Effective Optimization Criteria and Relay Selection Algorithms for Physical-Layer Security in Multiple-Antenna Relay Networks

Xiaotao Lu and Rodrigo C. de Lamare, Senior Member, IEEE

Abstract—Physical-layer security for wireless networks has become an effective approach and recently drawn significant attention in the literature. In particular, the deployment and allocation of resources such as relays to assist the transmission have gained significant interest due to their ability to improve the secrecy rate of wireless networks. In this work, we examine relay selection criteria with arbitrary knowledge of the channels of the users and the eavesdroppers. We present alternative optimization criteria based on the signal-to-interference and the secrecy rate criteria that can be used for resource allocation and that do not require knowledge of the channels of the eavesdroppers and the interference. We then develop effective relay selection algorithms that can achieve a high secrecy rate performance without the need for the knowledge of the channels of the eavesdroppers and the interference. Simulation results show that the proposed criteria and algorithms achieve excellent performance.

Index Terms—Physical-layer security, secrecy rate optimization, relay selection, linear algebra techniques.

I. INTRODUCTION

In the era of modern wireless communications, transmission security is facing great challenges due to the nature of wireless broadcasting. To achieve transmission security in wireless links, physical-layer security has been proposed by Shannon [1] and investigated under various wireless networks [2], [3]. In order to measure the security of wireless networks, the secrecy rate (SR) has been defined as the difference between two mutual information terms associated with the channels of the legitimate users and the eavesdroppers, respectively. In [6], [2], the secrecy capacity of multi-input multi-output (MIMO) systems [2], [3] is shown to be equivalent to the maximum achievable SR. More specifically, the secrecy capacity for a particular wire-tap Gaussian MIMO channel is determined by an achievable scheme and the secrecy capacity region is established for the most general case with an arbitrary number of users. Furthermore, SR optimization is performed in the presence of a cooperative jammer.

Relay selection schemes are investigated in various scenarios such as multiuser relay networks, cooperative relay systems and cognitive relay networks. Relay selection methods are often considered with the impact of co-channel interference and the interference. Simulation results show that the proposed criteria and algorithms achieve excellent performance.

The performance in terms of secrecy rate can be significantly affected by the relay selection criterion adopted. Existing relay selection algorithms depend on the knowledge of the channels between the source to the relays and the relays to the users [10]. Taking the channels from the source to the eavesdroppers into account, a relay selection approach denoted max-ratio criterion has been proposed in [13] based on knowledge of the channels to both legitimate users and eavesdroppers. In prior work, the assumption of knowledge of the channels to the eavesdroppers has been adopted even though it is impractical. Studies have considered the max-ratio relay selection policy, which employs the signal-to-interference-plus-noise ratio (SINR) as the relay selection criterion and requires the knowledge of the interference between users and the channels to the eavesdroppers.

In this work, we examine the SR performance of multi-user relay selection algorithms based on the SINR and the SR criteria, which require the knowledge of the interference and the channels to the eavesdroppers in multiuser multiple-antenna relay networks. We present alternative optimization criteria based on the SINR and the SR criteria that can be used for resource allocation. We then develop novel effective relay selection algorithms based on the SINR and SR criteria that do not require knowledge of the channels of the eavesdroppers and interference by exploiting linear algebra properties and a simplification of the expressions. We also analyze the computational cost required by the proposed criteria for relay selection and their implication on the improvement of the secrecy rate of multiuser multiple-antenna relay networks. The SR performance of the proposed relaying criteria and relay algorithms is shown via simulations to approach that of techniques with full knowledge of the interference and the channels to the eavesdroppers.

In summary, the main contributions of this work are:

- Optimization criteria based on the SINR and the SR criteria that can be used for resource allocation without the need for the knowledge of the interference and the channels to the eavesdroppers.

Xiaotao Lu is with the Communications Research Group, Department of Electronics, University of York, YO10 5DD York, U.K. e-mail: xt1503@york.ac.uk. R. C. de Lamare is with CETUC, PUC-Rio, Brazil and with the Department of Electronic, University of York, YO10 5DD York, U.K. email: rcdl500@york.ac.uk.
• Effective relay selection algorithms based on the SINR and SR criteria, which do not need the knowledge of the interference and the channels to the eavesdroppers.
• Analysis of the computational cost and the impact of the proposed criteria and algorithms on the secrecy rate.
• A simulation study of the proposed criteria and relay selection algorithms in several scenarios of interest in multiuser multiple-antenna relay networks.

This paper is organized as follows. In Section II, the system model is introduced. The relay selection criteria are introduced in Section III, whereas the proposed algorithms are developed in Section IV. The simulations are presented and discussed in Section V. The conclusions are given in Section VI.

Notation: Bold uppercase letters \( \mathbf{A} \in \mathbb{C}^{M \times N} \) denote matrices with size \( M \times N \) and bold lowercase letters \( \mathbf{a} \in \mathbb{C}^{M \times 1} \) denote column vectors with length \( M \). Conjugate transpose, and conjugate transpose are represented by \((\cdot)^*\), \((\cdot)^T\) and \((\cdot)^H\), respectively; \( \mathbf{I}_M \) is the identity matrix of size \( M \times M \); \( \text{diag}\{\mathbf{a}\} \) denotes a diagonal matrix with the elements of the vector \( \mathbf{a} \) along its diagonal; \( \mathcal{C}N(\mu, \sigma^2) \) represents complex Gaussian random variables with independent and identically distributed \((i.i.d)\) entries with zero mean and variance equal to \( \sigma^2 \); \( \log(\cdot) \) denotes the base-2 logarithm of the argument.

II. SYSTEM MODEL

Fig. 1: Multiuser multiple-antenna network with the source device equipped with \( N_t \) antenna elements, \( T \) relay devices equipped with \( N_r \) antennas each, the destination user devices with \( N_r \) antenna elements each and eavesdroppers.

A description of the downlink multiuser multiple-antenna relay network considered in this work is illustrated in Fig. 1 where the system employs two time slots to transmit the data from the source node to the users. Each relay and each user are equipped with \( N_t \) and \( N_r \) antennas, respectively. We consider a source node, which transmits \( \mathbf{s} = [s_1^T, s_2^T, \ldots, s_M^T]^T \in \mathbb{C}^{MN_r \times 1} \) to relays. To transmit the signal simultaneously to \( M \) users, the total number of transmit antennas should be limited according to \( N_t^{\text{total}} \geq MN_r \). For convenience, we assume that the number of the active antennas used for transmitting user signals is \( N_t \) and \( N_r = MN_r \). At the same time, in order to receive the signals with a set of \( T \) relays, \( T \times N_r = N_t \) antennas at relays are employed. In the second time slot, the relays will forward the signals to \( M \) users. During the transmission from the source to the users, there are \( N_e \) eavesdroppers, which attempt to decode the signals. Each eavesdropper is equipped with \( N_e \) antennas.

In this system, we assume that the eavesdroppers do not jam the transmission and the data transmitted to each user, relay, jammer and eavesdropper experience a flat-fading multiple-antenna channel. The source node has knowledge of the channels from the source to the relays as well as from the relays to the users. The quantities \( \mathbf{H}_{\phi_i} \in \mathbb{C}^{N_t \times N_t} \) and \( \mathbf{H}_{e_k} \in \mathbb{C}^{N_t \times N_e} \) denote the channel matrices of the \( i \)-th relay and the \( k \)-th eavesdropper, respectively. If we assume \( \mathbf{\Psi} \) contains sets of \( T \)-combinations of the total relay set \( \mathbf{\Omega} \) then the task of relay selection is to choose the set of relays that satisfies a chosen criterion. Given the set of selected relays expressed as \( \varphi = [\phi_1, \phi_2, \ldots, \phi_T] \in \mathbf{\Psi} \), the channel from the transmitter to the relays and the eavesdroppers can be obtained as \( \mathbf{H}_i = [\mathbf{H}_{\phi_1}^T, \mathbf{H}_{\phi_2}^T, \ldots, \mathbf{H}_{\phi_T}^T]^T \in \mathbb{C}^{T N_t \times N_t} \) and \( \mathbf{H}_e = [\mathbf{H}_{e_1}^T, \mathbf{H}_{e_2}^T, \ldots, \mathbf{H}_{e_k}^T]^T \in \mathbb{C}^{K N_t \times N_e} \). The matrix \( \mathbf{H}_{\phi_i} \in \mathbb{C}^{N_r \times N_t} \) represents the channel between the \( i \)-th relay and the \( r \)-th user. The channels from the selected relays to the \( r \)-th user can be described by

\[
\mathbf{H}_r = [\mathbf{H}_{\phi_1 r}, \mathbf{H}_{\phi_2 r}, \ldots, \mathbf{H}_{\phi_T r}], \tag{1}
\]

where \( \mathbf{H}_r \in \mathbb{C}^{N_r \times TN_t} \) and \( \phi_i \) represents the \( i \)-th selected relay with a chosen relay selection criterion. In the following section we will further discuss various relay selection criteria, where \( T \) is the total number of selected relays \([80, 81, 82, 83, 84, 85, 86, 87, 101, 89, 90, 91, 92, 93, 94, 95, 96, 97, 98, 99, 100, 101, 102, 103, 104, 105, 106, 107, 108, 112, 110, 111, 112, 113, 114, 115, 116, 117, 118, 119, 120, 121, 122, 123, 124, 125, 126, 127, 128, 129, 130, 131]\).

In Phase I, the signal is transmitted from the source to the relays. If a precoder matrix \( \mathbf{U} = [\mathbf{U}_1 \ \mathbf{U}_2 \ \cdots \ \mathbf{U}_M] \in \mathbb{C}^{N_t \times MN_r} \) is applied, when the relay is selected, the received signal in all relays can be expressed as

\[
y_i = \mathbf{H}_i \mathbf{U} \mathbf{s} + \mathbf{n}_i \in \mathbb{C}^{TN_t \times 1}, \tag{2}
\]

where \( \mathbf{n}_i = [n_{\phi_1}, n_{\phi_2}, \ldots, n_{\phi_T}] \in \mathbb{C}^{TN_t \times 1} \) is the noise vector that is assumed to be Gaussian. If the interference for relay \( i \) is described by \( \mathbf{H}_{i} \sum_{j \neq i, j=1}^{T} \mathbf{U}_j \mathbf{s}_j \), then the received signal at relay \( i \) is given by

\[
y_{\phi_i} = \mathbf{H}_{\phi_i} \mathbf{U}_i \mathbf{s}_i + \mathbf{H}_{\phi_i} \sum_{j \neq i, j=1}^{T} \mathbf{U}_j \mathbf{s}_j + \mathbf{n}_{\phi_i}. \tag{3}
\]

In Phase II, the signal at the relay nodes is given by

\[
y_i = [y_{\phi_1}^T, y_{\phi_2}^T, \ldots, y_{\phi_T}^T]^T \in \mathbb{C}^{TN_t \times 1}.
\]
The received signal at user $r$ from the selected set of relays is described by
\[ y_r = H_r y + n_r \in \mathbb{C}^{N_r \times 1}, \] (4)
where $H_r \in \mathbb{C}^{N_r \times TN_r}$ represents the channel from the selected set of relays to user $r$ and $n_r \in \mathbb{C}^{N_r \times 1}$ is the noise vector at user $r$.

### III. Problem Statement and Relay Selection Criteria

In this section, we state the relay selection problem and present a generic multiple-relay selection algorithm, which relies on exhaustive searches and can be employed with arbitrary criteria. We then review several relay selection criteria that are available in the literature for the system under consideration.

#### A. Relay Selection Problem

In the presence of multiple relay nodes, relay selection is performed before transmission to the relays. In a half-duplex system, we use $\eta_1$ to represent a metric obtained with the information from the source to the relays and $\eta_2$ as another metric calculated with information from the relays to the users. Therefore, the relay selection criterion depends on $\eta_1$ and $\eta_2$ and can be expressed as
\[ \phi_{\text{select}} = \arg \max_{\phi} (\eta_1, \eta_2). \] (5)

A multiple-relay selection algorithm for this scenario is shown in Algorithm 1. More specifically, step 33 takes the channel gain as the selection criterion and it can be replaced with different selection criteria. Depending on the choice of relay selection a designer must alter steps 7, 22 and 33.

#### B. Max-ratio criterion

Conventional relay selection is based on the full channel information between the source to the relays and the relays to the users. A max-link relay selection is developed based on the max-min relay selection for decode-and-forward (DF) relay systems [2]. With the consideration of the eavesdropper, a max-ratio selection [13] in a single-antenna scenario is given by
\[ \phi_{\text{max-ratio}} = \arg \max_{\phi_i \in \phi} (\eta_1^\text{max-ratio}, \eta_2^\text{max-ratio}), \] (6)
where
\[ \eta_1^\text{max-ratio} = \max_{\phi_i \in \phi : Q(\phi_i) \neq L} \frac{||h_{s_i, \phi_i}||^2}{||h_{se}||^2} \] (7)
and
\[ \eta_2^\text{max-ratio} = \max_{\phi_i \in \phi : Q(\phi_i) \neq 0} \frac{||h_{\phi_i, d}||^2}{||h_{\phi_i, e}||^2}. \] (8)

Furthermore, in the scenario with only statistical distribution of the CSI to the eavesdroppers, the parameter of channel coefficient in (7) and (8) are replaced by statistical values.

### C. SINR criterion

Based on the max-ratio criterion, when we consider a multiuser MIMO system, the interference is taken into account in the relay selection criterion. According to (6), the SINR criterion can be expressed similarly as
\[ \varphi_{\text{SINR}} = \arg \max_{\varphi} (\eta_{\text{SINR}_1}, \eta_{\text{SINR}_2}), \] (9)
where $\eta_{\text{SINR}_1}$ is the average value of SINR over relay set $\varphi$. The SINR of the selected relay node $\phi_i$ can be obtained by
\[ \eta_{\text{SINR}_{\phi_i}} = \max_{\phi,\theta} \text{SINR}_{\phi_i} \]
\[ = \max_i \frac{1}{N_i} \sum_{n=1}^{N_i} \text{SINR}_n \]
\[ = \max_i \frac{1}{N_i} \sum_{n=1}^{N_i} h_{\phi_i,n}^H R_d h_{\phi_i,n} \] (10)
in (10), $h_{\phi_i,n} \in \mathbb{C}^{N_i \times 1}$ represents the $n$th stream for the $i$th relay. $R_d = U_i s_i U_i^H \in \mathbb{C}^{N_i \times N_t}$ is the correla-

| Algorithm 1 Relay selection algorithm with channel information |
|-----------------|-----------------|
| 1: $\Omega^0 = \Omega$ |
| 2: $\phi_{\text{total}} = \text{length}(\Omega)$ |
| 3: $Q = \text{zeros}(1 : \phi_{\text{total}})$ |
| 4: for $k = 1 : T$ do |
| 5: for $i = 1 : \phi_{\text{total}}$ do |
| 6: if $Q(i) = 0$ then |
| 7: $\theta_{\phi_i} = \text{trace}(H_{\phi_i, r} H_{\phi_i, r}^H)$ |
| 8: $Q(i) = Q(i) + 1$ |
| 9: else |
| 10: $\theta_{\phi_i} = 0$ |
| 11: end if |
| 12: end for |
| 13: $\phi_{\text{select}} = \arg \max_{\phi_i \in \Omega^k} \{\theta_{\phi_i}\}$ |
| 14: $\eta_k = \theta_{\phi_{\text{select}}}$ |
| 15: $\Omega^1 = [1 \ 2 \ \cdots \ \phi_i - 1 \ \phi_i + 1 \ \cdots \ \phi_{\text{total}}]$ |
| 16: end for |
| 17: $\eta_1 = \sum_{k=1}^{T} \eta_k$ |
| 18: $\Omega^1 = \Omega$ |
| 19: for $r = 1 : M$ do |
| 20: for $i = 1 : \phi_{\text{total}}$ do |
| 21: if $Q(i) \neq 0$ then |
| 22: $\theta_{\phi_i} = \text{trace}(H_{\phi_i, r} H_{\phi_i, r}^H)$ |
| 23: $Q(i) = Q(i) - 1$ |
| 24: else |
| 25: $\theta_{\phi_i} = 0$ |
| 26: end if |
| 27: end for |
| 28: $\phi_{\text{select}} = \arg \max_{\phi_i \in \Omega^1} \{\theta_{\phi_i}\}$ |
| 29: $\eta_r = \theta_{\phi_{\text{select}}}$ |
| 30: $\Omega^1 = [1 \ 2 \ \cdots \ \phi_i - 1 \ \phi_i + 1 \ \cdots \ \phi_{\text{total}}]$ |
| 31: end for |
| 32: $\eta_2 = \sum_{r=1}^{M} \eta_r$ |
| 33: $\phi_{\text{select}} = \arg \max_{\varphi} (\eta_1, \eta_2)$ |
tion matrix of the received signal for node $i$ and $R_{in} = \sum_{j \neq i, j=1}^{m} U_j s_j s_j^H U_j^H + n_j n_j^H \in \mathbb{C}^{N_i \times N_i}$ represents the sum of the correlation matrix of the interference and correlation matrix of the noise. Similarly, $\eta_{\text{SINR}}$ is the average value of SINR with relay set $\varphi$ to users. The SINR of user $r$ can then be calculated by

$$\eta_{\varphi,r}^{\text{SINR}} = \max_{r} \frac{1}{N_i} \sum_{n=1}^{N_i} \frac{h_{\phi_in}^H U_n, h_{\phi_in}^r}{h_{\phi_in}^H R_{in}, h_{\phi_in}^r},$$  \hspace{1cm} (11)

where $R_{in} = y_i y_i^H \in \mathbb{C}^{TN_i \times TN_i}$ and $h_{\phi_in}^r \in \mathbb{C}^{TN_i \times 1}$ is the $n$th stream for user $r$.

### D. Secrecy rate criterion

In a multi-user MIMO system, the secrecy-rate criterion for a multi-user MIMO system considering interferences [?] is given by

$$\varphi = \arg \max_{\varphi \in \Psi} \max_{\varphi \in \varphi} \{ \log[\det(I + \Gamma_{r,i})] - \log[\det(I + \Gamma_{e,i})] \},$$

where $\Gamma_{r,i}$ is given as

$$\Gamma_{r,i} = (H_r R_{in} H_r^H)^{-1} (H_r R_{in} H_r^H),$$  \hspace{1cm} (12)

and

$$\Gamma_{e,i} = (H_e R_{in} H_e^H)^{-1} (H_e R_{in} H_e^H).$$  \hspace{1cm} (13)

In (12), the criterion is based on the secrecy rate related to destination $i$ and in a relay system the destination can be relays as well as users.

### IV. PROPOSED RELAY SELECTION ALGORITHMS

In the aforementioned relay selection criteria, the channels of the source to eavesdroppers as well as the interference are assumed to be available at the transmitter. However, this assumption is hard to achieve in wireless transmissions [?]. To obviate this need, we propose effective relay selection algorithms with partial channel information.

#### A. Simplified SINR-Based (S-SINR) Relay Selection

The SINR selection criterion with full channel information is expressed in (9). The interference signal is used to obtain the expressions in (10) and (11). In the following, we choose the SINR criterion and develop a simplified SINR-based (S-SINR) relay selection algorithm with consideration of only the channels of the users, which can be readily obtained via feedback channels. If at the transmitter, a linear precoder $U$ is applied, the received signal can be expressed as

$$h_{\phi_in}^H R_{in} h_{\phi_in} = h_{\phi_in}^H U_i s_i s_i^H U_i^H h_{\phi_in}. \hspace{1cm} (15)$$

With linear zero-forcing precoding, we have $h_{\phi_in}^H U_i = [1 \ 0 \ \cdots \ 0]$ and (15) can be written as

$$h_{\phi_in}^H R_d h_{\phi_in} = \sigma_d^2, \hspace{1cm} (16)$$

where $R_d$ holds for independent and identically distributed entries of $s$ with $\sigma_d^2$ being the variance of the transmit signal. Based on (10) and (11), the proposed S-SINR algorithm solves

$$\eta_{\varphi,s}^{\text{SINR}} = \max_{r} \frac{1}{N_i} \sum_{n=1}^{N_i} \frac{\sigma_d^2}{h_{\phi_in}^r R_{in}, h_{\phi_in}^r}. \hspace{1cm} (17)$$

According to (17), the maximization performed over $N_i$ data streams is difficult to achieve. To implement the optimization as expressed in (17), the CSI to the relays and the correlation matrix of the interference are required. And the SINR value for each receive antenna is calculated with the obtained information. Not mention the accurate requirement of these information, the sum and invert operations for each antenna make it a sophisticated optimization algorithm. To further simplify the maximization we assume that the streams for a device or relay have similar SINR. With this assumption we can have

$$\eta_{\varphi,s}^{\text{SINR}} = \min_{i} h_{\phi_in}^H R_{in}, h_{\phi_in}, \hspace{1cm} (18)$$

We assume $R_{in} = D_{in} + G$. $D_{in}$ is a diagonal matrix with the diagonal elements of $R_{in}$ and $G$ containing the other elements of $R_{in}$. With $D_{in}$ and $G$, we can have

$$h_{\phi_in}^H R_{in}, h_{\phi_in}^r = h_{\phi_in}^H D_{in} h_{\phi_in}^r + h_{\phi_in}^H G h_{\phi_in}^r = \sigma_d^2 |h_{\phi_in}^r|^2 + \|h_{\phi_in}^H G h_{\phi_in}^r\|^2, \hspace{1cm} (19)$$

If we have two data streams and SINR$_1 >$ SINR$_2$, based on (17), we can get

$$h_{\phi_in}^H R_{in}, h_{\phi_in} < h_{\phi_2}^H R_{in}, h_{\phi_2}, \hspace{1cm} (20)$$

with (19), (20) can be expressed as,

$$\sigma_d^2 |h_{\phi_1}^r|^2 + \|h_{\phi_1}^H G h_{\phi_1}^r\|^2 < \sigma_d^2 |h_{\phi_2}^r|^2 + \|h_{\phi_2}^H G h_{\phi_2}^r\|^2, \hspace{1cm} (21)$$

rewrite (21), we can obtain

$$\|h_{\phi_1}^r|^2 < \|h_{\phi_2}^r|^2 + \frac{1}{\sigma_d^2} (\|h_{\phi_1}^H G h_{\phi_1}^r\|^2 - \|h_{\phi_2}^H G h_{\phi_2}^r\|^2), \hspace{1cm} (22)$$

If $G$ is small compared with $\sigma_d^2 I$, we omit the term $(\|h_{\phi_2}^H G h_{\phi_2}^r\|^2 - \|h_{\phi_1}^H G h_{\phi_1}^r\|^2)$. Finally if SINR$_1 >$ SINR$_2$, we can have

$$\|h_{\phi_1}^r|^2 < \|h_{\phi_2}^r|^2, \hspace{1cm} (23)$$

As a result, the SINR criterion can be simplified to the selection of the channel information as described by

$$\eta_{\varphi,s}^{\text{SINR}} = \min_{i,n} |h_{\phi_in}|^2. \hspace{1cm} (24)$$

With the criterion expressed in (24), the interference can be omitted and only the channel information is necessary. Comparing (24) and (17), the optimization is performed by calculating channel gains for each antenna which is obviously easier than calculating SINRs for every antenna. Similarly, (11) can be obtained as

$$\eta_{\varphi,r}^{\text{SINR}} = \min_{r,n} |h_{\phi_in}|^2. \hspace{1cm} (25)$$
Based on (24) and (25), the SINR criterion in (9) can be simplified and the proposed S-SINR algorithm is given by

$$\varphi_{S-SINR} = \arg \max_{\varphi} \left\{ \log \left( \det \left[ I + \Gamma_{r,i} \right] \right) \right\},$$

which only needs the channel information. In (26), the calculation of $\varphi_{S-SINR}$ and $\varphi_{S-SINR_2}$ is in the same way as in (9).

B. Simplified SR-Based (S-SR) Multiple-Relay Selection

In the proposed S-SR algorithm with partial channel information, the covariance matrix of the interference and the signal can be described as $R_I = \sum_{j \neq i} U_j s_j^H U_j^H$ and $R_d = U_i s_i^H U_i^H$, respectively. If precoding matrices are assumed perfectly known in the transmission, we can further obtain an alternative way of expressing S-SR criterion. The proposed SR-based relay selection criterion is given by

$$\varphi_{S-SR} = \max_{\phi_i \in \Phi, \phi \in \Psi} \left\{ \log \left( \det \left[ I + \Gamma_{r,i} \right] \right) \right\},$$

which can be achieved without knowledge of the channels of the eavesdroppers. In what follows, we detail the derivation of the S-SR relay selection algorithm.

Proof. From the original expression for the SR criterion, which is shown in (12), we propose the following approach:

$$\varphi = \arg \max_{\phi_i \in \Phi, \phi \in \Psi} \left\{ \log \left( \det \left[ I + \Gamma_{r,i} \right] \right) \right\},$$

In (28), our aim is to eliminate the channel information of eavesdroppers from the denominator. With square matrices, det$(AB) = \det(A) \det(B)$, to satisfy the requirement, the denominator can be expressed as

$$\det [A_1^{-1} A_1 + \Lambda_1^{-1} (H_e R_d H_e^H)],$$

where $A_1 = H_e R_I H_e^H$. As $A_1$ is a square matrix, (29) can be obtained as,

$$\det [A_1^{-1}] \det [A_1 + (H_e R_d H_e^H)],$$

Using the property of the determinant $\det(A^{-1}) = \frac{1}{\det(A)}$ [7], we have

$$\det [A_1^{-1}] \det [A_1 + (H_e R_d H_e^H)],$$

In (31), we separate the equation into two parts.

$$\det [A_1^{-1}] = \det \left[ H_e R_I H_e^H \right]^{-1},$$

$$\det [A_1 + (H_e R_d H_e^H)] = \det \left[ H_e \left( \sum_{j \neq i} U_j s_j^H U_j^H \right) H_e^H \right]^{-1}$$

on the left-hand side of equation (32), we multiply $U_i U_i^{-1} = I$ and on the right side we multiply $U_i H_i^{-1} U_i H_i = I$, we can have,

$$\det [A_1^{-1}] = \{ \det [H_e U_i] \} \\det [\sum_{j \neq i} U_i^{-1} U_j s_j^H U_j^H H_i H_i^{-1}] \\det [U_i H_i^{-1} U_i H_i^{-1}]^{-1},$$

Similarly, the second part in equation (31) can be obtained as,

$$\det [A_1 + (H_e R_d H_e^H)] = \det [H_e U_i] \\det \left[ \left( \sum_{j \neq i} U_i^{-1} U_j s_j^H U_j^H H_i H_i^{-1} \right) + s_i^H s_i^H \right] \\det [U_i H_i^{-1} H_e^H],$$

As the matrices $H_e U_i$ and $U_i^H H_i^H$ are square and have equal size, based on equation (31), (32) and (33) we can eliminate the term $\det [H_e U_i]$ and $\det [U_i^H H_i^H]$. The secrecy rate selection criterion (28) can be rewritten as,

$$\varphi = \arg \max_{\phi_i \in \Phi, \phi \in \Psi} \left\{ \log \left( \frac{\det [I + \Gamma_{r,i}]}{\det [I + U_i^H R_i^{-1} U_i R_d]} \right) \right\},$$

which is equivalent to (27). In the derivation, we assume the channel matrices of the users have the same matrix size as the channel of the eavesdroppers and the matrices are full rank.

V. SIMULATION RESULTS

In this section, we assess the secrecy rate performance in a multiuser MIMO downlink relay system. In the simulation, 5 relays are placed between the source and the users. Zero-forcing precoding is adopted and we assume that the channel for each user is uncorrelated with the remaining channels and the channel gains are generated following a complex circular Gaussian random variable with zero mean and unit variance.

In Fig. 2 single-antenna scenario, the SINR and SR criteria have a comparable SR performance. However, the SINR criterion requires the interference knowledge and the SR criterion needs the eavesdroppers channel which are both impractical in downlink transmissions. The proposed S-SR algorithm only requires the channels to the relays and the legitimate users and can achieve almost the same SR performance as the SR criterion with full channel knowledge. The proposed S-SINR algorithm suffers a larger degradation than that of the SR criterion.

In Fig. 3 we compare the SR performance for scenarios with square and equal channel matrices and that with the zeros filled out. When we decrease the number of eavesdroppers, the
SR performance increases. In this scenario, the proposed S-SR relay selection algorithm can still perform close to the SR relay selection criterion with full information.

In Figure 3 simplified criteria are compared along with different numbers of relays. The S-SR criterion provides the best secrecy rate performance among all investigated criteria. With more relays distributed between the source and users, the secrecy rate performance can be further improved by employing the proposed S-SR and S-SINR criteria.

VI. CONCLUSION

In this work, we have proposed effective multiple-relay selection algorithms for multiuser MIMO relay systems to enhance the legitimate users’ transmission. The proposed algorithms exploit the use of the available channel information to perform relay selection. Simulation results show that the proposed algorithms can provide a significantly better secrecy rate performance than existing approaches.

REFERENCES

[1] C. Shannon, “Communication theory of secrecy systems,” Bell System Technical Journal, vol. 28, no. 4, pp. 656-715, Oct 1949.
[2] T. L. Marzetta, Noncooperative cellular wireless with unlimited numbers of base station antennas, IEEE Trans. Wireless Commun., vol. 9, no. 11, pp. 3590-3600, Nov. 2010.
[3] R. C. de Lamare, “Massive MIMO Systems: Signal Processing Challenges and Future Trends”, URSI Radio Science Bulletin, 2013.
[4] A. D. Wyner, “The wire-tap channel,” Bell System Technical Journal, vol. 54, no. 8, pp. 1355-1387, 1975.
[5] I. Csiszar and J. Korner, “Broadcast channels with confidential messages,” IEEE Trans. Inform. Theory, vol. 24, no. 3, pp. 339-348, May 1978.
[6] 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.
[7] T. Liu and S. Shamai, “A note on the secrecy capacity of the multi-antenna wiretap channel,” IEEE Trans. Inform. Theory., vol. 55, no. 6, pp. 2547-2553, June 2009.
K. Zu, R. de Lamare, and M. Haardt, “Generalized design of low-complexity block diagonalization for mu-mimo systems,” IEEE Communications Letters, vol. 16, no. 6, pp. 925-927, June 2012.

K. Zu, R. de Lamare, and M. Haardt, “Low-complexity lattice reduction-aided precoding algorithms for large MIMO systems,” IEEE Trans. Communications, vol. 61, no. 10, pp. 4232-4242, October 2013.

K. Lu, K. Zu, R. de Lamare, and M. Haardt, “Multi-branch tomlinson-harashima precoding design for multi-mimo systems: Theory and algorithms,” IEEE Trans. Communications, vol. 62, no. 3, pp. 939-951, March 2014.

K. Lu, K. Zu, and R. C. de Lamare, “Lattice-reduction aided secure communications using opportunistic jammer selection: Secure doF and jammer scaling law,” IEEE Trans. Signal Processing, vol. 62, no. 4, pp. 8288-8301, Feb. 2014.

J. H. Lee and W. Choi, “Multiuser diversity for secrecy communications with Limited Feedback for Interference Mitigation in Multiantenna MC-CDMA Systems,” IEEE Trans. Communications, vol. 59, no. 10, pp. 2594-2607, July 2011.

Y. Cai, R. C. de Lamare, and R. Fa, “Switched Interleaving Techniques with Limited Feedback for Interference Mitigation in DS-CDMA Systems,” IEEE Transactions on Communications, vol. 59, no. 7, pp. 1946-1956, July 2011.

Y. Cai, R. C. de Lamare, and D. Le Ru, “Transmit Processing Techniques Based on Switched Interleaving and Limited Feedback for Interference Mitigation in Multiantenna MC-CDMA Systems,” IEEE Transactions on Vehicular Technology, vol. 60, no. 4, pp. 1559-1570, May 2011.

T. Wang, R. C. de Lamare, and P. D. Mitchell, “Low-Complexity Set-Membership Channel Estimation for Cooperative Wireless Sensor Networks,” IEEE Transactions on Vehicular Technology, vol. 60, no. 6, pp. 2594-2607, July 2011.

T. Wang, R. C. de Lamare and A. Schmeink, “Joint linear beamforming and RF impairment suppression in massive antenna arrays,” IEEE Journal of Communications and Networks, vol. 15, no. 1, pp. 77-88, 2013.

T. Wang and H. V. Poor, “Iterative (turbo) soft interference cancellation and decoding for coded CDMA,” IEEE Trans. Commun., vol. 47, pp. 1046-1061, July 1999.

T. Wang, R. C. de Lamare and R. Fa, “Switched Interleaving Techniques with Limited Feedback for Interference Mitigation in DS-CDMA Systems,” IEEE Transactions on Communications, vol. 59, no. 7, pp. 1946-1956, July 2011.

Y. Cai, R. C. de Lamare, and D. Le Ru, “Transmit Processing Techniques Based on Switched Interleaving and Limited Feedback for Interference Mitigation in Multiantenna MC-CDMA Systems,” IEEE Transactions on Vehicular Technology, vol. 60, no. 4, pp. 1559-1570, May 2011.

T. Wang, R. C. de Lamare, and P. D. Mitchell, “Low-Complexity Set-Membership Channel Estimation for Cooperative Wireless Sensor Networks,” IEEE Transactions on Vehicular Technology, vol. 60, no. 6, pp. 2594-2607, July 2011.

T. Wang, R. C. de Lamare and A. Schmeink, “Joint linear receiver design and power allocation using alternating optimization algorithms for wireless sensor networks,” IEEE Trans. on Veh. Tech., vol. 61, pp. 4129-4141, 2012.

R. C. de Lamare, “Joint iterative power allocation and linear interference suppression algorithms for cooperative DS-CDMA networks”, IET Communications, vol. 6, no. 13, 2012, pp. 1930-1942.
