Relay Selection for Multi-Destination in Cooperative Networks with Secrecy Constraints

Esa R. Alotaibi, Khairi A. Hamdi.
School of Electrical and Electronic Engineering,
The University of Manchester, Manchester M13 9PL, U.K.
Email: esa.alotaibi@postgrad.manchester.ac.uk, k.hamdi@manchester.ac.uk.

***Abstract*—Most of the prior researches in the field of relay selection techniques under security constraints for cooperative networks have only concentrated on single destination, although the factual communication environment comprehends multiple transmitters and receivers. This paper proposes relay selection for multi-destinations in cooperative networks. The study is implemented under a security constraint whereby an eavesdropper tries to eavesdrop on information sent from the sender. Hence, we investigate an optimal relay selection technique, in order to improve the level of security in the network by securing information sent to multi-destinations and thereby confusing the eavesdropper. The performance of the proposed system scheme is analysed using average secrecy capacity and outage probability, which are confirmed by numerical results based on simulations.**

***Index Terms*—Relay selection, cooperative networks, secrecy capacity, outage probability, multi-destination.**

I. INTRODUCTION

Relay selection is one of the major factors involved in cooperative wireless networks. In cooperative communication networks, multiple relay terminals are allocated to help a sender in forwarding its message to its destination, therefore providing full spatial diversity by enabling user nodes to contribute their antennas and create a virtual antenna array. Recent evolutions in the scope of cooperative networks have led to the current interest in relay selection techniques [1]–[3].

Cooperative communication not only enhances the throughput and reliability of wireless communications, but it also has great potential to improve wireless security against any attack from eavesdroppers. Physical layer security takes advantage of the physical features of wireless channels, to inhibit the eavesdropper from overhearing information sent from a sender to an intended receiver [4]–[7]. Numerous studies have contributed to using relay selection techniques for improving physical layer security. Zou, in his research [8], posited the concept of optimal relay selection for physical layer security in cooperative wireless networks with multiple helpers. The researchers analysed this scenario under two conditions: optimal relay selection with amplify-and-forward (AF) and decode-and-forward (DF) protocols, for the intend of comparison, they study the traditional AF and DF schemes by using relay selection technique, they also examine AF and DF types by utilising multiple relay combining MRC mechanism, where multiple relays share in forwarding the source information to destination which then combines its received message from the multiple relays. they used closed-form to derived outage probability expressions of the all schemes in the presence of eavesdropper, furthermore they analysed an asymptotic outage probability to estimate the performance of relay selection schemes improve the diversity. Moreover, their results display that for their optimal DF and AF rely selection schemes, the outage probability performance is better than both the traditional relay selection techniques and multiple relay combining schemes. However, the researchers considered only a single relay destination link as well as a single relay eavesdropper link for the performance analysis of their system.

In addition, many other study community organisations have investigated a single relay destination link for analysis and performance valuation [9]–[11]. Therefore, the real-life, practical scenario includes multiple senders, multiple receivers and multiple eavesdroppers.

Commonly, a cooperative wireless network is a gigantic network, just like any other conventional network. Many senders and destinations with multiple relays in the middle are taken into account when designing a cooperative network. In [12], the authors combined a relay selection technique and cooperative beamforming methods to enhance physical layer security by selecting two available relays for beamforming and information transmission, consequently minimising the number of relays sharing and decreasing the coding gain of cooperative beamforming, and thus reducing the complexity problem.

A proposed relay selection scheme for physical layer security in cognitive radio networks is investigated in [13]. The proposed protocol selects a decode-and-forward relay, to help a secondary user sender and increases the achievable secrecy capacity that based on the interference power constraints at the primary users for the different number of eavesdroppers and primary user under available channel state information, the others proved that the secrecy rate and the outage probability performance of their system model are enhanced. The work in [9] presents two new opportunistic relay selection schemes, based on the quality of the relay-eavesdropper channels, where the first technique supposes that channel state information on the eavesdropper channels is known and improves the achievable secrecy rate; however, the second scheme uses average channel state information on eavesdropper links, known as a suboptimal selection scheme.

Krikidis in other research work [14] investigated the opportunistic relay selection of two helper nodes, to improve secrecy rates against eavesdropping, where the first relay investigates

978-1-4799-4449-1/14/$31.00 ©2014 Crown

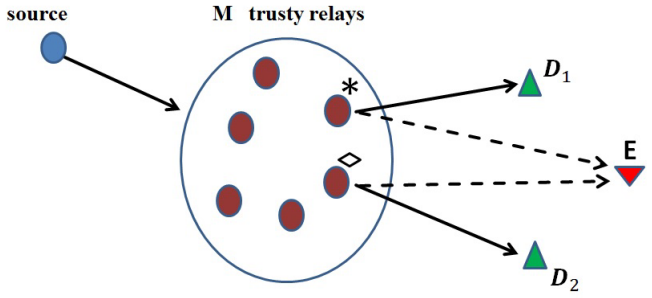

Fig. 1. System model of relay selection for multi-destinations in cooperative networks with secrecy constraints.

a conventional style and helps a sender to forward its message to a destination with a decode-and-forward protocol while the second helper node is exploited to produce intended jamming to confuse the eavesdropper and at the same time protect the destination without interference.

Our proposed scheme unites a physical layer security approach and an optimal relay selection with a multi-destination scenario. Secrecy capacity is calculated in terms of outage probability, and in addition enhancements to the selection technique are presented.

The contribution of this paper is twofold:

- First, an optimal relay selection mechanism is analysed in cooperative wireless communication when an eavesdropper is present in the network.
- Then, the analysis is extended to include secure relay selection with a multi-destination aspect.

The rest of the paper is arranged as follows. Section II introduces the proposed system model and presents a numerical analysis of the relay selection and outage probability. Numerical results and a performance evaluation of the proposed system model are shown in section III, followed by a paper conclusion in Section IV and a brief outline of future research.

II. System Model and Relay Selection

The proposed system model in this research is composed of one source (S), two destinations (D_1 , D_2), one eavesdropper (E) and a set of M relays. These relays utilise a decode-and-forward (DF) protocol. Fig.1 displays schematically the system model and the two phases of the deliberate cooperative system.

We consider the following assumptions:

- The source does not have a direct link to the destination and eavesdropper nodes.
- All the channels have slow-flat Rayleigh fading.

In this paper, we transact with a relay selection protocol in a cooperative communication system with two destinations and one eavesdropper, consequently enhancing physical layer security by maximising the capacity of the wireless channels to the destination terminals and minimising the capacity of the link to the eavesdropper. This paper concentrates on the effect of a relay selection strategy on physical layer security under the proposition of perfect channel state information (CSI).

When both destinations and the eavesdropper are active users of the network, in the first phase of this protocol the source broadcasts its signal to all the relay nodes. In the second phase, the first potential relay node chosen from the relays that successfully decodes the source message, forwards the re-encoded signal to the suitable destination and the eavesdropper, following which the second most suitable relay node forwards the re-encoded signal to the second destination. The channels between nodes $i \in \{m^*, m^\diamondsuit\}$ and $j \in \{D_1, D_2, \mathrm{E}\}$ are modelled as independent and slowly varying flat Rayleigh fading random variables. The channels remain static for one coherence interval (one slot) and change independently in different coherence intervals with a variance $\sigma^2_{i,j} = d^{-\beta}_{i,j}$, where $d_{i,j}$ is the Euclidean distance between node i and j and β is the path loss exponent. Noise is surmised to be additive white Gaussian noise (AWGN) with zero mean and unit variance.

Notation	Definition
m^*	Best relay for the first destination
$m^\diamondsuit$	Best relay for the second destination
$C_{D_1}(m^*)$	The instantaneous secrecy capacity for the first destination
$C_{D_2}(m^\diamondsuit)$	The instantaneous secrecy capacity for the second destination
$\gamma_{i,j}$	The instantaneous signal-to-noise ratio (SNR) for the link from i to j
$f_{i,j}$	The instantaneous channel coefficient for the link from i to j
P	The transmitted power
M	Number of trusty relays
$\mathrm{Z}_{\max}$	The equivalent instantaneous SNR at the output of the relay selection for the first destination
$\mathrm{Y}_{\max}$	The equivalent instantaneous SNR at the output of the relay selection for the second destination
$F_{\max}(z)$	The cumulative density function for the first destination
$\mathrm{F}_{\max}(\mathrm{y})$	The cumulative density function for the second destination
C_{s_i}	The instantaneous secrecy rate for i^{th} destination
R	Target rate
$f(\gamma_{m,i})$	The probability density function between m^{th} relays and i^{th} destination
$\lambda_{m,i}$	Parameter distribution between m^{th} relays and i^{th} destination

Table I
System Model Parameters

The instantaneous secrecy capacity (secrecy rate) of each destination channel is given respectively by

$$C_{D_1}(m^*) = \left[\frac{1}{2}\log_2\left(1+\gamma_{m^*,D_1}\right) - \frac{1}{2}\log_2\left(1+\gamma_{m^*,E}\right)\right]^+ = \left[\frac{1}{2}\log_2\left(\frac{1+\gamma_{m^*,D_1}}{1+\gamma_{m^*,E}}\right)\right]^+ \quad (1)$$

$$C_{D_2}(m^\diamondsuit) = \left[\frac{1}{2}\log_2\left(1+\gamma_{m^\diamondsuit,D_2}\right) - \frac{1}{2}\log_2\left(1+\gamma_{m^\diamondsuit,E}\right)\right]^+ = \left[\frac{1}{2}\log_2\left(\frac{1+\gamma_{m^\diamondsuit,D_2}}{1+\gamma_{m^\diamondsuit,E}}\right)\right]^+ \quad (2)$$

where $\gamma_{i,j} = \mathrm{P}\,|f_{i,j}|^2$ denotes the instantaneous signal-to-noise ratio (SNR) for the link from i to j , $(f_{i,j})$ is the

instantaneous channel coefficient for the link from i to j, P is the transmitted power, m^* is the best relay for the first destination, $m^\diamondsuit$ is the best relay for the second destination and $[x]^+ = \max\{x, 0\}$.

For high signal-to-noise ratios we approximate secrecy capacity at relay m, which can be written as

$$C_D(m) = \left[\frac{1}{2}\log_2\left(\frac{\gamma_{m,D}}{\gamma_{m,E}}\right)\right]^+ \tag{3}$$

The main aim of this work is to focus on selecting a suitable relay for each destination count in the relay selection technique, which will be explained in detail in the following section.

A. Optimal Relay Selection

The optimal relay has the maximum instantaneous scaled harmonic mean function of its source relay and relay destination channel gains among the M helping relays [2]. In this scheme, we suppose that the instantaneous goodness of relay-eavesdropper links is obtainable throughout a decision operation. This depends on the instantaneous secrecy capacity equations yielded in (1) and (2). The optimal selection technique for the first relay is written as

$$m^* = \arg\max_{m\in M_{relays}}\left\{\frac{\gamma_{m,D_1}}{\gamma_{m,E}}\right\} \tag{4}$$

Similarly, for the second relay, it is given as

$$m^\diamondsuit = \arg\max_{m\in M_{relays}}\left\{\frac{\gamma_{m,D_2}}{\gamma_{m,E}}\right\}, \qquad m \neq m^* \tag{5}$$

B. Outage Probability

The instantaneous secrecy rate for the first destination regarding m^{th} relay links is written in (1). In addition, we develop the secrecy rate for the second destination, as shown in (2). The equivalent instantaneous SNR at the output of the relay selection for the first destination can be expressed as

$$\mathrm{Z}_{\max} = \max\left[\mathrm{Z}_1,...,\mathrm{Z}_\mathrm{M}\right] \tag{6}$$

where

$$\mathrm{Z}_m = \frac{1+\gamma_{m,\mathrm{D}_1}}{1+\gamma_{m,\mathrm{E}}} \tag{7}$$

where, m here represents the relays from the first relay to the M relay. However, for the second destination the equivalent instantaneous SNR at the output of the relay selection can be written as

$$\mathrm{Y}_{\max} = \max\left[\mathrm{Y}_1,...,\mathrm{Y}_{\mathrm{M}-1}\right] \tag{8}$$

where

$$\mathrm{Y}_m = \frac{1+\gamma_{m,\mathrm{D}_2}}{1+\gamma_{m,\mathrm{E}}}, \qquad m \neq m^* \tag{9}$$

where, m denotes the relays from the first relay to the M relay except for the relay which is selected for the first destination. The cumulative density function (CDF) for the first destination is

$$\mathrm{F}_{\max}(z) = \prod_{m=1}^{M}\mathrm{F}_m(z) \tag{10}$$

where $\mathrm{F}_m(z)$ is the cumulative density function (CDF) of Z_m.

And the CDF of the second destination is expressed as

$$\mathrm{F}_{\max}(y) = \prod_{m=1}^{M-1}\mathrm{F}_m(y), \qquad m \neq m^* \tag{11}$$

where, m represents the relays from the first relay to the M relay, except for the relay which is selected for the first destination, and where $\mathrm{F}_m(y)$ is the cumulative density function (CDF) of Y_m. After relay selection, the instantaneous secrecy rate can be given by (for the first destination):

$$C_{s_1} = \max\left[\max(\mathrm{Z}_m, 0)\right] \tag{12}$$

and for the second destination

$$C_{s_2} = \max\left[\max(\mathrm{Y}_m, 0)\right], \qquad m \neq m^* \tag{13}$$

This work characterises relay selection with secrecy constraints in terms of outage probability. Outage probability defines the probability that instantaneous secrecy capacity will fall below a target rate R as

$$\begin{aligned}\mathrm{P}_{out}(\mathrm{R}) &= \mathrm{P}_r(C_s < \mathrm{R}) \\ &= \mathrm{F}_{\max}(2^{2\mathrm{R}})\end{aligned} \tag{14}$$

where, R is a target rate and C_s is the instantaneous secrecy rate. For the first destination

$$\mathrm{F}_m(z) = \int_0^\infty f(\gamma_{m,E})\mathrm{d}(\gamma_{\mathrm{m,E}}) \times \int_0^{Z(\gamma_{m,E})+Z-1} f(\gamma_{m,D_1})\mathrm{d}(\gamma_{\mathrm{m,D_1}})$$

as we assume all the channels are using Rayleigh fading, the probability density functions of the SNRs $f(\gamma_{m,D_1})$, $f(\gamma_{m,D_2})$ and $f(\gamma_{m,E})$ are exponentially distributed with parameters λ_{m,D_1}, λ_{m,D_2} and $\lambda_{m,E}$, respectively. Thus

$$\mathrm{F}_m(z) = 1 - \exp\left(-\frac{(z-1)}{\lambda_{m,D_1}}\right)\frac{\lambda_{m,D_1}}{z\lambda_{m,E}+\lambda_{m,D_1}} \tag{15}$$

Substituting (15) in (10), $\mathrm{F}_m(z)$ can be resolved. Therefore, in the event of an independent and identically distributed (IID) scenario, by utilising binomial expansion, the outage probability for target rate R for the first destination is given by

$$\mathrm{P}_{out} = \sum_{m=0}^{M} C_m^M\left(\frac{-\lambda_{m,D_1}}{2^{2\mathrm{R}}\lambda_{m,E}+\lambda_{m,D_1}}\right)^m \times\exp\left(-\frac{m(2^{2\mathrm{R}}-1)}{\lambda_{m,D_1}}\right) \tag{16}$$

where $C_m^M = \frac{M!}{m!(M-m)!}$, M is the number of relays.

For the second destination, $\mathrm{F}_m(y)$ for $m \neq m^*$ is expressed as

$$\mathrm{F}_m(y) = \int_0^{\infty} f(\gamma_{m,E})\mathrm{d}(\gamma_{\mathrm{m,E}}) \times \int_0^{y(\gamma_{m,E})+y-1} f(\gamma_{m,D_2})\mathrm{d}(\gamma_{\mathrm{m,D_2}}) = 1 - \exp\left(-\frac{y-1}{\lambda_{m,D_2}}\right)\frac{\lambda_{m,D_2}}{y\lambda_{m,E}+\lambda_{m,D_2}} \quad (17)$$

Substituting (17) in (11), $\mathrm{F}_m(y)$ can be resolved. Therefore, in the event of an independent identically and distributed (IID) scenario, by utilising the binomial expansion, the outage probability for target rate R for the second destination is given by

$$\mathrm{P}_{out} = \sum_{m=0}^{M-1} C_m^{M-1}\left(\frac{-\lambda_{m,D_2}}{2^{2R}\lambda_{m,E}+\lambda_{m,D_2}}\right)^m \times \exp\left(-\frac{m(2^{2\mathrm{R_s}}-1)}{\lambda_{m,D_2}}\right) \quad m \neq m^* \quad (18)$$

where $C_m^{M-1} = \frac{(M-1)!}{m!(M-m-1)!}$

1) Asymptotic outage probability: It is also important to examine the asymptotic behaviour of outage probability at high signal-to-noise ratios (SNRs). When $\lambda_{m,D_1} \to \infty$, $\lambda_{m,D_2} \to \infty$ and $\lambda_{m,E} \to \infty$ with constants $l = \frac{\lambda_{m,D_1}}{\lambda_{m,E}}$ and $p = \frac{\lambda_{m,D_2}}{\lambda_{m,E}}$, asymptotic outage probability is expressed for the first destination as

$$\mathrm{P}_{\mathrm{out(asym.D_1)}}(\mathrm{R}) = \left(\frac{2^{2\mathrm{R}}}{2^{2\mathrm{R}}+l}\right)^M \quad (19)$$

Similarly, asymptotic outage probability for the second destination is written as

$$\mathrm{P}_{\mathrm{out(asym.D_2)}}(\mathrm{R}) = \left(\frac{2^{2\mathrm{R}}}{2^{2\mathrm{R}}+p}\right)^{M-1} \quad (20)$$

III. Numerical Results and Performance Analysis

In line with the proposed system model for multi-destinations discussed in the previous section, a 2D square topology simulation model is developed, as shown in Fig. 2. The relay nodes are randomly deployed according to a uniform distribution. The topology model consists of a source, five relays which are set randomly, two destinations and one eavesdropper. S, D_1, D_2 and E are located as $\{\mathrm{X}_S, \mathrm{Y}_S\}$ = {0, 0}, $\{\mathrm{X}_{D_1}, \mathrm{Y}_{D_1}\}$={0, 1}, $\{\mathrm{X}_{D_2}, \mathrm{Y}_{D_2}\}$={1, 0} and $\{\mathrm{X}_E, \mathrm{Y}_E\}$={1, 1}, respectively. The dimension of the system is simplified to unit length. The path loss exponent is assumed to be three (β=3), spectral efficiency is set to two bits per channel (R_o=2) and the target rate is assumed to be equal (R= 0.5). Each relay node has two numerical values, the first of which is SNR from the relay to the first destination, while the second value is SNR from the relay to the second destination. The topology is shown clearly in Fig. 2.

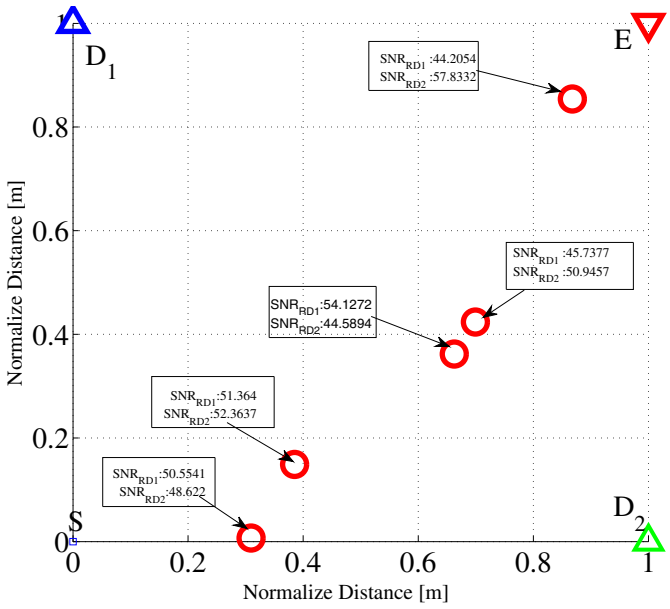

Fig. 2. Topology of the simulation environment of the system model

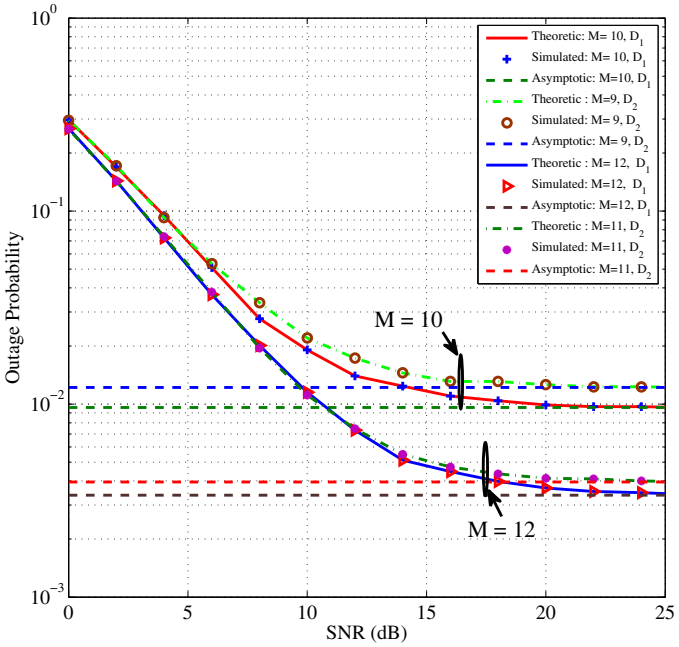

Fig. 3. Outage secrecy capacity for the first and second destinations against SNR (dB) for various numbers of relays

Fig. 3 shows the outage probability analysis for the proposed multi-destination cooperative network. The theoretical curves of outage probability in Fig. 3 were plotted using Equations (16) and (18), and the asymptotic outage probabilities curves in Fig. 3 were plotted using equations (19) and (20). As can be seen from the figures' curves, there is excellent agreement between the simulation and the theoretical results, thus confirming our derivations. Assuming R, increasing SNR provides good performance in terms of outage probabilities for the multi-destination scenario. When we add more relays,

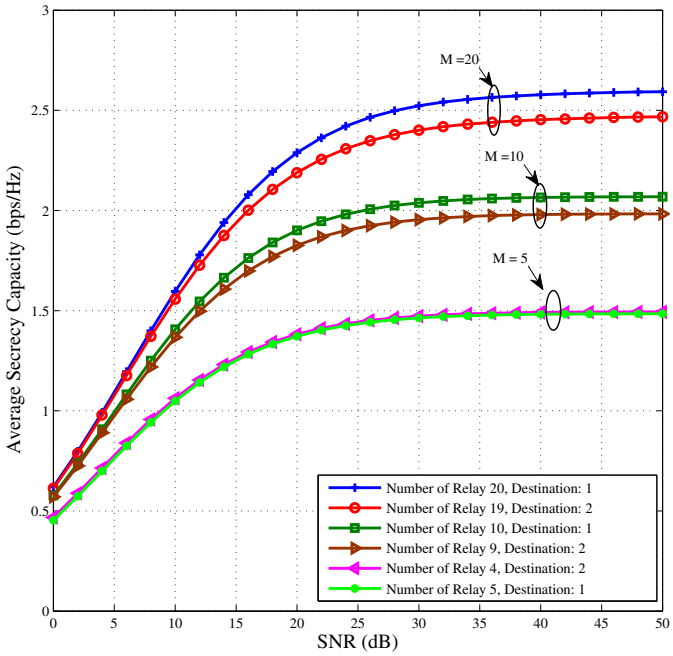

Fig. 4. Average secrecy capacity for the first and second destinations against SNR (dB) for various numbers of relays

the outage probabilities attain better values and we find that the outage probability for the first destination is better than that for the second destination. For M=12, and for D1 and D2, we achieve an outage probability almost below 10^{-2}. Also, for M=10, we observe that outage probability values for both destinations are close to 10^{-2}. Asymptotic outage probability for M=10 for D_2 is observed to be a little bit above 10^{-2} , while for D_1 it is observed to achieve a better value at slightly below 10^{-2}. Furthermore, by increasing the number of relays from M=10 to M=12, the outage probability performance of the cooperative network is observed to be considerably improved. As SNR increases from 25, the outage probability settles to a particular value somewhat below 10^{-2}.

Average secrecy capacities are depicted in Fig. 4. Compared to number of relays M=5, the average secrecy capacity for M=20 is observed as good, reaching almost 2.5, while for M=10, the average secrecy capacity achieved is around 2, although it is relatively less, i.e. 1.5, for M=5. The main reasons for the better results achieved in this study are due to relay cooperation.

IV. Conclusion

Previous researchers have concentrated on relay selection mechanisms under a security constraint for cooperative networks with only one destination. In this research, we have investigated a relay selection scheme with multi-destinations, in order to ensure the secrecy of the network against an eavesdropper posing as a network user. An optimal scheme for a decode-and-forward multi-destination cooperative network was investigated, and its performance improvements were validated by theoretical and numerical results. The real benefits of cooperation can be reaped by including multiple sources, multiple relays and multiple destinations. Furthermore, the cooperative communication concept is better realised with the help of multi-source and multi-destination systems. When there is one source, one relay and one destination, the communication system works more like a multi-hop rather than a cooperative system. The results obtained with our multi-destination concept are much better compared to a single destination, with the added advantage of security. In addition, our system puts forth the concept of relay selection for a multi-destination scenario by taking into consideration outage probability and average secrecy capacity. This work will be further extended for destination selection rather than relay selection relay. In addition, we will look to improve physical layer security for multi-source and multi-destination wireless cooperative communication systems.

References

[1] S. Nam, M. Vu, and V. Tarokh, "Relay selection methods for wireless cooperative communications," in *Proc. CISS, Princeton, NJ, Mar. 2008*, pp. 859–864.

[2] A. S. Ibrahim, A. K. Sadek, W. Su, and K. J. R. Liu, "Cooperative communications with relay-selection: when to cooperate and whom to cooperate with?," *IEEE Trans. Wireless Commun.*, vol. 7, no. 7, pp. 2814–2827, July 2008.

[3] A. Bletsas, A. Lippnian, and D. Reed, "A simple distributed method for relay selection in cooperative diversity wireless networks, based on reciprocity and channel measurements," in *Proc. 61st IEEE Veh. Technol. Conf. VTC 2005-Spring*, vol. 3, pp. 1484–1488, May 2005.

[4] Z. Zheng, S. Fu, K. Lu, J. Wang, and B. Chen, "On the relay selection for cooperative wireless networks with physical-layer network coding," *Wirel. Netw.*, vol. 18, pp. 653–665, Aug. 2012.

[5] J. Li, A. P. Petropulu, and S. Weber, "Optimal cooperative relaying schemes for improving wireless physical layer security," *CoRR*, vol. abs/1001.1389, 2010.

[6] K. Chen, B. Zhang, D. Liu, Y. Ma, and G. Yue, "Proactive relay selection in distributed multi-source cooperative networks," in *IEEE International Conf. ICCTA '09*, pp. 96–100, 2009.

[7] H. Long, W. Xiang, Y. Zhang, Y. Liu, and W. Wang, "Secrecy capacity enhancement with distributed precoding in multirelay wiretap systems," *IEEE Trans. Inf. Forensics and Security*, vol. 8, no. 1, pp. 229–238, Jan. 2013.

[8] Y. Zou, X. Wang, and W. Shen, "Optimal relay selection for physical-layer security in cooperative wireless networks," *IEEE Journal on Selected Areas in Communications*, vol. 31, pp. 2099–2111, October 2013.

[9] I. Krikidis, "Opportunistic relay selection for cooperative networks with secrecy constraints," *IET Commun.*, vol. 4, no. 15, pp. 1787 –1791, Oct. 2010.

[10] H. N. Vu and V. N. Q. Bao, "Study of relay selection for dual-hop networks under secrecy constraints with multiple eavesdroppers," in *ATC Commun.*, pp. 89 –92, Aug. 2011.

[11] X. Sun, C. Zhao, and M. Jiang, "Closed-form expressions for relay selection with secrecy constraints," *Computing Research Repository*, 2010.

[12] J. Kim, A. Ikhlef, and R. Schober, "Combined relay selection and cooperative beamforming for physical layer security," *Journal of Commun. and Networks*, vol. 14, pp. 364–373, Aug 2012.

[13] H. Sakran, M. Shokair, O. Nasr, S. El-Rabaie, and A. El-Azm, "Proposed relay selection scheme for physical layer security in cognitive radio networks," *IET Commun.*, vol. 6, pp. 2676–2687, Nov. 2012.

[14] I. Krikidis, J. Thompson, and S. McLaughlin, "Relay selection for secure cooperative networks with jamming," *IEEE Trans. on Wireless Commun.*, vol. 8, pp. 5003–5011, Oct. 2009.