbf{G}_{A_m}\mathbf{R}\mathbf{L}_m\right). \tag{34}$$

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

$$R_R^{\mathrm{UE}} = \frac{1}{2}\log\det\left[\mathbf{I} + \sum_{k=1}^{K}\left(\mathbf{H}_{A_k}\mathbf{F}_{A_k}\mathbf{F}_{A_k}^H\mathbf{H}_{A_k}^H + \mathbf{H}_{B_k}\mathbf{F}_{B_k}\mathbf{F}_{B_k}^H\mathbf{H}_{B_k}^H\right)\right]. \tag{35}$$

And the achievable information rate at eavesdropper is given as

$$R_{E_m}^{\mathrm{UE}} = \frac{1}{2}\log\det\left[\mathbf{I} + \mathbf{H}_{A_m}^E\mathbf{F}_{A_m}\mathbf{F}_{A_m}^H\left(\mathbf{H}_{A_m}^E\right)^H + \mathbf{H}_{B_m}^E\mathbf{F}_{B_m}\mathbf{F}_{B_m}^H\left(\mathbf{H}_{B_m}^E\right)^H\right]. \tag{36}$$

With (34), (35), and (36), we obtain the achievable secrecy channel capacity as

$$C_s^{\mathrm{UE}} = \frac{1}{2}\cdot\log\det\left\{\frac{\sum_{k=1}^{K}\left(\left(\mathbf{I} + \mathbf{L}_k^H\mathbf{R}\mathbf{G}_{B_k}^H\mathbf{K}_{A_k}^{-1}\mathbf{G}_{B_k}\mathbf{R}\mathbf{L}_k\right)\left(\mathbf{I} + \mathbf{L}_k^H\mathbf{R}\mathbf{G}_{A_k}^H\mathbf{K}_{B_k}^{-1}\mathbf{G}_{A_k}\mathbf{R}\mathbf{L}_k\right)/\left(\mathbf{I} + \mathbf{H}_{A_k}^E\mathbf{F}_{A_k}\mathbf{F}_{A_k}^H\left(\mathbf{H}_{A_k}^E\right)^H + \mathbf{H}_{B_k}^E\mathbf{F}_{B_k}\mathbf{F}_{B_k}^H\left(\mathbf{H}_{B_k}^E\right)^H\right)\right)}{\mathbf{I} + \sum_{k=1}^{K}\left(\mathbf{H}_{A_k}\mathbf{F}_{A_k}\mathbf{F}_{A_k}^H\mathbf{H}_{A_k}^H + \mathbf{H}_{B_k}\mathbf{F}_{B_k}\mathbf{F}_{B_k}^H\mathbf{H}_{B_k}^H\right)}\right\}. \tag{37}$$

Note here that C_s^{UE} has great probability equal to zero, and it is a common case independent of 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.

4. Secrecy Transmission Scheme with Physical Layer Encryption Approach

In the above section, we have discussed the secrecy transmission scheme based information theoretical analysis. However, the traditional information theoretical approach achieves 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 an 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 and then present the capacity analysis for physical layer encryption.

4.1. 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 users A_m and B_m. We consider the situation in A_m as a case. Containing two function parts, $\mathbf{P}_{A_m}$ can be artificially divided into two parts as follows:

$$\mathbf{P}_{A_m} = \mathbf{F}_{A_m}\mathbf{S}_{A_m}, \tag{38}$$

where $\mathbf{F}_{A_m}$ is designed same as the above discussion and $\mathbf{S}_{A_m}$ is designed for physical layer encryption. Note that the precoding matrix has been artificially separated into two matrices, that is, transmission matrix and security matrix; however, the precoding matrix will show the effect as a whole.

The encryption precoding matrix $\mathbf{S}_{A_m}$ or $\mathbf{S}_{B_m}$ is generated from a key stream $\mathbf{s}_m$ where $\mathbf{s}_m(i) \in \{1, -1\}$. 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, $\mathbf{S}_{A_m}$ 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, $\mathbf{S}_{A_m}$ and $\mathbf{S}_{B_m}$ will be different by dividing $\mathbf{s}_m$ into two parts. Note here that the key stream must be preshared between users 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 promotes the security performance under both untrusted and trusted models.

4.2. 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, if the proposed scheme is secure under untrusted relay adversary model, it will certainly be secure under all adversary 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

$$\mathbf{Y}_R^{\mathrm{Enc}} = \mathbf{R}\sum_{k=1}^{K}\mathbf{A}_k\left(\mathbf{S}_{A_k}\mathbf{c}_{A_k} + \mathbf{S}_{B_k}\mathbf{c}_{B_k}\right) + \mathbf{Z}_R = \mathbf{R}\begin{bmatrix}\mathbf{S}_{A_1}\mathbf{c}_{A_1} + \mathbf{S}_{B_1}\mathbf{c}_{B_1}\\ \mathbf{S}_{A_2}\mathbf{c}_{A_2} + \mathbf{S}_{B_2}\mathbf{c}_{B_2}\\ \vdots\\ \mathbf{S}_{A_K}\mathbf{c}_{A_K} + \mathbf{S}_{B_K}\mathbf{c}_{B_K}\end{bmatrix} + \mathbf{Z}_R. \tag{39}$$

Table 1: 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

Table 2: 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

By comparison, we also consider the relay receiving signal for information theoretical approach as (22). Considering BPSK modulation as a case, we assume the untrusted relay could get the Direction Rotation matrix **R**. Then, we obtain the data patterns for the two different approaches as shown in Tables 1 and 2.

With Table 2, 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 recovery for untrusted relay is significantly reduced. However, as in Table 1, the characteristics will be distorted by the encryption. For example, if $Y_R = 2$, the relay could easily recover the transmitting message pair as $X_{A_k} = 1$ and $X_{B_k} = 1$. However, if $Y_R^{\text{Enc}} = 2$, the transmitting message pair could be all the four cases. So, with the physical layer encryption, the untrusted relay will 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.

4.3. 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 the following theorem.

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

$$C_{\text{Enc}} = \left[\sum_{k=1}^{K}\left(R_{A_k} + R_{B_k}\right)\right]^{+}, \tag{40}$$

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 the Appendix.

By comparing (40) with (29), (33), and (37), we can have the following result: because the *log function* is an increasing function, the proposed physical layer encryption scheme evidently increases 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.

5. Simulation Results

In this section, we present three simulations for our proposed scheme using MATLAB. First, we show that our proposed scheme outperforms some of the well-known existing schemes in terms of transmission quality. In the second simulation, we, respectively, show that 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 that four pairs of users communicate at the same time via a relay, and the users, relay, and eavesdroppers are all equipped with four antennas; that is, $n_R = n_T = n_E = 4$. Note that all of these results are obtained by averaging over 10,000 realizations.

5.1. 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 Figure 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.

5.2. 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

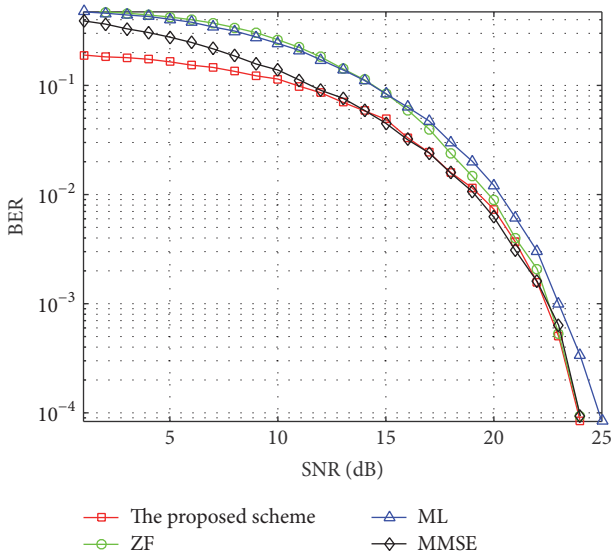

Figure 2: Transmission performance comparison between the proposed scheme and existing schemes.

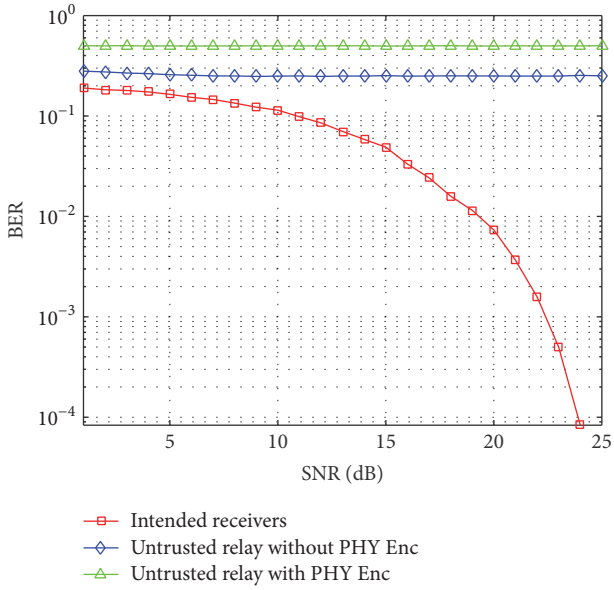

Figure 3: Security performance comparison between the intended receiver and the untrusted relay.

relay, and the eavesdropper. The BER comparison between the intended receiver and the untrusted relay is shown in Figure 3. We assume a stronger adversarial model where the relay can obtain all channel information including the Direction Rotation matrix R. From Figure 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 to the untrusted relay adversary model, we compare the BER between the intended receiver and the

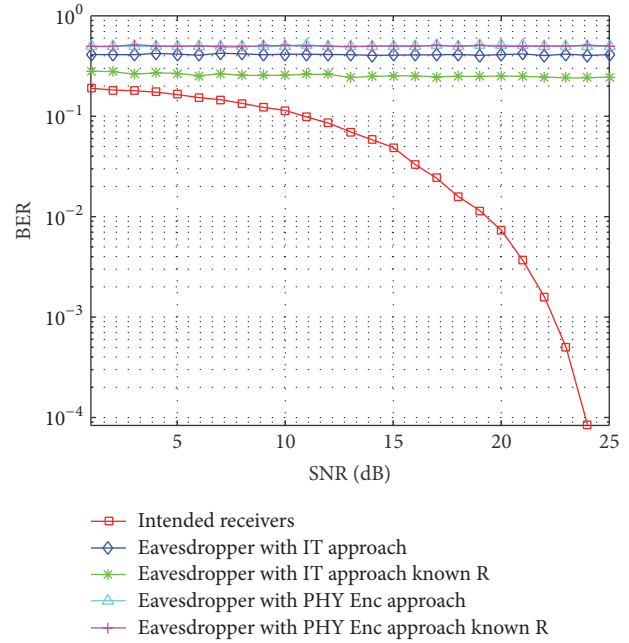

Figure 4: Security performance comparison between the intended receiver and the eavesdropper.

eavesdropper. The results are shown in Figure 4. To test different adversarial levels, 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 Figure 4, we can see that the eavesdropper gives the 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 fourth cases, we can see that the decoding error bit ratio of these two cases is almost the same which is identical to the error ratio of random guessing.

5.3. Secure Channel Capacity Analysis Evaluation under Different Adversary Models. In this subsection, we will give the secure channel capacity analysis under the three different adversary models. The results are shown in Figures 5–7.

We compare the secure capacities of information theoretical approach and physical layer encryption approach under untrusted relay adversary model in Figure 5. From the comparison result, we can see that, with the SNR increasing, the sum rates of the physical layer encryption approach are almost twice the sum rates of the information theoretical approach. And the simulation result is in accord with (29) and (40).

We then compare the secure capacities of information theoretical approach and physical layer encryption approach

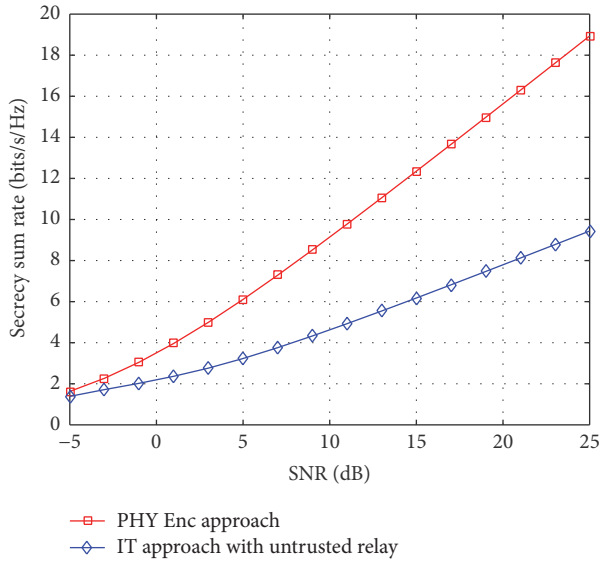

Figure 5: Capacity comparison between physical layer encryption approach and information theoretical approach under untrusted relay adversary model.

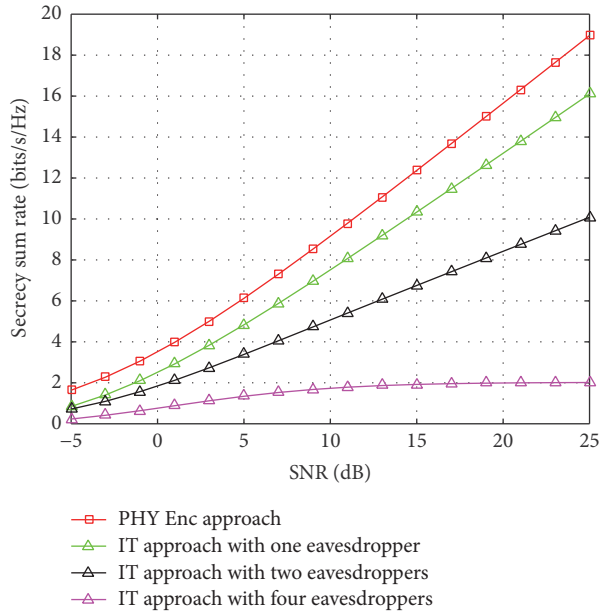

Figure 6: Capacity comparison between physical layer encryption approach and information theoretical approach under trusted relay with eavesdroppers model.

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

The secure capacities comparison between information theoretical approach and physical layer encryption approach under untrusted relay with eavesdroppers adversary model is shown in Figure 7. From Figure 7, we can see that the capacity

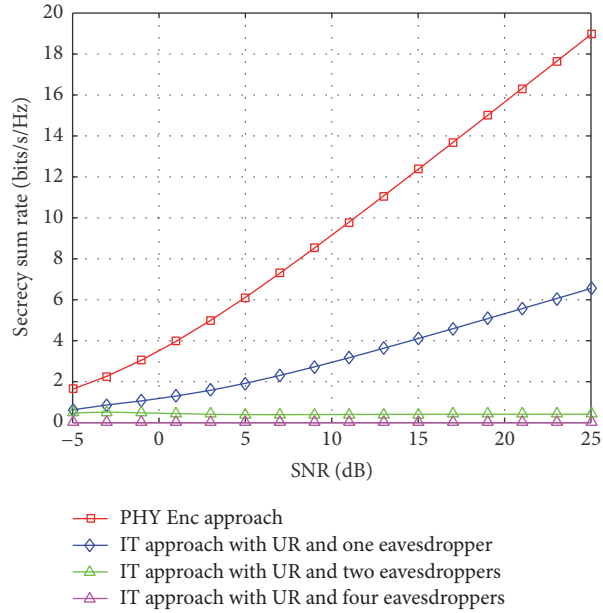

Figure 7: Capacity comparison between physical layer encryption approach and information theoretical approach under untrusted relay with eavesdroppers model.

of physical layer encryption approach shows no change 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 exist more than two eavesdroppers.

6. Conclusion

The security is one of the most important issues for 5G system architecture. Besides designing the security protocol from the view of system level, it is also desirable to consider the secure transmission for some basic transmission channel models, especially relevant to the key techniques for 5G.

In this paper, a novel transmission scheme has been introduced for MIMO TWRC channels, which is the basic channel model in HetNet and D2D networks. We consider three general attack models: untrusted relay adversarial model, trusted relay with eavesdropper adversarial model, and untrusted relay with eavesdropper adversarial model. Two different approaches, that is, 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 are aligned into the same signal direction. The direction rotation can avoid power loss in bad channel condition. And, with the physical layer encryption, the security of the system only depends on the security of the preshared key rather than the mutual information. Secrecy capacities of our proposed scheme are given for all the three models. Finally, simulation results show that 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 preshared key is needed. Thus, how to balance the trade-off between the system complexity and performance will be one of the future works. In addition, another future work lies in the modification of the proposed scheme fitting Massive MIMO which enjoys more implantation in 5G system.

Appendix

We consider the worst adversary model: untrusted relay with eavesdroppers model. If the physical layer encryption approach can achieve the proposed secrecy capacity like (40) in the worst case, it would certainly achieve the same capacity in the other two adversary models.

The achievable secrecy capacity under untrusted relay with eavesdroppers model has been shown in (11). By comparing (40) and (11), we can see that if we prove $R_R = 0$ and $R_{E_k} = 0$, we can prove (40). And R_R and R_{E_k} are

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

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

We now start to prove $R_R = 0$. With (A.1), we have

$$\begin{aligned} R_R &= \frac{1}{2} I\left(\mathbf{Y}_R; \mathbf{X}_{A_1}, \mathbf{X}_{A_2}, \ldots, \mathbf{X}_{A_k}, \mathbf{X}_{B_1}, \ldots, \mathbf{X}_{B_k}\right) \\ &\overset{(a)}{=} \frac{1}{2} I\left(\mathbf{X}_{A_1}, \mathbf{X}_{A_2}, \ldots, \mathbf{X}_{A_k}, \mathbf{X}_{B_1}, \ldots, \mathbf{X}_{B_k}; \mathbf{Y}_R\right) \\ &\overset{(b)}{=} \frac{1}{2} \\ &\cdot \sum_{k=1}^{K} \left[I\left(\mathbf{X}_{A_k}; \mathbf{Y}_R \mid \mathbf{X}_{A_{k-1}}, \ldots, \mathbf{X}_{A_1}, \mathbf{X}_{B_K}, \ldots, \mathbf{X}_{B_1}\right)\right. \\ &\left. + I\left(\mathbf{X}_{B_k}; \mathbf{Y}_R \mid \mathbf{X}_{B_{k-1}}, \ldots, \mathbf{X}_{B_1}\right)\right] \overset{(c)}{=} \frac{1}{2} \\ &\cdot \sum_{k=1}^{K} \left[I\left(\mathbf{X}_{A_k}; \mathbf{Y}_R\right) + I\left(\mathbf{X}_{B_k}; \mathbf{Y}_R\right)\right], \end{aligned} \tag{A.3}$$

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 the fact that all the transmitting signals are independent.

With (A.3), we can see that if we could show that 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 permitted.

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 1/2 and −1 with probability 1/2. And the key streams S_{A_k} and S_{B_k} will also be 1 with probability 1/2 and −1 with probability 1/2.

We have shown the signal pattern for BPSK in Table 1. With Table 1, we can compute the probability distributions of Y_R as shown in Table 3.

Table 3: Probability distributions of Y_R.

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

Table 4: 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	$\frac{1}{8}$	$\frac{1}{8}$

Table 5: Conditional probability distribution between Y_R and X_{A_k}.

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

And we can also compute the joint probability distributions of X_{A_k} and Y_R as shown in Table 4.

So, we can get the conditional probability distribution between Y_R and X_{A_k} as shown in Table 5.

With Tables 3, 4, and 5, we can compute $H(Y_R)$ and $H(Y_R \mid X_{A_k})$ as

$$\begin{aligned} H\left(Y_R\right) &= H\left(\frac{1}{4}, \frac{1}{2}, \frac{1}{4}\right) \\ &= \frac{1}{4}\log_2 4 + \frac{1}{2}\log_2 2 + \frac{1}{4}\log_2 4 = \frac{3}{2} \text{ bit}, \\ H\left(Y_R \mid X_{A_k}\right) &= \sum_{x_{A_k} \in \{1,-1\}} p\left(x_{A_k}\right) H\left(Y_R \mid X_{A_k} = x_{A_k}\right) \\ &= \frac{1}{2} H\left(\frac{1}{4}, \frac{1}{2}, \frac{1}{4}\right) + \frac{1}{2} H\left(\frac{1}{4}, \frac{1}{2}, \frac{1}{4}\right) \\ &= H\left(\frac{1}{4}, \frac{1}{2}, \frac{1}{4}\right) = \frac{3}{2} \text{ bit}. \end{aligned} \tag{A.4}$$

So, we can compute the mutual information $I(Y_R; X_{A_k})$ as

$$\begin{aligned} I\left(Y_R; X_{A_k}\right) &= H\left(Y_R\right) - H\left(Y_R \mid X_{A_k}\right) = \frac{3}{2} - \frac{3}{2} \\ &= 0 \text{ bits}. \end{aligned} \tag{A.5}$$

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

$$I\left(Y_{E_k}; X_{A_k}\right) = 0. \tag{A.6}$$

With (11), (A.5), and (A.5), we can prove (40).

The analysis of other modulation models is identical to BPSK models, so we omit the details.

Competing Interests

The authors declare that they have no competing interests regarding the publication of this paper.

References

[1] R. Vaze and R. W. Heath, "Capacity scaling for MIMO two-way relaying," in *Proceedings of the IEEE International Symposium on Information Theory (ISIT '07)*, pp. 1451–1455, Nice, France, June 2007.

[2] W. Nam, S.-Y. Chung, and Y. H. Lee, "Capacity of the Gaussian two-way relay channel to within 1/2 bit," *IEEE Transactions on Information Theory*, vol. 56, no. 11, pp. 5488–5494, 2010.

[3] R. Vaze and J. Heath, "On the capacity and diversity-multiplexing tradeoff of the two-way relay channel," *IEEE Transactions on Information Theory*, vol. 57, no. 7, pp. 4219–4234, 2011.

[4] H. J. Yang, J. Chun, and A. Paulraj, "Asymptotic capacity of the separated MIMO two-way relay channel," *IEEE Transactions on Information Theory*, vol. 57, no. 11, pp. 7542–7554, 2011.

[5] T. Yang, X. Yuan, L. Ping, I. B. Collings, and J. Yuan, "A new physical-layer network coding scheme with eigen-direction alignment precoding for MIMO two-way relaying," *IEEE Transactions on Communications*, vol. 61, no. 3, pp. 973–986, 2013.

[6] Z. Fang, X. Yuan, and X. Wang, "Towards the asymptotic sum capacity of the MIMO cellular two-way relay channel," *IEEE Transactions on Signal Processing*, vol. 62, no. 16, pp. 4039–4051, 2014.

[7] G. Zheng, "Joint beamforming optimization and power control for full-duplex MIMO two-way relay channel," *IEEE Transactions on Signal Processing*, vol. 63, no. 3, pp. 555–566, 2015.

[8] Y. Dong, M. J. Hossain, and J. Cheng, "Performance of wireless powered amplify and forward relaying over nakagami-*m* fading channels with nonlinear energy harvester," *IEEE Communications Letters*, vol. 20, no. 4, pp. 672–675, 2016.

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

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

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

[12] P. Parada and R. Blahut, "Secrecy capacity of SIMO and slow fading channels," in *Proceedings of the IEEE International Symposium on Information Theory (ISIT '05)*, pp. 2152–2155, Adelaide, Australia, September 2005.

[13] A. Khisti, G. Wornell, A. Wiesel, and Y. Eldar, "On the Gaussian MIMO wiretap channel," in *Proceedings of the IEEE International Symposium on Information Theory (ISIT '07)*, pp. 2471–2475, Nice, France, June 2007.

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

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

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

[17] Y. Oohama, "Capacity theorems for relay channels with confidential messages," in *Proceedings of the IEEE International Symposium on Information Theory (ISIT '07)*, pp. 926–930, IEEE, June 2007.

[18] A. Mukherjee, S. A. A. Fakoorian, J. Huang, and A. L. Swindlehurst, "Principles of physical layer security in multiuser wireless networks: a survey," *IEEE Communications Surveys and Tutorials*, vol. 16, no. 3, pp. 1550–1573, 2014.

[19] 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," *IEEE Transactions on Signal Processing*, vol. 60, no. 1, pp. 310–325, 2012.

[20] R. Zhang, L. Song, Z. Han, and B. Jiao, "Physical layer security for two-way untrusted relaying with friendly jammers," *IEEE Transactions on Vehicular Technology*, vol. 61, no. 8, pp. 3693–3704, 2012.

[21] J. Mo, M. Tao, Y. Liu, and R. Wang, "Secure beamforming for MIMO two-way communications with an untrusted relay," *IEEE Transactions on Signal Processing*, vol. 62, no. 9, pp. 2185–2199, 2014.

[22] Z. Ding, M. Peng, and H.-H. Chen, "A general relaying transmission protocol for MIMO secrecy communications," *IEEE Transactions on Communications*, vol. 60, no. 11, pp. 3461–3471, 2012.

[23] K. Jayasinghe, P. Jayasinghe, N. Rajatheva, and M. Latva-Aho, "Secure beamforming design for physical layer network coding based MIMO two-way relaying," *IEEE Communications Letters*, vol. 18, no. 7, pp. 1270–1273, 2014.

[24] Q. Liu, G. Gong, Y. Wang, and H. Li, "A novel physical layer security scheme for MIMO two-way relay channels," in *Proceedings of the IEEE Globecom Workshops (GC '15)*, pp. 1–6, San Diego, Calif, USA, December 2015.

[25] O. Longoria-Gandara and R. Parra-Michel, "Estimation of correlated MIMO channels using partial channel state information and DPSS," *IEEE Transactions on Wireless Communications*, vol. 10, no. 11, pp. 3711–3719, 2011.

[26] S. Chen, W. Yao, and L. Hanzo, "Semi-blind adaptive spatial equalization for MIMO systems with high-order QAM signalling," *IEEE Transactions on Wireless Communications*, vol. 7, no. 11, pp. 4486–4491, 2008.

[27] C.-L. Wang and H.-C. Wang, "Optimized joint fine timing synchronization and channel estimation for MIMO systems," *IEEE Transactions on Communications*, vol. 59, no. 4, pp. 1089–1098, 2011.

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