Opportunistic Relay and Jammer Cooperation Techniques for Physical-Layer Security in Buffer-aided Relay Networks

Xiaotao Lu and Rodrigo C. de Lamare

***Abstract*—In this paper, we investigate opportunistic relay and jammer cooperation schemes in multiple-input multiple-output (MIMO) buffer-aided relay networks. The network consists of one source, an arbitrary number of relay nodes, legitimate users and eavesdroppers, with the constraints of physical layer security. We propose an algorithm to select a set of relay nodes to enhance the legitimate users' transmission and another set of relay nodes to perform jamming of the eavesdroppers. With Inter-Relay interference (IRI) taken into account, interference cancellation can be implemented to assist the transmission of the legitimate users. Secondly, IRI can also be used to further increase the level of harm of the jamming signal to the eavesdroppers. By exploiting the fact that the jamming signal can be stored at the relay nodes, we also propose a hybrid algorithm to set a signal-to-interference and noise ratio (SINR) threshold at the node to determine the type of signal stored at the relay node. With this separation, the signals with high SINR are delivered to the users as conventional relay systems and the low SINR performance signals are stored as potential jamming signals. Simulation results show that the proposed techniques obtain a significant improvement in secrecy rate over previously reported algorithms.**

***Index Terms*—Physical-layer security techniques, secrecy-rate analysis, relay selection, jamming techniques.**

I. Introduction

In broadcast channels, secure transmission is difficult to achieve due to the broadcast nature of wireless communication systems. Traditional encryption techniques are implemented in the network layer. With complex algorithms, encryption keys which are nearly unbreakable are generated to ensure security while their costs are extremely high. To reduce the costs of encryption algorithms, researchers are investigating novel security techniques in the physical layer of wireless systems. Physical-layer security has been first illustrated in [1] from the viewpoint of information theory. The feasibility of physical-layer security has been discussed by Shannon at the theoretical level in the paper. Later on in [2] a wire-tap channel which can achieve positive secrecy rate has been proposed by Wyner under the assumption that the users experience a better channel than eavesdroppers. Since then, the wire-tap model along with other techniques such as the broadcast channel [3], MIMO channels [4], [5], artificial noise [6], beamforming [7] as well as relay systems [8] have been studied. In this work, we focus on relay systems and cooperation schemes involving relay and jamming strategies in relays equipped with buffers.

A. Prior and Related Work

In recent years [9], the concept of physical-layer security with multiuser wireless networks has been investigated in numerous studies. Approaches to achieving physical-layer security include the design of transmit precoding strategies without the need for a secret key and the exploitation of the wireless communication medium to develop secret keys over public channels. Relay-based cooperative systems [9] are an important evolution of secure transmission strategies that can further improve the performance of wireless systems. In this context, buffer-aided relay nodes have recently drawn much attention [10], [11] and [12] due to their potential to further improve the secrecy rate in wireless transmissions as compared to standard relays. In our prior investigation with [13], [14] and [15] we have reported precoding techniques [16] as well as buffer-aided relay system [17] which improve the secrecy rate performance in multiuser MIMO systems.

Prior work on buffer-aided relay systems with secure transmissions has been considered in half-duplex and full-duplex systems. In [10], the system model is described as one source, one half-duplex decode-and-forward (DF) buffer relay and one destination. Regarding the availability of the channel state information at the transmitter (CSIT), two schemes with fixed-rate transmission and mixed-rate transmission have been proposed. Based on the instantaneous signal-to-noise ratio (SNR) of the source-relay and relay-destination links a solution to the throughput-optimal problem has been reported [10]. In [11], a max-ratio relay selection policy has been proposed to optimize the secrecy transmission rate with the consideration of exact and average gains of the eavesdroppers's channels. In [12], a two-hop half-duplex buffer-aided relay system has been studied, where a relay selection which adapts reception and transmission time slots on the channel quality is proposed and the selection parameters are optimized to maximize the secrecy throughput or minimize the secrecy outage probability (SOP). Half-duplex systems can avoid the interference for the transmission at the relay nodes and their drawback lies in the requirement of two or more time slots for transmission, which decreases the transmission rate significantly.

Compared with half-duplex systems, full-duplex systems can provide a better performance in terms of transmission rate. An opportunistic relay scheme has been applied to buffer-aided systems in [18], [19] and [20]. In the opportunistic relay scheme, the inter-relay interference (IRI) is an important aspect that should be taken into account. In [18], IRI cancellation has been combined for the first time with buffer-aided relays and power adaptation to mitigate IRI and minimize the energy consumption. With one source and one destination, a new relay selection policy has been analyzed in terms of outage probability and diversity. Furthermore, in [19] a distributed joint relay-pair selection has been proposed with the aim of rate maximization in each time slot. By exploring the feasibility of IRI cancellation at the relay nodes, it gives the threshold to avoid increased relay-pair switching and CSI acquisition. With relay selection, in [20] and [21] jammer selection as well as a joint relay and jammer selection have been proposed. In such systems, relays may obtain a better transmission rate

Xiaotao Lu is with the Communications Research Group, Department of Electronics, University of York, YO10 5DD York, U.K., R. C. de Lamare is with CETUC, PUC-Rio, Brazil and with the Communications Research Group, Department of Electronics, University of York, YO10 5DD York, U.K. This work was supported by CNPq and FAPERJ. E-mails: xtl503@york.ac.uk; rodrigo.delamare@york.ac.uk.

978-1-4673-6540-6/15/$31.00 © 2015 IEEE

for the legitimate users, whereas jammers can interfere in the transmission to the eavesdropper, resulting in improvement of the secrecy rate. There are very few works in the literature which consider cooperation between opportunistic buffer-aided relay schemes with jamming techniques.

B. Contributions

Our work focuses on the use of the interference among buffer-aided relays to assist the secure transmission to the users. The major contributions in our paper are:

- Novel multi-user relay systems with relay and jammer function selection to achieve high secrecy rates.
- Novel multi-user buffer-aided relay systems with signals stored in the buffers which are capable of jamming eavesdroppers to achieve high secrecy rate.
- Secrecy rate analyses of the proposed relay and jammer selection schemes

The rest of this paper is organized as follows. In Section II, the system model and the performance metrics are introduced. A brief review of the buffer relay selection is included in Section III. The proposed relay and jammer function selection (RJF) as well as the buffer-aided RJF (BF-RJF) selection are introduced in Section IV. In Section IV, we discuss and present the simulation results. The conclusions are given in Section V.

C. Notation

Bold uppercase letters $\boldsymbol{A} \in \mathbf{C}^{M \times N}$ denote matrices with size $M \times N$ and bold lowercase letters $\boldsymbol{a} \in \mathbf{C}^{M \times 1}$ denote column vectors with length M. Conjugate, transpose, and conjugate transpose are represented by $(\cdot)^*$, $(\cdot)^T$ and $(\cdot)^H$ respectively; $\boldsymbol{I}_M$ is the identity matrix of size $M \times M$; $\text{diag}\{\boldsymbol{a}\}$ denotes a diagonal matrix with the elements of the vector $\boldsymbol{a}$ along its diagonal; $\mathcal{CN}(0, \sigma_n^2)$ represents complex Gaussian random variables with $i.i.d$ entries with zero mean and σ_n^2 variance.

II. System Model and Performance Metrics

In this section, we introduce the buffer-aided relay system model and describe the data transmission. The problem statement is then presented along with the performance metrics used to assess the proposed and existing techniques.

A. System Model

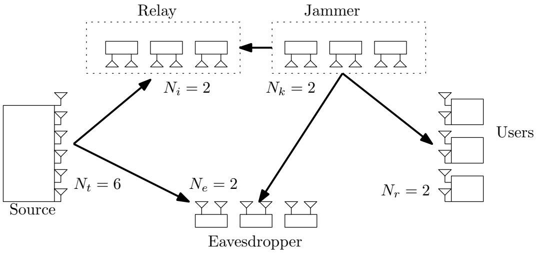


Fig. 1: System model of a MU-MIMO system with M users, N eavesdroppers T relays and K jammers

Fig. 1 gives a description of a transmitter with N_t antennas used to transmit the data streams to M users along with N eavesdroppers. With T relays and K jammers, in each time slot the selected relays and the eavesdroppers receive the signal from both the source and the jammers. Note that the signals from the jammers are the signals transmitted in the previous time slots. They exploit the buffers at the relay nodes. Each relay and jammer is equipped with N_i and N_k antennas. At the receiver side each user and eavesdropper is equipped with N_r and N_e receive antennas. In this system, we assume that the eavesdroppers do not jam the transmission of each user, relay or jammer and that the eavesdropper channel is a flat-fading MIMO channel. The quantities $\boldsymbol{H}_i \in \mathbf{C}^{N_i \times N_t}$ and $\boldsymbol{H}_e \in \mathbf{C}^{N_e \times N_t}$ denote the channel matrix from the source directly to the ith relay and the eth eavesdropper, respectively. The quantities $\boldsymbol{H}_{ke} \in \mathbf{C}^{N_e \times N_k}$ and $\boldsymbol{H}_{kr} \in \mathbf{C}^{N_r \times N_k}$ denote the channel matrix of the eth eavesdropper to the kth jammer and rth user to the kth jammer, respectively. The channel between the kth relay to the ith relay is described by $\boldsymbol{H}_{ki} \in \mathbb{C}^{N_i \times N_k}$.

The vector $\boldsymbol{s}_r^{(t)} \in \mathbb{C}^{N_r \times 1}$ represents the data symbols to be transmitted corresponding to each user in time slot t. The total transmit signal at the transmitter can be expressed as $\boldsymbol{s}^{(t)} = \begin{bmatrix} \boldsymbol{s}_1^{(t)^T} & \boldsymbol{s}_2^{(t)^T} & \boldsymbol{s}_3^{(t)^T} & \cdots & \boldsymbol{s}_M^{(t)^T} \end{bmatrix}^T$. In each phase the received signal $\boldsymbol{y}_i^{(t)} \in \mathbb{C}^{N_i \times 1}$ at each relay node can be expressed as

$$\boldsymbol{y}_i^{(t)} = \boldsymbol{H}_i \boldsymbol{s}^{(t)} + \sum_{k=1}^{K} \boldsymbol{H}_{ki} \boldsymbol{y}_k^{(pt)} + \boldsymbol{n}_i, \tag{1}$$

In (1), the superscript $(\cdot)^{(pt)}$ represents the previous time slot when the signal is stored as a jamming signal in the buffer at the relay nodes. The second term $\boldsymbol{H}_{ik} \boldsymbol{y}_k^{(pt)}$ is regarded as the inter-relay interference (IRI) between the ith relay and the kth relay. The received signal $\boldsymbol{y}_k^{(pt)}$ is determined as the jamming signal according to a signal-to-interference-plus-noise ratio (SINR) criterion illustrated in the paper. With the theorem in [18], IRI can be eliminated. The received signal at the eth eavesdropper is given by

$$\boldsymbol{y}_e^{(t)} = \boldsymbol{H}_e \boldsymbol{s}^{(t)} + \sum_{k=1}^{K} \boldsymbol{H}_{ke} \boldsymbol{y}_k^{(pt)} + \boldsymbol{n}_e, \tag{2}$$

where for the eavesdropper, the second term $\boldsymbol{H}_{ek} \boldsymbol{y}_k^{(pt)}$ acts as the jamming signal and this jamming signal can not be removed without the knowledge of the channel from the kth jammer to the eth eavesdropper.

In (1) and (2), the IRI term between relay nodes or the jamming signal to the eavesdropper is also the transmit signal from the relays nodes to the destination. We assume that the transmit signal from the relay nodes is described by $\boldsymbol{r}^{(t)} = \begin{bmatrix} \boldsymbol{y}_1^{(pt_1)^T} & \boldsymbol{y}_2^{(pt_2)^T} & \boldsymbol{y}_3^{(pt_3)^T} & \cdots & \boldsymbol{y}_T^{(pt_T)^T} \end{bmatrix}^T$. Note that the superscript $(\cdot)^{(pt)}$ represents the previous time slot due to the nature of relay nodes with buffers. The values for the ith relay node can be different so the previous time slot is represented by $(\cdot)^{(pt_i)}$. The received signal at the destination is expressed as

$$\boldsymbol{y}_r^{(t)} = \sum_{k=1}^{T} \boldsymbol{H}_{kr} \boldsymbol{y}_k^{(pt_k)} + \boldsymbol{n}_r, \tag{3}$$

Depending on the cancellation of the IRI at the relay nodes, two types of schemes can be applied. Without IRI cancellation, based on (1) the SINR at relay node i is given by

$$\mathit{\Gamma}_i^{(t)} = \frac{\boldsymbol{\gamma}_{S,R_i}}{\varphi(k,i)\boldsymbol{\gamma}_{R_k,R_i} + N_i\sigma_i^2}, \tag{4}$$

where $\varphi(k,i)$ is the factor indicating the performance of IRI cancellation which we will discuss later and $\boldsymbol{\gamma}_{m,n}$ represents the instantaneous received signal power for the link $m \longrightarrow n$:

$$\boldsymbol{\gamma}_{S,R_i} = \mathrm{trace}(\boldsymbol{H}_i\boldsymbol{H}_i^H), \tag{5}$$

$$\boldsymbol{\gamma}_{R_k,R_i} = \mathrm{trace}(\boldsymbol{H}_{ki}\boldsymbol{H}_i^{(pt)}{\boldsymbol{H}_i^{(pt)}}^H\boldsymbol{H}_{ki}^H), \tag{6}$$

Note that the superscript $\boldsymbol{H}_i^{(pt)}$ is applied due to the nature of the signal stored in the buffers. The SINR at the eavesdropper node e $\mathit{\Gamma}_e^{(t)}$ as well as the legitimate user r $\mathit{\Gamma}_r^{(t)}$ can be expressed as

$$\mathit{\Gamma}_e^{(t)} = \frac{\boldsymbol{\gamma}_{S,E_e}}{\boldsymbol{\gamma}_{R_k,E_e} + N_e\sigma_e^2}, \tag{7}$$

and

$$\mathit{\Gamma}_r^{(t)} = \frac{\boldsymbol{\gamma}_{R_k,R_r}}{N_r\sigma_r^2}, \tag{8}$$

where in (7) and (8) we have

$$\boldsymbol{\gamma}_{S,E_e} = \mathrm{trace}(\boldsymbol{H}_e\boldsymbol{H}_e^H), \tag{9}$$

$$\boldsymbol{\gamma}_{R_k,E_e} = \mathrm{trace}(\boldsymbol{H}_{ke}\boldsymbol{H}_i^{(pt)}{\boldsymbol{H}_i^{(pt)}}^H\boldsymbol{H}_{ke}^H), \tag{10}$$

$$\boldsymbol{\gamma}_{R_k,R_r} = \mathrm{trace}(\boldsymbol{H}_{kr}\boldsymbol{H}_i^{(pt)}{\boldsymbol{H}_i^{(pt)}}^H\boldsymbol{H}_{kr}^H), \tag{11}$$

If the IRI cancellation can be performed at the relay node, $\varphi(k,i)\boldsymbol{\gamma}_{R_k,R_i} = 0$ and the SINR at relay node i, eavesdropper e and receiver r can be expressed, respectively, as

$$\mathit{\Gamma}_i^{(t)} = \frac{\boldsymbol{\gamma}_{S,R_i}}{N_i\sigma_i^2}, \tag{12}$$

$$\mathit{\Gamma}_e^{(t)} = \frac{\boldsymbol{\gamma}_{S,E_e}}{\boldsymbol{\gamma}_{R_k,E_e} + N_e\sigma_e^2}, \tag{13}$$

$$\mathit{\Gamma}_r^{(t)} = \frac{\boldsymbol{\gamma}_{R_k,R_r}}{N_r\sigma_r^2}, \tag{14}$$

According to [18], the feasibility of IRI cancellation in single-input-single-output (SISO) channels is considered. When we consider the MIMO scenario with the same definition the factor $\varphi(k,i)$ can be expressed as,

$$\varphi(k,i) = \begin{cases} 0 & \text{if } \det\left((\frac{P}{N_t}\boldsymbol{H}_i\boldsymbol{H}_i^H + \boldsymbol{I})^{-1}\frac{P}{N_k}\boldsymbol{H}_{ki}\boldsymbol{H}_{ki}^H\right) \geqslant \gamma_0 \\ 1 & \text{otherwise,} \end{cases}$$

When interference cancellation is feasible, $\varphi(k,i) = 0$, the interfering signal is firstly decoded and then subtracted at the relay prior to the decoding of the source signal. In this case, the received signal at the relay node is not affected by the IRI.

B. Problem Formulation

In this subsection, we present the problem formulation and describe the main performance metrics used to assess the performance of the proposed algorithms.

The MIMO system secrecy capacity without consideration of interference is expressed as [5]:

$$\begin{aligned} C_s = \max_{\boldsymbol{Q}_s \geq 0, \mathrm{Tr}(\boldsymbol{Q}_s) = \mathrm{E_s}} & \log(\det(\boldsymbol{I} + \boldsymbol{H}_{ba}\boldsymbol{Q}_s\boldsymbol{H}_{ba}^H)) \\ & - \log(\det(\boldsymbol{I} + \boldsymbol{H}_{ea}\boldsymbol{Q}_s\boldsymbol{H}_{ea}^H)), \end{aligned} \tag{15}$$

In (15) $\boldsymbol{Q}_s$ is the covariance matrix associated with the signal and $\boldsymbol{H}_{ba}$ and $\boldsymbol{H}_{ea}$ represent the links between the source to the users and eavesdroppers, respectively. For the relay system [20], according to (1) and (3), with equal power P allocated to the transmitter and relay, the achievable rate of the users can be expressed as

$$R_r = \log(\det(\boldsymbol{I} + \boldsymbol{\Gamma}_r^{(t)})), \tag{16}$$

and the $\boldsymbol{\Gamma}_r^{(t)}$ according to (8) is given as

$$\boldsymbol{\Gamma}_r^{(t)} = \sum_{k=1}^{k=K}\frac{P}{N_k}\boldsymbol{H}_{kr}\boldsymbol{H}_{kr}^H(\boldsymbol{I} + \frac{P}{N_t}\boldsymbol{H}_i^{(pt)}{\boldsymbol{H}_i^{(pt)}}^H), \tag{17}$$

Similarly, for eavesdropper e the achievable rate assuming global knowledge for all the links is given by

$$R_e = \log(\det(\boldsymbol{I} + \boldsymbol{\Gamma}_e^{(t)})), \tag{18}$$

and $\boldsymbol{\Gamma}_e^{(t)}$ according to (7) is described by

$$\boldsymbol{\Gamma}_e^{(t)} = (\boldsymbol{I} + \boldsymbol{\Delta})^{-1}\frac{P}{N_t}\boldsymbol{H}_e{\boldsymbol{H}_e}^H, \tag{19}$$

where

$$\boldsymbol{\Delta} = \sum_{e=1}^{N}\sum_{k=1}^{K}\frac{P}{N_k}\boldsymbol{H}_{ke}\boldsymbol{H}_{ke}^H(\boldsymbol{I} + \frac{P}{N_t}\boldsymbol{H}_i^{(pt)}{\boldsymbol{H}_i^{(pt)}}^H), \tag{20}$$

With (16) and (18) the secrecy rate for the multiple users is expressed as

$$R = \sum_{r=1}^{T}\sum_{e=1}^{N}[R_r - R_e]^+, \tag{21}$$

where $[x]^+ = max(0,x)$.

Our objective is to develop an algorithm to select the best set of relay nodes to perform relay or jammer functions in order to maximize the secrecy rate. Then, the optimization problem can be formulated as

$$\begin{aligned} \max_{k,i} \quad & R \\ \text{s.t.} \quad & k, i \in \boldsymbol{\Psi} \end{aligned} \tag{22}$$

where $\boldsymbol{\Psi}$ represents the relay node poll. The quantities k and i denote the selected relay and jamming function nodes, respectively.

III. Buffer-aided Relay and Jammer Function Selection (BF-RJFS)

In this section a novel relay and jammer function selection policy based on the max-ratio relay selection policy in [11] and SINR criterion in [21] is proposed.

A. Motivation

The aforementioned max-min and max-link relay selection policy are effective in improving the transmission rate in the relay system, but the eavesdropper is not taken into consideration. Thus, we apply the max-ratio relay selection which considers the existence of an eavesdropper. Unlike the max-ratio relay selection policy, for relay selection we use the SINR criterion. To further enhance the secrecy rate performance, we assume the system operates in an opportunistic scheme so that the relay can also act as a jammer to the eavesdropper. In the following, we will give the details of the proposed algorithm.

B. Algorithm Description

We assume that the total number of relay nodes is Q. To apply the opportunistic scheme in the system, an initial state is set in each relay according to the SINR without jamming:

$$\varGamma_q = \arg\max_{\mathrm{q}\in\boldsymbol{\varPsi}} \det\left(\boldsymbol{H}_{\mathrm{q}}{\boldsymbol{H}_{\mathrm{q}}}^{\mathrm{H}}\right), \tag{23}$$

where the jamming relay nodes also transmit the signals to the users, the selected relay can be either best SINR performance ones which will benefit for the legitimate users transmission or worst SINR performance ones which provide jamming to the eavesdropper. Here we choose relays with the best SINR performance. When the K relays that forward the signals to the users are determined, the relays used for signal reception are chosen based on the SINR criterion, as given by

$$\boldsymbol{\phi}_m = \arg\max_{\mathrm{m}\in\boldsymbol{\varPsi}} \left((\boldsymbol{I}+\boldsymbol{\Gamma}_{\mathrm{e}}^{(\mathrm{t})})^{-1}(\boldsymbol{I}+\boldsymbol{\Gamma}_{\mathrm{m}}^{(\mathrm{t})})\right), \tag{24}$$

where $\boldsymbol{\phi}_m$ represents the selected relays and $\boldsymbol{\Gamma}_m^{(t)}$ is the SINR corresponding to the mth relay which is calculated based on (4) and is given by

$$\boldsymbol{\Gamma}_m^{(t)} = (\boldsymbol{I}+\boldsymbol{\varDelta}'_m)^{-1}(\boldsymbol{H}_m\boldsymbol{H}_m^H), \tag{25}$$

where

$$\boldsymbol{\varDelta}'_m = \sum_{k=1}^{K}\boldsymbol{H}_{km}\boldsymbol{H}_m^{(pt)}{\boldsymbol{H}_m^{(pt)}}^H\boldsymbol{H}_{km}^H, \tag{26}$$

with the SINR calculated for the eth eavesdropper described by

$$\boldsymbol{\Gamma}_e^{(t)} = (\boldsymbol{I}+\boldsymbol{\varDelta}'_e)^{-1}(\frac{P}{N_t}\boldsymbol{H}_e{\boldsymbol{H}_e}^H), \tag{27}$$

where

$$\boldsymbol{\varDelta}'_e = \sum_{e=1}^{N}\sum_{k=1}^{K}\frac{P}{N_k}\boldsymbol{H}_{ke}\boldsymbol{H}_{ke}^H(\boldsymbol{I}+\boldsymbol{\xi}), \tag{28}$$

and

$$\boldsymbol{\xi} = \frac{P}{N_t}\boldsymbol{H}_m^{(pt)}{\boldsymbol{H}_m^{(pt)}}^H, \tag{29}$$

Here the selection of the T relays used for signal reception is described. The selection of the set of jamming relays is performed simultaneously. Apart from the T selected relays, the rest of the relays are selected with the SINR criterion:

$$\boldsymbol{\phi}_n = \arg\max_{\mathrm{n}\in\boldsymbol{\varPsi}} \left((\boldsymbol{I}+\boldsymbol{\Gamma}_{\mathrm{e}}^{(\mathrm{t})})^{-1}(\boldsymbol{I}+\boldsymbol{\Gamma}_{\mathrm{n}}^{(\mathrm{t})})\right), \tag{30}$$

where $\boldsymbol{\Gamma}_n^{(t)}$ is the SINR corresponding to the nth relay which is calculated based on (8) and is given by

$$\boldsymbol{\Gamma}_n^{(t)} = \boldsymbol{H}_{nr}\boldsymbol{H}_n^{(pt)}{\boldsymbol{H}_n^{(pt)}}^H\boldsymbol{H}_{nr}^H, \tag{31}$$

With the SINR calculated for the eth eavesdropper given by

$$\boldsymbol{\Gamma}_e^{(t)} = (\boldsymbol{I}+\boldsymbol{\varDelta}''_e)^{-1}(\frac{P}{N_k}\boldsymbol{H}_{ne}\boldsymbol{H}_n^{(pt)}{\boldsymbol{H}_n^{(pt)}}^H\boldsymbol{H}_{ne}^H), \tag{32}$$

where

$$\boldsymbol{\varDelta}''_e = \sum_{e=1}^{N}\sum_{k=1}^{K}\frac{P}{N_k}\boldsymbol{H}_{ke}\boldsymbol{H}_{ke}^H(\boldsymbol{I}+\boldsymbol{\xi}), \tag{33}$$

and

$$\boldsymbol{\xi} = \frac{P}{N_t}\boldsymbol{H}_{ne}{\boldsymbol{H}_{ne}}^H, \tag{34}$$

Then the relays used for jamming in the next time slot are selected. With a loop of the selection of receiving relays and jamming relays the system can provide a better secrecy performance as compared to conventional relay systems. In Algorithm 1 the main steps are detailed.

Algorithm 1 BF-RJFS Algorithm

```
for $k = 1 : K$ do
  for $q = 1 : Q$ do
    $\varGamma_q = \arg\max_{\mathrm{q}\in\boldsymbol{\varPsi}} \det(\boldsymbol{H}_{\mathrm{q}}{\boldsymbol{H}_{\mathrm{q}}}^{\mathrm{H}})$
  end for
  ${\varGamma_k}^0 = \varGamma_q$
  $Q^0 = [1 \quad 2 \quad \cdots \quad q-1 \quad q+1\cdots Q]$
end for
$Q = Q^0$
loop
  for $i = 1 : T$ do
    for $m = 1 : Q^0$ do
      $\boldsymbol{\Gamma}_m^{(t)} = (\boldsymbol{I}+\boldsymbol{\varDelta}'_m)^{-1}(\boldsymbol{H}_m\boldsymbol{H}_m^H)$
      $\boldsymbol{\Gamma}_e^{(t)} = (\boldsymbol{I}+\boldsymbol{\varDelta}'_e)^{-1}(\frac{P}{N_t}\boldsymbol{H}_e{\boldsymbol{H}_e}^H)$
      $\boldsymbol{\phi}_m = \arg\max_{\mathrm{m}\in\boldsymbol{\varPsi}} \left((\boldsymbol{I}+\boldsymbol{\Gamma}_{\mathrm{e}}^{(\mathrm{t})})^{-1}(\boldsymbol{I}+\boldsymbol{\Gamma}_{\mathrm{m}}^{(\mathrm{t})})\right)$
      $Q^1 = [1 \quad 2 \quad \cdots \quad m-1 \quad m+1\cdots M]$
    end for
  end for
  for $k = 1 : K$ do
    for $n = 1 : M^1$ do
      $\boldsymbol{\Gamma}_n^{(t)} = \boldsymbol{H}_{nr}\boldsymbol{H}_n^{(pt)}{\boldsymbol{H}_n^{(pt)}}^H\boldsymbol{H}_{nr}^H$
      $\boldsymbol{\Gamma}_e^{(t)} = (\boldsymbol{I}+\boldsymbol{\varDelta}''_e)^{-1}(\frac{P}{N_k}\boldsymbol{H}_{ne}\boldsymbol{H}_n^{(pt)}{\boldsymbol{H}_n^{(pt)}}^H\boldsymbol{H}_{ne}^H)$
      $\boldsymbol{\phi}_n = \arg\max_{\mathrm{n}\in\boldsymbol{\varPsi}} \left((\boldsymbol{I}+\boldsymbol{\Gamma}_{\mathrm{e}}^{(\mathrm{t})})^{-1}(\boldsymbol{I}+\boldsymbol{\Gamma}_{\mathrm{n}}^{(\mathrm{t})})\right)$
      $Q^0 = [1 \quad 2 \quad \cdots \quad n-1 \quad n+1\cdots M]$
    end for
  end for
end loop
```

IV. Simulation Results

In the simulations, a system with $N_t = 6$ transmit antennas, $M = 3$ users and $N = 3$ eavesdroppers is considered. The total number of relays is set to $Q = 6$ and among them $T = 3$ and $K = 3$ relays nodes are selected. Each user, eavesdropper and relay node is equipped with $N_r = 2$, $N_e = 2$, $N_i = 2$ and $N_k = 2$ receive antennas.

In Fig. 2, in a single-antenna scenario, the secrecy performance with the proposed algorithm is better than that with the conventional algorithm. With IRI cancellation, the secrecy rate is better than the one without IRI cancellation. Compared with single antenna scenario, the multi-user MIMO system contributes to the improvement in the secrecy rate. In addition, the proposed algorithm with the selected set of buffer-aided

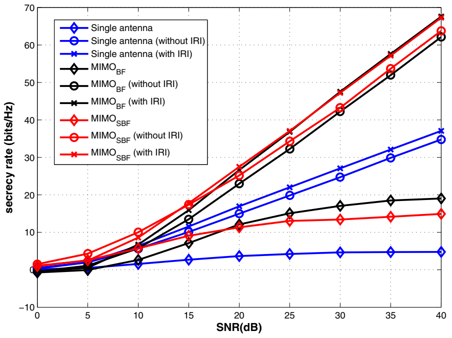
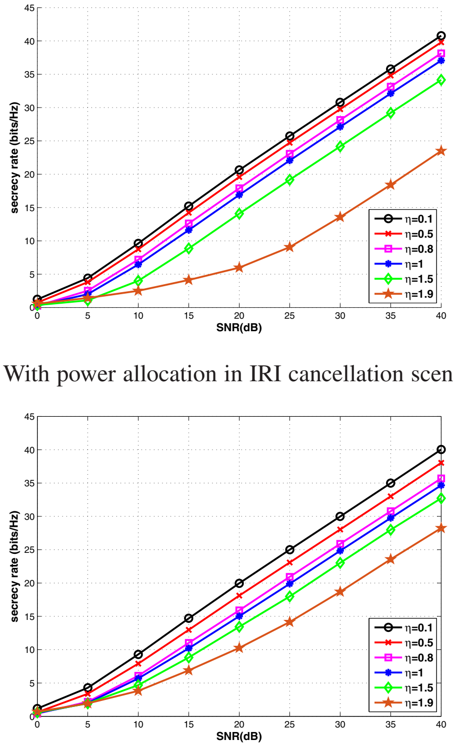


Fig. 2: Comparison of single-antenna with multi-user MIMO system



(a) With power allocation in IRI cancellation scenario

(b) With power allocation in existing of IRI scenario

Fig. 3: Secrecy rate performance with power allocation in different IRI cancellation scenarios

relays (SBF) selection policy is better than the conventional buffer-aided relay selection (BF).

In Fig. 3, the power allocation technique is implemented and the parameter η indicates the power allocated to the transmitter. If we assume in the equal power scenario that the power allocated to the transmitter as well as relays are both P, then the power allocated to the transmitter is ηP and the power allocated to the relays is $(2-\eta)P$. From Fig. 3 we can see that with more power allocated to the transmitter the secrecy rate will decrease. Comparing (a) with (b), when $\eta < 1.5$ the secrecy rate performance in IRI cancellation scenario is better than that without IRI cancellation. When $\eta > 1.5$ and without IRI cancellation, the secrecy rate can achieve a better performance.

V. Conclusion

In this work, we have proposed algorithms to select a set of relay nodes to enhance the legitimate users' transmission and another set of relay nodes to perform jamming of the eavesdroppers. The proposed selection algorithms can exploit the use of the buffers in the relay nodes that may remain silence during the data transmission. Simulation results show that the proposed buffer-aided relay and jammer function selection (BF-RJFS) can provide a better secrecy rate performance in a multiuser MIMO relay system than existing buffer-aided relay systems.

References

[1] C. Shannon, "Communication theory of secrecy systems," *Bell System Technical Journal*, vol. 28, no. 4, pp. 656–715, Oct 1949.

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

[3] I. Csiszar and J. Korner, "Broadcast channels with confidential messages," *IEEE Trans. Inform. Theory,*, vol. 24, no. 3, pp. 339–348, May 1978.

[4] F. Oggier and B. Hassibi, "The secrecy capacity of the mimo wiretap channel," *IEEE Trans. Inform. Theory,*, vol. 57, no. 8, pp. 4961–4972, Aug 2011.

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

[6] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE Trans. Wireless Commun.*, vol. 7, no. 6, pp. 2180–2189, June 2008.

[7] J. Zhang and M. Gursoy, "Collaborative relay beamforming for secrecy," in *IEEE International Conference on Communications (ICC)*, May 2010, pp. 1–5.

[8] Y. Oohama, "Capacity theorems for relay channels with confidential messages," in *IEEE International Symposium on Inform. Theory (ISIT)*, June 2007, pp. 926–930.

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

[10] N. Zlatanov and R. Schober, "Buffer-aided relaying with adaptive link selection-fixed and mixed rate transmission," *IEEE Trans. Inform. Theory,*, vol. 59, no. 5, pp. 2816–2840, May 2013.

[11] G. Chen, Z. Tian, Y. Gong, Z. Chen, and J. Chambers, "Max-ratio relay selection in secure buffer-aided cooperative wireless networks," *IEEE Trans. Inform. Forensics and Security,*, vol. 9, no. 4, pp. 719–729, April 2014.

[12] J. Huang and A. Swindlehurst, "Wireless physical layer security enhancement with buffer-aided relaying," in *2013 Asilomar Conference on Signals, Systems and Computers*, Nov 2013, pp. 1560–1564.

[13] K. Zu and R. de Lamare, "Low-complexity lattice reduction-aided regularized block diagonalization for mu-mimo systems," *IEEE Communications Letters*, vol. 16, no. 6, pp. 925–928, June 2012.

[14] K. Zu, R. de Lamare, and M. Haardt, "Generalized design of low-complexity block diagonalization type precoding algorithms for multiuser mimo systems," *IEEE Trans. Communications*, vol. 61, no. 10, pp. 4232–4242, October 2013.

[15] Z. K, R. de Lamare, and M. Haardt, "Multi-branch tomlinson-harashima precoding design for mu-mimo systems: Theory and algorithms," *IEEE Trans. Communications*, vol. 62, no. 3, pp. 939–951, March 2014.

[16] X. Lu, K. Zu, and R. C.de Lamare, "Lattice-reduction aided successive optimization tomlinson-harashima precoding strategies for physical-layer security in wireless networks," in *Sensor Signal Processing for Defence (SSPD), 2014*, Sept 2014, pp. 1–5.

[17] X. Lu and R. C. Lamare, "Buffer-aided relay selection for physical-layer security in wireless networks," in *Proceedings of 19th International ITG Workshop on Smart Antennas (WSA)*, March 2015, pp. 1–5.

[18] N. Nomikos, T. Charalambous, I. Krikidis, D. Skoutas, D. Vouyioukas, and M. Johansson, "Buffer-aided successive opportunistic relaying with inter-relay interference cancellation," in *IEEE 24th International Symposium on Personal Indoor and Mobile Radio Communications (PIMRC)*, Sept 2013, pp. 1316–1320.

[19] N. Nomikos, P. Makris, D. Vouyioukas, D. Skoutas, and C. Skianis, "Distributed joint relay-pair selection for buffer-aided successive opportunistic relaying," in *2013 IEEE 18th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD)*, Sept 2013, pp. 185–189.

[20] J. H. Lee and W. Choi, "Multiuser diversity for secrecy communications using opportunistic jammer selection: Secure dof and jammer scaling law," *IEEE Trans. Signal Processing,*, vol. 62, no. 4, pp. 828–839, Feb 2014.

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