Relay Selection Based on Secrecy Rate Criterion for Physical-Layer Security in Buffer-Aided Relay Networks

Xiaotao Lu and Rodrigo C. de Lamare

***Abstract*—In this paper, we investigate an opportunistic relay and jammer scheme along with relay selection algorithms based on the secrecy rate criterion in multiple-input multiple-output (MIMO) buffer-aided down link relay networks, which consist of one source, a number of relay nodes, legitimate users and eavesdroppers, with the constraints of physical layer security. The opportunistic relay and jammer scheme is employed to improve the transmission rate and different relay selection policies are performed to achieve better secrecy rate with the consideration of eavesdroppers. Among all the investigated relay selection policies, a relay selection policy which is developed to maximize the secrecy rate based on exhaustive searches outperforms other relay selection policies in terms of secrecy rate. Based on the secrecy rate criterion, we developed a new relay selection algorithm without knowledge of the channels of the eavesdroppers. We also devise a greedy search algorithm based on the secrecy rate criterion to reduce the computational complexity of the exhaustive search technique. Simulations show the superiority of the secrecy rate criterion over competing approaches.**

I. Introduction

Secure transmission is difficult to achieve in broadcast channels due to the nature of wireless communications. Traditional encryption techniques are implemented in the network layer with complex algorithms and high cost. To reduce such cost, researchers are exploring novel security techniques in the physical layer. Physical-layer security is first illustrated by Shannon in his work [1] which was published in 1949 from the view of information theory. The feasibility of the physical layer security is discussed by Shannon in the theoretical level in the paper. Later on in [2] a wire-tap channel which can achieve positive secrecy rate is proposed by Wyner under the assumption that the users have a better statistical channel than eavesdroppers. Since then, further research has been devoted to the wire-tap model and techniques such as broadcast channels [3], MIMO channels, artificial noise, beamforming as well as relay techniques. This paper focuses on relay techniques.

Recently, the concept of physical-layer security with multiuser wireless networks has been investigated [4]. Relay systems are an important evolution of secure transmission strategies and techniques to further improve the performance of relay systems such as buffer-aided relay nodes are drawing significant attention. Opportunistic relay schemes have been applied to buffer-aided systems [5], [6] and [7]. In opportunistic relay schemes, the inter-relay interference (IRI) is an important aspect that should be taken into account.

In our previous work [8], we have introduced an opportunistic relay and jammer scheme and investigated its potential for improving secrecy rate. In this work, we employ the same scheme and focus our research on different relay selection algorithms. Unlike the prior art which relies on the signal-to-interference-plus-noise (SINR) and channel state information [9] approaches, we examine the potential of using the secrecy rate as the criterion for selection of relays. In particular, a relay selection strategy is developed to maximize the secrecy rate based on exhaustive searches. A greedy search algorithm is then developed to reduce the computational complexity of the exhaustive search approach.

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. e-mails: xtl503@york.ac.uk; rodrigo.delamare@york.ac.uk.

II. System Model and Performance Metrics

In this section, a brief introduction of the buffer-aided relay system model is given to describe the data transmission. The performance metrics illustrate the assessment of the proposed and existing techniques described in this paper.

A. System Model

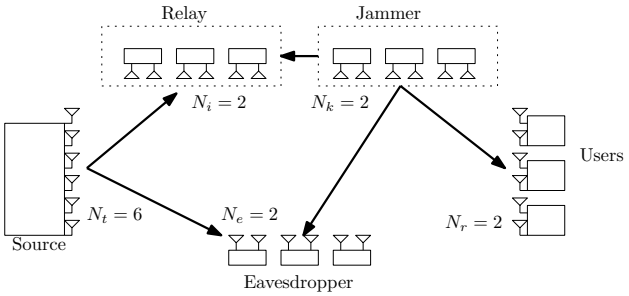

Fig. 1: System model of a MU-MIMO system with M users, N eavesdroppers T relays and K jammers

Fig. 1 gives a description of a source node with N_t antennas transmits the data streams to M users in the existing of N eavesdroppers. With T relays and K jammers, in each time slot, the selected relays will receive signals from both the source and the jammers. 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. The quantities $\boldsymbol{H}_i \in \mathbb{C}^{N_i \times N_t}$ and $\boldsymbol{H}_e \in \mathbb{C}^{N_e \times N_t}$ denote the channel matrices of the ith relay and eth eavesdropper, respectively. The quantities $\boldsymbol{H}_{ke} \in \mathbb{C}^{N_e \times N_k}$ and $\boldsymbol{H}_{kr} \in \mathbb{C}^{N_r \times N_k}$ denote the channel matrices of the eth eavesdropper to the kth jammer and the rth user to the kth jammer, respectively. The channel between the kth relay to the ith relay is $\boldsymbol{H}_{ki} \in \mathbb{C}^{N_i \times N_k}$. To support M users transmission, the source is equipped with $N_t \geqslant N_r M$ antennas.

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 prior work, precoding techniques are implemented to eliminate the interference between different users. In this paper, we use linear zero-forcing precoding and the precoding matrix can be obtained by $\boldsymbol{U}_i = \boldsymbol{H}_i{}^H (\boldsymbol{H}_i \boldsymbol{H}_i{}^H)^{-1}$. The channels of the selected jammers to the rth user are $\boldsymbol{H}_r{}^{(t)} = \begin{bmatrix} \boldsymbol{H}_{k_1 r}^{(t)^T} & \boldsymbol{H}_{k_2 r}^{(t)^T} & \boldsymbol{H}_{k_3 r}^{(t)^T} & \cdots & \boldsymbol{H}_{k_M r}^{(t)^T} \end{bmatrix}$. The channels of the jammers to the ith relay channel are $\boldsymbol{H}_{Ki}{}^{(t)} = \begin{bmatrix} \boldsymbol{H}_{k_1 i}^{(t)^T} & \boldsymbol{H}_{k_2 i}^{(t)^T} & \boldsymbol{H}_{k_3 i}^{(t)^T} & \cdots & \boldsymbol{H}_{k_M i}^{(t)^T} \end{bmatrix}$. To simplify the calculation, we assume that each relay will have the same antenna as

each user which means $\boldsymbol{s}_i^{(t)} = \boldsymbol{s}_r^{(t)}$. 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:

$$\boldsymbol{y}_i^{(t)} = \boldsymbol{H}_i \boldsymbol{U}_i \boldsymbol{s}_i^{(t)} + \sum_{j \neq i} \boldsymbol{H}_i \boldsymbol{U}_j \boldsymbol{s}_j^{(t)} + \boldsymbol{H}_{Ki}^{(t)} \boldsymbol{y}_k^{(pt)} + \boldsymbol{n}_i \quad (1)$$

In (1), the value pt represents the previous time slot when the signal is stored as a jamming signal in the buffer at the relay nodes. The term $\boldsymbol{H}_{Ki}\boldsymbol{y}_k^{(pt)}$ is regarded as the inter-relay interference (IRI) between the ith relay and K jammers and $\boldsymbol{y}_k^{(pt)}$ is determined as the jamming signal according to a SINR criterion as in [5]. With the theorem in [5], the IRI can be eliminated. The jammers to the eth eavesdropper channel $\boldsymbol{H}_{Ke}{}^{(t)} = \begin{bmatrix} \boldsymbol{H}_{k_1 e}^{(t)\,T} & \boldsymbol{H}_{k_2 e}^{(t)\,T} & \boldsymbol{H}_{k_3 e}^{(t)\,T} & \cdots & \boldsymbol{H}_{k_M e}^{(t)\,T} \end{bmatrix}$ At the same time the received signal at the eth eavesdropper is:

$$\boldsymbol{y}_e^{(t)} = \boldsymbol{H}_e \boldsymbol{U}_i \boldsymbol{s}_i^{(t)} + \sum_{j \neq i} \boldsymbol{H}_e \boldsymbol{U}_j \boldsymbol{s}_j^{(t)} + \boldsymbol{H}_{Ke}^{(t)} \boldsymbol{y}_k^{(pt)} + \boldsymbol{n}_e. \quad (2)$$

For the eavesdropper, the term $\boldsymbol{H}_{Ke}^{(t)}\boldsymbol{y}_k^{(pt)}$ 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 the relay nodes or the jamming signal to the eavesdropper is simultaneously the transmit signal from the relays nodes to the destination. We assume that the transmit signal from the relay nodes is $\boldsymbol{r}^{(t)} = \begin{bmatrix} \boldsymbol{y}_1^{(pt_1)\,T} & \boldsymbol{y}_2^{(pt_2)\,T} & \boldsymbol{y}_3^{(pt_3)\,T} & \cdots & \boldsymbol{y}_T^{(pt_T)\,T} \end{bmatrix}^T$. Note that pt represents the previous time slot and due to the characteristics of buffer relay nodes, the values can be different for each relay node. The received signal at the destination can be expressed as:

$$\boldsymbol{y}_r^{(t)} = \boldsymbol{H}_r \boldsymbol{y}_k^{(pt_k)} + \sum_{j \neq r} \boldsymbol{H}_r \boldsymbol{y}_j^{(pt_j)} + \boldsymbol{n}_r. \quad (3)$$

III. Selection with Jamming Function Relays in Multiuser MIMO Buffer-aided Relay System

In this section, a novel selection approach with jamming function relays is introduced. We first consider a simple single-antenna scenario and then the selection approach is extended to a MIMO scenario. After that, a further exploration of the relay selection in a multiuser MIMO buffer-aided relay system is undertaken.

A. Relay Selection Criterion

1) Conventional Relay Selection Criterion: The conventional selection relies only on the knowledge of channel information between source to relay and relay to users. In [10], a max-min relay selection is considered as the optimal selection scheme for conventional decode-and-forward (DF) relay setups. With a single antenna scenario the relay selection policy is given as:

$$R_i^* = \arg \max_{\mathrm{R_i} \in \boldsymbol{\Psi}} \min(\|\mathrm{h_{S,R_i}}\|^2, \|\mathrm{h_{R_i,D}}\|^2) \quad (4)$$

where h_{S,R_k} is the link between the source to the relay and $h_{R_k,D}$ is the relay to the destination.

With the consideration of the eavesdropper, a max-ratio selection policy is proposed in [11] and given by

$$R_i^{\max-\mathrm{ratio}} = \arg \max_{\mathrm{R_i} \in \boldsymbol{\Psi}} (\eta_{\max-\mathrm{ratio}_1}, \eta_{\max-\mathrm{ratio}_2}) \quad (5)$$

with

$$\eta_{\max-\mathrm{ratio}_1} = \frac{\max_{R_i \in \boldsymbol{\Psi}:\varphi(Q_p)\neq L} \|h_{S,R_i}\|^2}{\|h_{se}\|^2} \quad (6)$$

$$\eta_{\max-\mathrm{ratio}_2} = \max_{R_i \in \boldsymbol{\Psi}:\varphi(Q_p)\neq 0} \frac{\|h_{R_i,D}\|^2}{\|h_{R_i e}\|^2} \quad (7)$$

The aforementioned relay selection are based on the channel state information. In [9] there is also a conventional selection as well as optimal selection based on the SINR criterion.

2) Maximum Likelihood (ML) Relay Selection Criterion: Based on the conventional relay selection criterion, we substitute the channel state information with the ML rule which can be expressed as:

$$R_i^{\mathrm{ML}} = \arg \min_{\mathrm{R_i} \in \boldsymbol{\Psi}} (\eta_{\mathrm{ML}_1}, \eta_{\mathrm{ML}_2}) \quad (8)$$

with

$$\eta_{\mathrm{ML}_1} = \min_{R_i \in \boldsymbol{\Psi}:\varphi(Q_p)\neq L} \|y_i - h_{S,R_i} s_i\| \quad (9)$$

$$\eta_{\mathrm{ML}_2} = \min_{R_i \in \boldsymbol{\Psi}:\varphi(Q_p)\neq 0} \|y_r - h_{R_i,D} y_k^{(pt)}\| \quad (10)$$

the ML relay selection selects the relay which gives the minimum ML rule value.

3) Secrecy Rate Based Relay Selection Criterion: Similar to the ML relay selection criterion, the secrecy rate (SR) relay selection criterion is proposed to achieve better secrecy rate performance. The evaluation value can be expressed as:

$$R_i^{\mathrm{SR}} = \arg \min_{\mathrm{R_i} \in \boldsymbol{\Psi}} (\eta_{\mathrm{SR}_1}, \eta_{\mathrm{SR}_2}) \quad (11)$$

with

$$\eta_{\mathrm{SR}_1} = \max_{R_i \in \boldsymbol{\Psi}:\varphi(Q_p)\neq L} \frac{\|1 + h_{S,R_i} s_i\|}{\|1 + h_{se} s_i\|} \quad (12)$$

$$\eta_{\mathrm{SR}_2} = \min_{R_i \in \boldsymbol{\Psi}:\varphi(Q_p)\neq 0} \frac{\|1 + h_{R_i,D} y_k^{(pt)}\|}{\|1 + h_{R_i e} y_k^{(pt)}\|} \quad (13)$$

Based on the single-antenna scenario, the criterion for MIMO system is given by

$$\boldsymbol{\phi}_m = \arg \max_{\mathrm{m} \in \boldsymbol{\Psi}} \left((\boldsymbol{I} + \boldsymbol{\Gamma}_{\mathrm{e,i}}^{(\mathrm{t})})^{-1} (\boldsymbol{I} + \boldsymbol{\Gamma}_{\mathrm{r,i}}^{(\mathrm{t})}) \right), \quad (14)$$

where $\boldsymbol{\Gamma}_{r,i}^{(t)}$ is given as:

$$\boldsymbol{\Gamma}_{r,i}^{(t)} = \sum_{k=1}^{k=K} \frac{P}{N_k} \boldsymbol{H}_{kr} \boldsymbol{H}_{kr}^H (\boldsymbol{I} + \frac{P}{N_t} \boldsymbol{H}_i^{(pt)} \boldsymbol{H}_i^{(pt)\,H}). \quad (15)$$

and

$$\boldsymbol{\Gamma}_{e,i}^{(t)} = (\boldsymbol{I} + \boldsymbol{\Delta})^{-1} \frac{P}{N_t} \boldsymbol{H}_e \boldsymbol{H}_e{}^H, \quad (16)$$

where

$$\boldsymbol{\Delta} = \sum_{e=1}^{N} \sum_{k=1}^{K} \frac{P}{N_k} \boldsymbol{H}_{ke} \boldsymbol{H}_{ke}^H (\boldsymbol{I} + \frac{P}{N_t} \boldsymbol{H}_i^{(pt)} \boldsymbol{H}_i^{(pt)\,H}). \quad (17)$$

4) Proposed Secrecy Rate Based Relay Selection Criterion without Knowledge of Eavesdroppers: Based on (1) and (2), the covariance matrix of the interference and the signal can be obtained as $\boldsymbol{R}_I = \sum_{j \neq i} \boldsymbol{U}_j \boldsymbol{s}_j^{(t)} \boldsymbol{s}_j^{(t)\,H} \boldsymbol{U}_j{}^H$ and $\boldsymbol{R}_d = \boldsymbol{U}_i \boldsymbol{s}_i^{(t)} \boldsymbol{s}_i^{(t)\,H} \boldsymbol{U}_i{}^H$, when the matrices have equal size we can obtain the proposed secrecy rate based relay selection criterion as:

$$\phi_i = \max_i \Big[\log \big(\det \left[\boldsymbol{I} + \boldsymbol{R}_I + (\boldsymbol{H}_i \boldsymbol{R}_d \boldsymbol{H}_i^H) \right] \big) - \log \big(\det \left[\boldsymbol{I} + \boldsymbol{R}_d + (\boldsymbol{H}_i \boldsymbol{R}_I \boldsymbol{H}_i^H) \right] \big) \Big] \quad (18)$$

which can be achieved without knowledge of the channels of the eavesdroppers. The details of the derivation of the above expression will be given in the full paper if this abstract is accepted.

B. Greedy Algorithm in Relay Selection

When the relay selection criterion is determined, we will give an example using the greedy search algorithm. Here we choose relays according to the SR criterion. When the K relays that forward the signals to the users are selected, the relays used for signal reception are chosen based on the SR criterion, as given by

$$\boldsymbol{\phi}_m = \arg\max_{\mathrm{m}\in\boldsymbol{\Psi}} \left((\boldsymbol{I} + \boldsymbol{\Gamma}_{\mathrm{e,i}}^{(\mathrm{t})})^{-1} (\boldsymbol{I} + \boldsymbol{\Gamma}_{\mathrm{m}}^{(\mathrm{t})}) \right), \tag{19}$$

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

$$\boldsymbol{\Gamma}_m^{(t)} = (\boldsymbol{I} + \boldsymbol{\Delta}'_m)^{-1} (\boldsymbol{H}_m \boldsymbol{H}_m^H), \tag{20}$$

where

$$\boldsymbol{\Delta}'_m = \sum_{k=1}^{K} \boldsymbol{H}_{km} \boldsymbol{H}_m^{(pt)} \boldsymbol{H}_m^{(pt)\,H} \boldsymbol{H}_{km}^H, \tag{21}$$

with the SINR calculated for the eth eavesdropper described by

$$\boldsymbol{\Gamma}_{e,i}^{(t)} = (\boldsymbol{I} + \boldsymbol{\Delta}'_e)^{-1} (\frac{P}{N_t} \boldsymbol{H}_e \boldsymbol{H}_e{}^H), \tag{22}$$

where

$$\boldsymbol{\Delta}'_e = \sum_{e=1}^{N} \sum_{k=1}^{K} \frac{P}{N_k} \boldsymbol{H}_{ke} \boldsymbol{H}_{ke}^H (\boldsymbol{I} + \boldsymbol{\xi}), \tag{23}$$

and

$$\boldsymbol{\xi} = \frac{P}{N_t} \boldsymbol{H}_m^{(pt)} \boldsymbol{H}_m^{(pt)\,H}, \tag{24}$$

The main steps are described in Algorithm 3.

Algorithm 1 Greedy Algorithm

for $k = 1 : T$ **do**
  for $m = 1 : M$ **do**
    $\boldsymbol{\Gamma}_m^{(t)} = (\boldsymbol{I} + \boldsymbol{\Delta}'_m)^{-1} (\boldsymbol{H}_m \boldsymbol{H}_m^H)$
    $\boldsymbol{\xi} = \frac{P}{N_t} \boldsymbol{H}_m^{(pt)} \boldsymbol{H}_m^{(pt)\,H}$
    $\boldsymbol{\Gamma}_{e,i}^{(t)} = (\boldsymbol{I} + \boldsymbol{\Delta}'_e)^{-1} (\frac{P}{N_t} \boldsymbol{H}_e \boldsymbol{H}_e{}^H)$
    $\boldsymbol{\phi}_m = \arg\max_{\mathrm{m}\in\boldsymbol{\Psi}} \det \left((\boldsymbol{I} + \boldsymbol{\Gamma}_{\mathrm{e,i}}^{(\mathrm{t})})^{-1} (\boldsymbol{I} + \boldsymbol{\Gamma}_{\mathrm{m}}^{(\mathrm{t})}) \right)$
  end for
  $k = \boldsymbol{\phi}_m$
end for

IV. Simulation Results

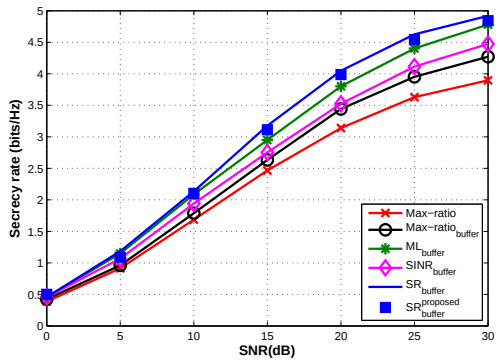

Fig. 2: Single-antenna secrecy rate with different thresholds

In Fig. 2, different relay selection criteria are simulated in a single-antenna scenario. The secrecy rate performance has an improvement if buffers are employed in the relay nodes. Among all the investigated relay selection criteria, SR relay selection can achieve the best secrecy rate performance. Interestingly, this approach is typically not used because of the need for knowledge about the channels of the eavesdroppers.

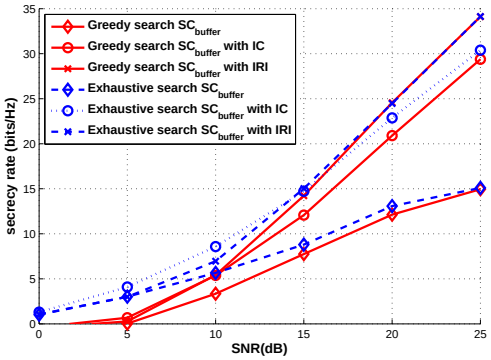

Fig. 3: Multi-user system scenario

In Fig. 3, 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.

V. Conclusion

In this work, we have employed an opportunistic relay and jammer scheme to enhance the physical layer secrecy rate performance. The proposed secrecy rate relay selection policy contributes to the improvement of the secrecy rate performance. Simulation results indicate that the secrecy rate criterion relay selection policy achieves the best secrecy rate performance and the greedy search can approach a higher 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, The*, 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. [Online]. Available: http://dx.doi.org/10.1002/j.1538-7305.1975.tb02040.x

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

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

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

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

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

[8] X. Lu and R. C. Lamare, "Opportunistic relay and jammer cooperation techniques for physical-layer security in buffer-aided relay networks," in *The Twelfth International Symposium on Wireless Communication Systems (ISWCS)*, 2015.

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

[10] I. Krikidis, T. Charalambous, and J. Thompson, "Buffer-aided relay selection for cooperative diversity systems without delay constraints," *Wireless Communications, IEEE Transactions on*, vol. 11, no. 5, pp. 1957–1967, May 2012.

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