Article

Full-Duplex Relay with Delayed CSI Elevates the SDoF of the MIMO X Channel

Tong Zhang [1], Gaojie Chen [2], Shuai Wang [1] and Rui Wang [1,*]

[1] The Department of Electrical and Electronic Engineering, Southern University of Science and Technology, Shenzhen 518055, China; zhangt7@sustech.edu.cn (T.Z.); wangs3@sustech.edu.cn (S.W.)
[2] 5GIC & 6GIC, Institute for Communication Systems, University of Surrey, Guildford GU2 7XH, UK; gaojie.chen@surrey.ac.uk
[*] Correspondence: wang.r@sustech.edu.cn

Abstract: In this article, the sum secure degrees-of-freedom (SDoF) of the multiple-input multiple-output (MIMO) X channel with confidential messages (XCCM) and arbitrary antenna configurations is studied, where there is no channel state information (CSI) at two transmitters and only delayed CSI at a multiple-antenna, full-duplex, and decode-and-forward relay. We aim at establishing the sum-SDoF lower and upper bounds. For the sum-SDoF lower bound, we design three relay-aided transmission schemes, namely, the relay-aided jamming scheme, the relay-aided jamming and one-receiver interference alignment scheme, and the relay-aided jamming and two-receiver interference alignment scheme, each corresponding to one case of antenna configurations. Moreover, the security and decoding of each scheme are analyzed. The sum-SDoF upper bound is proposed by means of the existing SDoF region of two-user MIMO broadcast channel with confidential messages (BCCM) and delayed channel state information at the transmitter (CSIT). As a result, the sum-SDoF lower and upper bounds are derived, and the sum-SDoF is characterized when the relay has sufficiently large antennas. Furthermore, even assuming no CSI at two transmitters, our results show that a multiple-antenna full-duplex relay with delayed CSI can elevate the sum-SDoF of the MIMO XCCM. This is corroborated by the fact that the derived sum-SDoF lower bound can be greater than the sum-SDoF of the MIMO XCCM with output feedback and delayed CSIT.

Keywords: delayed CSIT; information-theoretical security; MIMO X channel; MIMO relay; secure degrees-of-freedom

1. Introduction

The deployment of 5G and all of the connections to 6G around the world have all exacerbated the concerns for information-theoretic security in mobile communication networks [1–3]. The secure degrees-of-freedom (SDoF) of multiple-input multiple-output (MIMO) networks with confidential messages and perfect channel state information at the transmitter (CSIT) was studied in [4–9]. For the K-user single-input single-output (SISO) interference channel with confidential messages (ICCM), the sum-SDoF was characterized in [4]. For the multiple-input multiple-output (MIMO) ICCM, under symmetric antenna configurations, the sum-SDoF was derived in [5,6]. Then, the sum-SDoF of the MIMO ICCM with arbitrary antenna configurations was characterized in [7]. The X network with confidential messages has a more general message setting than that in ICCM. For the X network with confidential messages, the sum-SDoF was studied in [8]. The sum-SDoF of rank-deficient ICCM and broadcast channel with confidential messages (BCCM) was characterized in [9].

For the fast-fading wireless channel, the CSIT can be delayed, that is, mismatching with current CSI but matching with past CSI. Under this imperfect setting, i.e., delayed CSIT, the research of SDoF was stemmed from [10], where under arbitrary antenna configurations, the SDoF region of two-user MIMO BCCM and delayed CSIT was characterized. Thereafter,

the SDoF regions of two-user multiple-input single-output (MISO) BCCM with alternating CSIT was derived in [11]. The linear SDoF of blind multi-user MISO wiretap channel with delayed CSIT was characterized in [12]. Recently, in [13], the interplay of link connectivity and alternating CSIT in MISO BCCM was studied from the SDoF perspective. Aside from the BCCM, there are many efforts devoted to investigate the SDoF of two-user interference networks with delayed feedback [14–17]. In [14], under symmetric antenna configurations, a sum-SDoF lower bound for MIMO ICCM with delayed CSIT was obtained. In [15], under symmetric antenna configurations, a higher sum-SDoF lower bound than that in [14] was derived for MIMO XCCM with delayed CSIT, considering two more confidential messages. In [16], under symmetric antenna configurations, the sum-SDoF of MIMO ICCM with local output feedback was studied. In [17], under symmetric antenna configurations, the SDoF region of MIMO XCCM with output feedback and delayed CSIT was characterized, which has the highest sum-SDoF over that in [14–16].

Even with delayed CSI, it is shown in [18–22] that the decode-and-forward relay (for brevity, we henceforth use "relay" to stand for "decode-and-forward relay") can assist the communication and enhance the degrees-of-freedom (DoF) of MIMO networks. When there is no CSIT, reference [19–22] considered the assistance of the relay with delayed CSI. In [19], a multiple-antenna relay with delayed CSI elevated the DoF of K-user SISO interference channel. In [21], a multiple-antenna relay with delayed CSI elevated the DoF of the SISO X channel. For the MIMO X channel, it is shown in [22] that a multiple-antenna relay with delayed CSI was able to enhance the DoF. As for X networks, L multiple-antenna full-duplex relays enhanced the sum-DoF of the $2 \times K$ X networks, as shown in [20]. Furthermore, having the security constraints, only the work in [23] addressed the sum-SDoF characterization of $2 \times 2 \times 2$ SISO ICCM with delayed CSIT.

However, to summarize, none of existing works considered the SDoF of the relay-aided MIMO XCCM, where there is no CSI at two transmitters and a delayed CSI at the relay, such as the CSI model in [20,22]. For the first time, we consider the SDoF problem of such a system. Specifically, we consider a multiple-antenna full-duplex relay with delayed CSI in the MIMO XCCM with arbitrary antenna configurations, where there is no CSI at two transmitters. However, there are two major challenges. The first one is how to design a transmission scheme with security guarantee and transmission efficiency. The second one is how to create an upper bound for the sum-SDoF in a non-trivial way. We address these two problems in the following manner: We propose the relayed-aided jamming and interference alignment (IA) design for transmission scheme, which simultaneously fulfills security guarantee and transmission efficiency. In addition, we leverage the existing SDoF region of MIMO BCCM to design a sum-SDoF upper bound. The sum-SDoF lower and upper bounds are tight for partial antenna configurations, and thus, the sum-SDoF is derived therein. The main contributions of this paper are summarized as follows:

- To derive the sum-SDoF lower bound, under arbitrary antenna configurations, we propose three relay-aided transmission schemes, whose achievable sum-SDoF serves as the sum-SDoF lower bound. Specifically, we propose the relay-aided jamming scheme, and the relay-aided jamming and one-receiver IA scheme, and the relay-aided jamming and two-receiver IA scheme, where each scheme corresponds to one case of antenna configurations. In each scheme, the security and decoding are analyzed.

- To obtain the sum-SDoF upper bound, which does not appear in the existing literature and is non-trivial, we first treat two transmitters and the relay as a co-located transmitter, which is an enhanced scenario. Thereafter, we apply the results of the existing SDoF region of two-user MIMO BCCM, which is proven in [10], into this enhanced scenario.

- Our results show that if the full-duplex relay has double antennas of the receiver, the proposed sum-SDoF lower bound is not less than the sum-SDoF in existing two-user interference networks with delayed feedback in [14–17], and can be higher than the sum-SDoF of MIMO X channel with output feedback and delayed CSIT in [17]. Moreover, the proposed sum-SDoF lower bound matches with the sum-SDoF upper

bound for partial antenna configurations, characterizing the sum-SDoF for these antenna configurations.

Notations: The identity matrix of dimensions m is denoted by $\mathbf{I}_m$. The block-diagonal matrix with blocks $\mathbf{A}$ and $\mathbf{B}$ is denoted by $\mathcal{BD}\{\mathbf{A}, \mathbf{B}\}$. The rank of matrix $\mathbf{A}$ is denoted by $\mathcal{RK}\ \mathbf{A}$. The log is referred to $\log_2$. $[x]^+ = \max\{x, 0\}$.

Organizations: The rest of this paper is organized as follows: The system model is defined in Section 2. The main results and discussions are presented in Section 3. We prove the Theorem 1 in Section 4. We draw our conclusions in Section 5.

2. System Model

We consider the MIMO XCCM aided by a R-antennas full-duplex (the experimental studies and prototypes on full-duplex techniques can be found in [24–29], where the self-interference can be suppressed by radio frequency, analogue, and digital cancellations to achieve the noise floor; the details of self-interference suppression are out of the scope of this work) relay, where two transmitters (denoted by T_1 and T_2) have M_1 and M_2 antennas, respectively, and two receivers (denoted by R_1 and R_2) have N_1 and N_2 antennas, respectively, as shown in Figure 1. Namely, the antenna configurations are arbitrary. Without loss of generality, we have $N_1 \leq N_2$ by denoting the receiver with most antennas by R_2. The T_i has a confidential message $W_{i,j}$ for R_j, where $i, j = 1, 2$. The CSI matrix from T_1, T_2 and the relay to R_1, R_2 and the relay at time slot t is denoted by $\mathbf{H}_{i,j}[t], i, j = 1, 2, r$, respectively, where $\mathbf{H}_{i,j}[t]$ is time-varying and independently distributed across space and time. There is no CSI at two transmitters. At the time slot t, both R_1 and R_2 have the instantaneous knowledge of $\mathbf{H}_{i,1}$ and $\mathbf{H}_{i,2}, i = 1, 2, r$; the relay has the instantaneous knowledge of $\mathbf{H}_{i,r}, i = 1, 2$. Moreover, due to feedback delay (the CSI feedback link is assumed to be additional, compared with the data/artificial noise transmission link), the past CSI matrices $\mathbf{H}^{t-1} \triangleq \{\mathbf{H}_{i,j}[t-\tau], t > \tau \geq 1, i = 1, 2, r; j = 1, 2\}$ are available at the relay. Note that the definition of CSI in this paper is the same as that defined in [21,22].
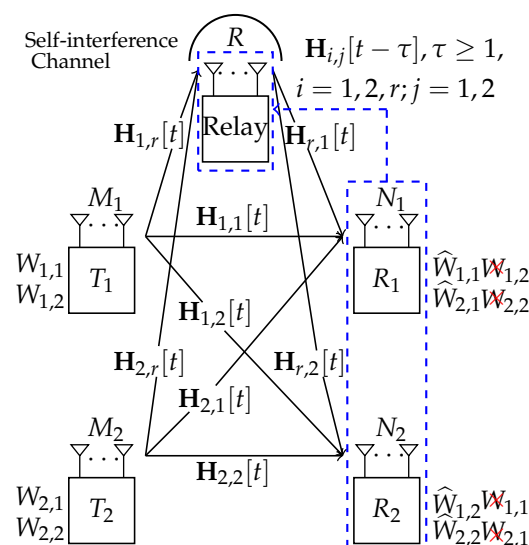

Figure 1. Illustration of the scenario, where there are delayed CSI at the relay and no CSI at two transmitters.

A code $\{2^{nR_{i,j}(\eta)}, i, j = 1, 2\}$ with achievable secrecy rates $R_{i,j}(\eta), i, j = 1, 2$ is defined below, where η denotes the signal-to-noise ratio (SNR). The communication process takes n channel uses (time slots) with confidential messages $W_{i,j} = [1, \cdots, 2^{nR_{i,j}(\eta)}]$ (from T_i to R_j). At the time slot t, a stochastic encoder $f_{i,j}(\cdot)$ at the T_i encodes confidential message $W_{i,j}$ to an input signal $\mathbf{x}_{i,j}[t]$, i.e., $\mathbf{x}_{i,j}[t] = f_{i,j}(W_{i,j})$. At the time slot t, a stochastic encoder $f_r(\cdot)$ at the full-duplex relay encodes the collection of received signals $\mathbf{y}_r^t \triangleq [\mathbf{y}_r[1], \cdots, \mathbf{y}_r[t]]$ and delayed CSI $\mathbf{H}^{t-1}$ to an input signal $\mathbf{x}_{r,j}^t$, i.e., $\mathbf{x}_{r,j}[t] = f_r(\mathbf{y}_r^t, \mathbf{H}^{t-1})$. At the time slot

n, a decoder $g_{i,j}(\cdot)$ at the R_j decodes the output signals $\mathbf{y}_j^n$ and CSI matrices $\mathbf{H}^n$ to an estimated message $\widehat{W}_{i,j}$, i.e., $\widehat{W}_{i,j} = g_{i,j}(\mathbf{y}_j^n, \mathbf{H}^n)$. According to [10], the secure code satisfies the reliability criterion,

$$\Pr[W_{i,j} \neq \widehat{W}_{i,j}] \leq \epsilon_n, \qquad i,j = 1,2, \tag{1}$$

and the weak secrecy criterion,

$$\frac{1}{n} I(W_{i,1}; \mathbf{y}_2^n) \leq \epsilon_n, \tag{2a}$$

$$\frac{1}{n} I(W_{i,2}; \mathbf{y}_1^n) \leq \epsilon_n, \qquad i = 1,2, \tag{2b}$$

where $\epsilon_n \to 0$ as $n \to \infty$.

The sum of the secure channel capacity is defined as $C_s = \max \sum_{i=1}^{2} \sum_{j=1}^{2} R_{i,j}(\eta)$. The sum-SDoF is a first-order approximation of the secure sum-capacity in the high SNR regime and defined as follows:

$$\sum_{i=1}^{2} \sum_{j=1}^{2} d_{i,j} = \lim_{\eta \to \infty} \frac{C_s}{\log \eta}. \tag{3}$$

3. Main Results and Discussions

Theorem 1. *(sum-SDoF lower bound under arbitrary antenna configurations).* *For the relay-aided MIMO XCCM with delayed CSI at the multiple-antenna full-duplex relay and no CSI at two transmitters, the sum-SDoF lower bound under arbitrary antenna configurations is given as follows:*

$$\sum_{i=1}^{2} \sum_{j=1}^{2} d_{i,j} \geq \begin{cases} \dfrac{(M_1 + M_2)(x_1 + x_2)}{1 + x_1 + x_2}, & M_1 + M_2 \leq N_1 \ \& \ N_2 < R, \\[2mm] \dfrac{\min\{M_1 + M_2, R\}x_1 + (M_1 + M_2)x_2}{1 + x_1 + x_2 + x_3}, & N_1 < M_1 + M_2 \leq N_2 \ \& \ N_2 < R, \\[2mm] \dfrac{(M_1 + M_2)x_1}{1 + x_1}, & M_1 + M_2 \leq N_2 \ \& \ N_1 < R \leq N_2, \\[2mm] \dfrac{\min\{M_1 + M_2, R, N_1 + N_2\}(x_1 + x_2)}{1 + x_1 + x_2 + \max\{x_4, x_5\}}, & N_2 < M_1 + M_2 \ \& \ N_2 < R, \\[2mm] \dfrac{\min\{M_1 + M_2, R, N_1 + N_2\}x_1}{1 + x_1 + x_5}, & N_2 < M_1 + M_2 \ \& \ N_1 < R \leq N_2, \\[2mm] 0, & R \leq N_1, \end{cases} \tag{4}$$

where

$$x_1 = \frac{\min\{N_2, R - N_1\}}{N_1}, \tag{5a}$$

$$x_2 = \frac{\min\{N_1, R - N_2\}}{N_2}, \tag{5b}$$

$$x_3 = \frac{\min\{M_1 + M_2 - N_1, R - N_1\} \min\{N_1, R - N_2\}}{\min\{N_1, R\} N_2}, \tag{5c}$$

$$x_4 = \frac{\min\{M_1 + M_2 - N_1, N_2, R - N_1\} \min\{N_1, R - N_2\}}{\min\{N_1, R\} N_2}, \tag{5d}$$

$$x_5 = \frac{\min\{M_1 + M_2 - N_2, N_1, R - N_2\} \min\{N_2, R - N_1\}}{\min\{N_1, R\} N_1}. \tag{5e}$$

Proof. Please refer to Section 4. $\square$

Remark 1. *(sum-SDoF lower bound under symmetric antenna configurations).* *For the relay-aided MIMO XCCM with delayed CSI at the multiple-antenna full-duplex relay and no CSI*

at two transmitters, the sum-SDoF lower bound under symmetric antenna configurations is given as follows by setting $N_1 = N_2 = N$ and $M_1 = M_2 = M$ in Theorem 1:

$$\sum_{i=1}^{2}\sum_{j=1}^{2} d_{i,j} \geq \begin{cases} \dfrac{4M}{3}, & 2M < N \ \& \ 2N < R, \\[2mm] \dfrac{4M(R-N)}{2R-N}, & 2M < N \ \& \ N < R \leq 2N, \\[2mm] \dfrac{2N\min\{M,N\}}{\min\{M+N,2N\}}, & N \leq 2M \ \& \ 2N < R, \\[2mm] \dfrac{2N\min\{2M,R\}(R-N)}{N^2+\min\{2M+N,R+N\}(R-N)}, & N \leq 2M \ \& \ N < R \leq 2N, \\[2mm] 0, & R \leq N. \end{cases} \quad (6)$$

Proposition 1. *(sum-SDoF upper bound under arbitrary antenna configurations). For the relay-aided MIMO XCCM with delayed CSI at the multiple-antenna full-duplex relay and no CSI at two transmitters, the sum-SDoF upper bound under arbitrary antenna configurations is given by the following:*

$$\sum_{i=1}^{2}\sum_{j=1}^{2} d_{i,j} \leq \frac{N_1\min\{M_1+M_2+R-N_2,N_1\}+N_2\min\{M_1+M_2+R-N_1,N_2\}}{\min\{M_1+M_2+R,N_1+N_2\}}. \quad (7)$$

Proof. We enhance the channel by supposing that the two transmitters and the relay constitute a co-located transmitter. Based on ([10], Theorem 3), Proposition 1 is proven. □

Proposition 2. *(antenna configurations for sum-SDoF characterization). For the relay-aided MIMO XCCM with delayed CSI at the multiple-antenna full-duplex relay and no CSI at two transmitters, the sum-SDoF is characterized by the following:*

$$\sum_{i=1}^{2}\sum_{j=1}^{2} d_{i,j} = N, \qquad N \leq M \ \& \ 2N \leq R \quad (8)$$

Proof. Following Theorem 1 and Proposition 1, we can verify the match of the sum-SDoF upper and lower bounds for $N \leq M$ and $2N \leq R$. Therefore, the value of sum-SDoF is N for $N \leq M$ and $2N \leq R$. □

Remark 2. *(advantages over existing results in two-user MIMO interference networks with delayed feedback [14–17]): Under symmetric antenna configurations, the advantages of the derived results over existing results in two-user MIMO interference networks with delayed feedback [14–17] are shown in Figure 2. In particular, Figure 2 shows that if $2N \leq R$, the derived sum-SDoF lower bound is higher than the sum-SDoF of MIMO XCCM with output feedback and delayed CSIT in [17] for $M < N$, the sum-SDoF of MIMO ICCM with local output feedback in [16] for $M < 2N$, the sum-SDoF lower bound of MIMO XCCM with delayed CSIT in [15] and the sum-SDoF lower bound of MIMO ICCM with delayed CSIT in [14] for all antenna configurations. The gain of our lower bound comes from the full-duplex relay taking over the artificial noise and interference transmission from the two transmitters.*
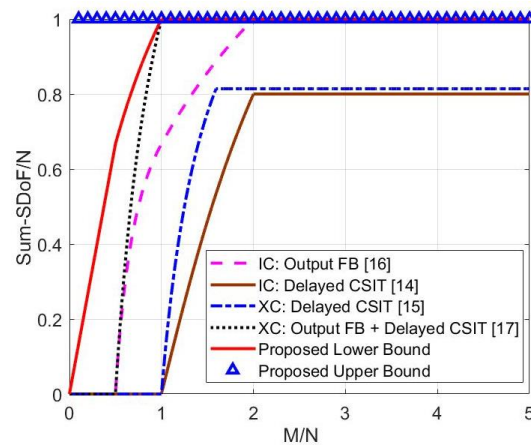
Figure 2. SDoF comparison with existing results [14–17] when $2N \leq R$.

Remark 3. (numerical calculation under arbitrary antenna configurations). *To illustrate the proposed upper and lower bounds for arbitrary antenna configurations, we have shown four examples in Figures 3–6, respectively. From Figures 3 and 4, it can be seen that the smaller difference between N_1 and N_2 leads to the smaller gap between the proposed upper and lower bounds, when M_1, M_2 are fixed and R is sufficiently large. Additionally, a higher N_2 leads to a higher value of the proposed lower bound, when N_1, M_1, M_2 are fixed. From Figures 5 and 6, it can be seen that when $N_1 + N_2$ is less than $M_1 + M_2$ and R is sufficiently large, the gap between the proposed upper and lower bounds becomes smaller.*
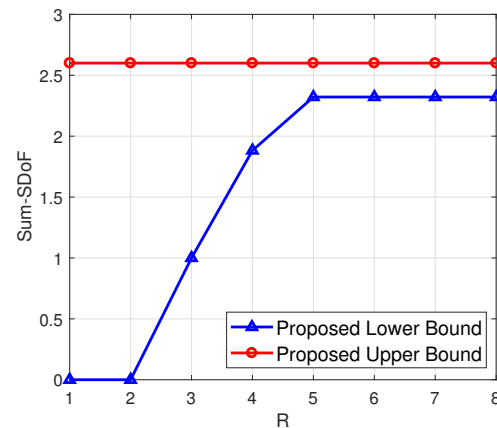

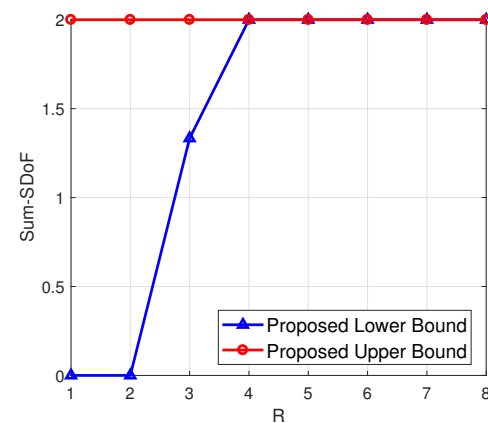**Figure 3.** $(N_1, N_2, M_1, M_2) = (2, 3, 2, 3)$.

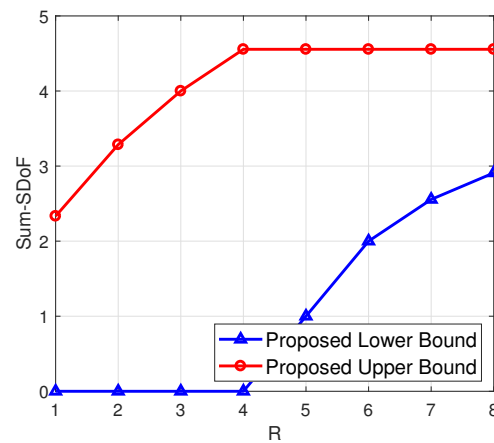**Figure 4.** $(N_1, N_2, M_1, M_2) = (2, 2, 2, 3)$.

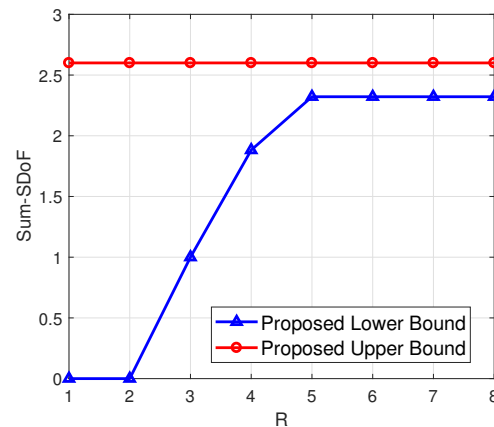**Figure 5.** $(N_1, N_2, M_1, M_2) = (4, 5, 2, 3)$.

Figure 6. $(N_1, N_2, M_1, M_2) = (2, 3, 4, 5)$.

4. Proof of Theorem 1: Relay-Aided Transmission Scheme Design

4.1. $M_1 + M_2 \leq N_1$ Case: The Relay-Aided Jamming Scheme

When $M_1 + M_2 \leq N_1$, each receiver can immediately decode the transmitted data symbols, which implies there is no need for IA. At the same time, the relay can send artificial noise symbols to ensure secure data symbol transmission. Therefore, we propose a relay-aided jamming scheme with three phases, where the relay cooperates with two transmitters for artificial noise transmission. In Phase I, the relay sends artificial noise symbols. In Phase II, two transmitters send data symbols for R_1; meanwhile, the output signal of Phase I at R_1 is reconstructed and re-transmitted by relay. In Phase III, two transmitters send data symbols for R_2; meanwhile, the output signal of Phase I at R_2 is reconstructed and re-transmitted by relay. The flowchart of this scheme is illustrated in Figure 7. Firstly, we define the holistic CSI matrices for this scheme as follows:

$$\mathbf{H}_{i,j}^{\text{P-I}} \triangleq \mathcal{BD}\{\mathbf{H}_{i,j}[1], \cdots, \mathbf{H}_{i,j}[\tau_1]\},$$

$$\mathbf{H}_{i,j}^{\text{P-II}} \triangleq \mathcal{BD}\{\mathbf{H}_{i,j}[\tau_1 + 1], \cdots, \mathbf{H}_{i,j}[\tau_1 + \tau_2]\},$$

$$\mathbf{H}_{i,j}^{\text{P-III}} \triangleq \mathcal{BD}\{\mathbf{H}_{i,j}[\tau_1 + \tau_2 + 1], \cdots, \mathbf{H}_{i,j}[\tau_1 + \tau_2 + \tau_3]\},$$

where $i, j = 1, 2, r$, and the value of τ_1, τ_2, and τ_3 is determined based on the security analysis of the scheme. Moreover, we introduce the pre-stored full-rank matrices $\mathbf{\Phi}_1 \in \mathbb{C}^{R\tau_2 \times N_1\tau_1}$ and $\mathbf{\Phi}_2 \in \mathbb{C}^{R\tau_3 \times N_2\tau_1}$, whose items follow complex Gaussian $\mathcal{CN}(0, 1)$. Next, the proposed three-phase transmission scheme and related analysis are elaborated.
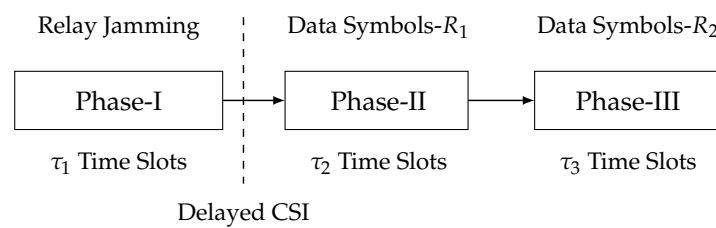
Relay Jamming   Data Symbols-R_1 Data Symbols-R_2

```
┌──────────┐     ┌──────────┐     ┌──────────┐
│ Phase-I  │ ──▶ │ Phase-II │ ──▶ │ Phase-III│
└──────────┘     └──────────┘     └──────────┘
```

τ_1 Time Slots τ_2 Time Slots τ_3 Time Slots

Delayed CSI

Figure 7. Flowchart of the relay-aided jamming scheme.

Phase I (Jamming by the Relay): This phase aims at sending $R\tau_1$ artificial noise symbols from the relay in τ_1 time slots by R antennas. Denote the artificial noise vector sent by R antennas in τ_1 time slots as $\mathbf{u} \in \mathbb{C}^{R\tau_1}$. The received signals of Phase-I at two receivers are expressed as follows:

$$\mathbf{y}_j^{\text{P-I}} = \mathbf{H}_{r,j}^{\text{P-I}}\mathbf{u}, \qquad j = 1, 2. \tag{9}$$

Note that additive white Gaussian noise (AWGN) is omitted, due to the SDoF analysis. The CSI matrices of Phase I return to the relay at the end of Phase I.

Phase II (joint data transmission for R_1 by two transmitters and Phase I output transmission by the relay): We aim at sending $M_1\tau_2$ data symbols to R_1 from T_1 and $M_2\tau_2$ data symbols to R_1 from T_2 in τ_2 time slots. With CSI matrices of Phase I, the relay re-constructs the Phase I output at receivers, i.e., $\mathbf{y}_1^{\text{P-I}}$ and $\mathbf{y}_2^{\text{P-I}}$. At each time slot, the data symbols for R_1 are sent from two transmitters, and simultaneously, the Phase I output at R_1 is sent from the relay. Denote the data symbols for R_1 sent from T_1 and T_2 as $\mathbf{s}_{1,1} \in \mathbb{C}^{M_1\tau_2}$ and $\mathbf{s}_{2,1} \in \mathbb{C}^{M_2\tau_2}$, respectively. Therefore, the transmit signals of Phase II at two transmitters are expressed as follows:

$$\mathbf{x}_i^{\text{P-II}} = \mathbf{s}_{i,1}, \qquad i = 1, 2. \tag{10}$$

The transmit signals of Phase-II at the relay are designed as follows:

$$\mathbf{x}_r^{\text{P-II}} = \mathbf{\Phi}_1\mathbf{y}_1^{\text{P-I}}. \tag{11}$$

The received signals of Phase-II at two receivers are written by the following:

$$\mathbf{y}_j^{\text{P-II}} = \mathbf{H}_{1,j}^{\text{P-II}}\mathbf{s}_{1,1} + \mathbf{H}_{2,j}^{\text{P-II}}\mathbf{s}_{2,1} + \mathbf{H}_{r,j}^{\text{P-II}}\mathbf{\Phi}_1\mathbf{y}_1^{\text{P-I}}, \quad j = 1, 2. \tag{12}$$

Phase III (joint data transmission for R_2 by two transmitters and Phase I output transmission by the relay): This phase aims at sending $M_1\tau_3$ data symbols to R_2 from T_1 and $M_2\tau_3$ data symbols to R_2 from T_2 in τ_3 time slots. At each time slot, the data symbols for R_2 are sent from two transmitters, and simultaneously, the Phase I output at R_2 is sent from the relay. Denote the data symbols for R_2 sent from T_1 and T_2 as $\mathbf{s}_{1,2} \in \mathbb{C}^{M_1\tau_3}$ and $\mathbf{s}_{2,2} \in \mathbb{C}^{M_2\tau_3}$, respectively. Therefore, the transmit signals of Phase III at two transmitters are expressed as follows:

$$\mathbf{x}_i^{\text{P-III}} = \mathbf{s}_{i,2}, \qquad i = 1, 2. \tag{13}$$

The transmit signals of Phase III at the relay are designed as follows:

$$\mathbf{x}_r^{\text{P-III}} = \mathbf{\Phi}_2\mathbf{y}_2^{\text{P-I}}. \tag{14}$$

The received signals of Phase III at two receivers are written by the following:

$$\mathbf{y}_j^{\text{P-III}} = \mathbf{H}_{1,j}^{\text{P-III}}\mathbf{s}_{1,2} + \mathbf{H}_{2,j}^{\text{P-III}}\mathbf{s}_{2,2} + \mathbf{H}_{r,j}^{\text{P-III}}\mathbf{\Phi}_2\mathbf{y}_2^{\text{P-I}}, \quad j = 1, 2. \tag{15}$$

Security analysis: Firstly, we need to verify the zero information leakage at R_1, when SNR goes to infinity. With $\mathbf{y}_1 \triangleq [\mathbf{y}_1^{\text{P-I}}; \mathbf{y}_1^{\text{P-II}}; \mathbf{y}_1^{\text{P-III}}]$, the information leakage is calculated as follows:

$$I(\mathbf{s}_{1,2}, \mathbf{s}_{2,2}; \mathbf{y}_1 | \mathbf{H}^n, \mathbf{s}_{1,1}, \mathbf{s}_{2,1})$$

$$\overset{(a)}{\leq} I(\mathbf{s}_{1,2}, \mathbf{s}_{2,2}, \mathbf{u}; \mathbf{y}_1 | \mathbf{H}^n, \mathbf{s}_{1,1}, \mathbf{s}_{2,1}) - I(\mathbf{u}; \mathbf{y}_1 | \mathbf{H}^n, \mathbf{s}_{1,1}, \mathbf{s}_{2,1}, \mathbf{s}_{1,2}, \mathbf{s}_{2,2})$$

$$\overset{(b)}{\leq} I(\mathbf{H}_{r,1}^{\text{P-I}}\mathbf{u}, \mathbf{H}_{1,1}^{\text{P-III}}\mathbf{s}_{1,2} + \mathbf{H}_{2,1}^{\text{P-III}}\mathbf{s}_{2,2} + \mathbf{H}_{r,1}^{\text{P-III}}\boldsymbol{\Phi}_2\mathbf{y}_2^{\text{P-I}}; \mathbf{y}_1 | \mathbf{H}^n, \mathbf{s}_{1,1}, \mathbf{s}_{2,1}) - I(\mathbf{u}; \mathbf{y}_1 | \mathbf{H}^n, \mathbf{s}_{1,1}, \mathbf{s}_{2,1}, \mathbf{s}_{1,2}, \mathbf{s}_{2,2})$$

(16)

$$\overset{(c)}{\underset{\eta \to \infty}{=}} \mathcal{RK} \underbrace{\begin{bmatrix} \mathbf{I}_{N_1 \tau_1} & \mathbf{0} \\ \mathbf{H}_{r,1}^{\text{P-II}}\boldsymbol{\Phi}_1 & \mathbf{0} \\ \mathbf{0} & \mathbf{I}_{N_1 \tau_3} \end{bmatrix}}_{\mathbf{A}_1} \log\eta - \mathcal{RK} \underbrace{\begin{bmatrix} \mathbf{H}_{r,1}^{\text{P-I}} \\ \mathbf{H}_{r,1}^{\text{P-II}}\boldsymbol{\Phi}_1\mathbf{H}_{r,1}^{\text{P-I}} \\ \mathbf{H}_{r,1}^{\text{P-III}}\boldsymbol{\Phi}_2\mathbf{H}_{r,2}^{\text{P-I}} \end{bmatrix}}_{\mathbf{A}_2} \log\eta$$

$$\overset{(d)}{=} N_1(\tau_1 + \tau_3)\log\eta - \min\{N_1\tau_1 + \min\{R, N_1\}\tau_3, (N_1 + N_2)\tau_1, R\tau_1\}\log\eta,$$

where the reason for each step is given as follows:

(a) Chain rule of mutual information.

(b) Applying the data processing inequality for the Markov chain $(\mathbf{s}_{1,2}, \mathbf{s}_{2,2}, \mathbf{u}) \to (\mathbf{H}_{r,1}^{\text{P-I}}\mathbf{u}, \mathbf{H}_{1,1}^{\text{P-III}}\mathbf{s}_{1,2} + \mathbf{H}_{2,1}^{\text{P-III}}\mathbf{s}_{2,2} + \mathbf{H}_{r,1}^{\text{P-III}}\boldsymbol{\Phi}_2\mathbf{y}_2^{\text{P-I}}) \to \mathbf{y}_1$.

(c) When the input is the circularly symmetric complex Gaussian, according to [30], rewrite the mutual information into $\log|\mathbf{I} + \eta\mathbf{A}_1\mathbf{A}_1^H| - \log|\mathbf{I} + \eta\mathbf{A}_2\mathbf{A}_2^H|$, and using ([10], Lemma 2), when SNR goes to infinity.

(d) The rank of matrix $\mathbf{A}_1$ is deduced by Gaussian elimination. The rank of matrix $\mathbf{A}_2$ is derived in Appendix A.

We shall ensure $I(\mathbf{s}_{1,2}, \mathbf{s}_{2,2}; \mathbf{y}_1 | \mathbf{H}^n, \mathbf{s}_{1,1}, \mathbf{s}_{2,1}) = o(\log\eta)$, or equivalently, (16) is zero. If $N_1 < R$, $N_1(\tau_1 + \tau_3) = N_1\tau_1 + \min\{R, N_1\}\tau_3$. If $N_1 + N_2 \leq R$, we have $N_1(\tau_1 + \tau_3) = (N_1 + N_2)\tau_1$. Otherwise, if $N_1 < R < N_1 + N_2$, we have $N_1(\tau_1 + \tau_3) = R\tau_1$. Those two equalities can be simplified to the following:

$$\frac{\tau_1}{\tau_3} = \frac{N_1}{\min\{N_2, R - N_1\}}. \tag{17}$$

Otherwise, if $R \leq N_1$, we cannot guarantee zero information leakage from transmitted data symbols $\mathbf{s}_{2,1}, \mathbf{s}_{2,1}$ to the undesired receiver R_2, which implies $\tau_3 = 0$.

Secondly, we only need to verify the zero information leakage at the R_2, when SNR goes to infinity. With $\mathbf{y}_2 \triangleq [\mathbf{y}_2^{\text{P-I}}; \mathbf{y}_2^{\text{P-II}}; \mathbf{y}_2^{\text{P-III}}]$, the information leakage is calculated as follows:

$$I(\mathbf{s}_{1,1}, \mathbf{s}_{2,1}; \mathbf{y}_2 | \mathbf{H}^n, \mathbf{s}_{1,2}, \mathbf{s}_{2,2})$$

$$\overset{(a)}{\leq} I(\mathbf{s}_{1,1}, \mathbf{s}_{2,1}, \mathbf{u}; \mathbf{y}_2 | \mathbf{H}^n, \mathbf{s}_{1,2}, \mathbf{s}_{2,2}) - I(\mathbf{u}; \mathbf{y}_2 | \mathbf{H}^n, \mathbf{s}_{1,1}, \mathbf{s}_{2,1}, \mathbf{s}_{1,2}, \mathbf{s}_{2,2})$$

$$\overset{(b)}{\leq} I(\mathbf{H}_{r,2}^{\text{P-I}}\mathbf{u}, \mathbf{H}_{1,2}^{\text{P-II}}\mathbf{s}_{1,1} + \mathbf{H}_{2,2}^{\text{P-II}}\mathbf{s}_{2,1} + \mathbf{H}_{r,2}^{\text{P-II}}\boldsymbol{\Phi}_1\mathbf{y}_1^{\text{P-I}}; \mathbf{y}_2 | \mathbf{H}^n, \mathbf{s}_{1,2}, \mathbf{s}_{2,2}) - I(\mathbf{u}; \mathbf{y}_2 | \mathbf{H}^n, \mathbf{s}_{1,1}, \mathbf{s}_{2,1}, \mathbf{s}_{1,2}, \mathbf{s}_{2,2})$$

(18)

$$\overset{(c)}{\underset{\eta \to \infty}{=}} \mathcal{RK} \underbrace{\begin{bmatrix} \mathbf{I}_{N_2 \tau_1} & \mathbf{0} \\ \mathbf{0} & \mathbf{I}_{N_2 \tau_2} \\ \mathbf{H}_{r,2}^{\text{P-III}}\boldsymbol{\Phi}_2 & \mathbf{0} \end{bmatrix}}_{\mathbf{B}_1} \log\eta - \mathcal{RK} \underbrace{\begin{bmatrix} \mathbf{H}_{r,2}^{\text{P-I}} \\ \mathbf{H}_{r,2}^{\text{P-II}}\boldsymbol{\Phi}_1\mathbf{H}_{r,1}^{\text{P-I}} \\ \mathbf{H}_{r,2}^{\text{P-III}}\boldsymbol{\Phi}_2\mathbf{H}_{r,2}^{\text{P-I}} \end{bmatrix}}_{\mathbf{B}_2} \log\eta$$

$$\overset{(d)}{=} N_2(\tau_1 + \tau_2)\log\eta - \min\{N_2\tau_1 + \min\{R, N_2\}\tau_2, (N_1 + N_2)\tau_1, R\tau_1\}\log\eta,$$

where the reason for each step is given as follows:

(a) Chain rule of mutual information.

(b) Applying the data processing inequality for the Markov chain $(\mathbf{s}_{1,1}, \mathbf{s}_{2,1}, \mathbf{u}) \to (\mathbf{H}_{r,2}^{\text{P-I}}\mathbf{u}, \mathbf{H}_{1,2}^{\text{P-II}}\mathbf{s}_{1,1} + \mathbf{H}_{2,2}^{\text{P-II}}\mathbf{s}_{2,1} + \mathbf{H}_{r,2}^{\text{P-II}}\boldsymbol{\Phi}_1\mathbf{y}_1^{\text{P-I}}) \to \mathbf{y}_2$.

(c) When the input is the circularly symmetric complex Gaussian, according to [30], and rewrite the mutual information into $\log|\mathbf{I} + \eta\mathbf{B}_1\mathbf{B}_1^H| - \log|\mathbf{I} + \eta\mathbf{B}_2\mathbf{B}_2^H|$, and using ([10], Lemma 2), when SNR goes to infinity.

(d)   The rank of matrix $\mathbf{B}_1$ is deduced by Gaussian elimination. The rank of matrix $\mathbf{B}_2$ is derived in Appendix A.

We shall ensure $I(\mathbf{s}_{1,1}, \mathbf{s}_{2,1}; \mathbf{y}_2 | \mathbf{H}^n, \mathbf{s}_{1,2}, \mathbf{s}_{2,2}) = o(\log \eta)$, or equivalently, (18) is zero. If $N_2 < R$, $N_2(\tau_1 + \tau_2) \leq N_2 \tau_1 + \min\{R, N_2\}\tau_2$. If $N_1 + N_2 \leq R$, we have $N_2(\tau_1 + \tau_2) = (N_1 + N_2)\tau_1$. Otherwise, if $N_2 < R < N_1 + N_2$, we have $N_2(\tau_1 + \tau_2) = R\tau_1$. Those two inequalities can be simplified to the following:

$$\frac{\tau_1}{\tau_2} = \frac{N_2}{\min\{N_1, R - N_2\}}. \tag{19}$$

If $R \leq N_2$, we cannot guarantee zero information leakage from transmitted data symbols $\mathbf{s}_{1,1}, \mathbf{s}_{1,2}$ to the undesired receiver R_2, which implies $\tau_2 = 0$.

Decoding analysis: Firstly, we need to verify the decoding of transmitted data symbols $\mathbf{s}_{1,1} \in \mathbb{C}^{M_1 \tau_2}, \mathbf{s}_{2,1} \in \mathbb{C}^{M_2 \tau_2}$ at R_1, which is enabled by the following cancellation:

$$\mathbf{y}_1^{\text{P-II}} - \mathbf{H}_{r,1}^{\text{P-II}}\mathbf{\Phi}_1\mathbf{y}_1^{\text{P-I}} = \mathbf{H}_{1,1}^{\text{P-II}}\mathbf{s}_{1,1} + \mathbf{H}_{2,1}^{\text{P-II}}\mathbf{s}_{2,1}, \tag{20}$$

At each time slot, there are N_1 observations at R_1. Thus, we are able to decode M_1 data symbols from T_1 and M_2 data symbols from T_2, due to the setting, i.e., $M_1 + M_2 \leq N_1$. Therefore, R_1 can decode $(M_1 + M_2)\tau_2$ data symbols.

Secondly, we need to verify the decoding of transmitted data symbols $\mathbf{s}_{1,2} \in \mathbb{C}^{M_1 \tau_3}$, $\mathbf{s}_{2,2} \in \mathbb{C}^{M_2 \tau_3}$ at R_2, which is enabled by the following cancellation:

$$\mathbf{y}_2^{\text{P-III}} - \mathbf{H}_{r,2}^{\text{P-III}}\mathbf{\Phi}_2\mathbf{y}_2^{\text{P-I}} = \mathbf{H}_{1,2}^{\text{P-III}}\mathbf{s}_{1,2} + \mathbf{H}_{2,2}^{\text{P-III}}\mathbf{s}_{2,2}, \tag{21}$$

At each time slot, there are N_2 observations at R_2. Thus, we are able to decode M_1 data symbols from T_1 and M_2 data symbols from T_2, due to the setting, i.e., $M_1 + M_2 \leq N_1 \leq N_2$. Therefore, R_2 can decode $(M_1 + M_2)\tau_3$ data symbols.

Achievable sum-SDoF analysis: As shown in the decoding analysis, two receivers can decode a total of $(M_1 + M_2)(\tau_2 + \tau_3)$ data symbols over $\tau_1 + \tau_2 + \tau_3$ time slots. This implies that the achievable sum-SDoF can be expressed as $(M_1 + M_2)(\tau_2 + \tau_3)/(\tau_1 + \tau_2 + \tau_3)$. According to the security analysis, the achievable sum-SDoF of proposed relay-aided jamming scheme is calculated through the following:

- If $N_2 < R$, we substitute (17) and (19) into $(M_1 + M_2)(\tau_2 + \tau_3)/(\tau_1 + \tau_2 + \tau_3)$ to derive the exact achievable sum-SDoF.
- If $N_1 < R \leq N_2$, we substitute $\tau_2 = 0$ and (17) into $(M_1 + M_2)(\tau_2 + \tau_3)/(\tau_1 + \tau_2 + \tau_3)$ to derive the exact achievable sum-SDoF.
- If $R \leq N_1$, we cannot ensure zero information leakage; hence, achievable sum-SDoF is zero.

The achievable sum-SDoF of the proposed relay-aided jamming scheme is given in (4) for $M_1 + M_2 \leq N_1$ & $N_2 < R$ Case, $M_1 + M_2 \leq N_1$ & $N_1 < R \leq N_2$ Case, and $R \leq N_1$ Case.

4.2. $N_1 < M_1 + M_2 \leq N_2$ Case: The Relay-Aided Jamming and One-Receiver IA Scheme

When $N_1 < M_1 + M_2 \leq N_2$, then R_1 can immediately decode the transmitted data symbols, while R_2 cannot. Therefore, the technique of IA can be adopted to enable the decoding of transmitted data symbols for R_2, where the interference at R_1 is re-transmitted to provide lacking equations for decoding. To this end, we propose a relay-aided jamming and the one-receiver IA scheme with four phases, where the relay cooperates with two transmitters for both artificial noise transmission and IA. In Phase I, the relay sends artificial noise symbols. In Phase II, two transmitters send data symbols for R_1; meanwhile, the output signal of Phase I at R_1 is reconstructed and re-transmitted by relay. In Phase III, two transmitters send data symbols for R_2; meanwhile, the output signal of Phase I at R_2 is reconstructed and re-transmitted by relay. In Phase IV, the interference at R_2 is re-

transmitted to provide lacking equations for R_1. The flowchart of this scheme is illustrated in Figure 8. Firstly, we define the holistic CSI matrices for this scheme as follows:

$$\mathbf{H}_{i,j}^{\text{P-I}} \triangleq \mathcal{BD}\{\mathbf{H}_{i,j}[1], \cdots, \mathbf{H}_{i,j}[\tau_1]\},$$

$$\mathbf{H}_{i,j}^{\text{P-II}} \triangleq \mathcal{BD}\{\mathbf{H}_{i,j}[\tau_1 + 1], \cdots, \mathbf{H}_{i,j}[\tau_1 + \tau_2]\},$$

$$\mathbf{H}_{i,j}^{\text{P-III}} \triangleq \mathcal{BD}\{\mathbf{H}_{i,j}[\tau_1 + \tau_2 + 1], \cdots, \mathbf{H}_{i,j}[\tau_1 + \tau_2 + \tau_3]\},$$

$$\mathbf{H}_{i,j}^{\text{P-IV}} \triangleq \mathcal{BD}\{\mathbf{H}_{i,j}[\tau_1 + \tau_2 + \tau_3 + 1], \cdots, \mathbf{H}_{i,j}[\tau_1 + \tau_2 + \tau_3 + \tau_4]\},$$

where $i, j = 1, 2, r$, and the value of τ_1, τ_2, and τ_3 is determined based on security analysis of the scheme. Moreover, we introduce the pre-stored full-rank matrices $\boldsymbol{\Phi}_1 \in \mathbb{C}^{R\tau_2 \times N_1 \tau_1}$, $\boldsymbol{\Phi}_2 \in \mathbb{C}^{R\tau_3 \times N_2 \tau_1}$, and $\boldsymbol{\Pi}_1 \in \mathbb{C}^{\min\{N_1, R\}\tau_4 \times N_2 \tau_2}$, whose items follow complex Gaussian $\mathcal{CN}(0, 1)$. Next, the proposed three-phase transmission scheme and related analysis are elaborated.
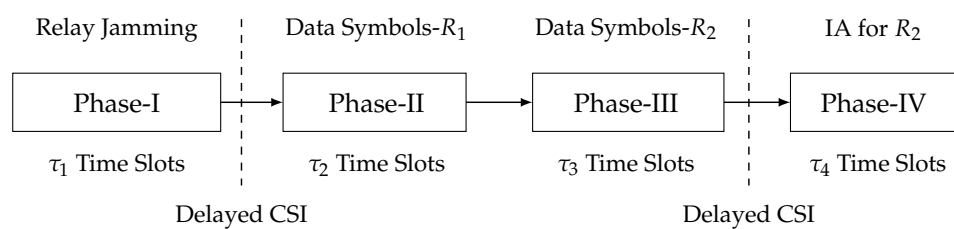
Relay Jamming	Data Symbols-R_1	Data Symbols-R_2	IA for R_2
Phase-I	Phase-II	Phase-III	Phase-IV
τ_1 Time Slots	τ_2 Time Slots	τ_3 Time Slots	τ_4 Time Slots

Delayed CSI   Delayed CSI

Figure 8. Flowchart of the relay-aided jamming and one-receiver IA scheme.

Phase I (jamming by the relay): This phase aims at sending $R\tau_1$ artificial noise symbols from the relay in τ_1 time slots by R antennas. Denote the artificial noise vector sent by R antennas in τ_1 time slots as $\mathbf{u} \in \mathbb{C}^{R\tau_1}$. The received signals of Phase I at two receivers are expressed as follows:

$$\mathbf{y}_j^{\text{P-I}} = \mathbf{H}_{r,j}^{\text{P-I}} \mathbf{u}, \qquad j = 1, 2. \tag{22}$$

The CSI matrices of Phase I return to the relay at the end of Phase I.

Phase II (joint data transmission for R_1 by two transmitters and Phase I output transmission by the relay): We aim at sending $M_1 \tau_2$ data symbols to R_1 from T_1 and $\min\{M_2, R - M_1\}\tau_2$ data symbols to R_1 from T_2 in τ_2 time slots. With CSI matrices of Phase I, the relay reconstructs the Phase I output at the receivers, i.e., $\mathbf{y}_1^{\text{P-I}}$ and $\mathbf{y}_2^{\text{P-I}}$. At each time slot, the data symbols for R_1 are sent from two transmitters, and simultaneously, the Phase I output at R_1 is sent from the relay. Denote the data symbols for R_1 sent from T_1 and T_2 as $\mathbf{s}_{1,1} \in \mathbb{C}^{M_1 \tau_2}$ and $\mathbf{s}_{2,1} \in \mathbb{C}^{\min\{M_2, R - M_1\}\tau_2}$, respectively. Therefore, the transmit signals of Phase-II at two transmitters are expressed as follows:

$$\mathbf{x}_i^{\text{P-II}} = \mathbf{s}_{i,1}, \qquad i = 1, 2. \tag{23}$$

The transmit signals of Phase II at the relay are designed as follows:

$$\mathbf{x}_r^{\text{P-II}} = \boldsymbol{\Phi}_1 \mathbf{y}_1^{\text{P-I}}. \tag{24}$$

The received signals of Phase II at two receivers are written as follows:

$$\mathbf{y}_j^{\text{P-II}} = \mathbf{H}_{1,j}^{\text{P-II}} \mathbf{s}_{1,1} + \mathbf{H}_{2,j}^{\text{P-II}} \mathbf{s}_{2,1} + \mathbf{H}_{r,j}^{\text{P-II}} \boldsymbol{\Phi}_1 \mathbf{y}_1^{\text{P-I}}, \quad j = 1, 2. \tag{25}$$

After the successful self-interference cancellation (for the successful interference cancellation, the residual self-interference can achieve noise floor; therefore, the residual self-interference does not affect the SDoF analysis) at the relay, the received signals of Phase II at the relay are expressed as follows:

$$\mathbf{y}_r^{\text{P-II}} = \mathbf{H}_{1,r}^{\text{P-II}} \mathbf{s}_{1,2} + \mathbf{H}_{2,r}^{\text{P-II}} \mathbf{s}_{2,2}. \tag{26}$$

Since there are R observations at the relay, the relay can immediately decode all transmitted $\min\{M_1 + M_2, R\}$ data symbols, given by $\mathbf{s}_{1,1}$ and $\mathbf{s}_{2,1}$. The CSI matrices of Phase II return to the relay at the end of Phase II.

Phase III (joint data transmission for R_2 by two transmitters and Phase I output transmission by the relay): This phase aims at sending $M_1\tau_3$ data symbols to R_2 from T_1 and $M_2\tau_3$ data symbols to R_2 from T_2 in τ_3 time slots. At each time slot, the data symbols for R_2 are sent from two transmitters, and simultaneously, the Phase I output at R_2 is sent from the relay. Denote the data symbols for R_1 sent from T_1 and T_2 as $\mathbf{s}_{1,2} \in \mathbb{C}^{M_1\tau_3}$ and $\mathbf{s}_{2,2} \in \mathbb{C}^{M_2\tau_3}$, respectively. Therefore, the transmit signals of Phase III at the two transmitters are expressed as follows:

$$\mathbf{x}_i^{\text{P-III}} = \mathbf{s}_{i,2}, \qquad i = 1, 2. \tag{27}$$

The transmit signals of Phase III at the relay are designed as follows:

$$\mathbf{x}_r^{\text{P-III}} = \mathbf{\Phi}_2 \mathbf{y}_2^{\text{P-I}}. \tag{28}$$

The received signals of Phase III at two receivers are written as follows:

$$\mathbf{y}_j^{\text{P-III}} = \mathbf{H}_{1,j}^{\text{P-III}}\mathbf{s}_{1,2} + \mathbf{H}_{2,j}^{\text{P-III}}\mathbf{s}_{2,2} + \mathbf{H}_{r,j}^{\text{P-III}}\mathbf{\Phi}_2\mathbf{y}_2^{\text{P-I}}, \quad j = 1, 2. \tag{29}$$

The CSI matrices of Phase III return to the relay at the end of Phase III.

Phase IV (one-receiver IA by the relay): In order to provide lacking equations for decoding, we aim at sending $\min\{N_1, R\}\tau_3$ combinations of interference at Phase II in τ_4 time slots. With CSI matrices of Phase I and Phase II, $\mathbf{s}_{1,1}$ and $\mathbf{s}_{2,1}$, the relay re-constructs the interference at Phase II, i.e., $\mathbf{y}_2^{\text{P-II}}$. The transmit signals of Phase IV at the relay are designed as follows:

$$\mathbf{x}_r^{\text{P-IV}} = \mathbf{\Pi}_1 \mathbf{y}_2^{\text{P-II}}. \tag{30}$$

At the same time, two transmitters keep silent. The received signals of Phase IV at two receivers are written as follows:

$$\mathbf{y}_j^{\text{P-IV}} = \mathbf{H}_{r,j}^{\text{P-IV}}\mathbf{\Pi}_1\mathbf{y}_2^{\text{P-II}}, \quad j = 1, 2. \tag{31}$$

Security Analysis: As the received signals in Phase IV can be constructed by the received signals in Phase II and CSI matrices, the security analysis is similar to that in the relay-aided jamming scheme. Therefore, it can be checked that to ensure zero information leakage at R_1 and R_2, when SNR goes to infinity, phase duration should follow (17) and (19), respectively.

Decoding analysis: Firstly, we need to verify the decoding of transmitted data symbols $\mathbf{s}_{1,1}$ and $\mathbf{s}_{2,1}$ at R_1. This is enabled by the following cancellation:

$$\begin{bmatrix} \mathbf{y}_1^{\text{P-II}} - \mathbf{H}_{r,1}^{\text{P-II}}\mathbf{\Phi}_1\mathbf{y}_1^{\text{P-I}} \\ \mathbf{y}_1^{\text{P-II}} - \mathbf{H}_{r,1}^{\text{P-IV}}\mathbf{\Pi}_1\mathbf{H}_{r,2}^{\text{P-II}}\mathbf{\Phi}_1\mathbf{y}_1^{\text{P-I}} \end{bmatrix} = \underbrace{\begin{bmatrix} \mathbf{H}_{1,1}^{\text{P-II}} & \mathbf{H}_{2,1}^{\text{P-II}} \\ \mathbf{H}_{r,1}^{\text{P-IV}}\mathbf{\Pi}_1\mathbf{H}_{1,2}^{\text{P-II}} & \mathbf{H}_{r,1}^{\text{P-IV}}\mathbf{\Pi}_1\mathbf{H}_{2,2}^{\text{P-II}} \end{bmatrix}}_{\mathbf{H}_1} \begin{bmatrix} \mathbf{s}_{1,1} \\ \mathbf{s}_{2,1} \end{bmatrix}, \tag{32}$$

where the rank of matrix $\mathbf{H}_1$ is $\min\{N_1\tau_2 + \min\{N_1\tau_4, R\tau_4\}, (M_1 + M_2)\tau_2, R\tau_2\}$. The reason is given in Appendix B. Since $\min\{M_1 + M_2, R\}\tau_2$ data symbols for R_1 are transmitted, to ensure the decoding, we shall follow that

$$\min\{M_1 + M_2, R\}\tau_2 \leq N_1\tau_2 + \min\{N_1\tau_4, R\tau_4\}, \tag{33}$$

which simplifies to the following:

$$\frac{\tau_2}{\tau_4} \leq \frac{\min\{N_1, R\}}{\min\{M_1 + M_2 - N_1, R - N_1\}}. \tag{34}$$

Then, multiplying (34) by (19), we have the following:

$$\frac{\tau_1}{\tau_4} \leq \frac{\min\{N_1, R\} N_2}{\min\{M_1 + M_2 - N_1, R - N_1\} \min\{N_1, R - N_2\}}. \tag{35}$$

Secondly, we need to verify the decoding of transmitted data symbols $\mathbf{s}_{1,2}$ and $\mathbf{s}_{2,2}$ at the receiver R_2, which is enabled by the following cancellation:

$$\mathbf{y}_2^{\text{P-III}} - \mathbf{H}_{r,2}^{\text{P-III}} \mathbf{\Phi}_2 \mathbf{y}_2^{\text{P-I}} = \mathbf{H}_{1,2}^{\text{P-III}} \mathbf{s}_{1,2} + \mathbf{H}_{2,2}^{\text{P-III}} \mathbf{s}_{2,2}, \tag{36}$$

At each time slot, there are N_2 observations at R_2. Thus, we are able to decode M_1 data symbols from T_1 and M_2 data symbols from T_2, due to the setting, i.e, $M_1 + M_2 \leq N_2$. Therefore, R_2 can decode $(M_1 + M_2)\tau_3$ data symbols.

Achievable sum-SDoF analysis: As shown in the decoding analysis, two receivers can decode a total of $\min\{M_1 + M_2, R\}\tau_2 + (M_1 + M_2)\tau_3$ data symbols over $\tau_1 + \tau_2 + \tau_3 + \tau_4$ time slots. This implies that the achievable sum-SDoF can be expressed as $(\min\{M_1 + M_2, R\}\tau_2 + (M_1 + M_2)\tau_3)/(\tau_1 + \tau_2 + \tau_3 + \tau_4)$. According to the security and decoding analysis, the achievable sum-SDoF of proposed relay-aided jamming and one-receiver IA scheme is calculated through the following:

- If $N_2 < R$, we substitute (17), (19), and (35) with equality into $(\min\{M_1 + M_2, R\}\tau_2 + (M_1 + M_2)\tau_3)/(\tau_1 + \tau_2 + \tau_3 + \tau_4)$ to derive the exact achievable sum-SDoF.
- If $N_1 < R \leq N_2$, we substitute (17), $\tau_2 = 0$, and $\tau_4 = 0$ into $(\min\{M_1 + M_2, R\}\tau_2 + (M_1 + M_2)\tau_3)/(\tau_1 + \tau_2 + \tau_3 + \tau_4)$ to derive the exact achievable sum-SDoF.
- If $R \leq N_1$, we cannot ensure zero information leakage, and hence, the achievable sum-SDoF is zero.

The achievable sum-SDoF of the proposed relay-aided jamming and one-receiver IA scheme is given in (4) for $N_1 < M_1 + M_2 \leq N_2$ & $N_2 < R$ Case, $M_1 + M_2 \leq N_2$ & $N_1 < R \leq N_2$ Case, and $R \leq N_1$ Case.

4.3. $N_2 < M_1 + M_2$ Case: The Relay-Aided Jamming and Two-Receiver IA Scheme

When $N_2 < M_1 + M_2$, both two receivers, i.e., R_1 and R_2, are unable to immediately decode the transmitted data symbols. Therefore, the technique of IA can be adopted to enable the decoding of transmitted data symbols for both two receivers, where the interference at both two receivers is re-transmitted to provide lacking equations for decoding. To this end, we propose a relay-aided jamming and two-receiver IA scheme with four phases, where the relay cooperates with two transmitters for both artificial noise transmission and IA. In Phase I, the relay sends artificial noise symbols. In Phase II, two transmitters send data symbols for R_1; meanwhile, the output signal of Phase I at R_1 is reconstructed and re-transmitted by relay. In Phase III, two transmitters send data symbols for R_2; meanwhile the output signal of Phase I at R_2 is reconstructed and re-transmitted by relay. In Phase IV, the interference at R_2 is re-transmitted to provide lacking equations for R_1; meanwhile, the interference at R_1 is re-transmitted to provide lacking equations for R_2. The flowchart of this scheme is illustrated in Figure 9. Firstly, we define the holistic CSI matrices as follows:

$$\mathbf{H}_{i,j}^{\text{P-I}} \triangleq \mathcal{BD}\{\mathbf{H}_{i,j}[1], \cdots, \mathbf{H}_{i,j}[\tau_1]\},$$
$$\mathbf{H}_{i,j}^{\text{P-II}} \triangleq \mathcal{BD}\{\mathbf{H}_{i,j}[\tau_1 + 1], \cdots, \mathbf{H}_{i,j}[\tau_1 + \tau_2]\},$$
$$\mathbf{H}_{i,j}^{\text{P-III}} \triangleq \mathcal{BD}\{\mathbf{H}_{i,j}[\tau_1 + \tau_2 + 1], \cdots, \mathbf{H}_{i,j}[\tau_1 + \tau_2 + \tau_3]\},$$
$$\mathbf{H}_{i,j}^{\text{P-IV}} \triangleq \mathcal{BD}\{\mathbf{H}_{i,j}[\tau_1 + \tau_2 + \tau_3 + 1], \cdots, \mathbf{H}_{i,j}[\tau_1 + \tau_2 + \tau_3 + \tau_4]\},$$

where $i, j = 1, 2, r$, and the values of τ_1, τ_2, τ_3, and τ_4 are determined based on security and decoding analysis of the scheme. Moreover, we introduce the pre-stored full-rank matrices $\mathbf{\Phi}_1 \in \mathbb{C}^{R\tau_2 \times N_1\tau_1}$, $\mathbf{\Phi}_1 \in \mathbb{C}^{R\tau_3 \times N_2\tau_1}$, $\mathbf{\Pi}_1 \in \mathbb{C}^{\min\{N_1, R\}\tau_4 \times N_2\tau_2}$, and $\mathbf{\Pi}_2 \in \mathbb{C}^{\min\{N_1, R\}\tau_4 \times N_1\tau_3}$, whose items follow complex Gaussian $\mathcal{CN}(0, 1)$. Next, the proposed four-phase transmission scheme and related analysis are elaborated.
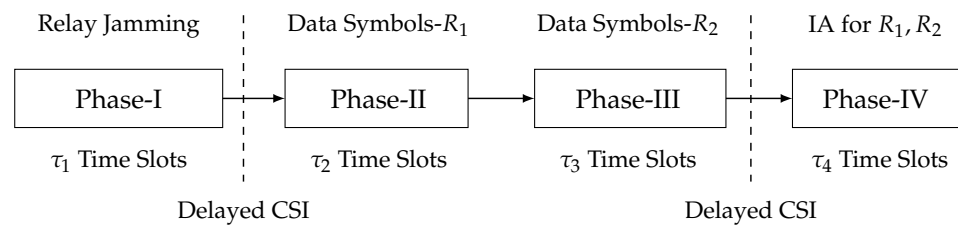
Relay Jamming	Data Symbols-R_1	Data Symbols-R_2	IA for R_1, R_2
Phase-I	Phase-II	Phase-III	Phase-IV
τ_1 Time Slots	τ_2 Time Slots	τ_3 Time Slots	τ_4 Time Slots
	Delayed CSI		Delayed CSI

Figure 9. Flowchart of the relay-aided jamming and two-receiver IA scheme.

Phase I (jamming by the relay): This phase aims at sending $R\tau_1$ artificial noise symbols from the relay by R antennas in τ_1 time slots. Denote the artificial noise vector sent by R antennas in τ_1 time slots as $\mathbf{u} \in \mathbb{C}^{R\tau_1}$. The received signals of Phase I at two receivers are expressed as follows:

$$\mathbf{y}_j^{\text{P-I}} = \mathbf{H}_{r,j}^{\text{P-I}}\mathbf{u}, \qquad j = 1, 2. \tag{37}$$

The CSI matrices of Phase I return to the relay at the end of Phase I.

Phase II (joint data transmission for R_1 by two transmitters and Phase I output transmission by the relay): We aim at sending $M_1\tau_2$ data symbols to R_1 from T_1 and $\min\{M_2, R - M_1, N_1 + N_2 - M_1\}\tau_2$ data symbols to R_1 from T_2 in τ_2 time slots. With CSI matrices of Phase I, the relay re-constructs the Phase I output at receivers, i.e., $\mathbf{y}_1^{\text{P-I}}$ and $\mathbf{y}_2^{\text{P-I}}$. At each time slot, the data symbols for R_1 are sent from two transmitters, and simultaneously, the Phase I output at R_1 is sent from the relay. Denote the data symbols for R_1 sent from T_1 and T_2 as $\mathbf{s}_{1,1} \in \mathbb{C}^{M_1\tau_2}$ and $\mathbf{s}_{2,1} \in \mathbb{C}^{\min\{M_2,R-M_1,N_1+N_2-M_1\}\tau_2}$, respectively. Therefore, the transmit signals of Phase II at two transmitters are expressed as follows:

$$\mathbf{x}_i^{\text{P-II}} = \mathbf{s}_{i,1}, \qquad i = 1, 2. \tag{38}$$

The transmit signals of Phase II at the relay are designed as follows:

$$\mathbf{x}_r^{\text{P-II}} = \mathbf{\Phi}_1\mathbf{y}_1^{\text{P-I}}. \tag{39}$$

The received signals of Phase II at two receivers are written as follows:

$$\mathbf{y}_j^{\text{P-II}} = \mathbf{H}_{1,j}^{\text{P-II}}\mathbf{s}_{1,1} + \mathbf{H}_{2,j}^{\text{P-II}}\mathbf{s}_{2,1} + \mathbf{H}_{r,j}^{\text{P-II}}\mathbf{\Phi}_1\mathbf{y}_1^{\text{P-I}}, \quad j = 1, 2. \tag{40}$$

After the successful self-interference cancellation at the relay, the received signals of Phase II at the relay are expressed as follows:

$$\mathbf{y}_r^{\text{P-II}} = \mathbf{H}_{1,r}^{\text{P-II}}\mathbf{s}_{1,1} + \mathbf{H}_{2,r}^{\text{P-II}}\mathbf{s}_{2,1}. \tag{41}$$

Since there are R observations at the relay, the relay can immediately decode all transmitted $\min\{M_1 + M_2, R, N_1 + N_2\}$ data symbols, given by $\mathbf{s}_{1,1}$ and $\mathbf{s}_{2,1}$. The CSI matrices of Phase II return to the relay at the end of Phase II.

Phase III (joint data transmission for R_2 by two transmitters and Phase I output transmission by the relay): We aim at sending $M_1\tau_2$ data symbols to R_2 from T_1 and $\min\{M_2, R - M_1, N_1 + N_2 - M_1\}\tau_2$ data symbols to R_2 from T_2 in τ_3 time slots. At each time slot, the data symbols for R_2 are sent from two transmitters, and simultaneously, the Phase I output at R_2 is sent from the relay. Denote the data symbols for R_2 sent from T_1 and T_2 as $\mathbf{s}_{1,2} \in \mathbb{C}^{M_1\tau_2}$ and $\mathbf{s}_{2,2} \in \mathbb{C}^{\min\{M_2,R-M_1,N_1+N_2-M_1\}\tau_2}$, respectively. Therefore, the transmit signals of Phase-III at two transmitters are expressed as follows:

$$\mathbf{x}_i^{\text{P-III}} = \mathbf{s}_{i,2}, \qquad i = 1, 2. \tag{42}$$

The transmit signals of Phase III at the relay are designed as follows:

$$\mathbf{x}_r^{\text{P-III}} = \mathbf{\Phi}_2\mathbf{y}_2^{\text{P-I}}. \tag{43}$$

The received signals of Phase II at two receivers are written as follows:

$$\mathbf{y}_j^{\text{P-III}} = \mathbf{H}_{1,j}^{\text{P-III}}\mathbf{s}_{1,2} + \mathbf{H}_{2,j}^{\text{P-III}}\mathbf{s}_{2,2} + \mathbf{H}_{r,j}^{\text{P-III}}\mathbf{\Phi}_2\mathbf{y}_2^{\text{P-I}}, \quad j = 1, 2. \tag{44}$$

After the successful self-interference cancellation at the relay, the received signals of Phase II at the relay are expressed as follows:

$$\mathbf{y}_r^{\text{P-III}} = \mathbf{H}_{1,r}^{\text{P-III}}\mathbf{s}_{1,2} + \mathbf{H}_{2,r}^{\text{P-III}}\mathbf{s}_{2,2}. \tag{45}$$

Since there are R observations at the relay, the relay can immediately decode all transmitted $\min\{M_1 + M_2, R, N_1 + N_2\}$ data symbols, given by $\mathbf{s}_{1,1}$ and $\mathbf{s}_{2,1}$. The CSI matrices of Phase III return to the relay at the end of Phase III.

Phase IV (two-receiver IA by the relay): In order to provide lacking equations for decoding, we aim at sending $\min\{N_1, R\}\tau_4$ combinations of interference at Phase II and Phase III by $\min\{N_1, R\}$ antennas in τ_4 time slots after Phase III. With CSI matrices of Phase I, Phase II, and Phase III, the relay re-constructs the interference at Phase II and Phase III, i.e, $\mathbf{y}_2^{\text{P-II}}$ and $\mathbf{y}_1^{\text{P-III}}$. The transmit signals of Phase-IV at the relay are designed as follows:

$$\mathbf{x}_r^{\text{P-IV}} = \mathbf{\Pi}_2\mathbf{y}_1^{\text{P-III}} + \mathbf{\Pi}_1\mathbf{y}_2^{\text{P-II}}. \tag{46}$$

At the same time, two transmitters keep silent. The received signals of Phase IV at two receivers are written by the following:

$$\mathbf{y}_j^{\text{P-IV}} = \mathbf{H}_{r,j}^{\text{P-IV}}\mathbf{\Pi}_2\mathbf{y}_1^{\text{P-III}} + \mathbf{H}_{r,j}^{\text{P-IV}}\mathbf{\Pi}_1\mathbf{y}_2^{\text{P-II}}, \quad j = 1, 2. \tag{47}$$

Security Analysis: As the received signals in Phase IV can be constructed by the received signals in Phase II, Phase III, and CSI matrices, the security analysis is similar to that in the relay-aided jamming scheme. Therefore, it can be checked that to ensure zero information leakage at R_1 and R_2, when SNR goes to infinity, the phase duration should follow (17) and (19), respectively.

Decoding analysis: Firstly, we need to verify the decoding of transmitted data symbols $\mathbf{s}_{1,1}$ and $\mathbf{s}_{2,1}$ at the receiver R_1. This is enabled by the following cancellation:

$$\begin{bmatrix} \mathbf{y}_1^{\text{P-II}} - \mathbf{H}_{r,1}^{\text{P-II}}\mathbf{\Phi}_1\mathbf{y}_1^{\text{P-I}} \\ \mathbf{y}_1^{\text{P-IV}} - \mathbf{H}_{r,1}^{\text{P-IV}}\mathbf{\Pi}_2\mathbf{y}_1^{\text{P-III}} - \mathbf{H}_{r,1}^{\text{P-IV}}\mathbf{\Pi}_1\mathbf{H}_{r,2}^{\text{P-II}}\mathbf{\Phi}_1\mathbf{y}_1^{\text{P-I}} \end{bmatrix} = \underbrace{\begin{bmatrix} \mathbf{H}_{1,1}^{\text{P-II}} & \mathbf{H}_{2,1}^{\text{P-II}} \\ \mathbf{H}_{r,1}^{\text{P-IV}}\mathbf{\Pi}_1\mathbf{H}_{1,2}^{\text{P-II}} & \mathbf{H}_{r,1}^{\text{P-IV}}\mathbf{\Pi}_1\mathbf{H}_{2,2}^{\text{P-II}} \end{bmatrix}}_{\mathbf{H}_1'}\begin{bmatrix} \mathbf{s}_{1,1} \\ \mathbf{s}_{2,1} \end{bmatrix}, \tag{48}$$

where the rank of matrix $\mathbf{H}_1'$ is $\min\{N_1\tau_2 + \min\{N_1, R\}\tau_4, (N_1 + N_2)\tau_2, (M_1 + M_2)\tau_2, R\tau_2\}$, and the reason is given in Appendix C. Since $\min\{M_1 + M_2, R, N_1 + N_2\}\tau_2$ data symbols for R_1 are transmitted, to ensure the decoding, we shall follow that

$$\min\{M_1 + M_2, R, N_1 + N_2\}\tau_2 \le \min\{N_1\tau_2 + \min\{N_1, R\}\tau_4, (N_1 + N_2)\tau_2\}. \tag{49}$$

If $M_1 + M_2 \le N_1 + N_2$, (49) simplifies to the following:

$$\frac{\tau_2}{\tau_4} \le \frac{\min\{N_1, R\}}{\min\{M_1 + M_2 - N_1, R - N_1\}}. \tag{50}$$

Otherwise, if $N_1 + N_2 < M_1 + M_2$, (49) simplifies to the following:

$$\frac{\tau_2}{\tau_4} \le \frac{\min\{N_1, R\}}{\min\{N_2, R - N_1\}}. \tag{51}$$

Combining (50) and (51), we have the following:

$$\frac{\tau_2}{\tau_4} \leq \frac{\min\{N_1, R\}}{\min\{M_1 + M_2 - N_1, N_2, R - N_1\}}. \tag{52}$$

Then, multiplying (52) by (19), we have the following:

$$\frac{\tau_1}{\tau_4} \leq \frac{\min\{N_1, R\} N_2}{\min\{M_1 + M_2 - N_1, N_2, R - N_1\} \min\{N_1, R - N_2\}}. \tag{53}$$

Secondly, we need to verify the decoding of transmitted data symbols $\mathbf{s}_{1,2}$ and $\mathbf{s}_{2,2}$ at the receiver R_2, which is enabled by the following cancellation:

$$\begin{bmatrix} \mathbf{y}_2^{\text{P-III}} - \mathbf{H}_{r,2}^{\text{P-III}} \mathbf{\Phi}_2 \mathbf{y}_2^{\text{P-I}} \\ \mathbf{y}_2^{\text{P-IV}} - \mathbf{H}_{r,2}^{\text{P-IV}} \mathbf{\Pi}_1 \mathbf{y}_2^{\text{P-II}} - \mathbf{H}_{r,2}^{\text{P-IV}} \mathbf{\Pi}_2 \mathbf{H}_{r,1}^{\text{P-III}} \mathbf{\Phi}_2 \mathbf{y}_2^{\text{P-I}} \end{bmatrix} = \underbrace{\begin{bmatrix} \mathbf{H}_{1,2}^{\text{P-III}} & \mathbf{H}_{2,2}^{\text{P-III}} \\ \mathbf{H}_{r,2}^{\text{P-IV}} \mathbf{\Pi}_2 \mathbf{H}_{1,1}^{\text{P-III}} & \mathbf{H}_{r,2}^{\text{P-IV}} \mathbf{\Pi}_2 \mathbf{H}_{2,1}^{\text{P-III}} \end{bmatrix}}_{\mathbf{H}_2'} \begin{bmatrix} \mathbf{s}_{1,2} \\ \mathbf{s}_{2,2} \end{bmatrix}, \tag{54}$$

where the rank of matrix $\mathbf{H}_2'$ is $\min\{N_2 \tau_3 + \min\{N_1, R\} \tau_4, (N_1 + N_2) \tau_3, (M_1 + M_2) \tau_3, R \tau_3\}$, and the reason is given in Appendix C. Since $\min\{M_1 + M_2, R, N_1 + N_2\} \tau_3$ data symbols for R_2 are transmitted, to ensure the decoding, we shall follow that

$$\min\{M_1 + M_2, R, N_1 + N_2\} \tau_3 \leq \min\{N_2 \tau_3 + \min\{N_1, R\} \tau_4, (N_1 + N_2) \tau_3\}. \tag{55}$$

If $M_1 + M_2 \leq N_1 + N_2$, (55) simplifies to the following:

$$\frac{\tau_3}{\tau_4} \leq \frac{\min\{N_1, R\}}{\min\{M_1 + M_2 - N_2, R - N_2\}}. \tag{56}$$

Otherwise, if $N_1 + N_2 < M_1 + M_2$, (49) simplifies to the following:

$$\frac{\tau_3}{\tau_4} \leq \frac{\min\{N_1, R\}}{\min\{N_1, R - N_2\}}. \tag{57}$$

Combining (56) and (57), we have the following:

$$\frac{\tau_3}{\tau_4} \leq \frac{\min\{N_1, R\}}{\min\{M_1 + M_2 - N_2, N_1, R - N_2\}}. \tag{58}$$

Then, multiplying (58) by (17), we have the following:

$$\frac{\tau_1}{\tau_4} \leq \frac{\min\{N_1, R\} N_1}{\min\{M_1 + M_2 - N_2, N_1, R - N_2\} \min\{N_2, R - N_1\}}. \tag{59}$$

Achievable sum-SDoF analysis: As shown in the decoding analysis, two receivers can decode a total of $\min\{M_1 + M_2, R, N_1 + N_2\}(\tau_2 + \tau_3)$ data symbols over $\tau_1 + \tau_2 + \tau_3 + \tau_4$ time slots. This implies that the achievable sum-SDoF can be expressed as $\min\{M_1 + M_2, R, N_1 + N_2\}(\tau_2 + \tau_3)/(\tau_1 + \tau_2 + \tau_3 + \tau_4)$. According to the security and decoding analysis, the achievable sum-SDoF of proposed relay-aided jamming and two-receiver IA scheme is calculated through the following:

- If $N_2 < R$, we substitute (17), (19), and (53) with equality or (59) with equality into $(\min\{M_1 + M_2, R, N_1 + N_2\}(\tau_2 + \tau_3)/(\tau_1 + \tau_2 + \tau_3 + \tau_4)$ to derive the exact achievable sum-SDoF.
- If $N_1 < R \leq N_2$, we substitute (17), $\tau_2 = 0$, and (59) with equality into $\min\{M_1 + M_2, R, N_1 + N_2\}(\tau_2 + \tau_3)/(\tau_1 + \tau_2 + \tau_3 + \tau_4)$ to derive the exact achievable sum-SDoF.
- If $R \leq N_1$, we cannot ensure zero information leakage; hence, achievable sum-SDoF is zero.

The achievable sum-SDoF of proposed relay-aided jamming and two-receiver IA scheme is given in (4) for $N_2 < M_1 + M_2$ & $N_2 < R$ Case, $N_2 < M_1 + M_2$ & $N_1 < R \leq N_2$ Case, and $R \leq N_1$ Case.

5. Conclusions

We studied the sum-SDoF of the multiple-antenna full-duplex relay-aided MIMO XCCM with arbitrary antenna configurations, where there is no CSI at two transmitters and delayed CSI at the relay. To establish a sum-SDoF lower bound, we designed three transmission schemes. For the proposed schemes, full-duplex relay was utilized to receive the data symbol signals meanwhile transmit jamming signals, as this method can increase the transmission efficiency in contrast to half-duplex systems. We also derived a sum-SDoF upper bound. We characterized the sum-SDoF for $2N \leq R$ and $N \leq M$. We showed that the derived sum-SDoF lower bound can be higher than the sum-SDoF of the MIMO XCCM with output feedback and delayed CSIT for $2N \leq R$ and $M < N$, which is not attained by the MIMO XCCM with no CSIT. Therefore, a multiple-antenna full-duplex relay with delayed CSI is beneficial for the MIMO XCCM with no CSIT from the SDoF perspective. In the future, there are several directions to extend this work, which are as follows: (1) a better sum-SDoF upper bound; (2) the impact of cognitive messages at transmitters/receivers; (3) MIMO X networks with more than two receivers; (4) the impact of imperfect self-interference cancellation on sum-SDoF characterization; and (5) the analysis of error performance of proposed schemes for finite SNR.

Appendix A. The Rank of Matrices $\mathbf{A}_2$, $\mathbf{B}_2$

The matrix $\mathbf{A}_2$ can be decomposed into the following:

$$\underbrace{\begin{bmatrix} \mathbf{I}_{N_1 \tau_1} & \mathbf{0} \\ \mathbf{H}_{r,1}^{\text{P-II}} \boldsymbol{\Phi}_1 & \mathbf{0} \\ \mathbf{0} & \mathbf{I}_{N_1 \tau_3} \end{bmatrix}}_{\mathbf{A}_{2,1}} \underbrace{\begin{bmatrix} \mathbf{H}_{r,1}^{\text{P-I}} \\ \mathbf{H}_{r,1}^{\text{P-III}} \boldsymbol{\Phi}_2 \mathbf{H}_{r,2}^{\text{P-I}} \end{bmatrix}}_{\mathbf{A}_{2,2}},$$

where the rank of matrix $\mathbf{A}_{2,1}$ is $N_1(\tau_1 + \tau_3)$ by Gaussian elimination, and the rank of matrix $\mathbf{A}_{2,2}$ is $\min\{N_1 \tau_1 + \min\{R, N_1\} \tau_3, (N_1 + N_2)\tau_1, R\tau_1\}$, due to $\mathcal{RK} \mathbf{H}_{r,1}^{\text{P-I}} = \min\{N_1, R\}\tau_1$, $\mathcal{RK} \mathbf{H}_{r,2}^{\text{P-I}} = \min\{N_2, R\}\tau_1$, $\mathcal{RK} \boldsymbol{\Phi}_2 = \min\{R\tau_3, N_2\tau_1\}$, and $\mathcal{RK} \mathbf{H}_{r,1}^{\text{P-III}} = \min\{R, N_1\}\tau_3$. Therefore, the rank of matrix $\mathbf{A}_2$ is $\min\{N_1 \tau_1 + \min\{R, N_1\} \tau_3, (N_1 + N_2)\tau_1, R\tau_1\}$.

The matrix $\mathbf{B}_2$ can be decomposed into the following:

$$\underbrace{\begin{bmatrix} \mathbf{I}_{N_2 \tau_1} & \mathbf{0} \\ \mathbf{0} & \mathbf{I}_{N_2 \tau_2} \\ \mathbf{H}_{r,2}^{\text{P-III}} \boldsymbol{\Phi}_2 & \mathbf{0} \end{bmatrix}}_{\mathbf{B}_{2,1}} \underbrace{\begin{bmatrix} \mathbf{H}_{r,2}^{\text{P-I}} \\ \mathbf{H}_{r,2}^{\text{P-II}} \boldsymbol{\Phi}_1 \mathbf{H}_{r,1}^{\text{P-I}} \end{bmatrix}}_{\mathbf{B}_{2,2}},$$

where the rank of matrix $\mathbf{B}_{2,1}$ is $N_2(\tau_1 + \tau_2)$ by Gaussian elimination, and the rank of matrix $\mathbf{B}_{2,2}$ is $\min\{N_2\tau_1 + \min\{R, N_2\}\tau_2, (N_1 + N_2)\tau_1, R\tau_1\}$, due to $\mathcal{RK}\,\mathbf{H}_{r,2}^{\text{P-I}} = \min\{N_2, R\}\tau_1$, $\mathcal{RK}\,\mathbf{H}_{r,1}^{\text{P-I}} = \min\{N_1, R\}\tau_1$, $\mathcal{RK}\,\mathbf{\Phi}_1 = \min\{R\tau_2, N_1\tau_1\}$, and $\mathcal{RK}\,\mathbf{H}_{r,2}^{\text{P-II}} = \min\{R, N_2\}\tau_2$. Therefore, the rank of matrix $\mathbf{B}_2$ is $\min\{N_2\tau_1 + \min\{R, N_2\}\tau_2, (N_1 + N_2)\tau_1, R\tau_1\}$.

Appendix B. The Rank of Matrices $\mathbf{H}_1$

The matrix $\mathbf{H}_1$ can be decomposed into the following:

$$\underbrace{\begin{bmatrix} \mathbf{I}_{N_1\tau_2} & \mathbf{0} \\ \mathbf{0} & \mathbf{H}_{r,1}^{\text{P-IV}}\mathbf{\Pi}_1 \end{bmatrix}}_{\mathbf{H}_{1,1}} \underbrace{\begin{bmatrix} \mathbf{H}_{1,1}^{\text{P-II}} & \mathbf{H}_{2,1}^{\text{P-II}} \\ \mathbf{H}_{1,2}^{\text{P-II}} & \mathbf{H}_{2,2}^{\text{P-II}} \end{bmatrix}}_{\mathbf{H}_{1,2}},$$

where the rank of matrix $\mathbf{H}_{1,1}$ is $\min\{N_1\tau_2 + \min\{N_1, R\}\tau_4, (N_1 + N_2)\tau_2\}$, due to $\mathcal{RK}\,\mathbf{H}_{r,1}^{\text{P-IV}} = \min\{N_1, R\}\tau_4$ and $\mathcal{RK}\,\mathbf{\Pi}_1 = \min\{N_2\tau_2, \min\{N_1, R\}\tau_4\}$, and the rank of matrix $\mathbf{H}_{1,2}$ is $\min\{(N_1 + N_2)\tau_2, (M_1 + M_2)\tau_2, R\tau_2\}$, due to $\mathcal{RK}\,\mathbf{H}_{1,j}^{\text{P-II}} = \min\{N_j, M_1\}\tau_2, j = 1, 2$, and $\mathcal{RK}\,\mathbf{H}_{2,j}^{\text{P-II}} = \min\{M_2, R - M_1, N_1 + N_2 - M_1, N_j\}\tau_2, j = 1, 2$. Therefore, the rank of matrix $\mathbf{H}_1$ follows $\min\{N_1\tau_2 + \min\{N_1, R\}\tau_4, (N_1 + N_2)\tau_2, (M_1 + M_2)\tau_2, R\tau_2\}$. With $N_1 < M_1 + M_2 \leq N_2$, the rank of matrix $\mathbf{H}_1$ is $\min\{N_1\tau_2 + \min\{N_1\tau_4, R\tau_4\}, (M_1 + M_2)\tau_2, R\tau_2\}$.

Appendix C. The Rank of Matrices $\mathbf{H}_1'$ and $\mathbf{H}_2'$

The rank of matrix $\mathbf{H}_1'$ can be decomposed into the following:

$$\underbrace{\begin{bmatrix} \mathbf{I}_{N_1\tau_2} & \mathbf{0} \\ \mathbf{0} & \mathbf{H}_{r,1}^{\text{P-IV}}\mathbf{\Pi}_1 \end{bmatrix}}_{\mathbf{H}_{1,1}'} \underbrace{\begin{bmatrix} \mathbf{H}_{1,1}^{\text{P-II}} & \mathbf{H}_{2,1}^{\text{P-II}} \\ \mathbf{H}_{1,2}^{\text{P-II}} & \mathbf{H}_{2,2}^{\text{P-II}} \end{bmatrix}}_{\mathbf{H}_{1,2}'},$$

where the rank of matrix $\mathbf{H}_{1,1}'$ is $\min\{\min\{N_1, R\}\tau_4, (N_1 + N_2)\tau_2\}$, due to $\mathcal{RK}\,\mathbf{H}_{r,1}^{\text{P-IV}} = \min\{N_1, R\}\tau_4$ and $\mathcal{RK}\,\mathbf{\Pi}_1 = \min\{N_2\tau_2, \min\{N_1, R\}\tau_4\}$, and the rank of matrix $\mathbf{H}_{1,2}'$ is $\min\{(N_1 + N_2)\tau_2, (M_1 + M_2)\tau_2, R\tau_2\}$, due to $\mathcal{RK}\,\mathbf{H}_{1,j}^{\text{P-II}} = \min\{N_j, M_1\}\tau_2, j = 1, 2$, and $\mathcal{RK}\,\mathbf{H}_{2,j}^{\text{P-II}} = \min\{M_2, R - M_1, N_1 + N_2 - M_1, N_j\}\tau_2, j = 1, 2$. Therefore, the rank of matrix $\mathbf{H}_1'$ is $\min\{N_1\tau_2 + \min\{N_1, R\}\tau_4, (N_1 + N_2)\tau_2, (M_1 + M_2)\tau_2, R\tau_2\}$.

The rank of matrix $\mathbf{H}_2'$ can be decomposed into the following:

$$\underbrace{\begin{bmatrix} \mathbf{I}_{N_2\tau_3} & \mathbf{0} \\ \mathbf{0} & \mathbf{H}_{r,2}^{\text{P-IV}}\mathbf{\Pi}_2 \end{bmatrix}}_{\mathbf{H}_{2,1}'} \underbrace{\begin{bmatrix} \mathbf{H}_{1,1}^{\text{P-III}} & \mathbf{H}_{2,1}^{\text{P-III}} \\ \mathbf{H}_{1,2}^{\text{P-III}} & \mathbf{H}_{2,2}^{\text{P-III}} \end{bmatrix}}_{\mathbf{H}_{2,2}'},$$

where the rank of matrix $\mathbf{H}_{2,1}'$ is $\min\{\min\{N_1, R\}\tau_4, (N_1 + N_2)\tau_3\}$, due to $\mathcal{RK}\,\mathbf{H}_{r,2}^{\text{P-IV}} = \min\{N_1, R\}\tau_4$ and $\mathcal{RK}\,\mathbf{\Pi}_2 = \min\{N_1\tau_3, \min\{N_1, R\}\tau_4\}$, and the rank of matrix $\mathbf{H}_{2,2}'$ is $\min\{(N_1 + N_2)\tau_3, (M_1 + M_2)\tau_3, R\tau_3\}$, due to $\mathcal{RK}\,\mathbf{H}_{1,j}^{\text{P-III}} = \min\{N_j, M_1\}\tau_3, j = 1, 2$, and $\mathcal{RK}\,\mathbf{H}_{2,j}^{\text{P-III}} = \min\{M_2, R - M_1, N_1 + N_2 - M_1, N_j\}\tau_3, j = 1, 2$. Therefore, the rank of matrix $\mathbf{H}_2'$ is $\min\{N_2\tau_3 + \min\{N_1, R\}\tau_4, (N_1 + N_2)\tau_3, (M_1 + M_2)\tau_3, R\tau_3\}$.

References

1. Bloch, M.; Günlü, O.; Yener, A.; Oggier, F.; Poor, H.V.; Sankar, L.; Schaefer, R.F. An Overview of Information-Theoretic Security and Privacy: Metrics, Limits and Applications. *IEEE J. Sel. Areas Inf. Theory* **2021**, *2*, 5–22. [CrossRef]
2. Cao, P.L.; Oechtering, T.J. Optimal Transmit Strategies for Gaussian MISO Wiretap Channels. *IEEE Trans. Inf. Forensics Secur.* **2020**, *15*, 829–838. [CrossRef]
3. Wang, S.; Wen, M.; Xia, M.; Wang, R.; Hao, Q.; Wu, Y.C. Angle Aware User Cooperation for Secure Massive MIMO in Rician Fading Channel. *IEEE J. Sel. Areas Commun.* **2020**, *38*, 2182–2196. [CrossRef]

4. Xie, J.; Ulukus, S. Secure Degrees of Freedom of One-Hop Wireless Networks. *IEEE Trans. Inf. Theory* **2014**, *60*, 3359–3378. [CrossRef]

5. Banawan, K.; Ulukus, S. Secure degrees of freedom of the Gaussian MIMO interference channel. In Proceedings of the 2015 49th Asilomar Conference Signals, Systems Computers, Pacific Grove, CA, USA, 8–11 November 2015; pp. 40–44. [CrossRef]

6. Banawan, K.; Ulukus, S. Secure Degrees of Freedom Region of Static and Time-Varying Gaussian MIMO Interference Channel. *IEEE Trans. Inf. Theory* **2019**, *65*, 444–461. [CrossRef]

7. Wang, Q.; Wang, Y.; Wang, H. Secure Degrees of Freedom of the Asymmetric Gaussian MIMO Interference Channel. *IEEE Trans. Veh. Technol.* **2017**, *66*, 8001–8009. [CrossRef]

8. Wang, Z.; Xiao, M.; Skoglund, M.; Poor, H.V. Secure Degrees of Freedom of Wireless X Networks Using Artificial Noise Alignment. *IEEE Trans. Commun.* **2015**, *63*, 2632–2646. [CrossRef]

9. Wang, Q.; Zhang, T.; Dong, D.; Li, X. Secure Degrees of Freedom of Rank-Deficient BCCM and Rank-Deficient ICCM. *IEEE Trans. Veh. Technol.* **2020**, *69*, 4033–4041. [CrossRef]

10. Yang, S.; Kobayashi, M.; Piantanida, P.; Shamai, S. Secrecy Degrees of Freedom of MIMO Broadcast Channels with Delayed CSIT. *IEEE Trans. Inf. Theory* **2013**, *59*, 5244–5256. [CrossRef]

11. Mukherjee, P.; Tandon, R.; Ulukus, S. Secure Degrees of Freedom Region of the Two-User MISO Broadcast Channel with Alternating CSIT. *IEEE Trans. Inf. Theory* **2017**, *63*, 3823–3853. [CrossRef]

12. Lashgari, S.; Avestimehr, A.S. Secrecy DoF of Blind MIMOME Wiretap Channel with Delayed CSIT. *IEEE Trans. Inf. Forensics Secur.* **2018**, *13*, 478–489. [CrossRef]

13. Awan, Z.H.; Sezgin, A. Secure MISO Broadcast Channel: An Interplay Between CSIT and Network Topology. *IEEE J. Sel. Areas Inf. Theory* **2021**, *2*, 121–138. [CrossRef]

14. Zhang, T.; Ching, P.C. Secure MIMO Interference Channel with Confidential Messages and Delayed CSIT. In Proceedings of the ICASSP 2019—2019 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), Brighton, UK, 12–17 May 2019; pp. 2437–2441.

15. Zhang, T.; Wang, R. Secure Degrees-of-Freedom of the MIMO X Channel with Delayed CSIT. *IEEE Wirel. Commun. Lett.* **2021**, *10*, 1319–1323. [CrossRef]

16. Zhang, T.; Xu, Y.; Wang, S.; Wen, M.; Wang, R. On Secure Degrees of Freedom of the MIMO Interference Channel with Local Output Feedback. *IEEE Internet Things J.* **2021**, 8, 15334–15348. [CrossRef]

17. Zaidi, A.; Awan, Z.H.; Shamai, S.; Vandendorpe, L. Secure Degrees of Freedom of MIMO X-Channels with Output Feedback and Delayed CSIT. *IEEE Trans. Inf. Forensics Secur.* **2013**, *8*, 1760–1774. [CrossRef]

18. Wang, Z.; Xiao, M.; Wang, C.; Skoglund, M. Degrees of Freedom of Multi-Hop MIMO Broadcast Networks with Delayed CSIT. *IEEE Wirel. Commun. Lett.* **2013**, *2*, 1–4. [CrossRef]

19. Shin, W.; Lee, B.; Shim, B.; Lee, J. A MIMO Relay with Delayed Feedback Can Improve DoF in *K*- User MISO Interference Channel with No CSIT. *IEEE Trans. Veh. Technol.* **2016**, *65*, 10188–10192. [CrossRef]

20. Shin, W.; Lee, N.; Yang, H.; Lee, J. Relay-Aided Successive Aligned Interference Cancellation for Wireless X Networks with Full-Duplex Relays. *IEEE Trans. Veh. Technol.* **2017**, *66*, 421–432. [CrossRef]

21. Tian, Y.; Yener, A. Guiding Blind Transmitters: Degrees of Freedom Optimal Interference Alignment Using Relays. *IEEE Trans. Inf. Theory* **2013**, *59*, 4819–4832. [CrossRef]

22. Shin, W.; Lee, N.; Lee, J.; Poor, H.V. Relay-Aided Space-Time Beamforming for Interference Networks with Partial Channel Knowledge. *IEEE Trans. Signal Process.* **2016**, *64*, 5119–5130. [CrossRef]

23. Wang, Z.; Xiao, M.; Skoglund, M. Secrecy Degrees of Freedom of the $2 \times 2 \times 2$ Interference Channel with Delayed CSIT. *IEEE Wirel. Commun. Lett.* **2014**, *3*, 341–344. [CrossRef]

24. Debaillie, B.; van den Broek, D.J.; Lavín, C.; van Liempd, B.; Klumperink, E.A.M.; Palacios, C.; Craninckx, J.; Nauta, B.; Pärssinen, A. Analog/RF Solutions Enabling Compact Full-Duplex Radios. *IEEE J. Sel. Areas Commun.* **2014**, *32*, 1662–1673. [CrossRef]

25. Yilan, M.; Ayar, H.; Nawaz, H.; Gurbuz, O.; Tekin, I. Monostatic Antenna In-Band Full Duplex Radio: Performance Limits and Characterization. *IEEE Trans. Veh. Technol.* **2019**, *68*, 4786–4799. [CrossRef]

26. Zhang, Z.; Long, K.; Vasilakos, A.V.; Hanzo, L. Full-Duplex Wireless Communications: Challenges, Solutions, and Future Research Directions. *Proc. IEEE* **2016**, *104*, 1369–1409. [CrossRef]

27. Duarte, M.; Dick, C.; Sabharwal, A. Experiment-Driven Characterization of Full-Duplex Wireless Systems. *IEEE Trans. Wirel. Commun.* **2012**, *11*, 4296–4307. [CrossRef]

28. Chung, M.; Sim, M.S.; Kim, J.; Kim, D.K.; Chae, C.b. Prototyping real-time full duplex radios. *IEEE Commun. Mag.* **2015**, *53*, 56–63. [CrossRef]

29. Duarte, M.; Sabharwal, A.; Aggarwal, V.; Jana, R.; Ramakrishnan, K.K.; Rice, C.W.; Shankaranarayanan, N.K. Design and Characterization of a Full-Duplex Multiantenna System for WiFi Networks. *IEEE Trans. Veh. Technol.* **2014**, *63*, 1160–1177. [CrossRef]

30. Telatar, E. Capacity of multi-antenna Gaussian channels. *Eur. Trans. Telecommun.* **1999**, *10*, 585–595. [CrossRef]