WFRFT-Based Signal Domain Secure Communication for Two-Way Relay Systems

Heng Dong*, Zunqi Li*, Xiaojie Fang*, Xuejun Sha*, Zhuoming Li*, Dirk Slock†
Harbin Institute of technology, Harbin, China*; Eurecom, Biot, France†
Email: {dongheng, lizunqi}@stu.hit.edu.cn, {fangxiaojie, shaxuejun, zhuoming}@hit.edu.cn, slock@eurecom.fr

***Abstract*—In this paper, the weighted fractional Fourier transform (WFRFT) signal domain is introduced to enhance the security performance of two-way trusted relay systems at the signal level. The proposed scheme, which requires only a single relay node, leverages the multi-component energy distribution characteristics of WFRFT signals to improve security with low complexity and high power efficiency. The inherent security mechanism of WFRFT analyzed in this paper can be simply summarized as follows: the superposition of components in WFRFT signals that do not satisfy specific constraints will result in the inability to perfectly reconstruct the message signal. Based on this, confidential information is encoded into WFRFT signals with private transform orders, allowing legitimate users to achieve perfect decoding. Since WFRFT signals exhibit energy concentration only in specific transformation domains, mismatched transform orders adopted by the eavesdropper cause energy loss in the information-bearing signal, leading to inter-component interference that further degrades the quality of the recovered signal. The advantages of the proposed scheme in limiting information leakage and improving the achievable secrecy sum rate (SSR) are analyzed. Numerical results validate the theoretical analysis and demonstrate the secrecy performance of the proposed scheme.**

***Index Terms*—Physical layer security (PLS), two-way trusted relay, weighted fractional Fourier transform (WFRFT), power efficiency.**

I. Introduction

Traditionally, secure communication is guaranteed by encryption algorithms on the higher layers to prevent the interception of information based on computational security. Although these key-dependent algorithms have proven effective in certain communication scenarios, key management and distribution, as well as high computational power requirements, pose significant challenges for multi-node or lightweight networks [1]. As an alternative, physical layer security (PLS) can provide secure communication from the bottom layer of the system [2]–[4]. Recently, there has been increasing attention paid to PLS in two-way relay networks due to the network's ability to expand coverage, increase spectral efficiency, and reduce overall power consumption.

In two-way trusted relay (TWTR) systems with eavesdroppers, relay selection is efficient for enhancing the difference between the legitimate channel and the wiretap channel, which is based on channel selection using sufficient space domain resources. A low-complexity relay selection criterion is proposed in [5] to improve the security performance of large-scale two-way amplify-and-forward (AF) relay systems, and the impact of node density is analyzed. Additionally, [6] proposed a relay selection criterion that relies only on the channel state information (CSI) of legitimate channels, based on the inherent secrecy characteristics brought by the superimposed legitimate signals. Cooperative jamming (CJ) schemes can actively reduce the quality of the received signal at the eavesdropper, and they are typically combined with relay selection for better performance [7], [8]. For instance, in [7], the node with the best connection with two legitimate sources is selected as the relay to enhance the legitimate links, and the weakest node is selected as a jamming node. Unlike the aforementioned single-antenna-based systems, secure precoding schemes with multi-antenna base station [9], relay [10], or both [11] show better secrecy performance. However, these schemes are often difficult to apply to systems with lightweight requirements.

In general, existing methods to ensure security performance for TWTR systems rely on two aspects: 1) increasing spatial domain resources through system complexity, such as multiple relay nodes and multiple antenna devices; and 2) increasing cooperative resources through energy consumption. Therefore, this paper aims to address the challenge of ensuring secure communication for lightweight systems without consuming valuable transmit power.

Motivated by the above, the weighted fractional Fourier transform (WFRFT) signal domain is introduced into TWTR systems to provide additional security gains at the signal level. Although in our previous work [12], we introduced WFRFT into multi-antenna Intelligent Transport Systems (ITS) to enhance the security performance of the system, the focus was on the impact of imperfect CSI caused by the mobility of Vehicle User Equipment (VUE) and the theoretical expression of performance in high signal-to-noise ratio (SNR) regions. This paper focuses on the design of a general single-antenna node lightweight PLS scheme and a detailed analysis of the security mechanism based on the multiple components of WFRFT at the signal level. The contribution of this paper can be summarized as:

1) The inherent security mechanism provided by the four components of the WFRFT is analyzed in detail, and a quantitative expression for the security gains is derived. Specifically, the superposition of WFRFT signal components violating specific constraints hinders perfect signal reconstruction. A mismatched transform order at the eavesdropper causes energy loss in the information-

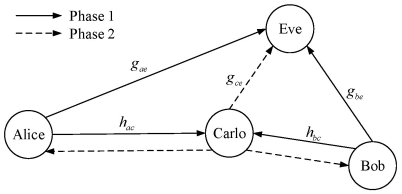


Fig. 1. System model with two-way trusted relay model.

bearing signal, which transforms into inter-component interference, further disrupting the eavesdropper.

2) A WFRFT-based signal domain secure communication scheme for TWTR systems is proposed. Additionally, we derive the achievable secrecy sum rate (SSR) when the eavesdropper uses either maximum ratio combining (MRC) or selection combining (SC). Notably, we also highlight the advantages of the proposed scheme when the eavesdropper can separate the superimposed signals from legitimate nodes, where traditional TWTR security features fail, further underscoring the benefits of signal-level security.

II. System Model and Signal Model

A. Secure Two-Way Relay System Model

Consider the problem of secure communication between two nodes assisted by an AF relay, where each node is equipped with only a single antenna. We assume that there is no direct communication link between two source nodes. One complete two-way communication process between Alice and Bob requires two consecutive phases, namely the multiple access (MAC) phase and broadcast (BC) phase.

As shown in Fig. 1, Alice and Bob communicate with each other through the assistance of the TWTR Carlo, which has been authenticated and is not eavesdropping on the exchange of messages. However, a passive eavesdropper named Eve, attempting to decode the information-bearing signals, is presented in the system. In phase 1, Alice and Bob simultaneously transmit their information bearing signals to Carlo. In phase 2, Carlo forwards the superimposed signals received in phase 1 to Alice and Bob, who decode their desired signals after removing the residual self-interference. During each of these processes, Eve attempts to decode the information from the eavesdropped signals. For simplicity, all channels are assumed to be quasi-static and reciprocal. We denote the channel coefficients of the "Alice $\leftrightarrow$ Carlo" and "Bob $\leftrightarrow$ Carlo" links as h_{ac} and h_{bc}, respectively. Moreover, g_{ae}, g_{be} and g_{ce} represent the channel coefficients from Alice, Bob, and Carlo to Eve, respectively. Without loss of generality, we assume that h_{ac} and h_{bc} are publicly known to all nodes, but g_{ae}, g_{be} and g_{ce} are not available for the legitimate nodes.

B. WFRFT Signal Model

WFRFT is a generalization of the Fourier transform, and can be expressed as a weighted sum of the 1 to 4 times of the normalized discrete Fourier transform (DFT) of a sequence. For an N-length complex sequence $\mathbf{x} = [x_0, x_1, \ldots, x_{N-1}]^{\mathrm{T}} \in \mathbb{C}^{N\times 1}$, the α-order WFRFT can be defined as:

$$\mathcal{F}_4^{\alpha}[\mathbf{x}] = (\omega_0\mathbf{I} + \omega_1\mathbf{F} + \omega_2\mathbf{\Pi} + \omega_3\mathbf{\Pi F})\,\mathbf{x}, \tag{1}$$

where the N-points normalized DFT transform matrix $[\mathbf{F}]_{n,k} = (1/\sqrt{N})\cdot\exp(-\mathrm{i}2\pi nk/N)$ and $\mathbf{I}$ denotes an $N\times N$ identity matrix. $[\mathbf{\Pi}]_{n,k} = \delta(\langle n+k\rangle_N)$ denotes an $N\times N$ permutation matrix, in which $\delta(\cdot)$ and $\langle\cdot\rangle_N$ denote Kronecker delta and modulo-N calculation, respectively. The weight coefficients $\omega_l(\alpha)(l = 0,1,2,3)$ of the four components of WFRFT can be respectively expressed as:

$$\omega_l(\alpha) = \cos\left[\frac{(\alpha-l)\pi}{4}\right]\cos\left[\frac{2(\alpha-l)\pi}{4}\right]\exp\left[\frac{3(l-\alpha)\pi\mathrm{i}}{4}\right]. \tag{2}$$

The necessary properties of WFRFT for the proposed scheme can be summarized as:

- *Boundary property*: $\mathcal{F}_4^0[\mathbf{x}] = \mathbf{x},\ \mathcal{F}_4^1[\mathbf{x}] = \mathcal{F}[\mathbf{x}]$;
- *Additive property*: $\mathcal{F}_4^{\alpha+\beta}[\mathbf{x}] = \mathcal{F}_4^{\alpha}[\mathcal{F}_4^{\beta}[\mathbf{x}]] = \mathcal{F}_4^{\beta}[\mathcal{F}_4^{\alpha}[\mathbf{x}]]$;
- *Unitary property*: $[\mathcal{F}_4^{\alpha}]^{-1}[\mathbf{x}] = [\mathcal{F}_4^{\alpha}]^{\mathrm{H}}[\mathbf{x}]$;
- *Periodicity property*: $\mathcal{F}_4^{\alpha}[\mathbf{x}] = \mathcal{F}_4^{\alpha+4}[\mathbf{x}]$;
- *Parseval's Theorem*: $\sum_{n=0}^{N-1}|x_n|^2 = \sum_{n=0}^{N-1}|[\mathcal{F}_4^{\alpha}[\mathbf{x}]]_n|^2$.

The boundary property and additive property ensure that the information can be recovered by inverse-WFRFT iff with corresponding transform order, i.e., $\mathbf{x} = \mathcal{F}_4^{\alpha}\left[\mathcal{F}_4^{-\alpha}[\mathbf{x}]\right]$. Unitary property is the basis for applying WFRFT to communication systems and periodicity property provides guidance for the convention and delivery of WFRFT transformation order. Parseval's Theorem is necessary for analyzing the energy distribution of the signal in subsequent scheme design.

III. WFRFT-based Secure Transmission Scheme with the Two-way Trusted Relay

In this section, the proposed WFRFT-based scheme with two-way trusted relay is introduced from the aspects of signal description, security mechanisms, and security performance.

A. Communication Process Among Legitimate Nodes

In the first phase, Alice and Bob perform α-order and β-order WFRFT on their data symbol sequences $\mathbf{s}_a \in \mathbb{C}^{N\times 1}$ and $\mathbf{s}_b \in \mathbb{C}^{N\times 1}$, thus the transmitted signal vectors $\mathbf{x}_a = \mathcal{F}_4^{\alpha}[\mathbf{s}_a] \in \mathbb{C}^{N\times 1}$ and $\mathbf{x}_b = \mathcal{F}_4^{\beta}[\mathbf{s}_b] \in \mathbb{C}^{N\times 1}$ are obtained. Then, Alice and Bob send $\mathbf{x}_a$ and $\mathbf{x}_b$ to Carlo, simultaneously. The received signal vector $\mathbf{y} \in \mathbb{C}^{N\times 1}$ of Carlo can be expressed as:

$$\begin{aligned}\mathbf{y} &= \sqrt{P_a}h_{ac}\mathbf{x}_a + \sqrt{P_b}h_{bc}\mathbf{x}_b + \mathbf{n}\\ &= \sqrt{P_a}h_{ac}\mathcal{F}_4^{\alpha}[\mathbf{s}_a] + \sqrt{P_b}h_{bc}\mathcal{F}_4^{\beta}[\mathbf{s}_b] + \mathbf{n},\end{aligned} \tag{3}$$

where $\mathbf{n} \in \mathbb{C}^{N\times 1}$ is the zero-mean complex additive white Gaussian noise (AWGN) with covariance matrix $\sigma_n^2\mathbf{I}_N$. P_a and P_b denote the transmit power of Alice and Bob, respectively.

In the second phase, Carlo amplifies the received signal $\mathbf{y}$ according to its available transmit power and forwards a scaled signal $\mathbf{r} = \xi\mathbf{y}$. The amplification coefficient is given by:

$$\xi = \sqrt{P_c/[(|h_{ac}|^2P_a + |h_{bc}|^2P_b + \sigma_n^2)]}, \tag{4}$$

where P_c denotes the transmit power of Carlo. Subsequently, the received signals at Alice and Bob are given by:

$$\mathbf{r}^A = \xi\sqrt{P_a}h_{ac}^2\mathbf{x}_a + \xi\sqrt{P_b}h_{ac}h_{bc}\mathbf{x}_b + \mathbf{n}^A, \tag{5}$$

$$\mathbf{r}^B = \xi\sqrt{P_a}h_{bc}h_{ac}\mathbf{x}_a + \xi\sqrt{P_b}h_{bc}^2\mathbf{x}_b + \mathbf{n}^B, \tag{6}$$

where $\mathbf{n}^A = \xi h_{ac}\mathbf{n} + \mathbf{n}'_a$ and $\mathbf{n}^B = \xi h_{bc}\mathbf{n} + \mathbf{n}'_b$ are the total AWGN at Alice and Bob, respectively, in which $\mathbf{n}'_a \sim \mathcal{CN}(\mathbf{0}_N, \sigma_n^2\mathbf{I}_N)$ and $\mathbf{n}'_b \sim \mathcal{CN}(\mathbf{0}_N, \sigma_n^2\mathbf{I}_N)$. Thus, the elements of $\mathbf{n}^A$ and $\mathbf{n}^B$ are i.i.d. $\mathcal{CN}(0, \xi^2|h_{ac}|^2\sigma_n^2 + \sigma_n^2)$ and $\mathcal{CN}(0, \xi^2|h_{bc}|^2\sigma_n^2 + \sigma_n^2)$, respectively. Since Alice knows its transmit signal, it could subtract the self-interference term $\xi\sqrt{P_a}h_{ac}^2\mathbf{x}_a$ from (5). Then Alice could restore the data symbol by WFRFT with matching transform order $-\beta$. The process can be expressed as:

$$\begin{aligned}\mathbf{p}^A &= \mathcal{F}_4^{-\beta}[\mathbf{r}^A - \xi\sqrt{P_a}h_{ac}^2\mathbf{x}_a] \\ &= \mathcal{F}_4^{-\beta}\left[\xi\sqrt{P_b}h_{ac}h_{bc}\mathcal{F}_4^{\beta}[\mathbf{s}_b]\right] + \mathcal{F}_4^{-\beta}[\mathbf{n}^A] \\ &= \xi\sqrt{P_b}h_{ac}h_{bc}\mathbf{s}_b + \mathbf{n}^{A'}, \end{aligned} \tag{7}$$

where $\mathbf{n}^{A'} = \mathcal{F}_4^{-\beta}[\mathbf{n}^A]$ is the AWGN after WFRFT, which has the same distribution characteristics as $\mathbf{n}^A$. Similar to (7), the restored data symbol of Bob can be expressed as:

$$\mathbf{p}^B = \xi\sqrt{P_a}h_{bc}h_{ac}\mathbf{s}_a + \mathbf{n}^{B'}, \tag{8}$$

where $\mathbf{n}^{B'} = \mathcal{F}_4^{-\alpha}[\mathbf{n}^B]$ has the same distribution characteristics as $\mathbf{n}^B$. According to (7) and (8), the instantaneous SNR at Alice ($\mathbf{s}_b$ is the desired data) and Bob ($\mathbf{s}_a$ is the desired data) can be respectively expressed as:

$$\gamma^A = \frac{\xi^2 P_b|h_{ac}|^2|h_{bc}|^2}{\xi^2|h_{ac}|^2\sigma_n^2 + \sigma_n^2}, \gamma^B = \frac{\xi^2 P_a|h_{bc}|^2|h_{ac}|^2}{\xi^2|h_{bc}|^2\sigma_n^2 + \sigma_n^2}. \tag{9}$$

B. Analysis of Signals Received by the Eavesdropping Node

Assuming that Eve has full knowledge of the WFRFT technique, but lacks real-time and precise transform orders of WFRFT used by Alice and Bob. This assumption can be easily met in practical systems, owing to the extremely small data volume of the WFRFT transform order. For example, parameters can be guaranteed through an additional secure link, while reliable upper-layer cryptography encryption technology or dynamic parameter codebooks agreed upon by legal nodes can be utilized to safeguard the parameters against Eve during the communication process. Specifically, traditional key generation protocols such as Diffie-Hellman key exchange, or physical layer key generation techniques, can ensure the secure and dynamic exchange of WFRFT parameters.

In the first phase, Eve receives the superimposed signal of $\mathbf{x}_a$ and $\mathbf{x}_b$, which can be expressed as:

$$\mathbf{z}_1 = \sqrt{P_a}g_{ae}\mathbf{x}_a + \sqrt{P_b}g_{be}\mathbf{x}_b + \mathbf{e}_1, \tag{10}$$

where $\mathbf{e}_1 \in \mathbb{C}^{N\times 1}$ is the zero-mean AWGN with covariance matrices $\sigma_e^2\mathbf{I}_N$. According to (10), the information bearing signal shows the superposition of $\mathbf{s}_a$ and $\mathbf{s}_b$ undergoing different orders of WFRFT. When Eve adopts $(-\hat{\alpha})$-order WFRFT to restore $\mathbf{s}_a$, the result is given by:

$$\begin{aligned}\mathbf{p}_1^{EA} &= \mathcal{F}_4^{-\hat{\alpha}}[\sqrt{P_a}g_{ae}\mathcal{F}_4^{\alpha}[\mathbf{s}_a] + \sqrt{P_b}g_{be}\mathcal{F}_4^{\beta}[\mathbf{s}_b] + \mathbf{e}_1] \\ &= \sqrt{P_a}g_{ae}\mathcal{F}_4^{\Delta\alpha}[\mathbf{s}_a] + \sqrt{P_b}g_{be}\mathcal{F}_4^{\beta-\hat{\alpha}}[\mathbf{s}_b] + \mathbf{e}_1{}', \end{aligned} \tag{11}$$

where $\Delta\alpha = \alpha - \hat{\alpha}$ is the WFRFT transform order error used by Eve to restore $\mathbf{s}_a$. $\mathbf{e}_1{}' = \mathcal{F}_4^{-\hat{\alpha}}[\mathbf{e}_1]$. Due to the parameter mismatch with Alice, the eavesdropper is inevitably affected by the inter-component interference brought by the energy aggregation characteristics of WFRFT signal in specific transform domain. According to the Parseval's Theorem, WFRFT does not affect the energy of the second term of (11). Thus, the power of inter-user interference is $P_b|g_{be}|^2$, and the inter-component interference only exists in the first term.

According to the Additive Property of WFRFT, $\mathcal{F}_4^{\Delta\alpha}[\mathbf{s}_a] = \mathcal{F}_4^{-\hat{\alpha}}\mathcal{F}_4^{\alpha}[\mathbf{s}_a]$. Therefore, the information bearing signal for Eve in $\mathcal{F}_4^{\Delta\alpha}[\mathbf{s}_a]$ is equal to the component of data sequence $\mathbf{s}_a$ that can be recovered by performing $\mathcal{F}_4^{-\hat{\alpha}}[\cdot]$ on sequence $\mathcal{F}_4^{\alpha}[\mathbf{s}_a]$. At the same time, the inter-component interference of Eve in $\mathcal{F}_4^{\Delta\alpha}[\mathbf{s}_a]$ is caused by the inability of each component in WFRFT to be effectively superimposed into the form of WFRFT signal.

According to (2), the weighted coefficients in the transform $\mathcal{F}_4^{-\hat{\alpha}}[\cdot]$ can be expressed as:

$$\begin{aligned}\omega_l(-\hat{\alpha}) &= \omega_l(-\alpha + \Delta\alpha) \\ &= \cos\left[(-\alpha + \Delta\alpha - l)\pi/4\right]\cos\left[2(-\alpha + \Delta\alpha - l)\pi/4\right] \\ &\quad \exp\left[-3(-\alpha + \Delta\alpha - l)\pi\mathrm{i}/4\right], \quad l = 0, 1, 2, 3. \end{aligned} \tag{12}$$

In order to restore the data in $\mathcal{F}_4^{\alpha}[\mathbf{s}_a]$, it is necessary to reconstruct the transform matrix $\mathbf{F}_4^{-\alpha}$. Therefore, expanding the cosine function in (12) to construct $\omega_l(-\hat{\alpha})$, which can be further expressed as:

$$\omega_l(-\hat{\alpha}) = \omega_l(-\alpha)\varphi(\Delta\alpha) + \nu_l(\alpha, \Delta\alpha), \tag{13}$$

where $\varphi(\Delta\alpha)$ is the energy attenuation factor and $\nu_l(\alpha, \Delta\alpha)$ is the weighted coefficient of the l-th additive interference component, when the signal sequence $\mathcal{F}_4^{\alpha}[\mathbf{s}_a]$ is restored by $(-\hat{\alpha})$-order WFRFT. The expression for $\varphi(\Delta\alpha)$ is given by:

$$\varphi(\Delta\alpha) = \cos[\Delta\alpha\pi/4]\cos[2\Delta\alpha\pi/4]\exp[-3\Delta\alpha\pi\mathrm{i}/4]. \tag{14}$$

It can be seen that $\varphi(\Delta\alpha)$ with period 4 only depends on $\Delta\alpha$ and is independent of the specific transform order α. $\nu_l(\alpha, \Delta\alpha)$ in (15) can be expressed as:

$$\nu_l(\alpha, \Delta\alpha) = \sum_{n=0}^{2}\phi_{n,l}(\alpha, \Delta\alpha)\exp[3(\alpha - \Delta\alpha + l)\pi\mathrm{i}/4], \tag{15}$$

where $\phi_{n,l}(\alpha, \Delta\alpha)(n = 0, 1, 2)$ can be expressed as:

$$\begin{aligned}\phi_{0,l}(\alpha, \Delta\alpha) &= \cos[u_l(\alpha)]\sin[2u_l(\alpha)]\cos[m(\Delta\alpha)]\sin[2m(\Delta\alpha)], \\ \phi_{1,l}(\alpha, \Delta\alpha) &= \sin[u_l(\alpha)]\cos[2u_l(\alpha)]\sin[m(\Delta\alpha)]\cos[2m(\Delta\alpha)], \\ \phi_{2,l}(\alpha, \Delta\alpha) &= \sin[u_l(\alpha)]\sin[2u_l(\alpha)]\sin[m(\Delta\alpha)]\sin[2m(\Delta\alpha)], \end{aligned} \tag{16}$$

where $u_l(\alpha) = (\alpha + l)\pi/4$ and $m(\Delta\alpha) = \Delta\alpha\pi/4$.

Based on the above analysis, the recovery result of Eve for the first term in (11) can be further expressed as:

$$\begin{aligned}\mathcal{F}_4^{-\hat{\alpha}}\left[\mathcal{F}_4^{\alpha}[\mathbf{s}_a]\right] &= \textstyle\sum_{l=0}^{3}\omega_l(-\hat{\alpha})\mathcal{F}^l\left[\mathcal{F}_4^{\alpha}[\mathbf{s}_a]\right] \\ &= \textstyle\sum_{l=0}^{3}[\omega_l(-\alpha)\varphi(\Delta\alpha) + \nu_l(\alpha, \Delta\alpha)]\mathcal{F}^l\left[\mathcal{F}_4^{\alpha}[\mathbf{s}_a]\right] \\ &= \varphi(\Delta\alpha)\textstyle\sum_{l=0}^{3}\omega_l(-\alpha)\mathcal{F}^l\left[\mathcal{F}_4^{\alpha}[\mathbf{s}_a]\right] + \boldsymbol{\psi}(\alpha, \Delta\alpha, \mathbf{s}_a) \\ &= \varphi(\Delta\alpha)\mathbf{s}_a + \boldsymbol{\psi}(\alpha, \Delta\alpha, \mathbf{s}_a), \end{aligned} \tag{17}$$

where $\boldsymbol{\psi}(\alpha, \Delta\alpha, \mathbf{s}_a) \in \mathbb{C}^{N\times 1}$ is the total inter-component interference, its specific form can be expressed as:

$$\boldsymbol{\psi}(\alpha, \Delta\alpha, \mathbf{s}_a) = \sum_{l=0}^{3}\nu_l(\alpha, \Delta\alpha)\mathcal{F}^l\left[\mathcal{F}_4^{\alpha}[\mathbf{s}_a]\right], \tag{18}$$

where the inter-component interference generated by the l-th

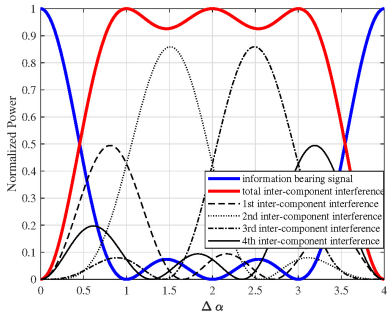


Fig. 2. Energy distribution characteristics of information bearing signal and inter-component interference versus $\Delta\alpha$ ($\alpha = 0.5$).

component is $\nu_l(\alpha, \Delta\alpha)\mathcal{F}^l\left[\mathcal{F}_4^{\alpha}[\mathbf{s}_a]\right]$.

Therefore, the restoration result of the received signal with respect to the data sequence $\mathbf{s}_a$ at Eve in (11) can be further expressed as:

$$\mathbf{p}_1^{EA} = \underbrace{\sqrt{P_a} g_{ae}\varphi(\Delta\alpha)\mathbf{s}_a}_{\text{information bearing signal}} + \underbrace{\sqrt{P_a} g_{ae}\boldsymbol{\psi}(\alpha, \Delta\alpha, \mathbf{s}_a)}_{\text{inter-component interference}} + \underbrace{\sqrt{P_b} g_{be}\mathcal{F}_4^{\beta-\hat{\alpha}}[\mathbf{s}_b]}_{\text{inter-user interference}} + \underbrace{\mathbf{e}_1{}'}_{\text{AWGN}}. \tag{19}$$

In (19), the energy of the information bearing signal is given by $P_{a,1}^{\text{inf}} = P_a|g_{ae}|^2|\varphi(\Delta\alpha)|^2$. According to (14), $|\varphi(\Delta\alpha)|^2 \leq 1$ always holds, thus the energy loss of the restored information bearing signal by Eve is inevitable when $\Delta\alpha \neq 4m, m \in \mathbb{Z}$.

Based on the form of $\boldsymbol{\psi}(\alpha, \Delta\alpha, \mathbf{s}_a)$ as shown in (18), the total energy of the inter-component interference is given by:

$$\begin{aligned} P_{a,1}^{\text{int,c}} &= P_a|g_{ae}|^2\textstyle\sum_{l=0}^{3}|\nu_l(\alpha, \Delta\alpha)|^2 \\ &\overset{\text{a}}{=} P_a|g_{ae}|^2\left(1 - |\varphi(\Delta\alpha)|^2\right), \end{aligned} \tag{20}$$

where (20) is derived based on the Parseval's Theorem of WFRFT. Specifically, the total energy of $\mathbf{s}_a$ and $\mathcal{F}_4^{-\hat{\alpha}}\left[\mathcal{F}_4^{\alpha}[\mathbf{s}_a]\right]$ are equality. Since the energy of the information bearing signal in $\mathcal{F}_4^{-\hat{\alpha}}\left[\mathcal{F}_4^{\alpha}[\mathbf{s}_a]\right]$ is $|\varphi(\Delta\alpha)|^2$, the total energy of additive interference generated by all four components is $1-|\varphi(\Delta\alpha)|^2$. That is to say, the energy of inter-component interference that only affects Eve is entirely attributed to the energy loss incurred when recovering the useful signal, rather than the system's consumption of extra transmit power. This effectively enhances the energy efficiency of the system.

Fig. 2 shows the impact of the energy distribution characteristics of the WFRFT signal ($\alpha = 0.5$) on the eavesdropper, as $\Delta\alpha$ changes over one period. Additionally, the WFRFT signal with different α exhibits different levels of inter-component interference of each component. However, the energy distribution of the total inter-component interference obtained by their superposition remains the same.

Then, the instantaneous received signal to interference-plus-noise ratio (SINR) for the wiretap link "Alice $\rightarrow$ Eve" in the first phase can be expressed as:

$$\gamma_1^{EA} = \frac{P_a|g_{ae}|^2|\varphi(\Delta\alpha)|^2}{P_a|g_{ae}|^2\left(1 - |\varphi(\Delta\alpha)|^2\right) + P_b|g_{be}|^2 + \sigma_e^2}. \tag{21}$$

Similarly, in the first phase, when Eve adopts $(-\hat{\beta})$-order WFRFT to restore $\mathbf{s}_b$ for the link "Bob $\rightarrow$ Alice", the resulting expression is given by:

$$\begin{aligned} \mathbf{p}_1^{EB} &= \sqrt{P_b} g_{be}\mathcal{F}_4^{\Delta\beta}[\mathbf{s}_b] + \sqrt{P_a} g_{ae}\mathcal{F}_4^{\alpha-\hat{\beta}}[\mathbf{s}_a] + \mathbf{e}_1{}'', \\ &= \sqrt{P_b} g_{be}\varphi(\Delta\beta)\mathbf{s}_b + \sqrt{P_b} g_{be}\boldsymbol{\psi}(\beta, \Delta\beta, \mathbf{s}_b) \\ &\quad + \sqrt{P_a} g_{ae}\mathcal{F}_4^{\alpha-\hat{\beta}}[\mathbf{s}_a] + \mathbf{e}_1{}'', \end{aligned} \tag{22}$$

where $\varphi(\Delta\beta)$ is the energy attenuation coefficient of $\mathbf{s}_b$, $\boldsymbol{\psi}(\beta, \Delta\beta, \mathbf{s}_b)$ is the total inter-component interference generated by $\mathbf{s}_b$, and $\mathbf{e}_1{}'' = \mathcal{F}_4^{-\hat{\beta}}[\mathbf{e}_1]$. The instantaneous received SINR for the wiretap link "Bob $\rightarrow$ Eve" in the first phase is:

$$\gamma_1^{EB} = \frac{P_b|g_{be}|^2|\varphi(\Delta\beta)|^2}{P_b|g_{be}|^2\left(1 - |\varphi(\Delta\beta)|^2\right) + P_a|g_{ae}|^2 + \sigma_e^2}. \tag{23}$$

In the second phase, Eve receives the signal $\mathbf{r}$ forwarded by Carlo, and the received signal can be expressed as:

$$\begin{aligned} \mathbf{z}_2 &= g_{ce}\xi\mathbf{r} + \mathbf{e}_2 \\ &= g_{ce}\xi\sqrt{P_a}h_{ac}\mathcal{F}_4^{\alpha}[\mathbf{s}_a] + g_{ce}\xi\sqrt{P_b}h_{bc}\mathcal{F}_4^{\beta}[\mathbf{s}_b] + \mathbf{e}_2{}', \end{aligned} \tag{24}$$

where $\mathbf{e}_2{}' = g_{ce}\xi\mathbf{n} + \mathbf{e}_2$ is the total AWGN, whose elements are $\mathcal{CN}(0, |g_{ce}|^2\xi^2\sigma_n^2 + \sigma_e^2)$. Comparing (10) and (24), it can be seen that the form of the signal received by Eve is similar in both phases. Similarly, assume that Eve adopts the same methods as the first phase to restore $\mathbf{s}_a$ and $\mathbf{s}_b$ in $\mathbf{z}_2$, respectively. Thus, the instantaneous received SINRs for the link "Carlo ($\mathbf{s}_a$) $\rightarrow$ Eve" and "Carlo ($\mathbf{s}_b$) $\rightarrow$ Eve" in the second phase, respectively, are given by (25) and (26).

In order to maximize the total SINRs of the wiretap links, Eve can perform whatever operations with the signals in the previous two phases. In this paper, we consider two most common and effective signal combining techniques in current communication systems, viz., MRC and SC. The proposed secure transmission scheme is still effective in improving the secrecy performance of the system when Eve utilizes other operations. Because the mechanism that using WFRFT signal characteristics to reduce the SINR of the eavesdropper is not affected by different signal combining techniques.

Under the MRC and SC techniques as discussed in [8], [9], the instantaneous SINRs of the wiretap links "Alice & Carlo ($\mathbf{s}_a$) $\rightarrow$ Eve" and "Bob & Carlo ($\mathbf{s}_b$) $\rightarrow$ Eve" are given by:

$$\gamma_{\text{MRC}}^{Ei} = \gamma_1^{Ei} + \gamma_2^{Ei}, \quad \gamma_{\text{SC}}^{Ei} = \max\left\{\gamma_1^{Ei}, \gamma_2^{Ei}\right\}. \tag{27}$$

where $i \in \{A, B\}$.

$$\gamma_2^{EA} = \frac{P_a\xi^2|g_{ce}|^2|h_{ac}|^2|\varphi(\Delta\alpha)|^2}{P_a\xi^2|g_{ce}|^2|h_{ac}|^2\left(1 - |\varphi(\Delta\alpha)|^2\right) + P_b\xi^2|g_{ce}|^2|h_{bc}|^2 + \xi^2|g_{ce}|^2\sigma_n^2 + \sigma_e^2}, \tag{25}$$

$$\gamma_2^{EB} = \frac{P_b\xi^2|g_{ce}|^2|h_{bc}|^2|\varphi(\Delta\beta)|^2}{P_b\xi^2|g_{ce}|^2|h_{bc}|^2\left(1 - |\varphi(\Delta\beta)|^2\right) + P_a\xi^2|g_{ce}|^2|h_{ac}|^2 + \xi^2|g_{ce}|^2\sigma_n^2 + \sigma_e^2}. \tag{26}$$

C. Secrecy Performance Analysis

The achievable secrecy rate for each one-way link can be expressed as:

$$R_{\varrho}^{i}=\frac{1}{2}\left[\log(1+\gamma^{\bar{i}})-\log(1+\gamma_{\varrho}^{Ei})\right]^{+}, \tag{28}$$

where $i,\bar{i}\in\{A,B\}$ and $i\neq\bar{i}$, A and B denote the communication link "Alice $\rightarrow$ Carlo $\rightarrow$ Bob" and "Bob $\rightarrow$ Carlo $\rightarrow$ Alice", respectively. $[\cdot]^{+}=\max\{\cdot,0\}$, and $\varrho\in\{\mathrm{MRC},\mathrm{SC}\}$ denotes different signal combining techniques adopted by Eve. Further, the achievable SSR is given by:

$$R_{\varrho}^{\mathrm{sum}}=R_{\varrho}^{A}+R_{\varrho}^{B}. \tag{29}$$

It is apparent that when $\Delta\alpha=\Delta\beta=0$, the proposed scheme achieves the same achievable SSR as the traditional TWTR system. However, when $\Delta\alpha$ or $\Delta\beta$ is non-zero, the introduction of the WFRFT enhances the achievable SSR of the system by decreasing the capacity of wiretap channels.

Since Eve is a passive eavesdropper, it is difficult for legitimate nodes to know the CSI of wiretap channels, and hence to perform optimal power allocation. Next, we analyze the secrecy performance of the proposed scheme when all nodes are assigned equal power, i.e., $P_a=P_b=P_c=P$. At the same time, without loss of generality, assume $\sigma_e^2=\sigma_n^2$.

D. Analysis When the Eavesdropper Can Separate the Signals of Two Legitimate Nodes

In traditional TWTR system, the superimposed signals at Eve provide a natural PLS advantage. However, considering the complex distribution of nodes in practical system and the randomness of the location of passive eavesdroppers, a specific practical scenario should be considered as follows. In the first phase, Eve only receives the information bearing signal from one of the legitimate nodes without interference from the other legitimate node. Based on this, in the second phase, Eve can separate another information bearing signal from the superimposed signal forwarded by the trusted relay through self-interference cancellation.

In this scenario, the inherent security advantage of the two-way relay system and the security performance provided by relay selection algorithms no longer exists. However, the proposed scheme can still ensure the secrecy performance from the perspective of WFRFT signal domain.

Consider that Eve only receives the signal from Alice (or Bob; hereafter, Alice is used as an example) in the first phase, and it could separate the superimposed signal in the second phase. Specifically, in the first phase, the second term of (10) no longer exists, the received signal is given by:

$$\mathbf{z}_{1,a}=\sqrt{P_a}g_{ae}\mathcal{F}_4^{\alpha}[\mathbf{s}_a]+\mathbf{e}_1. \tag{30}$$

When Eve adopts the same method as (11) to restore $\mathbf{s}_a$, the result can be expressed as:

$$\mathbf{p}_{1,a}^{EA}=\sqrt{P_a}g_{ae}\left[\varphi(\Delta\alpha)\mathbf{s}_a+\boldsymbol{\psi}(\alpha,\Delta\alpha,\mathbf{s}_a)\right]+\mathbf{e}_1{}'. \tag{31}$$

In the second phase, Eve could remove the first term in (24), in order to restore $\mathbf{s}_b$. Considering the most favorable situation for Eve, which is when Eve separates the $\mathbf{s}_b$ term without introducing any additional interference, including AWGN. The signal to be restored can be expressed as:

$$\mathbf{z}_{2,b}=g_{ce}\xi\sqrt{P_b}h_{bc}\mathcal{F}_4^{\beta}[\mathbf{s}_b]+\mathbf{e}_2{}'. \tag{32}$$

Thus, the restoration result of (32) can be expressed as:

$$\mathbf{p}_{2,b}^{EB}=g_{ce}\xi\sqrt{P_b}h_{bc}\left[\varphi(\Delta\beta)\mathbf{s}_b+\boldsymbol{\psi}(\beta,\Delta\beta,\mathbf{s}_b)\right]+\mathbf{e}_2{}'', \tag{33}$$

where $\mathbf{e}_2{}''=\mathcal{F}_4^{-\hat{\beta}}[\mathbf{e}_2{}']$ is the AWGN, whose elements are $\mathcal{CN}(0,|g_{ce}|^2\xi^2\sigma_n^2+\sigma_e^2)$. Based on the above strict assumptions, Eve can perform serial interference cancellation (SIC) in the second phase in order to achieve better restoration performance for $\mathbf{s}_a$, i.e., removing $\mathbf{z}_{2,b}$ in (32) from $\mathbf{z}_2$ in (24). Under the condition of perfect SIC, the restoration result for $\mathbf{s}_a$ can be expressed as:

$$\mathbf{p}_{2,a}^{EA}=g_{ce}\xi\sqrt{P_a}h_{ac}\left[\varphi(\Delta\alpha)\mathbf{s}_a+\boldsymbol{\psi}(\alpha,\Delta\alpha,\mathbf{s}_a)\right]. \tag{34}$$

Moreover, according to (34) and (31), the SINRs of the wiretap link "Alice & Carlo ($\mathbf{s}_a$) $\rightarrow$ Eve" under MRC and SC techniques, respectively, can be represented as:

$$\begin{cases}\gamma_{\mathrm{MRC}}^{EA}=\dfrac{P_a|g_{ae}|^2|\varphi(\Delta\alpha)|^2}{P_a|g_{ae}|^2\left(1-|\varphi(\Delta\alpha)|^2\right)+\sigma_e^2}+\dfrac{|\varphi(\Delta\alpha)|^2}{1-|\varphi(\Delta\alpha)|^2}\\ \gamma_{\mathrm{SC}}^{EA}=\dfrac{|\varphi(\Delta\alpha)|^2}{1-|\varphi(\Delta\alpha)|^2}.\end{cases} \tag{35}$$

Comparing (35) with (27), in the scenario of this subsection, the energy of the information bearing signal does not decrease, and inter-user interference no longer exists for Eve. However, the inter-component interference provided by the WFRFT signal domain is not affected and can still effectively reduce the SINR of the signal restored by Eve, thereby ensuring the secrecy performance of the system.

For the wiretap link "Bob & Carlo ($\mathbf{s}_b$)$\rightarrow$ Eve", Eve could restore $\mathbf{s}_b$ without inter-user interference. According to (33), the SINR can be represented as:

$$\gamma^{EB}=\frac{P_b\xi^2|g_{ce}|^2|h_{bc}|^2|\varphi(\Delta\beta)|^2}{P_b\xi^2|g_{ce}|^2|h_{bc}|^2\left(1-|\varphi(\Delta\beta)|^2\right)+\xi^2|g_{ce}|^2\sigma_n^2+\sigma_e^2}. \tag{36}$$

Considering (35) and (36) jointly, the achievable SSR can be expressed as:

$$R_{\varrho}^{\mathrm{sum}}=R_{\varrho}^{A}+R^{B}. \tag{37}$$

IV. Numerical Results and Discussion

In this section, simulation results are provided to evaluate the secrecy performance of the proposed WFRFT-based schemes for TWTR systems. The noise variances $\sigma_n^2=\sigma_e^2=1$ and the path loss coefficient is 3. For simplicity and without loss of generality, we assume that Alice, Bob, Carlo and Eve are located at (−1, 0), (1, 0), (0, 0) and (0, 0.5), respectively. Additionally, for the scenario where eavesdroppers have signal separation capability, as discussed in Section III.D, we assume that Alice, Bob, Carlo, and Eve are located at coordinates (−1, 0), (1, 0), (0, 0), and (−1, 0.5), respectively. The relay selection scheme in [4] is taken as the baseline, where K relays are uniformly distributed within a square region with diagonal vertices at (−0.5,−0.5) and (0.5,0.5).

Fig. 3 shows the achievable SSR under MRC or SC versus the SNR with different $\Delta\alpha$ and $\Delta\beta$. The achievable SSR

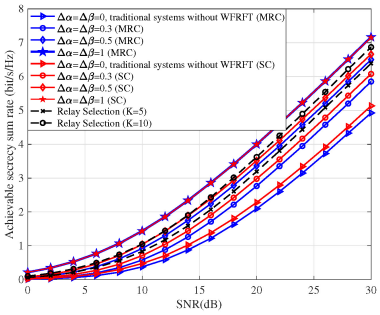
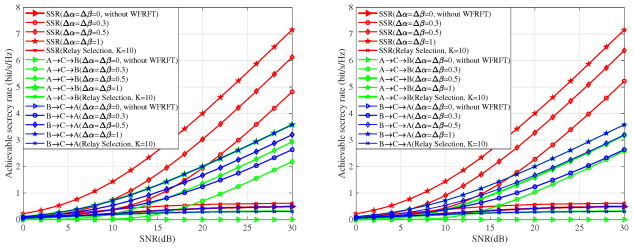


Fig. 3. Achievable secrecy sum rate under MRC or SC versus the SNR, with different $\Delta\alpha$ and $\Delta\beta$.



(a) MRC. (b) SC.

Fig. 4. Achievable secrecy rate under MRC or SC versus the SNR with different $\Delta\alpha$ and $\Delta\beta$, when Eve can separate the signals of Alice and Bob.

monotonically increases with the SNR, and increasing of $\Delta\alpha$ and $\Delta\beta$ within the range of [0,1] also enhances the secrecy performance of the system. This is because as SNR increases, the achievable information rate of the legitimate links monotonically increases without an upper bound, while the wiretap links saturate to a constant rate. Based on the energy distribution characteristics of the WFRFT signal domain discussed in III.A, increasing $\Delta\alpha$ and $\Delta\beta$ within the range [0,1] reduces the achievable information rate of wiretap links, which leads to an improvement in the achievable SSR. Even though the relay selection scheme requires more system resources, the proposed scheme demonstrates better performance under certain conditions. Additionally, compared to SC, the eavesdropper can achieve a higher SINR and thus a higher achievable information rate when using MRC. However, when $\Delta\alpha = \Delta\beta = 1$, regardless of the combining technique, the eavesdropper cannot intercept any information. In this case, the proposed scheme performs the same and optimally under both combining techniques.

For the scenario discussed in Section III.D, Fig. 4 also shows the achievable secrecy rate versus the SNR with different $\Delta\alpha$ and $\Delta\beta$ under MRC and SC, respectively. For the discussed communication scenario, the secrecy performance of both the traditional two-way relay system ($\Delta\alpha = \Delta\beta = 0$) and the relay selection scheme is poor, and secure communication on link "A $\rightarrow$ C $\rightarrow$ B" cannot be achieved at all. Due to the introduction of inter-component interference, the proposed scheme can significantly improve the achievable secrecy rate of both legitimate links, thereby bringing higher achievable SSR to the system. Moreover, when Eve adopts SC, link "A $\rightarrow$ C $\rightarrow$ B" can achieve similar secrecy performance to link "B $\rightarrow$ C $\rightarrow$ A" with the increase of SNR.

V. Conclusion

In this paper, WFRFT signal domain secure communication scheme for TWTR systems is proposed. The proposed scheme achieves PLS in a single-antenna two-way relay system without requiring meaningless cooperative jamming or extra nodes. Specifically, the proposed scheme reduces the energy of information bearing signal at the eavesdropper in both phases, and the lost energy transforms into additive inter-component interference, which further reduces the SINR at the eavesdropper. Although the eavesdropper can extract more information by MRC compared to SC, its achievable information rate is still limited by a constant upper bound and even to zero under certain conditions. In particular, when the eavesdropper can separate the superimposed signals of legitimate nodes, the proposed scheme can still guarantee secure communication, whereas the traditional scheme cannot.

Acknowledgments

This work was supported in part by the National Key Research and Development Program of China (Grant 2022YFB2902404) and the Key Program of the National Natural Science Foundation of China (Grant U23A20278).

References

[1] Y. Liu, H.-H. Chen, and L. Wang, "Physical layer security for next generation wireless networks: Theories, technologies, and challenges," *IEEE Commun. Surv. Tuts.*, vol. 19, no. 1, pp. 347–376, 2017.

[2] L. Hu, J. Fan, H. Wen, J. Tang and Q. Chen. "Interference alignment based secure transmission scheme in multi-user interference networks," *Chinese Journal on Internet of Things*, vol. 7, no. 2, pp. 98-108, 2023.

[3] C. E. Shannon, "Communication theory of secrecy systems," *Bell Syst. Tech. J.*, vol. 28, no. 4, pp. 656–715, 1949.

[4] W. Jiang, X. Yuan, Q. Wang and L. Qian. "NOMA-based secure computation offloading in marine Internet of things," *Chinese Journal on Internet of Things*, vol. 8, no. 3, pp. 102-111, 2024.

[5] C. Zhang, J. Ge, J. Li, F. Gong, and H. Ding, "Complexity-aware relay selection for 5G large-scale secure two-way relay systems," *IEEE Trans. Veh. Technol.*, vol. 66, no. 6, pp. 5461–5465, 2017.

[6] C. Zhang, J. Ge, F. Gong, Y. Ji, and J. Li, "Improving physical-layer security for wireless communication systems using duality-aware two-way relay cooperation," *IEEE Syst. J.*, vol. 13, no. 2, pp. 1241–1249, 2019.

[7] Z. Ding, M. Xu, J. Lu, and F. Liu, "Improving wireless security for bidirectional communication scenarios," *IEEE Trans. Veh. Technol.*, vol. 61, no. 6, pp. 2842–2848, 2012.

[8] J. Chen, R. Zhang, L. Song, Z. Han, and B. Jiao, "Joint relay and jammer selection for secure two-way relay networks," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 1, pp. 310–320, 2012.

[9] M. K. Shukla, S. Yadav, and N. Purohit, "Secure transmission in cellular multiuser two-way amplify-and-forward relay networks," *IEEE Trans. Veh. Technol.*, vol. 67, no. 12, pp. 11 886–11 899, 2018.

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

[11] S. Gong, C. Xing, S. Ma, Z. Zhang, and Z. Fei, "Secure wideband beamforming design for two-way MIMOmimo relaying systems," *IEEE Trans. Veh. Technol.*, vol. 68, no. 4, pp. 3472–3486, 2019.

[12] H. Dong, R. Gao, J. Li, X. Fang, X. Sha, and Z. Li, "Physical layer security communication for IoT-aided intelligent transport systems: An approach in WFRFT signal domain," *Comput. Electr. Eng.*, 118: 109309, 2024.