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 Li1

1State Key Lab of ISN, Xidian University, Xi’an, Shaanxi, China
2Department 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

Copyright © 2017 Qiao Liu et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

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

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 $A_k$ ($k \in \kappa \{1, 2, \ldots, K\}$) 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 $H_m$, which is an $n_R \times n_T$ matrix. The channel coefficient between
The transmitted signal vector of user $A_k$ follows:

$Y_R = \sum_{k=1}^{K} (H_{A_k} X_{A_k} + H_{B_k} X_{B_k}) + Z_R,$  \hspace{1cm} (1)

where $X_{A_k}$ is an $n_r \times 1$ column vector that represents the transmitted signal vector of user $A_k$ containing the information message $c_{A_k}$; $X_{B_k}$ represents the transmitted signal of user $B_k$; $Y_R$ denotes the received signal vector by relay, which is an $n_r \times 1$ column vector; and $Z_R$ is an $n_r \times 1$ zero mean circularly symmetric complex Gaussian noise vector at the relay node modelled by $Z_R \sim \mathbb{C} \mathcal{N}(0, I)$.

We denote the covariances of the channel inputs in user $m$ as $Q_m = \epsilon (X_m X_m^H)$. Then, we have the power constraint in uplink phase like

$$\text{Tr} \left\{ \sum_{k=1}^{K} (Q_{A_k} + Q_{B_k}) \right\} \leq P_T.$$  \hspace{1cm} (2)

(3) Downlink Phase. In the downlink (BC) phase, the relay broadcasts its signal $X_R$ 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 $X_R$ of the relay is just the same as the received signal $Y_R$.

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

$$Y_{A_m} = G_{A_m} X_R + Z_{A_m},$$  \hspace{1cm} (3)

where $Z_{A_m}$ is the zero mean circularly symmetric complex Gaussian noise vector at the user $A_m$ modelled by $Z_{A_m} \sim \mathbb{C} \mathcal{N}(0, I)$. The user $A_m$ then decodes the partner’s message $c_{B_m}$ 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 $C_s^{\text{UR}}$ as follows:

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

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

$$R_{A_k}^{\text{UR}} = \frac{1}{2} I \left( Y_{R_k}; X_{A_k} \mid Y_R, X_k \right), \hspace{1cm} (5)$$

$$R_{B_k}^{\text{UR}} = \frac{1}{2} I \left( Y_{A_k}; X_{B_k} \mid Y_R, X_k \right).$$

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

$$R_R^{\text{UR}} = \frac{1}{2} I \left( Y_R; X_{A_1}, X_{A_2}, \ldots, X_{A_k}, X_{B_1}, \ldots, X_{B_k} \right).$$  \hspace{1cm} (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 $H^E_{A_m}$ and $H^E_{B_m}$, respectively; then, the received signal by the eavesdropper $Y_{E_m}$ is

$$Y_{E_m} = H^E_{A_m}X_{A_m} + H^E_{B_m}X_{B_m} + Z_{E_m},$$

where $Z_{E_m}$ is the noise at eavesdropper $E_m$. And upon receiving $Y_{E_m}$, the eavesdropper tries to recover the information messages $c_{A_m}$ and $c_{B_m}$.

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

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

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

$$R_{A_k}^{TR} = \frac{1}{2} \left[ I \left( Y_{E_k}; X_{A_k} \mid Y_L, X_R \right) \right],$$

$$R_{B_k}^{TR} = \frac{1}{2} \left[ I \left( Y_{E_k}; X_{B_k} \mid Y_L, X_R \right) \right].$$

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

$$R_{E_k}^{TR} = \frac{1}{2} \left[ I \left( Y_{E_k}; X_{A_k}, X_{B_k} \right) \right].$$

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

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

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 identical analysis as (5):

$$R_{A_k}^{UE} = \frac{1}{2} \left[ I \left( Y_{R}; X_{A_k} \mid Y_L, X_R \right) \right],$$

$$R_{B_k}^{UE} = \frac{1}{2} \left[ I \left( Y_{R}; X_{B_k} \mid Y_L, X_R \right) \right].$$

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

$$R_{E_k}^{UE} = \frac{1}{2} \left[ I \left( Y_{R}; X_{A_k}, X_{B_k} \right) \right],$$

$$R_{R}^{UE} = \frac{1}{2} \left[ I \left( Y_{R}; X_{A_k}, X_{B_k} \right) \right].$$

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 $c_{A_k}$ (or $c_{A_k}$) 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 $F_{A_k}$. Then, the transmitted signal could be rewritten as $X_{A_k} = F_{A_k} \cdot c_{A_k}$.

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

$$H_{A_k} = U_{A_k} \Sigma_{A_k} V_{A_k}^H,$$

where $U_{A_k}$ and $V_{A_k}$ are unitary matrices and $\Sigma_{A_k}$ is a diagonal matrix with positive diagonal elements. So, we define $F_{A_k}$ in the following form:

$$F_{A_k} = V_{A_k} \Sigma_{A_k}^{-1} U_{A_k}^H R \Psi_{A_k} L_k,$$

where $R$ is an $n_L \times n_R$ unitary matrix called Direction Rotation matrix and $\Sigma_{A_k}^{-1}$ denotes the pseudoinverse of $\Sigma_{A_k}$. $\Psi_{A_k}$ represents the allocated transmission power for user $A_k$. In addition, we assume it is identical for all users in this work. $L_k$ is called channel allocation matrix to guarantee that multipair users communicate simultaneously. $L_k$ allocates the
constructed equivalent parallel subchannels to corresponding users. The design and optimization of $R$ and $L_k$ will affect the transmission efficiency of the proposed scheme. Then, we will introduce the design of $R$ and $L_k$, 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 $R$, we first define a new matrix $G$ as

$$G = \sum_{k=1}^{K} \left\{ U_A \Sigma_{A_k}^{-1} U_A^H + \frac{1}{m} \Sigma_{B_k}^{-1} U_B^H \right\}. \quad (16)$$

Using eigendecomposition, $G$ could be represented as

$$G = U_g \Lambda_g U_g^H. \quad (17)$$

where $U_g$ is a unitary matrix and $\Lambda_g$ is a diagonal matrix whose nonzero elements are the eigenvalues of $G$ arranged in the ascending order. Then, we choose $R$ as

$$R = U_g. \quad (18)$$

**Design of Channel Allocation Matrix.** Before designing $L_k$, we first define two varieties $d_k$ and $D_k$. $d_k$ is the independent signal streams of the $k$th communication pair, and $D_k$ is the sum independent signal streams of the $k$th communication pair to the $k$th pair as $D_k = \sum_{k=1}^{K} d_k$. In order to align the signals from the same communication pair to the same directions, we define $L_{A_k} = L_{B_k} = L_k$. And $L_k$ is designed by collecting the $D_k + d_k$ column vector from the $n_R \times n_R$ unit matrix, so $L_k$ is in the size of $n_R \times d_k$. $L_k$ is shown as follows:

$$L_k = \begin{bmatrix} d_k \\ 00 \cdots 0 \\ 00 \cdots 0 \\ \vdots \\ 00 \cdots 0 \\ 10 \cdots 0 \\ 01 \cdots 0 \\ \vdots \\ 00 \cdots 1 \\ 00 \cdots 0 \\ \vdots \\ 00 \cdots 0 \end{bmatrix}. \quad (19)$$

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

$$Y_R = \sum_{k=1}^{K} \left( H_{A_k} F_{A_k} c_{A_k} + H_{B_k} F_{B_k} c_{B_k} \right) + Z_R \quad (20)$$

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

$$H_k F_k = U_k \Sigma_{k}^{-1} U_k^H \quad \text{and} \quad H_k F_k = R L_k = \text{RL}_k \quad (21)$$

so the received signal $Y_R$ could be rewritten as

$$Y_R = R \sum_{k=1}^{K} L_k \left( c_{A_k} + c_{B_k} \right) + Z_R \quad \text{as follows:} \quad Y_R = \begin{bmatrix} c_{A_1} + c_{B_1} \\ c_{A_2} + c_{B_2} \\ \vdots \\ c_{A_K} + c_{B_K} \end{bmatrix} + Z_R. \quad (22)$$

As shown in (22), the signals from the same communication pairs have been aligned into the same directions.

Upon receiving $Y_R$, the relay generates its transmitting signal $X_R$. In the Amplify-and-Forward (AF) agreements, the relationship between $X_R$ and $Y_R$ is simply written as $X_R = Y_R$. 

**(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

$$Y_{B_m} = G_{B_m} X_R + Z_{B_m} \quad (23)$$

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

$$\tilde{Y}_{B_m} = G_{B_m} X_{A_m} + G_{B_m} Z_R + Z_{A_m}. \quad (24)$$

The interference cancellation will be accomplished by the detection vector $D_{A_m}$. $D_{A_m}$ is dependent on $G_{A_m}$. Consider the case where $G_{A_m}$ is simply the transpose of $H_{A_m}$. Then, $D_{B_m}$ is designed such that $D_{B_m} = \sum_{k=1}^{K} \left( H_{A_k} F_{A_k} c_{A_k} + H_{B_k} F_{B_k} c_{B_k} \right) + G_{B_m} Z_R \quad (25)$

Consequently, the received signal will be

$$\tilde{Y}_{B_m} = D_{B_m} Y_{B_m} = D_{B_m} \left( H_{B_m}^H X_{A_m} + Z_{B_m} \right)$$

where $Z_{B_m}$ 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 $c_{A_m}$ by the XOR operation with its self-information symbols $c_{B_m}$. 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 $R_{tr}^{UR}$ and $\{R_{A_1}^{UR}, R_{A_2}^{UR}, \ldots, R_{A_K}^{UR}, R_{B_1}^{UR}, \ldots, R_{B_K}^{UR}\}$. 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

$$R_{A_m}^{UR} = \frac{1}{2} \log \det \left( I + F_{A_m}^H H_{A_m}^H G_{B_m} K_{A_m}^{-1} G_{B_m} H_{A_m} F_{A_m} \right)$$

$$= \frac{1}{2} \log \det \left( I + F_{m}^H R G_{B_m} K_{A_m}^{-1} G_{B_m} R L_{m} \right),$$

where $K_{A_m} = G_{B_m} G_{B_m}^H + I$.

Similarly, the information rate from $B_m$ to $A_m$ is

$$R_{B_m}^{UR} = \frac{1}{2} \log \det \left( I + L_{m}^H R G_{A_m} K_{B_m}^{-1} G_{A_m} R L_{m} \right).$$

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:

$$R_{tr}^{UR} = \frac{1}{2} \log \det \left( I \right)$$

$$+ \sum_{k=1}^{K} \left( H_{A_k} F_{A_k} F_{A_k}^H H_{A_k}^H + H_{B_k} F_{B_k} F_{B_k}^H H_{B_k}^H \right).$$

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

$$C_{s}^{UR} = \frac{1}{2} \log \det \left[ \prod_{k=1}^{K} \left( I + L_{m}^H R G_{B_m} K_{A_m}^{-1} G_{B_m} R L_{m} \right) \right]$$

$$\quad + \sum_{k=1}^{K} \left( H_{A_k} F_{A_k} F_{A_k}^H H_{A_k}^H + H_{B_k} F_{B_k} F_{B_k}^H H_{B_k}^H \right).$$

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

$$Y_{E_m} = H_{A_m}^E F_{A_m} c_{A_m} + H_{B_m}^E F_{B_m} c_{B_m} + Z_{E_m},$$

where $Z_{E_m}$ is noise at eavesdropper $E_m$. Consequently, we have the achievable information rate as

$$C_{s}^{TR} = \frac{1}{2} \log \det \left[ \prod_{k=1}^{K} \left( I + L_{m}^H R G_{B_m} K_{A_m}^{-1} G_{B_m} R L_{m} \right) \right]$$

$$\quad + \sum_{k=1}^{K} \left( H_{A_k} F_{A_k} F_{A_k}^H H_{A_k}^H + H_{B_k} F_{B_k} F_{B_k}^H H_{B_k}^H \right).$$

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 $R_{A_m}^{UE}$ and $R_{B_m}^{UE}$ are given as
\[
R_{A_m}^{UE} = \frac{1}{2} \log \det \left( I + L_{m}^{H} R_{B_m}^{H} K_{A_m}^{-1} G_{B_m} RL_{m} \right),
\]
\[
R_{B_m}^{UE} = \frac{1}{2} \log \det \left( I + L_{m}^{H} R_{A_m}^{H} K_{B_m}^{-1} G_{A_m} RL_{m} \right).
\]  
(34)

And the achievable information rate at the untrusted relay is given as
\[
R_{R}^{UE} = \frac{1}{2} \log \left[ I + \sum_{k=1}^{K} \left( H_{A_k} F_{A_k} F_{A_k}^{H} + H_{B_k} F_{B_k} F_{B_k}^{H} \right) \right].
\]  
(35)

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 $P_{A_m}$ and $P_{B_m}$ for users $A_m$ and $B_m$. We consider the situation in $A_m$ as a case. Containing two function parts, $P_{A_m}$ can be artificially divided into two parts as follows:
\[
P_{A_m} = F_{A_m} S_{A_m},
\]  
(38)

And the achievable information rate at eavesdropper is given as
\[
R_{E}^{UE} = \frac{1}{2} \log \left[ I + H_{A_m}^{E} F_{A_m} F_{A_m}^{H} \left( H_{A_m}^{E} \right)^{H} \right]
\]
\[
+ H_{B_m}^{E} F_{B_m} F_{B_m}^{H} \left( H_{B_m}^{E} \right)^{H} \].
\]  
(36)

With (34), (35), and (36), we obtain the achievable secrecy channel capacity as
\[
C_s^{UE} = \frac{1}{2} \log \left[ \frac{\sum_{k=1}^{K} \left( I + L_{m}^{H} R_{B_m}^{H} K_{A_m}^{-1} G_{B_m} RL_{m} \right) \left( I + L_{m}^{H} R_{A_m}^{H} K_{B_m}^{-1} G_{A_m} RL_{m} \right) / \left( I + \sum_{k=1}^{K} H_{A_k} F_{A_k} F_{A_k}^{H} + H_{B_k} F_{B_k} F_{B_k}^{H} \right) \right]}{I + \sum_{k=1}^{K} H_{A_k} F_{A_k} F_{A_k}^{H} + H_{B_k} F_{B_k} F_{B_k}^{H} \right)}. \]  
(37)

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

The encryption precoding matrix $S_{A_m}$ or $S_{B_m}$ is generated from a key stream $s_m$ where $s_m(t) \in \{1, -1\}$. The generation of $S_{A_m}$ and $S_{B_m}$ will depend on the security level of the system. For low security level, $S_{A_m}$ and $S_{B_m}$ will just be equal to $s_m$ as $S_{A_m} = S_{B_m} = s_m$. For high level security, $S_{A_m}$ and $S_{B_m}$ will be different by dividing $s_m$ into two parts. Note here that the key stream must be preshared between users $A_m$ and $B_m$ before the transmission, and $s_m$ is produced by pseudorandom sequence generators (PRSG).

With $S_{A_m}$ and $S_{B_m}$, 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
\[
Y^{Enc}_{R} = R \sum_{k=1}^{K} A_k \left( S_{A_k} c_{A_k} + S_{B_k} c_{B_k} \right) + Z_R
\]
\[
= R \begin{bmatrix}
S_{A_1} c_{A_1} + S_{B_1} c_{B_1} \\
S_{A_2} c_{A_2} + S_{B_2} c_{B_2} \\
\vdots \\
S_{A_K} c_{A_K} + S_{B_K} c_{B_K}
\end{bmatrix} + Z_R.
\]  
(39)
Table 1: BPSK data patterns of user transmitting signals and relay receiving signal for physical layer encryption approach.

<table>
<thead>
<tr>
<th>$X_{A_k}$</th>
<th>$S_{A_k}$</th>
<th>$X_{B_k}$</th>
<th>$S_{B_k}$</th>
<th>$Y_{Enc}^k$</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>-1</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>-1</td>
<td>1</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>-1</td>
<td>-1</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>-1</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>-1</td>
<td>1</td>
<td>-1</td>
<td>-2</td>
<td></td>
</tr>
<tr>
<td>-1</td>
<td>1</td>
<td>-1</td>
<td>-2</td>
<td></td>
</tr>
<tr>
<td>-1</td>
<td>-1</td>
<td>-1</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>-1</td>
<td>-1</td>
<td>-1</td>
<td>-2</td>
<td></td>
</tr>
</tbody>
</table>

Table 2: BPSK data patterns of user transmitting signals and relay receiving signal for information theoretical approach.

<table>
<thead>
<tr>
<th>$X_{A_k}$</th>
<th>$X_{B_k}$</th>
<th>$Y_R$</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>1</td>
<td>-1</td>
<td>0</td>
</tr>
<tr>
<td>-1</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>-1</td>
<td>-1</td>
<td>-2</td>
</tr>
</tbody>
</table>

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 $Y_{Enc}^k = 2$, 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

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

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...
The proposed scheme
ML
MMSE

Intended receivers
Eavesdropper with IT approach
Eavesdropper with IT approach known R
Eavesdropper with PHY Enc approach
Eavesdropper with PHY Enc approach known R

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

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
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

$$R_R = \frac{1}{2} I \left( \{ Y_R; X_{A_1}, X_{A_2}, \ldots, X_{A_k}, X_{B_1}, \ldots, X_{B_k} \} \right)$$ (A.1)

$$R_{E_k} = \frac{1}{2} I \left[ \left( \{ Y_{E_k}; X_{A_1}, X_{B_1} \} \right) \right].$$ (A.2)

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

$$R_R = \frac{1}{2} I \left( \{ Y_R; X_{A_1}, X_{A_2}, \ldots, X_{A_k}, X_{B_1}, \ldots, X_{B_k} \} \right)$$

(a) $\frac{1}{2} I \{ X_{A_1}, X_{A_2}, \ldots, X_{A_k}, X_{B_1}, \ldots, X_{B_k}; Y_R \}$

(b) $\frac{1}{2} I \{ X_{A_1}, X_{A_2}, \ldots, X_{A_k}, Y_R \}$

(c) $\frac{1}{2}$

$$\sum_{k=1}^{K} \left[ I \{ X_{A_k}; Y_R | X_{A_{k-1}}, \ldots, X_{A_1}, X_{B_{k-1}}, \ldots, X_{B_1} \} \right] + I \{ X_{B_k}; Y_R \}$$ (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 $I(\{ X_{A_k}; Y_R \})$ or $I(\{ X_{B_k}; Y_R \})$ is zero, the proposition will be permitted.

So, we move on to the proof of $I(\{ X_{A_k}; Y_R \}) = 0$. 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>
<thead>
<tr>
<th>$Y_R$</th>
<th>$X_{A_k}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>−1</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>−2</td>
<td>1</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
</tr>
</tbody>
</table>

Table 4: Joint probability distributions of $X_{A_k}$ and $Y_R$.

<table>
<thead>
<tr>
<th>$Y_R$</th>
<th>$X_{A_k}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>−2</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
</tr>
</tbody>
</table>

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

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 $H(Y_R | X_{A_k})$ as

$$H(Y_R) = H\left( \frac{1}{4}, \frac{1}{4}, \frac{1}{4}, \frac{1}{4} \right)$$

$$= \frac{1}{4} \log_2 4 + \frac{1}{4} \log_2 4 + \frac{1}{4} \log_2 4 + \frac{1}{4} \log_2 4 = \frac{3}{2} \text{ bit,}$$

$$H(Y_R | X_{A_k}) = \sum_{x_{A_k} \in \{1, -1\}} p(\{x_{A_k}\}) H(Y_R | X_{A_k} = x_{A_k})$$ (A.4)

$$= \frac{1}{2} H\left( \frac{1}{4}, \frac{1}{2}, \frac{1}{4} \right) + \frac{1}{2} H\left( \frac{1}{4}, \frac{1}{2}, \frac{1}{4} \right)$$

$$= H\left( \frac{1}{4}, \frac{1}{2}, \frac{1}{4} \right) = \frac{3}{2} \text{ bit.}$$

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

$$I(Y_R; X_{A_k}) = H(Y_R) - H(Y_R | X_{A_k}) = \frac{3}{2} - \frac{3}{2} = 0 \text{ bit.}$$ (A.5)

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

$$I(Y_R; X_{A_k}) = 0.$$ (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


Submit your manuscripts at https://www.hindawi.com