Information Leakage Neutralization for the Multi-Antenna Non-Regenerative Relay-Assisted Multi-Carrier Interference Channel

Zuleita Ho *Member, IEEE*, Eduard Jorswieck *Senior Member, IEEE* and Sabrina Gerbracht

***Abstract*— In heterogeneous dense networks where spectrum is shared, users privacy remains one of the major challenges. On a multi-antenna relay-assisted multi-carrier interference channel, each user shares the spectral and spatial resources with all other users. When the receivers are not only interested in their own signals but also in eavesdropping other users' signals, the cross talk on the spectral and spatial channels becomes information leakage. In this paper, we propose a novel secrecy rate enhancing relay strategy that utilizes both spectral and spatial resources, termed as *information leakage neutralization*. To this end, the relay matrix is chosen such that the effective channel from the transmitter to the colluding eavesdropper is equal to the negative of the effective channel over the relay to the colluding eavesdropper and thus the information leakage to zero. Interestingly, the optimal relay matrix in general is not block-diagonal which encourages users' encoding over the frequency channels. We proposed two information leakage neutralization strategies, namely *efficient information leakage neutralization* (EFFIN) and *local-optimized information leakage neutralization* (LOPTIN). EFFIN provides a simple and efficient design of relay processing matrix and precoding matrices at the transmitters in the scenario of limited power and computational resources. LOPTIN, despite its higher complexity, provides a better sum secrecy rate performance by optimizing the relay processing matrix and the precoding matrices jointly. The proposed methods are shown to improve the sum secrecy rates over several state-of-the-art baseline methods.**

***Index Terms*— Interference relay channel; Interference neutralization; Non-potent relay; Full-duplex relay; Amplify-and-forward relay; secrecy rate; worst-case secrecy rate; frequency selective; multi-antenna systems; colluding eavesdroppers**

I. Introduction

The trend of future wireless network systems is towards spectrum sharing over different wireless infrastructures such as LTE networks, smart grid sensor networks and WiMAX networks. With isolated wireless infrastructures, such as multiple non-cooperating LTE cells (as shown in Figure 1), ensuring data security remains a major technical challenge. While cryptography techniques are employed in most established communication standards, physical layer security techniques provide an alternative approach when the communicating front-ends are of limited computation capability and are not able to carry out standard cryptography methods such as symmetric key and asymmetric key encryption. These applications include but are not limited to ubiquitous or pervasive computing [2].

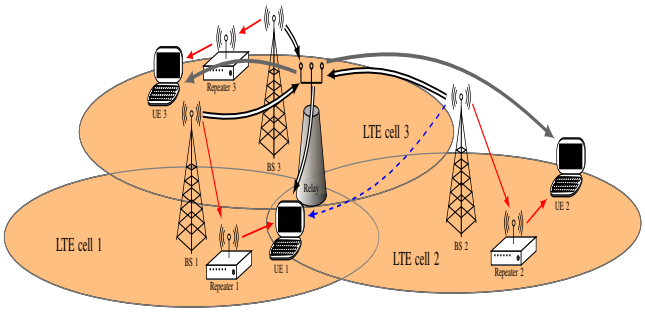


Fig. 1. Three overlapping LTE cells. The sum secrecy rates over the cells can be improved if a smart multi-antenna relay is introduced into the system. The emphasized arrows from BS 1 to the smart relay in the middle and then to UE 1 illustrate that desired signal strength (together with the direct channel path in red) can be boosted by choosing an appropriate relay strategy. The emphasized arrows from BS 2 to the smart relay and then to UE 1 illustrate that information leakage (shown by a dashed arrow in blue) can be neutralized by choosing the relay strategy appropriately.

With the high demand of wireless applications in recent years, the issues of communication security become ever more important. Physical layer security techniques [3]–[5] provide an additional protection to the conventional secure transmission methods using cryptography. As early as four decades ago, the seminal work on the secrecy capacity on the wire-tap channel [6] - the most fundamental model consisting of one source node, one destination node and one eavesdropper - started the era of research on physical layer security. Extensive analysis and designs have been conducted ever since; physical layer security results can be found in [3]–[5] and recent tutorial papers [7], [8].

With advantages such as increased cell coverage and transmission rates, relays are incorporated into the standards of current wireless infrastructures. The wireless resources in these systems are frequently shared by many users/subscribers and a potential malicious user in the system can lead to compromised confidentiality. Many novel strategies have been proposed to improve the secrecy in

The authors are with Institut für Nachrichtentechnik, Fakultät Elektro- und Informationstechnik, Technische Universität Dresden, Germany. ({zuleita.ho, eduard.jorswieck, Sabrina.Gerbracht}@tu-dresden.de)

A conference version of this paper is published in [1].

Manuscript received Sept. 17, 2012; revised Mar. 11, 2013; accepted Apr. 29, 2013. The editor coordinating the review of this paper and approving it for publication was Prof. Larry Milstein.

This work has been performed in the framework of the European research project DIWINE, which is partly funded by the European Union under its FP7 ICT Objective 1.1 - The Network of the Future.

This work is supported in part by the German Research Foundation (DFG) in the Collaborative Research Center 912 "Highly Adaptive Energy-Efficient Computing".

- relay systems, including cooperative jamming (CJ) [9]–[11], noise-forwarding (NF) [12], a mixture of CJ and NF [13], signal-forwarding strategies such as amplify-and-forward (AF) and decode-and-forward (DF) [14]–[16][1].
- multi-carrier systems [20]–[22] and multi-carrier relay systems with external eavesdropper(s) [15], [23].

Yet, a joint optimization of secrecy rates over the frequency-spatial resources in a relay-assisted multi-user interference channel (with internal eavesdroppers) remains an open problem, as considered here.

We assume that the relay employs an amplify-and-forward (AF) strategy which provides flexibility in implementation as the relay is transparent to the modulation and coding schemes and induces negligible signal processing delays [24]. The novel notion of *relay-without-delays*, also known as instantaneous relays if the relays are memoryless [25]–[28], refers to relays that forward signals consisting of both current symbol and symbols in the past, instead of only the past symbols as in conventional relays. As shown in Figure 2, the instantaneous relay models a layer-1 repeaters connected networks (such as LTE network and WiMAX networks [29]) and helps us analyze the system performance of nowadays repeaters connected networks[2].

In order to provide secure transmission over relay-assisted multi-carrier networks, we propose a relay strategy termed as *information leakage neutralization* which by choosing relay forwarding strategies algebraically neutralizes information leakage from each transmitter in the network to each eavesdropper on each frequency subcarrier. This method is adopted from a technique on relay networks, termed as interference neutralization (IN). IN has been applied to eliminate interference in various single-carrier systems, such as deterministic channels [31], [32], two-hop relay channels [24], [33], [34] and instantaneous relay channels [35]. Our prior work shows that IN is effective in improving secrecy rates in a two-hop wiretap channel [36]. Information leakage neutralization differs from previous works above as shown in the following.

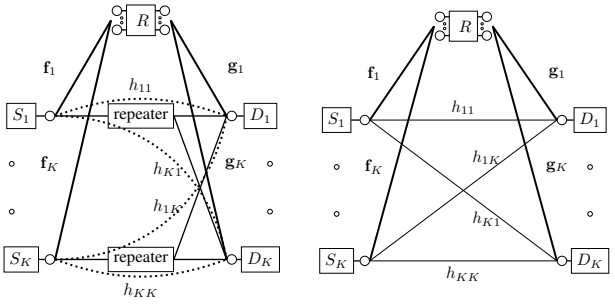
- Conventional physical layer security methods that rely on the confusion of eavesdroppers, such as artificial noise forwarding, require additional wiretap codes for protection [37]. Information leakage neutralization ensures secrecy by setting the equivalent leakage channel to zero and thus does not require an additional wiretap code. Moreover, information leakage neutralization offers an additional advantage of desired signal power amplification which is not taken into consideration in artificial noise forwarding methods.
- Information leakage neutralization provides a systematic way of optimizing the secrecy rates by simplifying the highly non-convex secrecy rates expression to a conventional single log-determinant function. In the scenarios of high SNR or strong information leakage, the secrecy rates are maximized when the information leakage is zero which is guaranteed by the information leakage neutralization.
- With the assumption of colluding eavesdroppers and multiple antennas at the relay, the neutralization proposed here over multi-carrier systems is of significantly higher complexity than the single-carrier system in the previous works [35], [36].
- The problem of information leakage neutralization is fundamentally different from interference neutralization. This can be realized in a simple example. Assume that we have two transmitter-receiver pairs. Transmitter one transmits only on the first subcarrier whereas the second transmitter only transmits on the second subcarrier. In interference neutralization, no work needs to be done because there is no interference. However, for information leakage neutralization, the relay must neutralize the leakage of user one's signal on subcarrier one at the second receiver. Hence, the problem studied here differs from [35].

The contributions and outline of this manuscript are summarized as follows:

- We transform a general and complicated sum secrecy rate optimization problem on a relay-assisted multi-carrier interference channel with mutually eavesdropping users to an optimization-ready formulation. Systematic optimization techniques can then be applied to solve for the sum-secrecy-rate-optimal relay strategies and precoding matrices at the transmitters. The achievable secrecy sum rate function of the aforementioned multi-carriers system is significantly different from the single-carrier problem in our previous work [35].
- An illustrative example is given in Section II-A for a basic setting to highlight the efficiency of information leakage neutralization.
- We propose a novel idea of information leakage neutralization strategies in Section III-A. These strategies neutralize information leakage from each user to its colluding eavesdroppers on each frequency-spatial channel. The resulting secrecy rate expression is significantly simplified. Detailed analyzes for the multi-carrier information leakage neutralization methods are provided. In particular, the minimum number of antennas at the relay for complete information leakage neutralization is computed in Proposition 1. The required number of antennas depends on the number of data streams sent by each user, the number of frequency subcarriers and the number of users in the system. Relevant to applications where relay power must be reserved, the minimum power at the relay required for information leakage neutralization is computed in Proposition 2.
- We propose an efficient and simple information leakage neutralization strategy (EFFIN) which ensures secure transmissions in the scenarios of limited power

[1]All aforementioned works assume that the relays are cooperative and trusted. For secure transmission strategies with untrusted relays, please refer to [17]–[19].

[2]In modern networks such as LTE, wireless links are often connected using boosters or layer-1 repeaters (simple amplifiers) [30]. If the time consumed for the signals to travel from a source to a repeater or from a repeater to a destination is counted as one unit, then the total time for the signal to travel from a source to a destination is two units - the same amount of time for the signal to travel from a source through a smart AF relay to a destination.



(a) a relay-assisted network (b) instantaneous relay network

Fig. 2. The wireless relay-assisted network with layer one repeaters and one smart relay is shown in subfigure (a). The dotted lines demonstrate the equivalent links between a source and a destination taking into account the presence of the repeaters. All paths from source to destination nodes take two time slots (through either the smart relay or repeaters). The equivalent channel is established in subfigure (b) by replacing the relay as an instantaneous relay. Information going through the instantaneous relay arrives at the destinations at the same time as over the direct links.

and computational resources at relay and transmitters. With sufficient power at the relay, we propose an local-optimized information leakage neutralization technique (LOPTIN) to maximize the secrecy rates while ensuring zero information leakage.

- The achievable secrecy rates from proposed strategies EFFIN and LOPTIN are compared to several baseline strategies by numerical simulations in Section V. Baseline 1 is a scenario where the relay is a layer-1 repeater and baseline 2 is a scenario with no relay. Simulation results show that the proposed strategies outperform the baseline strategies significantly in various operating SNRs.

A. Notations

The set $\mathbb{C}^{a\times b}$ denotes a set of complex matrices of size a by b and is shortened to $\mathbb{C}^a$ when $a = b$. The notation $\mathcal{N}(\mathbf{A})$ is the null space of $\mathbf{A}$. The operator $\otimes$ denotes the Kronecker product. The superscripts $^{\mathrm{T}}$, $^{\mathrm{H}}$, † represent transpose, Hermitian transpose and Moore-Penrose inverse respectively whereas the superscript * denotes the conjugation operation. The Euclidean norm for scalars is written as $|.|$. The trace of matrix $\mathbf{A}$ is denoted as $\mathrm{tr}(\mathbf{A})$. Vectorization stacks the columns of a matrix $\mathbf{A}$ to form a long column vector denoted as $\mathrm{vec}(\mathbf{A})$. The function $\mathcal{C}(\mathbf{A})$ denotes the log- determinant function of matrix $\mathbf{A}$, $\log_2 \det(\mathbf{A})$. The identity and zero matrices of dimension $K \times K$ are written as $\mathbf{I}_K$ and $\mathbf{0}_K$. The vector $\mathbf{e}_i$ represents a column vector with zero elements everywhere and one at the i-th position. The notation $[\mathbf{A}]_{ml}$ denotes the m-th row and l-th column element of the matrix $\mathbf{A}$. The notation $\mathbf{p}_{a:b}$, $0 \le a \le b \le n$, denotes a vector which has elements $[p_a, p_{a+1}, \ldots, p_b]$ where $\mathbf{p} = [p_1, \ldots, p_n]$.

II. System Model

In the following subsection, we give an example of an interference relay channel with two transmitter-receiver pairs where the relay has two antennas and all nodes share two frequency subcarriers. We shall illustrate that the conventional assumption of block diagonal relay matrix (which maximizes achievable rates in peaceful systems) cannot be adopted a-priori when secrecy rates are considered.

A. An example of two transmitters on two frequencies with two antennas at the relay

Transmitter (TX) i, $i = 1, 2$, transmits symbols $\mathbf{x}_i \in \mathbb{C}^{M\times 1}$ which are spread over M frequency subcarriers by precoding matrix $\mathbf{P}_i$. For the ease of notation, we assume that the precoding matrix $\mathbf{P}_i$ is a square matrix $\mathbf{P}_i \in \mathbb{C}^M$. When TX i transmits $S_i \le M$ symbols, then zeros are padded in $\mathbf{x}_i$ so that its dimension is always $M \times 1$ and correspondingly zero columns are padded in $\mathbf{P}_i$. We assume that the TXs do not overload the system and therefore S_i is smaller than or equal to the number of frequency subcarriers, here two. Note that $\mathbf{P}_i$ may have low row rank when certain subcarriers are not used. For example, if TX i transmits one symbol on subcarrier 1 but nothing on subcarrier 2, then $\mathbf{P}_i = [a, 0; 0, 0]$ for some complex scalar a. If $\mathbf{P}_i$ is diagonal, then each symbol is only sent on one frequency. Denote the m-th transmit symbol of TX i as $\mathbf{x}_i(m)$ which is randomly generated, mutually independent and with covariance matrix $\mathbf{I}_2$. The precoding matrix $\mathbf{P}_i$ satisfies the transmit power constraint of TX i: $\mathrm{tr}\left(\mathbf{P}_i \mathbf{P}_i^{\mathrm{H}}\right) \le P_i^{max}$. Denote the channel gain from transmitter i to receiver (RX) j on frequency m as $h_{ji}(m)$. For simplicity of the example, we let S_i equal two. The received signal of TX i is a vector whose m-th element is the received signal on the m-th frequency subcarrier,

$$\mathbf{y}_i = \begin{bmatrix} \mathbf{y}_i(1) \\ \mathbf{y}_i(2) \end{bmatrix} = \sum_{j=1}^{2} \begin{bmatrix} h_{ij}(1) & 0 \\ 0 & h_{ij}(2) \end{bmatrix} \mathbf{P}_j \begin{bmatrix} x_j(1) \\ x_j(2) \end{bmatrix} + \begin{bmatrix} n_i(1) \\ n_i(2) \end{bmatrix}.$$

The circular Gaussian noise with unit variance received on the m-th subcarrier at RX i is denoted as $n_i(m)$. If a relay with two antennas is introduced into the system, it receives the broadcasting signal from TXs and forwards them to RXs. We denote the received signal at the relay as a stacked vector of the received signal at each frequency m, with $\mathbf{y}_r(m) \in \mathbb{C}^{2\times 1}$ representing the received signal on frequency m and the a-th element in $\mathbf{y}_r(m)$ representing the signal at the a-th antenna:

$$\mathbf{y}_r = \begin{bmatrix} \mathbf{y}_r(1) \\ \mathbf{y}_r(2) \end{bmatrix} = \sum_{j=1}^{2} \begin{bmatrix} \mathbf{f}_j(1) & \mathbf{0}_{2\times 1} \\ \mathbf{0}_{2\times 1} & \mathbf{f}_j(2) \end{bmatrix} \mathbf{P}_j \begin{bmatrix} x_j(1) \\ x_j(2) \end{bmatrix} + \begin{bmatrix} \mathbf{n}_r(1) \\ \mathbf{n}_r(2) \end{bmatrix}$$

where $\mathbf{n}_r(m) \in \mathbb{C}^{2\times 1}$ is a circular Gaussian noise vector received at frequency m with identity covariance matrix and $\mathbf{f}_j(m)$ is the complex vector channel from TX j to the relay on frequency m. The relay processes the received signal $\mathbf{y}_r$ by a multiplication of matrix $\mathbf{R} \in \mathbb{C}^4$ and forwards the signal to the RXs. Denote the channel from relay to RX i on frequency

m by $\mathbf{g}_i(m) \in \mathbb{C}^{2\times 1}$. At RX i, the received signal is

$$\mathbf{y}_i = \sum_{j=1}^{2} \left(\begin{bmatrix} h_{ij}(1) & 0 \\ 0 & h_{ij}(2) \end{bmatrix} + \begin{bmatrix} \mathbf{g}_i^{\mathrm{H}}(1) & \mathbf{0}_{1\times 2} \\ \mathbf{0}_{1\times 2} & \mathbf{g}_i^{\mathrm{H}}(2) \end{bmatrix} \mathbf{R} \begin{bmatrix} \mathbf{f}_j(1) & \mathbf{0}_{2\times 1} \\ \mathbf{0}_{2\times 1} & \mathbf{f}_j(2) \end{bmatrix} \right) \mathbf{P}_j \begin{bmatrix} x_j(1) \\ x_j(2) \end{bmatrix} + \begin{bmatrix} \mathbf{g}_i^{\mathrm{H}}(1) & \mathbf{0}_{1\times 2} \\ \mathbf{0}_{1\times 2} & \mathbf{g}_i^{\mathrm{H}}(2) \end{bmatrix} \mathbf{R} \begin{bmatrix} \mathbf{n}_r(1) \\ \mathbf{n}_r(2) \end{bmatrix} + \begin{bmatrix} n_i(1) \\ n_i(2) \end{bmatrix}.$$

Denote channel matrices

$$\mathbf{H}_{ij} = \begin{bmatrix} h_{ij}(1) & 0 \\ 0 & h_{ij}(2) \end{bmatrix}, \ \mathbf{G}_i^{\mathrm{H}} = \begin{bmatrix} \mathbf{g}_i^{\mathrm{H}}(1) & \mathbf{0}_{1\times 2} \\ \mathbf{0}_{1\times 2} & \mathbf{g}_i^{\mathrm{H}}(2) \end{bmatrix}, \ \mathbf{F}_j = \begin{bmatrix} \mathbf{f}_j(1) & \mathbf{0}_{2\times 1} \\ \mathbf{0}_{2\times 1} & \mathbf{f}_j(2) \end{bmatrix},$$

and the equivalent channel from TX j to RX i as

$$\bar{\mathbf{H}}_{ij} = \mathbf{H}_{ij} + \mathbf{G}_i^{\mathrm{H}} \mathbf{R} \mathbf{F}_j . \tag{1}$$

With circular Gaussian transmit symbols $\mathbf{x}_i$, the following rate of TX-RX pair 1 is achievable,

$$r_1(\mathbf{R}) = \mathcal{C}\left(\mathbf{I}_2 + \bar{\mathbf{H}}_{11} \mathbf{P}_1 \mathbf{P}_1^{\mathrm{H}} \bar{\mathbf{H}}_{11}^{\mathrm{H}} \cdot \mathbf{\Xi}_1^{-1} \right) \tag{2}$$

where $\mathbf{\Xi}_1$ is the covariance of the interference and noise $\mathbf{\Xi}_1 = \bar{\mathbf{H}}_{12} \mathbf{P}_2 \mathbf{P}_2^{\mathrm{H}} \bar{\mathbf{H}}_{12}^{\mathrm{H}} + \mathbf{G}_1^{\mathrm{H}} \mathbf{R} \mathbf{R}^{\mathrm{H}} \mathbf{G}_1 + \mathbf{I}_2$. Consider that RX 2 is an eavesdropper. We compute the worst-case scenario in which RX 2 decodes all other symbols perfectly before decoding the messages from TX 1 and RX 2 sees a multiple-input-multiple-output (MIMO) channel and decodes messages $x_1(1)$ and $x_1(2)$ utilizing both frequencies (with a minimum-mean-squared-error (MMSE) receive filter for example) in (3) at the top of next page. An achievable rate is then $r_{2\leftarrow 1}(\mathbf{R}) = \mathcal{C}\left(\mathbf{I}_2 + \bar{\mathbf{H}}_{21} \mathbf{P}_1 \mathbf{P}_1^{\mathrm{H}} \bar{\mathbf{H}}_{21}^{\mathrm{H}} \left(\mathbf{G}_2^{\mathrm{H}} \mathbf{R} \mathbf{R}^{\mathrm{H}} \mathbf{G}_2 + \mathbf{I}_2 \right)^{-1} \right)$. An achievable secrecy rate of TX-RX pair 1 is then its achievable rate $r_1(\mathbf{R})$ minus the leakage rate to RX 2 $r_{2\leftarrow 1}(\mathbf{R})$ [38]:

$$r_1^s(\mathbf{R}) = \left(r_1(\mathbf{R}) - r_{2\leftarrow 1}(\mathbf{R}) \right)^+ \tag{4}$$

The relay processing matrix is defined as

$$\mathbf{R} = \begin{bmatrix} \mathbf{R}_{11} & \mathbf{R}_{12} \\ \mathbf{R}_{21} & \mathbf{R}_{22} \end{bmatrix} \tag{5}$$

where each submatrix block $\mathbf{R}_{mn}$ forwards signals from frequency n to frequency m. In a peaceful MIMO interference relay channel, $\mathbf{R}$ bares a block diagonal structure, $\mathbf{R}_{12} = \mathbf{R}_{21} = \mathbf{0}_2$. The intuition is that relays should not generate cross talk over frequency channels. However, it is not trivial to examine the effect of $\mathbf{R}_{12}$ and $\mathbf{R}_{21}$ on secrecy rates as illustrated below and the conventional block diagonal structure should not be a-priori assumed.

As a numerical example, we compute the secrecy rates with the following randomly generated channels given in Table I.

The values are generated with Gaussian distribution with zero mean and unit variance. We set the precoding matrices of TX 1 and TX 2 to be

$$\mathbf{P}_1 = \begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix}, \quad \mathbf{P}_2 = \begin{bmatrix} 1 & 4 \\ -4 & 1 \end{bmatrix}$$

which means that TX 1 transmits only one data stream on both subcarriers and TX 2 transmits two data streams spread over both frequency subcarriers with orthogonal sequences. With relay matrix $\mathbf{R}^{\mathrm{IN}}$ (see Table I) a sum secrecy rate of 3.4104 is achievable whereas with block diagonal matrix $\mathbf{R}^{\mathrm{IN},d}$ the sum secrecy rate is 3.1881. A block diagonal relay matrix does not always improve secrecy rate and therefore in the following we assume a general non-block-diagonal structure $\mathbf{R}$. In fact, the relay matrix $\mathbf{R}^{\mathrm{IN}}$ is chosen such that the secrecy leakage is zero: $(\mathbf{H}_{12} + \mathbf{G}_1^{\mathrm{H}} \mathbf{R} \mathbf{F}_2) \mathbf{P}_2 = \mathbf{0}$ and $(\mathbf{H}_{21} + \mathbf{G}_2^{\mathrm{H}} \mathbf{R} \mathbf{F}_1) \mathbf{P}_1 = \mathbf{0}$. Thus, the secrecy rate from (4) can be simplified to

$$r_1^s = \mathcal{C}\left(\mathbf{I}_2 + \bar{\mathbf{H}}_{11} \mathbf{P}_1 \mathbf{P}_1^{\mathrm{H}} \bar{\mathbf{H}}_{11}^{\mathrm{H}} \left(\mathbf{G}_1^{\mathrm{H}} \mathbf{R} \mathbf{R}^{\mathrm{H}} \mathbf{G}_1 + \mathbf{I}_2 \right)^{-1} \right).$$

where $\bar{\mathbf{H}}_{11}$ is defined in (1).

This motivates our following proposition on information leakage neutralization techniques. Interestingly, with information leakage neutralization, we can simplify the optimization problem significantly. The idea is to set the information leakage from each TX at each frequency to zero, in particular, by setting the equivalent channel of $\mathbf{x}_1$ from TX 1 to RX 2 and vice versa in (3) to zero,

$$\begin{cases} \left(\mathbf{H}_{12} + \mathbf{G}_1^{\mathrm{H}} \mathbf{R} \mathbf{F}_2 \right) \mathbf{P}_2 = \mathbf{0} \\ \left(\mathbf{H}_{21} + \mathbf{G}_2^{\mathrm{H}} \mathbf{R} \mathbf{F}_1 \right) \mathbf{P}_1 = \mathbf{0} . \end{cases} \tag{6}$$

With the properties of the Kronecker product, (6) can be written as

$$\mathbf{B} \, \mathrm{vec}(\mathbf{R}) = \mathbf{b} . \tag{7}$$

where $\mathbf{B} = \left[(\mathbf{F}_2 \mathbf{P}_2)^{\mathrm{T}} \otimes \mathbf{G}_1^{\mathrm{H}}; (\mathbf{F}_1 \mathbf{P}_1)^{\mathrm{T}} \otimes \mathbf{G}_2^{\mathrm{H}} \right]$ and $\mathbf{b} = -\left[\mathrm{vec}(\mathbf{H}_{12} \mathbf{P}_2); \mathrm{vec}(\mathbf{H}_{21} \mathbf{P}_1) \right]$. The stacked matrix $\mathbf{B}$ in the above equation is a fat matrix[3]. We obtain the relay matrix that can perform information leakage neutralization:

$$\mathrm{vec}(\mathbf{R}) = \mathbf{B}^{\mathrm{H}} \left(\mathbf{B} \mathbf{B}^{\mathrm{H}} \right)^{-1} \mathbf{b} . \tag{8}$$

Substitute the channel realizations in Table I into the above equation and reverse the vectorization operation, we obtain the relay matrix $\mathbf{R}^{\mathrm{IN}}$ (please refer to the table for numerical values).

Remark 1: If the precoding matrices $\{\mathbf{P}_i\}$ are invertible, then the relay matrix $\mathbf{R}$ obtained using (8) is block diagonal. A block diagonal relay matrix means that the relay sets cross talk over frequency subcarriers to zero and due to the interference leakage neutralization, the interference from TXs on the same frequency is also zero. This results in KM parallel channels without interference. We propose in Section IV-A a suboptimal but very efficient algorithm which optimizes the achievable rates in this case[4].

In fact, the matrix in (8) is not unique, any matrix which is a sum of $\mathrm{vec}(\mathbf{R})$ in (8) and a vector in the null space of $\mathbf{B}$ can

[3]Care must be taken when users send less than M data streams (when $\mathbf{P}_i$ has zero columns. More discussion is provided later in Proposition 2).

[4]The achievable rates here are secrecy rates as the information leakage is zero.

$$\begin{aligned}\mathbf{y}_{2\leftarrow 1} = &\left(\begin{bmatrix} h_{21}(1) & 0 \\ 0 & h_{21}(2) \end{bmatrix} + \begin{bmatrix} \mathbf{g}_2^{\mathrm{H}}(1) & \mathbf{0}_{1\times 2} \\ \mathbf{0}_{1\times 2} & \mathbf{g}_2^{\mathrm{H}}(2) \end{bmatrix} \mathbf{R} \begin{bmatrix} \mathbf{f}_1(1) & \mathbf{0}_{2\times 1} \\ \mathbf{0}_{2\times 1} & \mathbf{f}_1(2) \end{bmatrix}\right) \mathbf{P}_1 \begin{bmatrix} x_1(1) \\ x_1(2) \end{bmatrix} \\ &+ \begin{bmatrix} \mathbf{g}_2^{\mathrm{H}}(1) & \mathbf{0}_{1\times 2} \\ \mathbf{0}_{1\times 2} & \mathbf{g}_2^{\mathrm{H}}(2) \end{bmatrix} \mathbf{R} \begin{bmatrix} \mathbf{n}_r(1) \\ \mathbf{n}_r(2) \end{bmatrix} + \begin{bmatrix} n_2(1) \\ n_2(2) \end{bmatrix}\end{aligned} \tag{3}$$

TABLE I

RANDOMLY GENERATED CHANNEL REALIZATIONS FOR A TWO USER TWO FREQUENCY INTERFERENCE RELAY CHANNEL WITH TWO ANTENNAS AT RELAY AND SINGLE ANTENNA AT TXS AND RXS.

$$\mathbf{H}_{11} = \begin{bmatrix} 0.5129+0.4605i & 0 \\ 0 & 0.3504+0.0950i \end{bmatrix}, \quad \mathbf{H}_{21} = \begin{bmatrix} 0.4337+0.0709i & 0 \\ 0 & 0.1160+0.0078i \end{bmatrix}$$

$$\mathbf{H}_{12} = \begin{bmatrix} 0.3693+0.0336i & 0 \\ 0 & 0.1922+0.4714i \end{bmatrix}, \quad \mathbf{H}_{22} = \begin{bmatrix} 0.1449+0.0718i & 0 \\ 0 & 0.6617+0.0432i \end{bmatrix}$$

$$\mathbf{G}_1 = \begin{bmatrix} 0.4460+0.5281i & 0 \\ 0.5083+0.5729i & 0 \\ 0 & 0.3608+0.1733i \\ 0 & 0.3365+0.0861i \end{bmatrix}, \quad \mathbf{G}_2 = \begin{bmatrix} 0.3933+0.0111i & 0 \\ 0.8044+0.2331i & 0 \\ 0 & 0.9339+0.7859i \\ 0 & 0.2268+0.4107i \end{bmatrix}$$

$$\mathbf{F}_1 = \begin{bmatrix} 0.1194+0.8624i & 0 \\ 0.6344+0.1582i & 0 \\ 0 & 0.6012+0.6261i \\ 0 & 0.1176+0.8351i \end{bmatrix}, \quad \mathbf{F}_2 = \begin{bmatrix} 0.9404+0.2720i & 0 \\ 0.4156+0.9280i & 0 \\ 0 & 0.9213+0.8129i \\ 0 & 0.5420+0.1664i \end{bmatrix}$$

$$\mathbf{R}^{\mathrm{IN}} = \begin{bmatrix} -0.0364-0.0035i & -0.1793-0.0233i & 0.0234-0.0575i & 0.0574+0.0596i \\ -0.1046+0.0925i & -0.2837-0.0390i & -0.0832-0.0249i & 0.0029+0.1567i \\ 0.2729+0.0708i & -0.1376+0.1714i & -0.3130-0.2977i & 0.2012-0.1606i \\ 0.0529+0.0099i & -0.1388+0.0348i & -0.4690-0.3154i & -0.0414-0.1751i \end{bmatrix}$$

$$\mathbf{R}^{\mathrm{IN},d} = \begin{bmatrix} -0.0364-0.0035i & -0.1793-0.0233i & 0 & 0 \\ -0.1046+0.0925i & -0.2837-0.0390i & 0 & 0 \\ 0 & 0 & -0.3130-0.2977i & 0.2012-0.1606i \\ 0 & 0 & -0.4690-0.3154i & -0.0414-0.1751i \end{bmatrix}$$

$$\mathbf{R}^{\mathrm{IN},z} = \begin{bmatrix} -0.2709+0.2267i & -0.0820+0.1738i & -0.0770+0.0704i & -0.1357+0.1183i \\ -0.1509+0.0212i & -0.3225-0.4885i & -0.2088-0.0485i & 0.6810+0.1046i \\ 0.2459+0.1223i & -0.1315+0.0682i & -0.2702-0.2781i & 0.2683-0.2842i \\ -0.0155+0.1640i & -0.2285-0.0472i & -0.5114-0.2436i & -0.0346-0.1960i \end{bmatrix}$$

also neutralize information leakage,

$$\mathrm{vec}(\mathbf{R}) = \mathbf{B}^{\mathrm{H}} \left(\mathbf{B}\,\mathbf{B}^{\mathrm{H}}\right)^{-1} \mathbf{b} + \mathbf{z}, \tag{9}$$

where $\mathbf{z} \in \mathcal{N}(\mathbf{B})$. With the channel realizations given in Table I, we can generate another matrix $\mathbf{R}^{\mathrm{IN},z}$ which achieves a higher secrecy rate 4.1553, a 17.8% increase of secrecy rate by optimization over $\mathbf{z}$. This motivates us to investigate an efficient method to find $\mathbf{z}$ and consequently $\mathbf{R}$ which neutralizes information leakage and optimizes the secrecy rate at the same time.

Remark 2: With the optimization over $\mathbf{z}$, the relay matrix is no longer block diagonal which couples the frequency channels. Although the problem is more complicated, we have shown in the above example that one can get a better secrecy rate performance. In Section IV-B, we propose an iterative sum secrecy rates optimization over the relay matrix $\mathbf{R}$ and the precoding matrices $\{\mathbf{P}_i\}$.

In the following section, we illustrate how the relay matrix can be chosen carefully to amplify the desired signal strength and at the same time neutralize information leakage in the multi-user scenario.

III. GENERAL MULTI-USER MULTI-ANTENNA MULTI-CARRIER SCENARIO

In this section, we let the number of TXs and RXs be $K \geq 2$. The TXs and RXs have single antenna and the relay has N antennas. Let the number of frequency subcarriers be M. Denote the complex channel from TX i to RX j, as a diagonal matrix $\mathbf{H}_{ji} \in \mathbb{C}^M$ and the complex channel from TX i to relay as $\mathbf{F}_i \in \mathbb{C}^{NM\times M}$ and from relay to RX j as $\mathbf{G}_j \in \mathbb{C}^{MN\times M}$. The signal received at the relay is,

$$\mathbf{y}_r = \sum_{i=1}^{K} \mathbf{F}_i\,\mathbf{P}_i\,\mathbf{x}_i + \mathbf{n}_r \tag{10}$$

where $\mathbf{F}_i = \mathrm{diag}\left(\mathbf{f}_i(1), \ldots, \mathbf{f}_i(M)\right)$ and $\mathbf{x}_i \in \mathbb{C}^{M\times 1}$ are the circular Gaussian transmit symbols from TX i, with zero mean and identity covariance matrix. The matrix $\mathbf{P}_i \in \mathbb{C}^M$ satisfies the power constraint:

$$\mathrm{tr}\left(\mathbf{P}_i\,\mathbf{P}_i^{\mathrm{H}}\right) \leq P_i^{max}. \tag{11}$$

With AF strategy, the relay multiplies the received signal $\mathbf{y}_r$ on the left by processing matrix $\mathbf{R}$ and transmits $\mathbf{R}\,\mathbf{y}_r$. The transmit power of the relay is constrained by P_r^{max},

$$\mathrm{tr}\left(\mathbf{R}\left(\sum_{i=1}^{K} \mathbf{F}_i\,\mathbf{P}_i\,\mathbf{P}_i^{\mathrm{H}}\,\mathbf{F}_i^{\mathrm{H}} + \mathbf{I}_{MN}\right)\mathbf{R}^H\right) \leq P_r^{max}. \tag{12}$$

The received signal at RX j is

$$\mathbf{y}_j = \sum_{i=1}^{K} \left(\mathbf{H}_{ji} + \mathbf{G}_j^{\mathrm{H}}\,\mathbf{R}\,\mathbf{F}_i\right)\mathbf{P}_i\,\mathbf{x}_i + \mathbf{G}_j^{\mathrm{H}}\,\mathbf{R}\,\mathbf{n}_r + \mathbf{n}_j \tag{13}$$

where $\mathbf{n}_j$ is the circular Gaussian noise at RX j with zero mean and identity covariance matrix and $\mathbf{G}_j =$

$\mathrm{diag}(\mathbf{g}_j(1),\ldots,\mathbf{g}_j(M))$. For the ease of notation, we define the equivalent channel from i to j as

$$\bar{\mathbf{H}}_{ji} = \mathbf{H}_{ji} + \mathbf{G}_j^H \, \mathbf{R} \, \mathbf{F}_i \tag{14}$$

and its (f,m)-element is $[\bar{\mathbf{H}}_{ji}]_{fm} = h_{ji} + \mathbf{g}_j^{\mathrm{H}}(f)\,\mathbf{R}_{fm}\,\mathbf{f}_i(m)$ which is the equivalent channel from TX i to RX j frequency f on frequency m.

Each RX is not only interested in decoding its own signal but also eavesdropping from other TXs. In the following, we define the worst case achievable secrecy rate with colluding eavesdroppers. For messages $\mathbf{x}_i$, all RXs except RX i collaborate to form an eavesdropper with multiple antennas and the message $\mathbf{x}_i$ goes through a multi-carrier MIMO channel to the colluding eavesdroppers. A worst case secrecy rate is then to assume that all other messages $\mathbf{x}_j, j \neq i$ are decoded perfectly and subtracted before decoding $\mathbf{x}_i$. The received signals at RX i and the colluding eavesdroppers are

$$\begin{cases} \mathbf{y}_i = \sum_{k=1}^{K} \bar{\mathbf{H}}_{ik}\,\mathbf{P}_k\,\mathbf{x}_k + \mathbf{G}_i^{\mathrm{H}}\,\mathbf{R}\,\mathbf{n}_r + \mathbf{n}_i \\ \mathbf{y}_{-i} = \begin{bmatrix} \bar{\mathbf{H}}_{1i} \\ \vdots \\ \bar{\mathbf{H}}_{(i-1)i} \\ \bar{\mathbf{H}}_{(i+1)i} \\ \vdots \\ \bar{\mathbf{H}}_{Ki} \end{bmatrix} \mathbf{P}_i\,\mathbf{x}_i + \begin{bmatrix} \mathbf{G}_1^{\mathrm{H}} \\ \vdots \\ \mathbf{G}_{i-1}^{\mathrm{H}} \\ \mathbf{G}_{i+1}^{\mathrm{H}} \\ \vdots \\ \mathbf{G}_k^{\mathrm{H}} \end{bmatrix} \mathbf{R}\,\mathbf{n}_r + \begin{bmatrix} \mathbf{n}_1 \\ \vdots \\ \mathbf{n}_{i-1} \\ \mathbf{n}_{i+1} \\ \vdots \\ \mathbf{n}_K \end{bmatrix} \\ \qquad = \bar{\mathbf{H}}_{-i}\,\mathbf{P}_i\,\mathbf{x}_i + \mathbf{G}_{-i}^{\mathrm{H}}\,\mathbf{R}\,\mathbf{n}_r + \mathbf{n}_{-i}\,. \end{cases} \tag{15}$$

The secrecy rate of TX-RX pair i is [38] given in (16) at the top of next page. Recall from (14) that the equivalent channel from Tx j to Rx i $\bar{\mathbf{H}}_{ij}$ is a function of the relay processing matrix $\mathbf{R}$, $\bar{\mathbf{H}}_{ij} = \mathbf{H}_{ij} + \mathbf{G}_i^{\mathrm{H}}\,\mathbf{R}\,\mathbf{F}_j$. The optimization of the aforementioned secrecy rates is highly complicated due to their non-convex structure. In the following, we propose the information leakage neutralization technique [35] which is able to neutralize all information leakage to all eavesdroppers in the air by choosing the relay strategy in a careful manner. As illustrated in the previous section, with information leakage neutralization, the secrecy rate expression (16) can be simplified to

$$r_i^s = \mathcal{C}\left(\mathbf{I}_M + \bar{\mathbf{H}}_{ii}\,\mathbf{P}_i\,\mathbf{P}_i^{\mathrm{H}}\,\bar{\mathbf{H}}_{ii}^{\mathrm{H}}\left(\mathbf{G}_i^{\mathrm{H}}\,\mathbf{R}\,\mathbf{R}^{\mathrm{H}}\,\mathbf{G}_i + \mathbf{I}_M\right)^{-1}\right). \tag{17}$$

In the following section, we illustrate how we can choose $\mathbf{R}$ to achieve a secrecy rate as such.

A. Information Leakage Neutralization

We choose $\mathbf{R}$ such that the equivalent channel of message $\mathbf{x}_i$ to the eavesdropper in (15) is neutralized to zero. The challenge of information leakage neutralization in multi-subcarrier environment as compared to the single-subcarrier case [35] is that the information leakage neutralization constraints must be modified to incorporate frequency sharing:

$$\left(\mathbf{H}_{ji} + \mathbf{G}_j^{\mathrm{H}}\,\mathbf{R}\,\mathbf{F}_i\right)\mathbf{P}_i = 0, \qquad i,j = 1,\ldots,K, i \neq j. \tag{18}$$

Note that we consider the most general scenario where TX-RX pairs may only use part of the spectrum and send less than M data streams and thus $\mathbf{P}_i$ may have zero rows and zero columns. In the following, we show the dependency of the number of antennas at the relay for information leakage neutralization on these system parameters.

Proposition 1: The number of antennas at the relay, N, required to neutralize all information leakage from each of the K TX-RX pairs at each frequency subcarrier, in a total of M subcarriers, satisfies

$$N \geq \sqrt{\frac{K-1}{M}\sum_{i=1}^{K} S_i} \tag{19}$$

where S_i is the number of data streams sent by TX i .

For the proof, please refer to Appendix I. Proposition 1 offers the minimum number of antennas required to ensure secrecy which depends on the number of TX-RX pairs K, the number of subcarriers M and the number of data streams transmitted S_i.

- If every TX employs full frequency multiplexing $S_i = M$, we have then

$$N \geq \sqrt{\frac{K-1}{M}\sum_{i=1}^{K} M} = \sqrt{K(K-1)}. \tag{20}$$

  As N is an integer, we have $N \geq K$ which is the same criteria as in the flat-fading case [35].
- If every TX sends $S_i = aM$ data streams and $0 \leq a \leq 1$, we have then

$$N \geq \sqrt{\frac{K-1}{M}\sum_{i=1}^{K} aM} = \sqrt{aK(K-1)}. \tag{21}$$

  For example, in a scenario of $K = 3$ TXs, $M = 16$ frequency subcarriers and each TX transmits $S_i = 8$ data streams $\left(a = \frac{1}{2}\right)$, the relay must have at least $\left\lceil\sqrt{\frac{1}{2}\cdot 3\cdot 2}\right\rceil = \lceil\sqrt{3}\rceil = 2$ antennas to completely remove any information leakage from any TX to any RX. This is less than $\lceil\sqrt{3(2)}\rceil = 3$ if all TXs send $S_i = M = 16$ data streams.
- Note that the number of antennas required for information leakage neutralization is *independent* to the number of frequency subcarriers used by each TX (the number of non-zero rows of $\mathbf{P}_i$)[5]. However, the power required to neutralize information leakage depends on how crowded the subcarriers are. If a lot of frequency subcarriers are occupied, the relay may not have enough power to neutralize all information leakage as we will see in the following.

When the number of antennas at the relay is sufficient for information leakage neutralization, we can use the following

[5]The reason is that even if a TX does not transmit on a certain frequency, the relay must make sure that it does not forward the TX's information on other subcarriers to this subcarrier at which the eavesdroppers can decode the information.

$$r_i^s = \left(\mathcal{C} \left(\mathbf{I}_M + \bar{\mathbf{H}}_{ii} \mathbf{P}_i \mathbf{P}_i^{\mathrm{H}} \bar{\mathbf{H}}_{ii}^{\mathrm{H}} \left(\sum_{j \neq i} \bar{\mathbf{H}}_{ij} \mathbf{P}_j \mathbf{P}_j^{\mathrm{H}} \bar{\mathbf{H}}_{ij}^{\mathrm{H}} + \mathbf{G}_i^{\mathrm{H}} \mathbf{R} \mathbf{R}^{\mathrm{H}} \mathbf{G}_i + \mathbf{I}_M \right)^{-1} \right) \right.$$
$$\left. - \mathcal{C} \left(\mathbf{I}_{M(K-1)} + \bar{\mathbf{H}}_{-i} \mathbf{P}_i \mathbf{P}_i^{\mathrm{H}} \bar{\mathbf{H}}_{-i}^{\mathrm{H}} \left(\mathbf{G}_{-i}^{\mathrm{H}} \mathbf{R} \mathbf{R}^{\mathrm{H}} \mathbf{G}_{-i} + \mathbf{I}_{M(K-1)} \right)^{-1} \right) \right)^{+}. \tag{16}$$

method to compute the relay forwarding matrix $\mathbf{R}$ for such purpose.

Proposition 2: Any relay matrix $\mathbf{R}$ satisfying the information leakage neutralization constraint (35) has the following form:

$$\mathrm{vec}(\mathbf{R}) = \mathbf{A}^{\dagger}\, \mathbf{b} + \mathbf{z}$$

where

$$\mathbf{A} = \left[\left(\left(\hat{\mathbf{P}}_1^{\mathrm{T}} \mathbf{F}_1^{\mathrm{T}} \right) \otimes \mathbf{G}_{-1}^{\mathrm{H}} \right)^{\mathrm{H}}, \ldots, \left(\left(\hat{\mathbf{P}}_K^{\mathrm{T}} \mathbf{F}_K^{\mathrm{T}} \right) \otimes \mathbf{G}_{-K}^{\mathrm{H}} \right)^{\mathrm{H}} \right]^{\mathrm{H}}$$

$$\mathbf{b} = \left[-\mathrm{vec} \left(\mathbf{H}_{-1} \hat{\mathbf{P}}_1 \right)^{\mathrm{H}}, \ldots, -\mathrm{vec} \left(\mathbf{H}_{-K} \hat{\mathbf{P}}_K \right)^{\mathrm{H}} \right]^{\mathrm{H}}$$

$$\mathbf{z} \in \mathcal{N}(\mathbf{A})$$

and $\hat{\mathbf{P}}_i$ is a submatrix of $\mathbf{P}_i$, containing its non-zero columns.

For the proof, please refer to Appendix II. From Proposition 2, it follows that there is a minimum power requirement for information leakage neutralization.

Corollary 1: The minimum power required for information leakage neutralization is

$$P_r^{max} \geq \left(\mathbf{A}^{\dagger}\, \mathbf{b} \right)^{\mathrm{H}} \left(\left(\sum_{i=1}^{K} \mathbf{F}_i \mathbf{P}_i \mathbf{P}_i^{\mathrm{H}} \mathbf{F}_i^{\mathrm{H}} + \mathbf{I}_{MN} \right) \otimes \mathbf{I}_{MN} \right) \left(\mathbf{A}^{\dagger}\, \mathbf{b} \right).$$

For the proof, please refer to Appendix III. Depending on the available transmit power at the relay, one may only have enough power to neutralize information leakage but not enough power to further improve the transmission rates. If there is limited power resource and therefore one must ensure secure transmission with as little power as possible, then one can set $\mathbf{z}$ in Proposition 2 to zero. If there is a high priority of secrecy rates and with abundant transmit power, one can optimize $\mathbf{z}$ for the purpose of sum secrecy rate maximization. In the following, we investigate algorithms to address these applications.

IV. Information Leakage Neutralization Algorithms

In the previous section, we have shown that secrecy rates (17) are achievable by information leakage neutralization. Also, in order to implement information leakage neutralization, the number of antennas at the relay, the number of frequency subcarriers and the number of TX-RX pairs in the system must satisfy the relation in Proposition 1. In Proposition 2, we computed the minimum relay power required in order to perform information leakage neutralization. With more power available at the relay, we can improve the achievable secrecy rates by optimizing the relay matrix and the precoding matrices. The optimization of sum secrecy rates can be written formally in the following:

$$\begin{aligned} \max_{\mathbf{R}, \{\mathbf{P}_i\}} \quad & \sum_{i=1}^{K} \mathcal{C} \left(\mathbf{I}_M + \bar{\mathbf{H}}_{ii} \mathbf{P}_i \mathbf{P}_i^{\mathrm{H}} \bar{\mathbf{H}}_{ii}^{\mathrm{H}} \boldsymbol{\Xi}_i^{-1} \right) \\ \text{such that} \quad & \bar{\mathbf{H}}_{ii} = \mathbf{H}_{ii} + \mathbf{G}_i^{\mathrm{H}} \mathbf{R} \mathbf{F}_i, \\ & \boldsymbol{\Xi}_i = \mathbf{G}_i^{\mathrm{H}} \mathbf{R} \mathbf{R}^{\mathrm{H}} \mathbf{G}_i + \mathbf{I}_M, \\ & \mathrm{tr} \left(\mathbf{P}_i \mathbf{P}_i^{\mathrm{H}} \right) \leq P_i^{max}, \\ & \mathrm{tr} \left(\mathbf{R} \left(\sum_{i=1}^{K} \mathbf{F}_i \mathbf{P}_i \mathbf{P}_i^{\mathrm{H}} \mathbf{F}_i^{\mathrm{H}} \right) \mathbf{R}^{\mathrm{H}} \right) \leq P_r^{max}. \end{aligned}$$

In the following, we propose two algorithms. The computation of the algorithms are assumed to be performed at the relay because the relay has not only more computation power but is also able to gather the channel state information from different transmitters and receivers in the system. We assume that the transmitters and receivers are willing to feed back their channel state information to the relay and in return get an improved secrecy rate performance. After the relay performs the computation, the precoding design $\mathbf{P}_i$ is fed back to transmitter i. The first algorithm EFFIN, in Section IV-A, considers the scenario where $\mathbf{z} = \mathbf{0}$ in Proposition 2 and all TXs transmit the maximum number of data streams allowed $S_i = M$. We observe that in this situation, information leakage neutralization decomposes the system into KM parallel channels and consequently both the relay processing matrix $\mathbf{R}$ and the precoding matrix $\mathbf{P}_i$ can be computed very efficiently. The second algorithm LOPTIN, in Section IV-B, investigates a systematic method for the computation of $\mathbf{R}$ and $\mathbf{P}_i$ when there is enough transmit power budget at the relay to allow further optimization of secrecy rates.

A. Efficient Information Leakage Neutralization (EFFIN)

When every TX transmits $S_i = M$ data streams and $\mathbf{P}_i$ is invertible, we propose the following algorithm that decomposes the K users interference relay channels with M frequency subcarriers and N antennas at the relay to KM parallel secure channels *with no interference and no information leakage*. The information leakage neutralization criteria $\left(\mathbf{H}_{ij} + \mathbf{G}_i^{\mathrm{H}} \mathbf{R} \mathbf{F}_j \right) \mathbf{P}_i = \mathbf{0}$, when $\mathbf{P}_i$ is invertible, is equivalent to

$$\mathbf{H}_{ij} + \mathbf{G}_i^{\mathrm{H}} \mathbf{R} \mathbf{F}_j = \mathbf{0}.$$

Due to the block diagonal structure of $\mathbf{H}_{ij}$, $\mathbf{G}_i$ and $\mathbf{F}_j$, one feasible solution of the above equation is a block diagonal $\mathbf{R}$. With the block diagonal structure, the resulting secrecy rates may be suboptimal, but the information leakage neutralization constraint can be broken down to the optimization over the diagonal blocks $\mathbf{R}_{mm}$ in $\mathbf{R}$:

$$h_{ji}(m) + \mathbf{g}_j^{\mathrm{H}}(m)\,\mathbf{R}_{mm}\,\mathbf{f}_i(m) = 0, \quad i,j = 1,\ldots,K, i \neq j. \tag{22}$$

Following the same approach as before, we stack the constraints for all $j \neq i$ and define

$$\begin{aligned}\mathbf{h}_{-i}(m) &= \left[h_{1i}^{\mathrm{H}}(m),\ldots,h_{(i-1)i}^{\mathrm{H}}(m),h_{(i+1)i}^{\mathrm{H}}(m),\ldots,h_{Ki}^{\mathrm{H}}(m)\right]^{\mathrm{H}}\\ \mathbf{G}_{-i}(m) &= \left[\mathbf{g}_1(m),\ldots,\mathbf{g}_{i-1}(m),\mathbf{g}_{i+1}(m),\ldots,\mathbf{g}_K(m)\right].\end{aligned}$$

We obtain $\mathbf{h}_{-i}(m)+\mathbf{G}_{-i}^{\mathrm{H}}(m)\,\mathbf{R}_{mm}\,\mathbf{f}_i(m) = \mathbf{0}_{(K-1)\times 1}$ which is equivalent to

$$\left(\mathbf{f}_i^{\mathrm{T}}(m)\otimes\mathbf{G}_{-i}^{\mathrm{H}}(m)\right)\mathrm{vec}\left(\mathbf{R}_{mm}\right) = -\,\mathbf{h}_{-i}(m).$$

Stacking constraints for all i, we have

$$\begin{aligned}\mathbf{A}(m) &= \left[\left(\mathbf{f}_1^{\mathrm{T}}(m)\otimes\mathbf{G}_{-1}^{\mathrm{H}}(m)\right);\ldots;\left(\mathbf{f}_K^{\mathrm{T}}(m)\otimes\mathbf{G}_{-K}^{\mathrm{H}}(m)\right)\right],\\ \mathbf{b}(m) &= \left[-\,\mathbf{h}_{-1}(m);\ldots;-\,\mathbf{h}_{-K}(m)\right].\end{aligned} \tag{23}$$

With a limited power budget at relay, we propose to implement information leakage neutralization with the least relay transmit power and utilize the result from Proposition 2, the relay matrix has the m-th diagonal block equal to

$$\mathbf{R}_{mm} = \mathrm{vec}^{-1}\left(\left(\mathbf{A}(m)\right)^{\dagger}\mathbf{b}(m)\right) \tag{24}$$

where $\mathrm{vec}(.)^{-1}$ is to reverse the vectorization of a vector columnwise to a $M\times M$ matrix. After the computation of the relay matrix in (24), $\mathbf{R} = \mathrm{diag}\left(\mathbf{R}_{11},\ldots,\mathbf{R}_{MM}\right)$, the optimal precoding matrices $\{\mathbf{P}_i\}$ are computed by solving $\mathcal{Q}_1$.

$$\begin{aligned}\mathcal{Q}_1: \max_{\{\mathbf{Q}_i\},\mathbf{Q}_i\succeq 0} \quad & \sum_{i=1}^{K}\mathcal{C}\left(\mathbf{I}_M+\mathbf{Q}_i\,\mathbf{W}_i\right)\\ \text{such that} \quad & \mathrm{tr}\left(\mathbf{Q}_i\right)\leq P_i^{max},\ \ i=1,\ldots,K,\\ & \sum_{i=1}^{K}\mathrm{tr}\left(\mathbf{Q}_i\,\mathbf{X}_i\right)\leq \bar{P}_r^{max}.\end{aligned}$$

We replace $\mathbf{P}_i\,\mathbf{P}_i^{\mathrm{H}}$ by positive semi-definite variable $\mathbf{Q}_i$ and denote the following matrices

$$\begin{aligned}\mathbf{W}_i &= \left(\mathbf{H}_{ii}+\mathbf{G}_i^{\mathrm{H}}\,\mathbf{R}\,\mathbf{F}_i\right)^{\mathrm{H}}\cdot\\ &\qquad\left(\mathbf{G}_i^{\mathrm{H}}\,\mathbf{R}\,\mathbf{R}^{\mathrm{H}}\,\mathbf{G}_i+\mathbf{I}_M\right)^{-1}\left(\mathbf{H}_{ii}+\mathbf{G}_i^{\mathrm{H}}\,\mathbf{R}\,\mathbf{F}_i\right),\\ \mathbf{X}_i &= \mathbf{F}_i^{\mathrm{H}}\,\mathbf{R}^{\mathrm{H}}\,\mathbf{R}\,\mathbf{F}_i,\\ \bar{P}_r^{max} &= P_r^{max}-\mathrm{tr}\left(\mathbf{R}\,\mathbf{R}^{\mathrm{H}}\right).\end{aligned} \tag{25}$$

The objective in $\mathcal{Q}_1$ is concave in $\mathbf{Q}_i$ as $\mathbf{W}_i$ is positive semi-definite and the constraints are linear in $\mathbf{Q}_i$. Thus, $\mathcal{Q}_1$ is a semi-definite program and can be solved readily using convex optimization solvers, e.g. CVX[6]. The optimal $\mathbf{P}_i$ is obtained by performing eigenvalue decomposition on $\mathbf{Q}_i = \mathbf{U}_i\,\mathbf{D}_i\,\mathbf{U}_i^{\mathrm{H}}$ and $\mathbf{P}_i = \mathbf{U}_i\,\mathbf{D}_i^{1/2}$. The pseudo-code of the EFFIN is given in Algorithm 1.

Algorithm 1 The pseudo-code for Efficient Information Leakage Neutralization (EFFIN)

1: **for** $m = 1 \to M$ **do** ▷ Compute block diagonal relay processing matrix
2: Compute $\mathbf{R}_{mm} = \mathrm{vec}^{-1}\left(\left(\mathbf{A}(m)\right)^{\dagger}\mathbf{b}(m)\right)$ with $\mathbf{A}(m)$ and $\mathbf{b}(m)$ defined in (23).
3: **end for**
4: The relay processing matrix is $\mathbf{R} = \mathrm{diag}\left(\mathbf{R}_{11},\ldots,\mathbf{R}_{MM}\right)$.
5: Solve $\mathcal{Q}_1$ using convex optimization solvers and obtain optimal $\{\mathbf{Q}_i\}$.
6: **for** $i = 1 \to K$ **do** ▷ Compute precoding matrices
7: Perform eigen-value decomposition, $\mathbf{Q}_i = \mathbf{U}_i\,\mathbf{D}_i\,\mathbf{U}_i^{\mathrm{H}}$. Set $\mathbf{P}_i = \mathbf{U}_i\,\mathbf{D}_i^{1/2}$.
8: **end for**

B. Local-Optimized Information Leakage Neutralization (LOPTIN)

In the previous subsection, we have discussed a simple, efficient and relay transmit power saving solution of the relay matrix and precoding matrices for secure transmission. One drawback of the efficient method is that its performance may be suboptimal. In this subsection, we discuss how to choose the relay and precoding matrices such that the sum secrecy rates are optimized while ensuring zero information leakage.

To this end, we rewrite the information leakage neutralization constraint (18) to promote the optimization of secrecy rates,

$$\left(\mathbf{H}+\mathbf{G}^{\mathrm{H}}\,\mathbf{R}\,\mathbf{F}\right)\mathbf{P} = \mathbf{T} \tag{26}$$

where $\mathbf{H} = [\mathbf{H}_{11},\ldots,\mathbf{H}_{1K};\ldots;\mathbf{H}_{K1},\ldots,\mathbf{H}_{KK}]$, $\mathbf{G}^{\mathrm{H}} = \left[\mathbf{G}_1^{\mathrm{H}};\ldots;\mathbf{G}_K^{\mathrm{H}}\right]$, $\mathbf{F} = [\mathbf{F}_1,\ldots,\mathbf{F}_K]$ and $\mathbf{P} = \mathrm{diag}(\mathbf{P}_1,\ldots,\mathbf{P}_K)$. The block diagonal matrix $\mathbf{T} = \mathrm{diag}(\mathbf{T}_1,\ldots,\mathbf{T}_K)$ is the new optimization variable. $\mathbf{T}_i$ is the equivalent desired channel from TX i to RX i as $\mathbf{T}_i = \left(\mathbf{H}_{ii}+\mathbf{G}_i^{\mathrm{H}}\,\mathbf{R}\,\mathbf{F}_i\right)\mathbf{P}_i$. By applying pseudo-inverses[7] of $\mathbf{G}^{\mathrm{H}}$ and $\mathbf{F}\,\mathbf{P}$ ($\mathbf{G}^{\mathrm{H}\,\dagger}$ and $\left(\mathbf{F}\,\mathbf{P}\right)^{\dagger}$ respectively), one can rewrite (26) to the following

$$\mathbf{R} = \mathbf{G}^{\mathrm{H}\,\dagger}\left(\mathbf{T}-\mathbf{H}\,\mathbf{P}\right)\left(\mathbf{F}\,\mathbf{P}\right)^{\dagger}. \tag{27}$$

[6]Given block diagonal $\mathbf{R}$ in (24), the equivalent channel $\mathbf{W}_i$ and matrix $\mathbf{X}_i$ are also block diagonal. It is possible to solve $\mathcal{Q}_1$ using water-filling with $K+1$ Lagrange multipliers. For large problem size, it may be more computational efficient using a tailor made water-filling method. For medium size problems and illustrative purposes, we propose here to solve by semi-definite programming.

[7]Note that $\mathbf{G}^{\mathrm{H}}$ has dimension $MK\times MN$ and $\mathbf{F}\,\mathbf{P}$ has dimension $MN\times KM$. If $MN\geq MK$, then $\mathbf{G}^{\mathrm{H}\,\dagger} = \mathbf{G}\left(\mathbf{G}^{\mathrm{H}}\,\mathbf{G}\right)^{-1}$ and $\left(\mathbf{F}\,\mathbf{P}\right)^{\dagger} = \left(\left(\mathbf{F}\,\mathbf{P}\right)^{\mathrm{H}}\left(\mathbf{F}\,\mathbf{P}\right)\right)^{-1}\left(\mathbf{F}\,\mathbf{P}\right)^{\mathrm{H}}$. If $MN<KM$, then $\mathbf{G}^{\mathrm{H}\,\dagger} = \left(\mathbf{G}\,\mathbf{G}^{\mathrm{H}}\right)^{-1}\mathbf{G}$ and $\left(\mathbf{F}\,\mathbf{P}\right)^{\dagger} = \left(\mathbf{F}\,\mathbf{P}\right)^{\mathrm{H}}\left(\mathbf{F}\,\mathbf{P}\left(\mathbf{F}\,\mathbf{P}\right)^{\mathrm{H}}\right)^{-1}$.

The maximum achievable sum secrecy rate is the solution of the following problem

$$\max_{\mathbf{R},\mathbf{T},\{\mathbf{P}_i\}} \quad \sum_{i=1}^{K} \mathcal{C}\left(\mathbf{I}_M + \mathbf{T}_i\,\mathbf{P}_i\,\mathbf{P}_i^{\mathrm{H}}\,\mathbf{T}_i^{\mathrm{H}} \cdot \mathbf{\Xi}_i^{-1}\right) \tag{28a}$$

$$\text{such that} \quad \mathbf{\Xi}_i = \mathbf{G}_i^{\mathrm{H}}\,\mathbf{R}\,\mathbf{R}^{\mathrm{H}}\,\mathbf{G}_i + \mathbf{I}_M, \tag{28b}$$

$$\mathrm{tr}\left(\mathbf{P}_i\,\mathbf{P}_i^{\mathrm{H}}\right) \le P_i^{max}, \;\; i = 1,\ldots,K, \tag{28c}$$

$$\left(\mathbf{H} + \mathbf{G}^{\mathrm{H}}\,\mathbf{R}\,\mathbf{F}\right)\mathbf{P} = \mathbf{T}, \tag{28d}$$

$$\mathrm{tr}\left(\mathbf{R}\left(\mathbf{F}\,\mathbf{P}\,\mathbf{P}^{\mathrm{H}}\,\mathbf{F}^{\mathrm{H}} + \mathbf{I}_{MN}\right)\mathbf{R}^{\mathrm{H}}\right) \le P_r^{max} \tag{28e}$$

$$\mathbf{T} = \mathrm{diag}\left(\mathbf{T}_1,\ldots,\mathbf{T}_K\right). \tag{28f}$$

Note that in the objective function, the information leakage is neutralized for each TX-RX pair. Constraints (28c) and (28e) are the transmit power constraints at the TXs and at the relay respectively. The information leakage neutralization constraint is written as (28d). The optimization is not jointly convex in $\mathbf{R}$, $\mathbf{T}$ and $\{\mathbf{P}_i\}$. To simplify the optimization problem, we propose the following iterative optimization algorithm. Given $\mathbf{R}$ and $\mathbf{T}$, we solve $\mathbf{P}_i$ optimally using $\mathcal{Q}_1$ in EFFIN. The second part of the iterative algorithm is to compute the optimal relay strategy $\mathbf{R}$ and the auxiliary variable $\mathbf{T}$ (by solving $\mathcal{Q}_2$) if the precoding matrices $\mathbf{P}_i$ as the solutions of $\mathcal{Q}_1$ are given.

$$\begin{aligned}
&\mathcal{Q}_2: \\
&\max_{\mathbf{R},\mathbf{T}} \quad \sum_{i=1}^{K} \mathcal{C}\left(\mathbf{I}_M + \mathbf{T}_i\,\mathbf{T}_i^{\mathrm{H}}\left(\mathbf{G}_i^{\mathrm{H}}\,\mathbf{R}\,\mathbf{R}^{\mathrm{H}}\,\mathbf{G}_i + \mathbf{I}_M\right)^{-1}\right) \\
&\text{such that} \quad \mathbf{R} = \mathbf{G}^{\mathrm{H}\,\dagger}\left(\mathbf{T} - \mathbf{H}\,\mathbf{P}\right)\left(\mathbf{F}\,\mathbf{P}\right)^{\dagger}, \\
&\qquad \mathrm{tr}\left(\mathbf{R}\left(\mathbf{F}\,\mathbf{P}\,\mathbf{P}^{\mathrm{H}}\,\mathbf{F}^{\mathrm{H}} + \mathbf{I}_{MN}\right)\mathbf{R}^{\mathrm{H}}\right) \le P_r^{max}, \\
&\qquad \mathbf{T} = \mathrm{diag}(\mathbf{T}_1,\ldots,\mathbf{T}_K).
\end{aligned}$$

Problem $\mathcal{Q}_2$ is non-convex. The major challenge is due to the sum of log-determinants in the objective function and the equality constraints. In the following, we utilize the first equality constraint and replace $\mathbf{R}$ as a function of $\mathbf{T}$. The optimization problem $\mathcal{Q}_2$ can be written as,

$$\begin{aligned}
&\mathcal{Q}_2': \\
&\max_{\mathbf{T}} \quad \sum_{i=1}^{K}\left(\mathcal{C}\left(\mathbf{X}_i + \bar{\mathbf{T}}_i\,\mathbf{Z}_i\,\bar{\mathbf{T}}_i^{H}\right) - \mathcal{C}\left(\mathbf{X}_i + \bar{\mathbf{T}}_i\,\mathbf{Y}_i\,\bar{\mathbf{T}}_i^{\mathrm{H}}\right)\right) \\
&\text{such that} \quad \mathrm{tr}\left(\mathbf{G}^{\mathrm{H}\,\dagger}\left(\mathbf{T} - \mathbf{H}\,\mathbf{P}\right)\left(\tilde{\mathbf{F}} + \mathbf{I}_{MK}\right)\cdot\right. \\
&\qquad\qquad \left.\left(\mathbf{T} - \mathbf{H}\,\mathbf{P}\right)^{\mathrm{H}}\,\mathbf{G}^{\dagger}\right) \le P_r^{max}, \\
&\qquad \bar{\mathbf{T}}_i = \left[\mathbf{T}_i, \mathbf{I}_M\right], \\
&\qquad \mathbf{T} = \mathrm{diag}(\mathbf{T}_1,\ldots,\mathbf{T}_K).
\end{aligned}$$

The variables $\mathbf{X}_i, \mathbf{Y}_i, \mathbf{Z}_i, \tilde{\mathbf{F}}$ are defined as follows

$$\tilde{\mathbf{F}} = \left(\mathbf{F}\,\mathbf{P}\right)^{\dagger}\left(\mathbf{F}\,\mathbf{P}\right)^{\mathrm{H}\,\dagger}, \qquad \mathbf{X}_i = \sum_{m=1}^{K}\sum_{l=1}^{K}\mathbf{H}_{im}\,\mathbf{P}_m\,\tilde{\mathbf{F}}_{ml}\,\mathbf{P}_l^{\mathrm{H}}\,\mathbf{H}_{il}^{\mathrm{H}},$$

$$\mathbf{Y}_i = \begin{bmatrix} \tilde{\mathbf{F}}_{ii} & -\sum_{l=1}^{K}\tilde{\mathbf{F}}_{il}\,\mathbf{P}_l^{\mathrm{H}}\,\mathbf{H}_{il}^{H} \\ -\sum_{m=1}^{K}\mathbf{H}_{im}\,\mathbf{P}_m\,\tilde{\mathbf{F}}_{mi} & \mathbf{I}_M \end{bmatrix},$$

$$\mathbf{Z}_i = \begin{bmatrix} \mathbf{I}_M & \mathbf{0}_M \\ \mathbf{0}_M & \mathbf{0}_M \end{bmatrix} + \mathbf{Y}_i\,.$$

Please see the proof in Appendix IV. Although the optimization problem is simplified, it is still non-convex in $\mathbf{T}$. In the following, we propose to solve $\mathcal{Q}_2'$ with gradient descent method. To this end, we write the Lagrangian of $\mathcal{Q}_2'$ as $L(\mathbf{T},\lambda)$ in (29) and the gradient of the Lagrangian with respect to $\mathbf{T}^*$ in (30) at the top of next page. Please see the proof in Appendix V. We update the new variable $\mathbf{T}^{(t+1)}$ at the $t+1$-th iteration to be the sum of the current variable $\mathbf{T}^{(t)}$ and the product of the derivative and ϵ,

$$\mathbf{T}^{(t+1)} = \mathbf{T}^{(t)} + \epsilon\mathcal{D}_{\mathbf{T}^*}(\mathbf{T},\lambda) \tag{31}$$

where λ is the Lagrange multiplier and ϵ is chosen as

$$\epsilon = \arg\max_{\epsilon\ge 0}\left(L(\mathbf{T}^*,\lambda) + \epsilon\mathcal{D}_{\mathbf{T}^*}(\mathbf{T}^{(t)},\lambda)\right). \tag{32}$$

This update step, termed as gradient ascent method, steers the operating point towards a new operating point in the direction of the greatest increment of the objective function. This guarantees an increase in the objective.

We summarize in Algorithm 2 the proposed iterative algorithm on sum secrecy rate optimization. The algorithm first initializes the choice of beamforming matrices $\{\mathbf{P}_i\}$ and the relay matrix $\mathbf{R}$ using EFFIN. Then the algorithm optimizes the relay matrix $\mathbf{R}$ using a gradient ascent method. With the optimized $\mathbf{R}$, $\{\mathbf{P}_i\}$ is obtained by solving a convex optimization problem $\mathbf{Q}_1$. Then the algorithm iterates until the achievable secrecy rate at the current iteration is less than the achievable secrecy rate at the previous iteration plus a small

Algorithm 2 The pseudo-code for Local-Optimized Information Leakage Neutralization (LOPTIN)

1: **while do** ▷ Compute relay processing matrix
2: Initialize $\{\mathbf{P}_i\}$ and $\mathbf{R}$ as the solutions of EFFIN.
3: Solve $\mathcal{Q}_2'$ using gradient descent method with gradient (30) and obtain optimal solution $\mathbf{T}$. Obtain relay processing matrix $\mathbf{R}$ from $\mathbf{T}$ using (27).
4: With $\mathbf{R}$ and $\mathbf{T}$ above, solve $\mathcal{Q}_1$ using convex optimization solvers and obtain optimal $\{\mathbf{Q}_i\}$.
5: **for** $i = 1 \to K$ **do** ▷ Compute precoding matrices
6: Perform eigen-value decomposition, $\mathbf{Q}_i = \mathbf{U}_i\,\mathbf{D}_i\,\mathbf{U}_i^{\mathrm{H}}$. Set $\mathbf{P}_i = \mathbf{U}_i\,\mathbf{D}_i^{1/2}$.
7: **end for**
8: **if** sum secrecy rate improvement is less than a predefined threshold **then**
9: Convergence reached. Break.
10: **end if**
11: **end while**

$$
\begin{aligned}
L(\mathbf{T},\lambda) &= \sum_{i=1}^{K} \left(\mathcal{C}\left(\mathbf{X}_i + \bar{\mathbf{T}}_i \, \mathbf{Z}_i \, \bar{\mathbf{T}}_i^{H} \right) - \mathcal{C}\left(\mathbf{X}_i + \bar{\mathbf{T}}_i \, \mathbf{Y}_i \, \bar{\mathbf{T}}_i^{\mathrm{H}} \right) \right) \\
&\quad - \lambda \left(\mathrm{tr}\left(\mathbf{G}^{\mathrm{H}\,\dagger} \left(\mathbf{T} - \mathbf{H}\,\mathbf{P} \right) \left(\tilde{\mathbf{F}} + \mathbf{I}_{MK} \right) \left(\mathbf{T} - \mathbf{H}\,\mathbf{P} \right)^{\mathrm{H}} \mathbf{G}^{\dagger} \right) - P_r^{max} \right) \\
&= \sum_{i=1}^{K} f_i(\mathbf{T}_i) - \lambda g(\mathbf{T}).
\end{aligned}
\tag{29}
$$

$$
\begin{aligned}
\mathcal{D}_{\mathbf{T}^*} L(\mathbf{T},\lambda) = \frac{1}{\ln(2)} &\begin{bmatrix} \mathcal{D}_{\mathbf{T}_1^*} f_1(\mathbf{T}_1) & \mathbf{0}_M & \dots & \mathbf{0}_M \\ \mathbf{0}_M & \mathcal{D}_{\mathbf{T}_2^*} f_2(\mathbf{T}_2) & \dots & \mathbf{0}_M \\ & & \ddots & \vdots \\ \mathbf{0}_M & \dots & & \mathcal{D}_{\mathbf{T}_K^*} f_K(\mathbf{T}_K) \end{bmatrix} \\
&- \lambda\, \mathbf{G}^{\dagger}\, \mathbf{G}^{\mathrm{H}\,\dagger} \left(\mathbf{T} - \mathbf{H}\,\mathbf{P} \right) \left(\tilde{\mathbf{F}} + \mathbf{I}_{KM} \right).
\end{aligned}
\tag{30}
$$

predefined constant ϵ. Since at each step of the optimization, we guarantee an increase of the secrecy rate and the secrecy rate is naturally finite due to finite power, we conclude that the proposed algorithm converges to a local optimum.

V. Simulation Results

To illustrate the effectiveness of the proposed algorithms, we provide in this section numerical simulations for different system settings. As an example, we simulate the secrecy rates of a relay assisted network with $K = 2$ TX-RX pairs, $M = 8$ frequency subcarriers and $N = 2$ antennas at the relay, unless otherwise stated. To examine the performance of the algorithms with respect to the system's signal-to-noise ratio, we vary the transmit power constraint at the relay from 0 to $30\,\mathrm{dB}$ while keeping the transmit power constraint at the TXs at $10\,\mathrm{dB}$ (see Figure 3.) Similarly, we examine the algorithms by varying the transmit power constraint at the TXs from 0 to $30\,\mathrm{dB}$ while keeping the transmit power at the relay constrained at $23, 27, 30\,\mathrm{dB}$. Note that by varying the power constraints, we do not force the power of the optimized precoding matrices and the relay processing matrix to be equal to the power constraints. In the following, we compare the following algorithms:

- Baseline 1 (Repeater): the relay is a layer-1 relay and is only able to forward signals without additional signal processing. This corresponds to setting $\mathbf{R} = \mathbf{I}_{MN} \sqrt{\frac{P_r^{max}}{MN}}$.
- Baseline 2 (IC): the relay shuts down, i.e. $\mathbf{R} = \mathbf{0}_{MN}$, and we obtain an interference channel where the RXs eavesdrop each other.
- Proposed algorithm EFFIN: an efficient relay and precoding matrices optimization algorithm outlined in Algorithm 1.
- Proposed algorithm LOPTIN: an local-optimal algorithm whose performance exceeds EFFIN with a price of higher complexity. LOPTIN is outlined in Algorithm 2.

For each baseline algorithm, we examine the effect of spectrum sharing on achievable secrecy rates by employing either one of the following spectrum sharing methods:

- Full spectrum sharing (FS): TXs are allowed to use the entire spectrum. Each TX measures the channel qualities of the direct channel and the channel from itself to other RXs. Based on the measured channel qualities, each TX excludes frequency subcarriers with zero secrecy rates and transmits on the channels with non-zero secrecy rates. For subcarriers at which more than one TX would like to transmit, we assume that the TXs coordinate so that the TX with a high secrecy rate would transmit on that subcarrier. Despite such coordination, each RX eavesdrops other TX-RX pairs on each subcarrier.
- Orthogonal spectrum sharing (OS): TXs are assigned exclusive portion of spectrum. Each TX excludes subcarriers with zero secrecy rates and transmits on the channels with non-zero secrecy rates. Each RX eavesdrops other TX-RX pairs on each subcarrier.

A. Secrecy rates with increasing relay power

In Figure 3, we show achievable sum secrecy rates over the transmit power constraint at the relay from 0 to $30\,\mathrm{dB}$ while keeping the transmit power constraint at the TXs at $10\,\mathrm{dB}$. As the IC does not utilize the relay, the achievable sum secrecy rates (plotted with triangles) are constant as the relay power constraint increases. As expected from intuition, the performance of IC with FS is better than OS because OS has an additional constraint of subcarrier assignment. The achievable sum secrecy rates achieved by a repeater decreases with relay transmit power. This is due to the increased amplification noise in AF relaying. Interestingly, the non-intelligent relaying scheme, e.g. a repeater, may decrease the secrecy rate significantly, even worse than switching off the relay. However, utilizing an intelligent relay and choosing the relaying scheme, one can improve the achievable secrecy rate significantly, about 550% over a simple repeater and about 200% over IC. Although EFFIN is very simple and efficient, it achieves 94.5% of the sum secrecy rate achieved by the more complicated algorithm LOPTIN with EFFIN as initialization point and 88% of that by LOPTIN with 6 randomized initialization points. Each initialization point leads to a potentially different convergence point in LOPTIN and the maximum out of the converged sum secrecy rates is plotted in solid black curve with diamond marks.

The saturation of the secrecy rates is due to the nature of

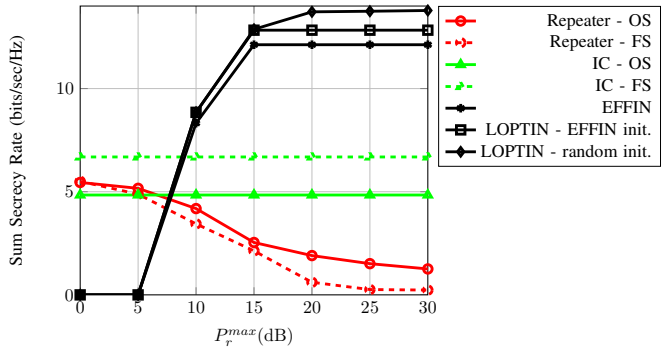


Fig. 3. The achievable secrecy rates of a two-user interference relay channel with 8 frequency subcarriers is shown with varying relay power constraint. The TX power constraints are 10 dB and there are two antennas at the relay. The proposed scheme EFFIN and LOPTIN outperform baseline algorithms Repeater and IC by 550% and 200% respectively.

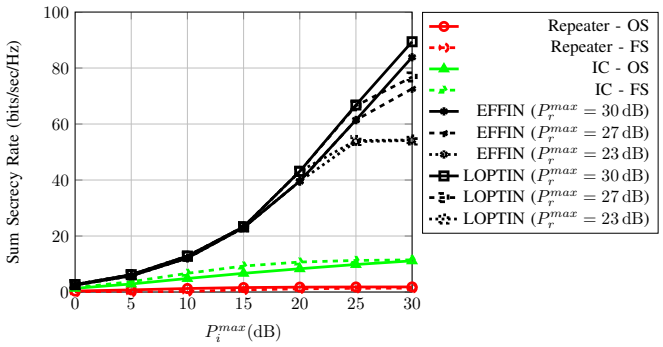


Fig. 4. The achievable secrecy rates of a two-user interference relay channel with 8 frequency subcarriers is shown with varying transmitter power constraints. The relay power constraint is 30 dB and there are two antennas at the relay. The secrecy rates achieved by EFFIN and LOPTIN grows unbounded with the transmit power at TX whereas the secrecy rates achieved by baseline algorithms saturate in high SNR regime.

the amplify-and-forward relaying and the fixed transmit power of the transmitters. Since the relay is chosen to neutralize information leakage and therefore mutual interference at the same time, the signal-to-noise ratio is the ratio of the desired signal power to the sum of amplification noise and background noise power. When the transmit powers of the transmitters are kept constant, the increase of relay power increases both the desired signal power and the amplification noise power, causing the saturation of the signal-to-noise ratio and consequently the secrecy rate. In order for the secrecy rate to scale indefinitely, both the transmit power and the relay power should be increased at the same time as shown in Figure 4.

B. Secrecy rates with increasing TX power

In Figure 4, we simulate the achievable sum secrecy rate by the transmit power constraint at TXs from 0 to 30 dB while keeping the transmit power at relay constrained at $23, 27, 30$ dB. As the transmit power at the TX increases, the sum secrecy rates saturate in both baseline algorithms, Repeater and IC. With the proposed information leakage neutralization, we see that the sum secrecy rates grow unbounded with the TX power as each TX-RX pair enjoys a leakage free frequency channel. Note that the sum secrecy rates achieved by relay with power constraint at $23, 27, 30$ dB are plotted in dotted, dashed and solid lines respectively. When there is only 23 dB available, there is only enough power for information leakage neutralization, but not enough to further optimize the system performance. Hence, the achievable sum secrecy rates of EFFIN and LOPTIN overlap. With more power available, it is possible to optimize the sum secrecy rates while neutralizing information leakage and the performance of LOPTIN is better than EFFIN.

C. Secrecy rates with larger systems

In Figure 5, we examine the performance of the proposed algorithms in a slightly larger systems with $N = 4$ antennas at the relay and $M = 16$ frequency subcarriers. The relay processing matrix is therefore a 64×64 matrix. The proposed

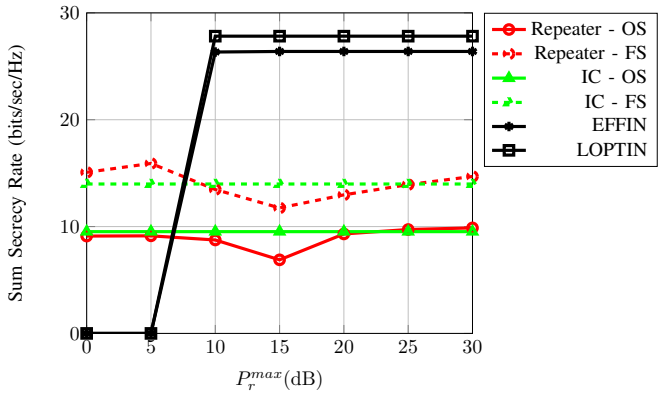


Fig. 5. The achievable sum secrecy rates of a two-user interference relay channel with 16 frequency subcarriers and 4 antennas at the relay is shown with varying relay power constraint. The TX power constraints are 10 dB and there are two antennas at the relay. The proposed scheme EFFIN and LOPTIN outperform baseline algorithms Repeater and IC by 200%. EFFIN achieves 94.86% of the sum secrecy rate performance by LOPTIN.

scheme EFFIN and LOPTIN outperform baseline algorithms Repeater and IC by 200% whereas the efficient EFFIN algorithm achieves 94.86% of the sum secrecy rate performance achieved by LOPTIN.

VI. Future Extensions

In this paper, we have proposed two relay design for the sum secrecy rates maximization on the multi-carrier relay-assisted interference channel, by utilizing the concept of information leakage neutralization. A natural and very essential extension of this work is to investigate the appropriate strategies in scenarios where the relay does not have perfect channel information of the interference network. The relay is assumed to have perfect channel information for channels going to and leaving from the relay as the relay should be able to estimate these channels in the corresponding uplink and downlink transmissions. However, the channel coefficients of the channels that do not go through the relay are fed back

to the relay by the transmitters and receivers and therefore are prompt to be imperfect. In such scenario, the relay is not able to completely neutralize information leakage. It is interesting to investigate the robustness of the information leakage neutralization scheme. At an extreme situation where the channel information is completely outdated, the relay may be able to improve the achievable secrecy rate by transmitting an artificial noise signal. The cut off point of channel information outdatedness for the transition from information leakage neutralization to artificial noise should be computed.

If the transmitters are equipped with multiple transmit antennas and the receivers are equipped with single antenna, the results obtained in this paper can be applied directly. This is because the addition of spatial dimension due to transmit antennas have the same effects of the multi-frequency channel studied in the manuscript. When the receivers are allowed to have multiple antenna, the problem becomes significantly more complicated because the relay or the transmitters are not able to predict the receive filters processing at the eavesdroppers.

One possible future extension is to integrate both artificial noise and information leakage neutralization in the following:

$$\mathbf{y}_r = \mathbf{R}(\mathbf{x}_r + \mathbf{n}_r) + \mathbf{R}_w\,\mathbf{w} \tag{33}$$

where $\mathbf{y}_r, \mathbf{x}_r$ are the output and input of the relay respectively; $\mathbf{n}_r$ is the background noise at relay; $\mathbf{w}$ is the artificial noise vector and $\mathbf{R}_w$ is the corresponding precoding matrix for the artificial noise vector. By choosing both $\mathbf{R}$ and $\mathbf{R}_w$, the relay can also take the role of a helper which transmits artificial noise. Note that the usage of artificial noise does not guarantee zero information leakage whereas information leakage neutralization sets the equivalent channel to zero and guarantees zero information leakage. In the scenario where information leakage neutralization is not possible, e.g., when the relay does not have enough power or antennas, it is possible to increase the secrecy rate by using artificial noise.

Appendix I
Proof of Proposition 1

If TX i transmits $S_i \leq M$ data streams, then $M - S_i$ columns of $\mathbf{P}_i$ are zeros. For example, in a system with 4 subcarriers where TX i transmits 2 data streams spread over 3 subcarriers, $\mathbf{P}_i$ has the following form,

$$\mathbf{P}_i = \begin{bmatrix} * & * & 0 & 0 \\ * & * & 0 & 0 \\ 0 & 0 & 0 & 0 \\ * & * & 0 & 0 \end{bmatrix}. \tag{34}$$

Denote the non-zero columns of $\mathbf{P}_i$ by $\hat{\mathbf{P}}_i \in \mathbb{C}^{M\times S_i}$. The information leakage constraint (18) is equivalent to

$$\left(\mathbf{H}_{ji} + \mathbf{G}_j^{\mathrm{H}}\,\mathbf{R}\,\mathbf{F}_i\right)\hat{\mathbf{P}}_i = 0, \qquad i,j = 1,\ldots,K, i \neq j. \tag{35}$$

For each i, we stack the constrains for all $j \neq i$ by using $\mathbf{G}_{-i}^{\mathrm{H}}$ from (15) and defining

$$\mathbf{H}_{-i} = [\mathbf{H}_{1i}^{\mathrm{H}}, \ldots, \mathbf{H}_{(i-1)i}^{\mathrm{H}}, \mathbf{H}_{(i+1)i}^{\mathrm{H}}, \ldots, \mathbf{H}_{Ki}^{\mathrm{H}}]^{\mathrm{H}}.$$

We write (35) as

$$\left(\mathbf{H}_{-i} + \mathbf{G}_{-i}^{\mathrm{H}}\,\mathbf{R}\,\mathbf{F}_i\right)\hat{\mathbf{P}}_i = 0, \qquad i = 1,\ldots,K \tag{36}$$

which can be manipulated to the following by performing vectorization on the matrices,

$$\left(\left(\hat{\mathbf{P}}_i^{\mathrm{T}}\,\mathbf{F}_i^{\mathrm{T}}\right)\otimes \mathbf{G}_{-i}^{\mathrm{H}}\right)\mathrm{vec}(\mathbf{R}) = -\,\mathrm{vec}\left(\mathbf{H}_{-i}\,\hat{\mathbf{P}}_i\right), \;\; i = 1,\ldots,K. \tag{37}$$

The matrix $\mathbf{H}_{-i}$ has dimension $(K-1)M \times M$ and the matrix $\hat{\mathbf{P}}_i$ has dimension $M \times S_i$. Hence, the product $\mathbf{H}_{-i}\,\mathbf{P}_i$ has dimension $(K-1)M \times S_i$. The number of constraints in (37) is the number of elements in $\mathbf{H}_{-i}\,\mathbf{P}_i$, which is $(K-1)MS_i$. Summing up all constraints for $i = 1,\ldots,K$, we have the total number of constraints $(K-1)M\sum_{i=1}^{K} S_i$. The number of variables is the number of elements in $\mathbf{R}$ which equals to M^2N^2. To neutralize information leakage at all users, we must satisfy (37) for all i. To this end, the relay must have the number of antennas N satisfying $M^2N^2 \geq (K-1)M\sum_{i=1}^{K} S_i$, or

$$N \geq \sqrt{\frac{K-1}{M}\sum_{i=1}^{K} S_i}. \tag{38}$$

Appendix II
Proof of Proposition 2

Stacking the matrices in (35) for all i, we obtain $\mathbf{A}\,\mathrm{vec}(\mathbf{R}) = \mathbf{b}$. The matrix $\mathbf{A}$ is a block matrix with vertically stacked blocks $\left(\hat{\mathbf{P}}_i^{\mathrm{T}}\,\mathbf{F}_i^{\mathrm{T}}\right)\otimes\mathbf{G}_{-i}^{\mathrm{H}}$, for $i = 1,\ldots,K$, and therefore has dimension $\sum_{i=1}^{K} S_i(K-1)M \times M^2N^2$. The matrix $\mathbf{G}_{-i}$ concatenates matrices $\mathbf{G}_j$ for $j \neq i$, e.g., $\mathbf{G}_{-1} = [\mathbf{G}_2,\ldots,\mathbf{G}_K]$. As $\mathbf{G}_{-i}$ are not mutually independent, $\mathbf{A}$ is of low rank. Denote the number of rows of $\mathbf{A}$ by $\alpha = \sum_{i=1}^{K} S_i(K-1)M$ and the rank of $\mathbf{A}$ by $\beta = \mathrm{rank}(\mathbf{A})$. The pseudo-inverse of $\mathbf{A}$ can be computed by performing singular-value-decomposition on $\mathbf{A}$,

$$[\mathbf{A}]_{\alpha\times M^2N^2} = [\mathbf{U}_1 \,|\, \mathbf{U}_2]\begin{bmatrix} \mathbf{\Gamma} & \mathbf{0}_{\beta\times(M^2N^2-\beta)} \\ \mathbf{0}_{(\alpha-\beta)\times\beta} & \mathbf{0}_{(\alpha-\beta)\times(M^2N^2-\beta)} \end{bmatrix}\begin{bmatrix} \mathbf{V}_1^{\mathrm{H}} \\ \mathbf{V}_2^{\mathrm{H}} \end{bmatrix}, \tag{39}$$

where $\mathbf{U}_1 \in \mathbb{C}^{\alpha\times\beta}, \mathbf{U}_2 \in \mathbb{C}^{\alpha\times(\alpha-\beta)}$ are the left singular vectors in the signal space and null space of $\mathbf{A}$ respectively; $\mathbf{V}_1^{\mathrm{H}} \in \mathbb{C}^{\beta\times M^2N^2}$, $\mathbf{V}_2^{\mathrm{H}} \in \mathbb{C}^{(M^2N^2-\beta)\times M^2N^2}$ are the right singular vectors in the signal space and null space of $\mathbf{A}$ respectively; $\mathbf{\Gamma} \in \mathbb{C}^{\beta\times\beta}$ holds the non-zero singular values in the diagonal and zeros everywhere else. Thus, the solution of $\mathrm{vec}(\mathbf{R})$ satisfying $\mathbf{A}\,\mathrm{vec}(\mathbf{R}) = \mathbf{b}$ is

$$\mathrm{vec}(\mathbf{R}) = \mathbf{V}_1\,\mathbf{\Gamma}^{-1}\,\mathbf{U}_1^{\mathrm{H}}\,\mathbf{b} + \mathbf{V}_2\,\mathbf{y} \tag{40}$$

where $\mathbf{y}$ is any vector in the space of $\mathbb{C}^{M^2N^2\times 1}$. The result follows by setting $\mathbf{z} = \mathbf{V}_2\,\mathbf{y}$ as a vector in the null space of $\mathbf{A}$.

APPENDIX III
PROOF OF COROLLARY 1

Using the properties of Kronecker products, the relay transmit power from (12) is equivalent to $\left(\mathbf{A}^\dagger\,\mathbf{b}+\mathbf{z}\right)^{\mathrm{H}}\left(\left(\sum_{i=1}^{K}\mathbf{F}_i\,\mathbf{P}_i\,\mathbf{P}_i^{\mathrm{H}}\,\mathbf{F}_i^{\mathrm{H}}+\mathbf{I}_{MN}\right)\otimes\mathbf{I}_{MN}\right)\left(\mathbf{A}^\dagger\,\mathbf{b}+\mathbf{z}\right)$. By Proposition 2 and (12), the minimum transmit power required to satisfy information leakage neutralization is attained when $\mathbf{z}=\mathbf{0}$. This is due to the fact that $\mathbf{z}$ is in the null space of $\mathbf{A}$ and $\mathbf{Q}=\left(\sum_{i=1}^{K}\mathbf{F}_i\,\mathbf{P}_i\,\mathbf{P}_i^{\mathrm{H}}\,\mathbf{F}_i^{\mathrm{H}}+\mathbf{I}_{MN}\right)\otimes\mathbf{I}_{MN}$ is positive semi-definite and $\mathbf{z}^{\mathrm{H}}\,\mathbf{Q}\,\mathbf{z}\geq 0$ for any $\mathbf{z}$.

APPENDIX IV
FORMULATION OF $\mathcal{Q}_2'$

Let $\mathbf{E}_i^T=\mathbf{e}_i^T\otimes\mathbf{I}_M$, $\bar{\mathbf{T}}_i=[\mathbf{T}_i,\mathbf{I}_M]$ and

$$\begin{aligned}
&\tilde{\mathbf{F}}=\left(\mathbf{F}\,\mathbf{P}\right)^{\dagger}\left(\mathbf{F}\,\mathbf{P}\right)^{\mathrm{H}\,\dagger},\mathbf{X}_i=\sum_{m=1}^{K}\sum_{l=1}^{K}\mathbf{H}_{im}\,\mathbf{P}_m\,\tilde{\mathbf{F}}_{ml}\,\mathbf{P}_l^{\mathrm{H}}\,\mathbf{H}_{il}^{\mathrm{H}},\\
&\mathbf{Y}_i=\begin{bmatrix}\tilde{\mathbf{F}}_{ii} & -\sum_{l=1}^{K}\tilde{\mathbf{F}}_{il}\,\mathbf{P}_l^{\mathrm{H}}\,\mathbf{H}_{il}^{H}\\ -\sum_{m=1}^{K}\mathbf{H}_{im}\,\mathbf{P}_m\,\tilde{\mathbf{F}}_{mi} & \mathbf{I}_M\end{bmatrix},\\
&\mathbf{Z}_i=\begin{bmatrix}\mathbf{I}_M & \mathbf{0}_M\\ \mathbf{0}_M & \mathbf{0}_M\end{bmatrix}+\mathbf{Y}_i\,.
\end{aligned}\tag{41}$$

With the equality constraint (26), the amplification noise can be written as (42) where $\tilde{\mathbf{F}}_{ml}\in\mathbb{C}^M$ is the (m,l)-th block matrix in $\tilde{\mathbf{F}}$. As a result, the objective can be written as

$$\begin{aligned}
&\sum_{i=1}^{K}\mathcal{C}\left(\mathbf{I}_M+\mathbf{T}_i\,\mathbf{T}_i^{\mathrm{H}}\left(\mathbf{G}_i^{\mathrm{H}}\,\mathbf{R}\,\mathbf{R}^{\mathrm{H}}\,\mathbf{G}_i+\mathbf{I}_M\right)^{-1}\right)\\
&=\sum_{i=1}^{K}\left(\mathcal{C}\left(\mathbf{I}_M+\mathbf{T}_i\,\mathbf{T}_i^{\mathrm{H}}+\mathbf{G}_i^{\mathrm{H}}\,\mathbf{R}\,\mathbf{R}^{\mathrm{H}}\,\mathbf{G}_i\right)\right.\\
&\qquad\left.-\mathcal{C}\left(\mathbf{I}_M+\mathbf{G}_i^{\mathrm{H}}\,\mathbf{R}\,\mathbf{R}^{\mathrm{H}}\,\mathbf{G}_i\right)\right)\\
&=\sum_{i=1}^{K}\left(\mathcal{C}\left(\mathbf{X}_i+\bar{\mathbf{T}}_i\,\mathbf{Z}_i\,\bar{\mathbf{T}}_i^{H}\right)-\mathcal{C}\left(\mathbf{X}_i+\bar{\mathbf{T}}_i\,\mathbf{Y}_i\,\bar{\mathbf{T}}_i^{\mathrm{H}}\right)\right).
\end{aligned}$$

Similarly, the power constraint is written as (43).

APPENDIX V
COMPUTATION OF THE GRADIENT OF LAGRANGIAN (29)

We compute the gradient of the Lagrangian (29) with respect to $\mathbf{T}$,

$$\mathcal{D}_{\mathbf{T}^*}\,L(\mathbf{T},\lambda)=\mathcal{D}_{\mathbf{T}^*}\sum_{i=1}^{K}f_i(\mathbf{T}_i)-\lambda\,\mathcal{D}_{\mathbf{T}^*}\,g(\mathbf{T}).$$

As $f_i(\mathbf{T}_i)$ is independent to $\mathbf{T}_j$ for $j\neq i$, the derivative can be written in a block diagonal form

$$\begin{aligned}
&\mathcal{D}_{\mathbf{T}^*}\,L(\mathbf{T},\lambda)\\
&=\mathrm{diag}\left(\mathcal{D}_{\mathbf{T}_1^*}\,f_1(\mathbf{T}_1),\ldots,\mathcal{D}_{\mathbf{T}_K^*}\,f_K(\mathbf{T}_K)\right)-\lambda\,\mathcal{D}_{\mathbf{T}^*}\,g(\mathbf{T}).
\end{aligned}\tag{44}$$

The gradient of the objective function $f_i(\mathbf{T}_i)$ with respect to $\mathbf{T}_i^*$ is

$$\begin{aligned}
&\mathcal{D}_{\mathbf{T}_i^*}\,f_i(\mathbf{T}_i)\\
&=\mathcal{D}_{\mathbf{T}_i^*}\,\mathcal{C}\left(\mathbf{X}_i+\bar{\mathbf{T}}_i\,\mathbf{Z}_i\,\bar{\mathbf{T}}_i^{H}\right)-\mathcal{D}_{\mathbf{T}_i^*}\,\mathcal{C}\left(\mathbf{X}_i+\bar{\mathbf{T}}_i\,\mathbf{Y}_i\,\bar{\mathbf{T}}_i^{\mathrm{H}}\right).
\end{aligned}\tag{45}$$

We begin with

$$\begin{aligned}
&\ln(2)\,\mathcal{D}_{\mathbf{T}_i^*}\,\mathcal{C}\left(\mathbf{X}_i+\bar{\mathbf{T}}_i\,\mathbf{Z}_i\,\bar{\mathbf{T}}_i^{H}\right)\\
&=\mathcal{D}_{\bar{\mathbf{T}}_i^*}\ln\det\left(\mathbf{X}_i+\bar{\mathbf{T}}_i\,\mathbf{Z}_i\,\bar{\mathbf{T}}_i^{H}\right)\cdot\mathcal{D}_{\mathbf{T}_i^*}\,\bar{\mathbf{T}}_i^*\\
&=\mathrm{vec}\left(\left(\mathbf{X}_i+\bar{\mathbf{T}}_i\,\mathbf{Z}_i\,\bar{\mathbf{T}}_i^{H}\right)^{-1}\bar{\mathbf{T}}_i\,\mathbf{Z}_i\right)^{\mathrm{T}}\cdot\frac{\partial\,\mathrm{vec}(\bar{\mathbf{T}}_i^*)}{\partial\,\mathrm{vec}(\mathbf{T}_i^*)}\\
&=\mathrm{vec}\left(\left(\mathbf{X}_i+\bar{\mathbf{T}}_i\,\mathbf{Z}_i\,\bar{\mathbf{T}}_i^{H}\right)^{-1}\bar{\mathbf{T}}_i\,\mathbf{Z}_i\right)^{\mathrm{T}}\begin{bmatrix}\mathbf{I}_{M^2}\\ \mathbf{0}_{M^2}\end{bmatrix}\\
&=\left[\left(\mathbf{X}_i+\bar{\mathbf{T}}_i\,\mathbf{Z}_i\,\bar{\mathbf{T}}_i^{H}\right)^{-1}\bar{\mathbf{T}}_i\,\mathbf{Z}_i\right]_{(:,1:M)}\\
&=\left(\mathbf{X}_i+\bar{\mathbf{T}}_i\,\mathbf{Z}_i\,\bar{\mathbf{T}}_i^{H}\right)^{-1}\bar{\mathbf{T}}_i\begin{bmatrix}\mathbf{I}_M+\tilde{\mathbf{F}}_{ii}\\ -\sum_{m=1}^{K}\mathbf{H}_{im}\,\mathbf{P}_m\,\tilde{\mathbf{F}}_{mi}\end{bmatrix}.
\end{aligned}\tag{46}$$

Similarly, we have

$$\begin{aligned}
&\ln(2)\,\mathcal{D}_{\mathbf{T}_i^*}\,\mathcal{C}\left(\mathbf{X}_i+\bar{\mathbf{T}}_i\,\mathbf{Y}_i\,\bar{\mathbf{T}}_i^{H}\right)\\
&=\left(\mathbf{X}_i+\bar{\mathbf{T}}_i\,\mathbf{Y}_i\,\bar{\mathbf{T}}_i^{H}\right)^{-1}\bar{\mathbf{T}}_i\begin{bmatrix}\tilde{\mathbf{F}}_{ii}\\ -\sum_{m=1}^{K}\mathbf{H}_{im}\,\mathbf{P}_m\,\tilde{\mathbf{F}}_{mi}\end{bmatrix}.
\end{aligned}\tag{47}$$

Thus, we have the gradient of $f_i(\mathbf{T}_i)$ as

$$\begin{aligned}
&\mathcal{D}_{\mathbf{T}_i^*}\,f_i(\mathbf{T}_i)\\
&=\frac{1}{\ln(2)}\left(\left(\mathbf{X}_i+\bar{\mathbf{T}}_i\,\mathbf{Z}_i\,\bar{\mathbf{T}}_i^{H}\right)^{-1}\bar{\mathbf{T}}_i\begin{bmatrix}\mathbf{I}_M+\tilde{\mathbf{F}}_{ii}\\ -\sum_{m=1}^{K}\mathbf{H}_{im}\,\mathbf{P}_m\,\tilde{\mathbf{F}}_{mi}\end{bmatrix}\right.\\
&\left.-\left(\left(\mathbf{X}_i+\bar{\mathbf{T}}_i\,\mathbf{Y}_i\,\bar{\mathbf{T}}_i^{H}\right)^{-1}\bar{\mathbf{T}}_i\begin{bmatrix}\tilde{\mathbf{F}}_{ii}\\ -\sum_{m=1}^{K}\mathbf{H}_{im}\,\mathbf{P}_m\,\tilde{\mathbf{F}}_{mi}\end{bmatrix}\right)\right).
\end{aligned}\tag{48}$$

The last step of computing the gradient of the Lagrangian is to compute

$$\begin{aligned}
&\mathcal{D}_{\mathbf{T}^*}\,\mathrm{tr}\left(\mathbf{G}^{\mathrm{H}\,\dagger}\left(\mathbf{T}-\mathbf{H}\,\mathbf{P}\right)\left(\tilde{\mathbf{F}}+\mathbf{I}_{KM}\right)\left(\mathbf{T}-\mathbf{H}\,\mathbf{P}\right)^{\mathrm{H}}\mathbf{G}^{\dagger}\right)\\
&=\mathbf{G}^{\dagger}\,\mathbf{G}^{\mathrm{H}\,\dagger}\left(\mathbf{T}-\mathbf{H}\,\mathbf{P}\right)\left(\tilde{\mathbf{F}}+\mathbf{I}_{KM}\right).
\end{aligned}\tag{49}$$

Combining (44), (48) and (49), the gradient of the Lagrangian is obtained.

REFERENCES

[1] Z. K.-M. Ho, E. Jorswieck, and S. Gerbracht, "Efficient Information Leakage Neutralization on a Relay-assisted Multi-carrier Interference Channel," in *Proceedings of ICASSP*, 2013.

[2] F. Mattern, "Wireless Future : Ubiquitous Computing," in *Proceedings of Wireless Congress*, 2004, pp. 1–10.

[3] Y. Liang, H. V. Poor, and S. Shamai (Shitz), *Information Theoretic Security*, Now Publishers Inc., 2009.

[4] R.-H. Liu and W. Trappe, Eds., *Securing Wireless Communications at the Physical Layer*, Springer, 2009.

[5] M. Bloch and J. Barros, *Physical-Layer Security: From Information Theory to Security Engineering*, Cambridge University Press, 2011.

[6] A. D. Wyner, "The Wiretap Channel," *Bell Systems Technology Journal*, vol. 54, pp. 1355– 1387, 1975.

$$
\begin{aligned}
&\mathbf{G}_i^{\mathrm{H}}\,\mathbf{R}\,\mathbf{R}^{\mathrm{H}}\,\mathbf{G}_i = \mathbf{E}_i^{\mathrm{T}}\,\mathbf{G}^{\mathrm{H}}\,\mathbf{R}\,\mathbf{R}^{\mathrm{H}}\,\mathbf{G}\,\mathbf{E}_i \\
&= \mathbf{E}_i^{\mathrm{T}}\,(\mathbf{T}-\mathbf{H}\,\mathbf{P})\,(\mathbf{F}\,\mathbf{P})^{\dagger}\,(\mathbf{F}\,\mathbf{P})^{\mathrm{H}\,\dagger}\,(\mathbf{T}-\mathbf{H}\,\mathbf{P})^{\mathrm{H}}\,\mathbf{E}_i \\
&= [-\mathbf{H}_{i1}\,\mathbf{P}_1,\ldots,\mathbf{T}_i-\mathbf{H}_{ii}\,\mathbf{P}_i,\ldots,-\mathbf{H}_{iK}\,\mathbf{P}_K]\begin{bmatrix}\tilde{\mathbf{F}}_{11} & \ldots & \tilde{\mathbf{F}}_{1K}\\ \vdots & \ddots & \vdots \\ \tilde{\mathbf{F}}_{K1} & \ldots & \tilde{\mathbf{F}}_{KK}\end{bmatrix}\begin{bmatrix}-\mathbf{P}_1^{\mathrm{H}}\,\mathbf{H}_{i1}^{\mathrm{H}}\\ \vdots \\ \mathbf{T}_i^{\mathrm{H}}-\mathbf{P}_i^{\mathrm{H}}\,\mathbf{H}_{ii}^{\mathrm{H}}\\ \vdots \\ -\mathbf{P}_K^{\mathrm{H}}\,\mathbf{H}_{iK}^{\mathrm{H}}\end{bmatrix} \\
&= \sum_{m=1}^{K}\sum_{l=1}^{K}\mathbf{H}_{im}\,\mathbf{P}_m\,\tilde{\mathbf{F}}_{ml}\,\mathbf{P}_l^{\mathrm{H}}\,\mathbf{H}_{il}^{\mathrm{H}} - \mathbf{T}_i\sum_{l=1}^{K}\tilde{\mathbf{F}}_{il}\,\mathbf{P}_l^{\mathrm{H}}\,\mathbf{H}_{il}^{H} - \sum_{m=1}^{K}\mathbf{H}_{im}\,\mathbf{P}_m\,\tilde{\mathbf{F}}_{mi}\,\mathbf{T}_i^{\mathrm{H}} + \mathbf{T}_i\,\tilde{\mathbf{F}}_{ii}\,\mathbf{T}_i^{\mathrm{H}} \\
&= \mathbf{X}_i - \mathbf{I}_M + [\mathbf{T}_i,\mathbf{I}_M]\begin{bmatrix}\tilde{\mathbf{F}}_{ii} & -\sum_{l=1}^{K}\tilde{\mathbf{F}}_{il}\,\mathbf{P}_l^{\mathrm{H}}\,\mathbf{H}_{il}^{H}\\ -\sum_{m=1}^{K}\mathbf{H}_{im}\,\mathbf{P}_m\,\tilde{\mathbf{F}}_{mi} & \mathbf{I}_M\end{bmatrix}\begin{bmatrix}\mathbf{T}_i^{H}\\ \mathbf{I}_M\end{bmatrix} \\
&= \mathbf{X}_i - \mathbf{I}_M + \bar{\mathbf{T}}_i\,\mathbf{Y}_i\,\bar{\mathbf{T}}_i^{\mathrm{H}},
\end{aligned}
\tag{42}
$$

$$
\begin{aligned}
&\mathrm{tr}\left(\mathbf{R}\left(\mathbf{F}\,\mathbf{P}\,\mathbf{P}^{\mathrm{H}}\,\mathbf{F}^{\mathrm{H}}+\mathbf{I}_{MN}\right)\mathbf{R}^{\mathrm{H}}\right) \\
&= \mathrm{tr}\left(\mathbf{G}^{\mathrm{H}\,\dagger}\,(\mathbf{T}-\mathbf{H}\,\mathbf{P})\,(\mathbf{F}\,\mathbf{P})^{\dagger}\left(\mathbf{F}\,\mathbf{P}\,\mathbf{P}^{\mathrm{H}}\,\mathbf{F}^{\mathrm{H}}+\mathbf{I}_{MN}\right)(\mathbf{F}\,\mathbf{P})^{\dagger\,\mathrm{H}}\,(\mathbf{T}-\mathbf{H}\,\mathbf{P})^{\mathrm{H}}\,\mathbf{G}^{\dagger}\right) \\
&= \mathrm{tr}\left(\mathbf{G}^{\mathrm{H}\,\dagger}\,(\mathbf{T}-\mathbf{H}\,\mathbf{P})\left((\mathbf{F}\,\mathbf{P})^{\dagger}\,(\mathbf{F}\,\mathbf{P})^{\dagger\,\mathrm{H}}+\mathbf{I}_{KM}\right)(\mathbf{T}-\mathbf{H}\,\mathbf{P})^{\mathrm{H}}\,\mathbf{G}^{\dagger}\right) \\
&= \mathrm{tr}\left(\mathbf{G}^{\mathrm{H}\,\dagger}\,(\mathbf{T}-\mathbf{H}\,\mathbf{P})\left(\tilde{\mathbf{F}}+\mathbf{I}_{KM}\right)(\mathbf{T}-\mathbf{H}\,\mathbf{P})^{\mathrm{H}}\,\mathbf{G}^{\dagger}\right) \le P_r^{max}.
\end{aligned}
\tag{43}
$$

[7] Y.-S. Shiu, S.-Y. Chang, H.-C. Wu, S. C.-H. Huang, and H.-W. Chen, "Physical Layer Security in Wireless Networks: A Tutorial," *IEEE Transactions on Wireless Communications*, vol. 18, no. 2, pp. 66–74, Apr. 2011.

[8] H. V. Poor, "Information and Inference in the Wireless Physical Layer," *IEEE Transactions on Wireless Communications*, vol. 19, no. 1, pp. 40–47, Feb. 2012.

[9] G. Zheng, L. C. Choo, and K. K. Wong, "Optimal Cooperative Jamming To Enhance Physical Layer Security Using Relays," *IEEE Transactions on Signal Processing*, vol. 59, no. 3, pp. 1317–1322, Mar. 2011.

[10] L. Dong and H. Jafarkhani, "Cooperative Jamming and Power Allocation for Wireless Relay Networks in Presence of Eavesdropper," in *Proceedings of IEEE International Conference on Communications (ICC)*, 2011.

[11] J. Huang and A. L. Swindlehurst, "Cooperative Jamming for Secure Communications in MIMO Relay Networks," *IEEE Transaction on Signal Processing*, vol. 59, no. 10, pp. 4871–4884, Oct. 2011.

[12] L. Lai and H. El Gamal, "The Relay-Eavesdropper Channel: Cooperation for Secrecy," *IEEE Transactions on Information Theory*, vol. 54, no. 9, pp. 4005–4019, Sept. 2008.

[13] R. Bassily and S. Ulukus, "Deaf Cooperation for Secrecy with Multiple Antennas at the Helper," *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 6, pp. 1855 – 1864, Dec. 2012.

[14] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor, "Improving Wireless Physical Layer Security via Cooperating Relays," *IEEE Transactions on Signal Processing*, vol. 58, no. 3, pp. 1875–1888, Mar. 2010.

[15] D. W.-K. Ng, E. S. Lo, and R. Schober, "Secure Resource Allocation and Scheduling for OFDMA Decode-and-Forward Relay Networks," *IEEE Transactions on Wireless Communications*, vol. 10, no. 10, pp. 3528–3540, Oct. 2011.

[16] R. Bassily and S. Ulukus, "Secure Communication in Multiple Relay Networks Through Decode-and-Forward Strategies," *Journal of Communications and Networks*, vol. 14, no. 4, pp. 352–363, Aug. 2012.

[17] X. He and A. Yener, "Cooperation With an Untrusted Relay: A Secrecy Perspective," *IEEE Transactions on Information Theory*, vol. 56, no. 8, pp. 3807–3827, Aug. 2010.

[18] H. Khodakarami and F. Lahouti, "Link Adaptation for Fixed Relaying with Untrusted Relays: Transmission Strategy Design and Performance Analysis," in *Proceedings of International Conference on Telecommunications*, 2011, pp. 309–314.

[19] C. Jeong, I. M. Kim, and D. I. Kim, "Joint Secure Beamforming Design at the Source and the Relay for an Amplify-and-Forward MIMO Untrusted Relay System," *IEEE Transaction on Signal Processing*, vol. 60, no. 1, pp. 310 – 325, Jan. 2012.

[20] E. A. Jorswieck and A. Wolf, "Resource Allocation for the Wire-Tap Multi-Carrier Broadcast Channel," in *Proceedings of 2008 International Conference on Telecommunications*, June 2008, pp. 1–6.

[21] X.-W. Wang, M.-X. Tao, J.-H. Mo, and Y.-Y. Xu, "Power and Subcarrier Allocation for Physical-Layer Security in OFDMA-Based Broadband Wireless Networks," *IEEE Transactions on Information Forensics and Security*, vol. 6, no. 3, pp. 693–702, Sept. 2011.

[22] F. Renna, N. Laurenti, and H. V. Poor, "Physical-Layer Secrecy for OFDM Transmissions Over Fading Channels," *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 4, pp. 1354–1367, Aug. 2012.

[23] C. Jeong and I.-M. Kim, "Optimal Power Allocation for Secure Multicarrier Relay Systems," *IEEE Transactions on Signal Processing*, vol. 59, no. 11, pp. 5428–5442, Nov. 2011.

[24] S. Berger, M. Kuhn, and A. Wittneben, "Recent Advances in Amplify-and-Forward Two-Hop Relaying," *IEEE Communications Magazine*, vol. 47, no. 7, pp. 50–56, July 2009.

[25] A. El Gamal and N. Hassanpour, "Relay-without-Delay," in *Proceedings of International Symposium on Information Theory*, 2005, vol. 1, pp. 1078–1080.

[26] A. El Gamal, N. Hassanpour, and J. Mammen, "Relay Networks With Delays," *IEEE Transactions on Information Theory*, vol. 53, no. 10, pp. 3413–3431, Oct. 2007.

[27] V. R. Cadambe and S. A. Jafar, "Degrees of Freedom of Wireless Networks with Relays, Feedback, Co-operation and Full Duplex Operation," *IEEE Transactions on Information Theory*, vol. 55, no. 5, pp. 2334–2344, May 2009.

[28] N. Lee and S. A. Jafar, "Aligned Interference Neutralization and the Degrees of Freedom of the 2 User Interference Channel with Instantaneous Relay," *submitted to IEEE Transactions on Information Theory, available at http://arxiv.org/abs/1102.3833*, pp. 1–17, 2011.

[29] IEEE Std. 802.16j-2009, "IEEE Standard for Local and Metropolitan Area Networks - Part 16: Air Interface for Fixed Broadband Wireless Access Systems - Amendment 1: Multiple Relay Specification," 2009.

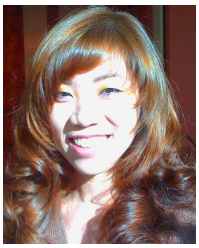
[30] E. Seidel, "Initial Thoughts on LTE Advanced for 3GPP Release 10," in *LTE World Summit, Berlin*, 2009.

[31] S. Mohajer, S. N. Diggavi, C. Fragouli, and D. N. C. Tse, "Transmission Techniques for Relay-Interference Networks," in *2008 46th Annual Allerton Conference on Communication, Control, and Computing*, Sept. 2008, pp. 467–474.

[32] S. Mohajer, S. N. Diggavi, and D. N. C. Tse, "Approximate Capacity of a Class of Gaussian Relay-Interference Networks," in *2009 IEEE International Symposium on Information Theory*, June 2009, vol. 57, pp. 31–35.
[33] S. Berger and A. Wittneben, "Cooperative Distributed Multiuser MMSE Relaying in Wireless Ad-Hoc Networks," in *Proceedings of Asilomar Conference on Signals, Systems and Computers*, 2005, pp. 1072–1076.
[34] B. Rankov and A. Wittneben, "Spectral Efficient Protocols for Half-duplex Fading Relay Channels," *IEEE Journal on Selected Areas in Communications*, vol. 25, no. 2, pp. 379–389, Feb. 2007.
[35] Z. K.-M. Ho and E. Jorswieck, "Instantaneous Relaying: Optimal Strategies and Interference Neutralization," *IEEE Transactions on Signal Processing*, vol. 60, no. 12, pp. 6655 – 6668, Dec. 2012.
[36] S. Gerbracht, E. A. Jorswieck, G. Zheng, and B. Ottersten, "Non-regenerative Two-Hop Wiretap Channels using Interference Neutralization," in *Proceedings of IEEE International Workshop on Information Forensics and Security (WIFS)*, 2012.
[37] M. Bloch and J. Barros, *Physical Layer Security From Information Theory to Security Engineering*, Cambridge University Press, 2011.
[38] A. Khisti and G. Wornell, "Secure Transmission with Multiple Antennas - Part II: The MIMOME Wiretap Channel," *IEEE Transactions on Information Theory*, vol. 56, no. 11, pp. 5515 – 5532, Nov. 2010.

ACKNOWLEDGMENT

The authors would like to thank the editor and all the reviewers for their helpful comments.



Zuleita Ho Zuleita K.-M. Ho (S'06-M'10) received her Ph.D. in wireless communication from EURECOM and Telecom Paris, France in 2010. In 2005 and 2007, She received her Bachelor and Master in Philosophy degree in Electronic Engineering (Wireless Communication) from Hong Kong University of Science and Technology (HKUST). From 2003 to 2004, she studied as a visiting student in Massachusetts Institute of Technology (MIT) supported by the HSBC scholarship for Overseas Studies. From 2011 till now, she has joined Chair for Communications Theory, Technische Universität Dresden, Germany. Zuleita enrolled into HKUST in 2002 through the Early Admission Scheme for gifted students. In 2003, she received the HSBC scholarship for Overseas Studies and visited MIT for 1 year. In 2007, she received one of the most prestigious scholarships in Hong Kong, The Croucher Foundation Scholarship , which supports her doctorate education in France. Other scholarships received include Sumida and Ichiro Yawata Foundation (2004, 2006), The Hong Kong Electric Co Ltd Scholarship (2004) and The IEE Outstanding Student Award (2004).

Eduard Jorswieck Eduard A. Jorswieck (S'01-M'05-SM'08) received his Diplom-Ingenieur degree and Doktor-Ingenieur (Ph.D.) degree, both in electrical engineering and computer science from the Berlin University of Technology (TUB), Germany, in 2000 and 2004, respectively. He was with the Fraunhofer Institute for Telecommunications, Heinrich-Hertz-Institute (HHI) Berlin, from 2001 to 2006. In 2006, he joined the Signal Processing Department at the Royal Institute of Technology (KTH) as a post-doc and became a Assistant Professor in 2007. Since February 2008, he has been the head of the Chair of Communications Theory and Full Professor at Dresden University of Technology (TUD), Germany. His research interests are within the areas of applied information theory, signal processing and wireless communications. He is senior member of IEEE and elected member of the IEEE SPCOM Technical Committee. From 2008-2011 he served as an Associate Editor and since 2012 as a Senior Associate Editor for IEEE SIGNAL PROCESSING LETTERS. Since 2011 he serves as an Associate Editor for IEEE TRANSACTIONS ON SIGNAL PROCESSING. Since 2013, Eduard serves as Associate Editor for IEEE Transactions on Wireless Communications. In 2006, he was co-recipient of the IEEE Signal Processing Society Best Paper Award.

Sabrina Gerbracht Sabrina Gerbracht received the Diplom Medien-Informatiker (M.S.) degree in media computer science from the Technische Universität Dresden (TUD), Germany, in 2007, where she is currently pursuing the Ph.D. degree. Since June 2007, she has been a Research Assistant with the Communications Laboratory, Department of Electrical and Computer Engineering, TUD. Her research interests include the fields of physical layer secrecy, wireless communications, and signal processing.