ISSN: 2229-6948(ONLINE)
DOI: 10.21917/ijct.2020.0334

SECRECY ENHANCEMENT IN COOPERATIVE NETWORKS VIA RELAY SELECTION AND POWER ALLOCATION

P.M. Shemi[1] and M.A. Ali[2]
[1]*Department of Electronics, MES College Marampally, India*
[2]*Department of Computer Applications, Government Engineering College, Thrissur, India*

Abstract

A performance comparison of relay selection based on the path probability selection of Ant Colony Optimization algorithm (ACO), among dual-hop amplify-and-forward and decode-and-forward relay networks is formulated in this paper. An adaptive power allocation strategy based on Brent's method has been proposed. The secrecy performance is evaluated in traditional, fading and path loss wireless models. Traditional best relay selection, exhaustive search optimization algorithm and equal power allocation strategy have been derived as schemes for comparison. The effect of number of relays on secrecy is also evaluated. Simulation results reveal the merits of the proposed relay selection and optimization schemes as compared to conventional schemes.

Keywords:

Brent's Method, Optimal Power Allocation, Ant Colony Optimization, Secrecy Rate

1. INTRODUCTION

Physical layer security (PLS) based on cooperative communication has been considered as an evolving technique that enhances the security of wireless systems against eavesdropping [1]. Cooperative relaying has attracted research interests, since it is capable of reducing both the shadowing and fading effects of wireless channels. Cooperation among nodes improves the network coverage and diversity without using multiple antennas [2]. The two common relaying protocols used in cooperative relaying are amplify-and-forward (AF) and decode-and-forward (DF). Secrecy rate is taken as an important performance parameter of PLS, which is defined as the difference of the information rate of the main channel and that of the wiretap channel. For a secure communication, a positive secrecy rate is to be guaranteed [3]. If the channel quality of legitimate channel is worse than that of the wiretap channel, secrecy rate will be zero. Hence, perfect secrecy cannot be always guaranteed due to channel fading [4]. Cooperative relaying has been proposed to overcome this situation as well as to ensure secure and reliable transmission.

The multiple relays in cooperative relaying techniques require multiple channel resources for transmission and these signals are to be combined at the destination by maximal ratio combining (MRC). As a result, the spectral efficiency of the system reduces and the hardware complexity increases, both of which can be overcome by relay selection (RS) techniques. In RS, one among a set of relays is selected, and the same is used for transmission. The selected relay is known as the best relay (BR). Thus it improves the system spectral efficiency. Also full diversity can be achieved with low overhead and complexity [5] [6]. Best relay selection (BRS) scheme for AF and DF protocols has been studied in [7] – [9]. In [7], closed form intercept probability for RS employing DF and AF relays in dual-hop cooperative relay system is derived. ACO based RS that employs equal power allocation (EPA) strategy for AF cooperative network is investigated in [8] and that for DF network is studied in [9].

Unlike the traditional RS schemes, where selection of relay is possible only in a specific wireless model, it could be done in three wireless scenarios in the ACO based RS schemes [8, 9]. Here, the coefficients of fading (h) and gain of the channel (G) defining a wireless channel are considered separately so as to apply the RS algorithm. The paper considers a practical scenario, where direct links exist between source and destination and between source and eavesdropper, with relays randomly distributed between the transmitting and receiving nodes. By considering the behavior of G and h together or by taking G or h alone, the secrecy performance is analyzed in the following cases: (i) in a traditional model characterized by both G and h (ii) in a fading model defined by only h and (iii) in a path loss model defined by only G. A performance comparison among AF and DF cooperative relays is then formulated in this work. Secrecy performance can be enhanced if proper power allocation is done among the source and relay nodes. Optimal power allocation (OPA) based on Brent's method (BM) and exhaustive search (ES) algorithms are also derived and their performance is compared with EPA scheme.

The main contributions of this work are outlined as:

A performance comparison of RS based on the path probability selection criterion of ACO algorithm in two-hop AF and DF cooperative networks with trusted relaying scheme in the presence of an external eavesdropper is formulated. OPA scheme based on Brent's method and exhaustive search algorithms for secrecy enhancement is derived. The performance comparison with EPA strategy and traditional RS methods is also done in this work.

The remainder of this paper is organized as follows. In section 2, the network model and transmission schemes are discussed. Section 3 highlights the relay selection schemes. Performance analysis is presented in Section 4 followed by results and analysis in Section 5. Finally, we conclude the paper in Section 6.

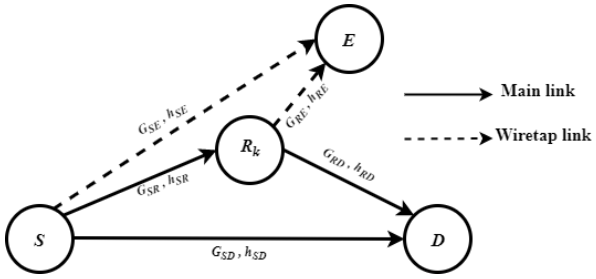
2. NETWORK MODEL AND TRANSMISSION SCHEMES

2.1 NETWORK MODEL FOR SECURE TRANSMISSION

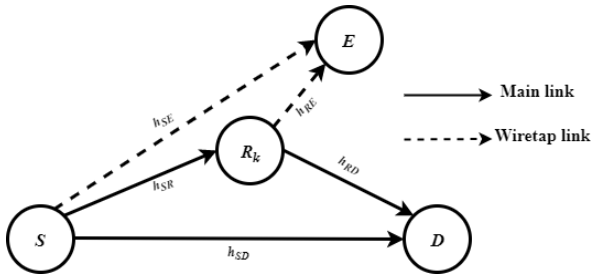
We consider a cooperative network, where a source (S) is sending information to its destination (D), via N relays in the presence of a passive eavesdropper (E). The relays indicated by $R = \{R_k | k=1,2,\ldots,N\}$, operate in half-duplex mode. They are assumed to be trusted and randomly located between the source

and destination nodes. The nodes are provided with a single omnidirectional antenna. Rayleigh fading channel model is used for simulation. The additive noise present at the receivers is characterized by Gaussian random variable with zero mean and variance σ^2, i.e., CN (0, σ^2). A time-division multiple-access based protocol is assumed. The signal transmission involves two phases. During the first phase, the signal x_s from the source is broadcasted to both the relays and destination with power $P_s = aP$; and during the second phase of transmission, the selected relay forwards the received signal to destination with power $P_r = (1\text{-}a)P$, where P is the total transmit power and $a \in (0, 1)$ is the power allocation factor between the source and relay nodes.

The channel coefficients for the proposed and conventional models are shown in Fig.1*a* and *b* respectively. In the proposed model, the channel is defined by two parameters namely, gain of the channel (G) and fading coefficients (h) [10] which helps to apply the proposed RS algorithm. In the conventional model, the gain of the channel or fading or the combined effects of both are considered as a single entity.



(a) Proposed Model



(b) Conventional Model with the Selected Relay R_k

Fig.1. Channel coefficients

Thus, the received signal at node j can be written as [10]

$$y_{ij} = \sqrt{P_i} G_{ij} h_{ij} x_i + n_j \tag{1}$$

where n_j is the additive noise at the receiving end j.

Hence, SNR at j is

$$\gamma_{ij} = P_i \frac{\left|G_{ij} h_{ij}\right|^2}{\sigma_j^2} \tag{2}$$

where $i \in (S,R)$; $j \in (R,D,E)$; i.e. i and j indicate the transmitting and receiving nodes respectively. G_{ij} - the gain of the channel between the nodes i and j is [10]

$$G_{ij} = G_0 \left(\frac{d_{ij}}{d_0}\right)^{-L/2} \tag{3}$$

where G_o is carrier wavelength, L is the path loss factor such that it satisfies $2 \le L \le 6$, d_{ij} is the separation among the nodes i and j, d_o is reference distance. G_{ij} is set equal to $(d_{ij})^{-0.5L}$, taking the other constants as unity.

2.2 AMPLIFY-AND-FORWARD SCHEME (AF)

During the relaying phase of transmission, the signal from the source is amplified by the selected relay k and then forwarded to destination. Since the eavesdropper and destination get signals from the relayed and direct path, MRC is done at the corresponding nodes. The overall SNR at the destination and eavesdropper is obtained as [8]

$$\gamma_{D_{AF}} = \gamma_{SD} + \frac{\gamma_{SR_k}\gamma_{R_kD}}{1+\gamma_{SR_k}\gamma_{R_kD}} \tag{4}$$

$$\gamma_{E_{AF}} = \gamma_{SE} + \frac{\gamma_{SR_k}\gamma_{R_kE}}{1+\gamma_{SR_k}\gamma_{R_kE}} \tag{5}$$

where the instantaneous SNR is obtained by Eq.(2).

Therefore, the transmission rate at the destination and eavesdropper are

$$R_{D_{AF}} = 0.5\log_2\left(1+\gamma_{SD} + \frac{\gamma_{SR_k}\gamma_{R_kD}}{1+\gamma_{SR_k}\gamma_{R_kD}}\right) \tag{6}$$

$$R_{E_{AF}} = 0.5\log_2\left(1+\gamma_{SE} + \frac{\gamma_{SR_k}\gamma_{R_kE}}{1+\gamma_{SR_k}\gamma_{R_kE}}\right) \tag{7}$$

2.3 DECODE-AND-FORWARD SCHEME (DF)

During the relaying phase of transmission, the relays decode the signal received from the source. Then, the selected relay re-encodes the decoded signal $\hat{x}_s$ and forwards to destination with power P_R=(1-a)P. The selected relay has good channel properties compared to others; therefore decoding errors can be neglected, hence $\hat{x}_s \approx x_s$ .The secrecy rate at the destination is [11]:

$$R_{D_{DF}} = \left[0.5\min\left\{\log_2\left(1+\gamma_{SR_k}\right), \log_2\left(1+\gamma_{SD}+\gamma_{R_kD}\right)\right\}\right] \tag{8}$$

Since eavesdropper intercepts the signal from the source and relay; and to improve SNR, MRC is done at the eavesdropper. The secrecy rate at the eavesdropper is therefore expressed as [12]

$$R_{D_{DF}} = 0.5\log_2\left(1+\gamma_{SE}+\gamma_{R_kE}\right) \tag{9}$$

For simplicity, the noise variances at all receiving nodes are presumed to be equal.

3. RELAY SELECTION

3.1 PROPOSED RELAY SELECTION ALGORITHM

The path probability selection criterion of Ant Colony Optimization algorithm (ACO) is used for relay selection. The probabilities of signal transmission during the transmission phases can be expressed as [13].

$$p_{S,R_k} = \frac{G_{SR_k}^{\alpha} h_{SR_k}^{\beta}}{\sum_{k=1}^{N} G_{SR_k}^{\alpha} h_{SR_k}^{\beta}} \tag{10}$$

$$p_{R_k,D} = \frac{G_{R_kD}^{\alpha} h_{R_kD}^{\beta}}{\sum_{k=1}^{N} G_{R_kD}^{\alpha} h_{R_kD}^{\beta}} \quad (11)$$

where α and β are positive numbers, which control G and h respectively and they are called as relevance parameters. If $\alpha = 0$, only h is considered and if $\beta = 0$, only G is considered for path selection. If $\alpha = \beta$ and $\alpha, \beta > 0$, both G and h are considered with same priority, whereas, if $\alpha \neq \beta$ and $\alpha > \beta$, G is given preference and if $\alpha \neq \beta$ and $\beta > \alpha$, h is given preference for path selection.

The relay that gives the best SNR at the destination is selected as the best relay. Accordingly, the best relay depends on the first and second hop SNRs for the traditional scheme [7, 14] and on the corresponding probabilities for the proposed scheme.

3.2 RELAY SELECTION FOR AF SCHEME

In the proposed AF scheme, the harmonic mean of the best probability pair $p_{S,Rk}$ and $p_{Rk,D}$ from the N pairs gives the best relay and is obtained as

$$\text{Best Relay}_{AF}^{P} = \arg\max_{k \in R} \left(\frac{p_{S,R_k} p_{R_k,D}}{p_{S,R_k} + p_{R_k,D}} \right) \quad (12)$$

For the traditional AF scheme, the harmonic mean of the corresponding instantaneous SNRs gives the best relay and it is expressed as [14]

$$\text{Best Relay}_{AF}^{T} = \arg\max_{k \in R} \left(\frac{\gamma_{SR_k} \gamma_{R_kD}}{\gamma_{SR_k} + \gamma_{R_kD}} \right) \quad (13)$$

3.3 RELAY SELECTION FOR DF SCHEME

Being simple and less complex, the max-min criterion is considered as an efficient BRS metric and is used for finding the relay in DF scheme. The best relay for the proposed and traditional schemes are expressed as

$$\text{Best Relay}_{DF}^{P} = \arg\max_{k \in R} \min \left(p_{S,R_k}, p_{R_k,D} \right) \quad (14)$$

$$\text{Best Relay}_{DF}^{T} = \arg\max_{k \in R} \min \left(\gamma_{SR_k}, \gamma_{R_kD} \right) \quad (15)$$

Normally, if there is a relay at the center of the network model, then, that relay is selected as the best relay, since it exhibits same source to relay SNR and relay to destination SNR.

4. PERFORMANCE ANALYISIS

4.1 SECRECY RATE

The secrecy rate R_S is defined as the maximum rate of transmission at which an eavesdropper cannot decode any of the information from the transmitting node. The instantaneous secrecy rate is evaluated by

$$R_S = \left(R_D - R_E \right)^{+} \quad (16)$$

where $(R)^{+} = \max\{0, R\}$

The secrecy rate of AF transmission scheme is therefore

$$R_{S_{AF}} = \left[\begin{array}{l} 0.5\log_2 \left(1 + \gamma_{SD} + \dfrac{\gamma_{SR_k} \gamma_{R_kD}}{1 + \gamma_{SR_k} \gamma_{R_kD}} \right) \\ +0.5\log_2 \left(1 + \gamma_{SE} + \dfrac{\gamma_{SR_k} \gamma_{R_kE}}{1 + \gamma_{SR_k} \gamma_{R_kE}} \right) \end{array} \right]^{+} \quad (17)$$

The secrecy rate for DF scheme is expressed as

$$R_{S_{AF}} = \left[\begin{array}{l} 0.5\min \left\{ \log_2 \left(1 + \gamma_{SR_k} \right), \log_2 \left(1 + \gamma_{SD} + \gamma_{R_kD} \right) \right\} \\ -0.5\log_2 \left(1 + \gamma_{SE} + \gamma_{R_kE} \right) \end{array} \right] \quad (18)$$

If a positive secrecy is assured by proper power allocation, then the instantaneous secrecy rate in Eq. (16) is expressed as [15].

$$R_s = R_D - R_E \quad (19)$$

3.4 OPTIMAL POWER ALLOCATION

For achieving maximum secrecy, the power allocation factor a in the secrecy rate equations given in Eq.(17) and Eq.(18) need to be optimized. Since these functions are continuous nonlinear functions, non-derivative optimization methods are preferred. So, for one dimensional optimization, Brent's method and exhaustive search algorithms have been used. The maximum achievable secrecy rate is given by

$$\text{Max achievable rate} = \arg\max_{a} \left(R_S \right) \quad (20)$$

3.4.1 Brent's Method (BM):

Since the secrecy rate functions are nonlinear, a non-gradient optimization method is used. Brent's method is a linear search method designed for use with continuous functions. It is a combination of the golden section search and a parabolic interpolation. The method does not require computation of the derivatives. The golden section search has a first order rate of convergence, which starts when the algorithm is initialized while the parabolic interpolation has an asymptotic rate that is better than super linear. BM combines the best features of these two approaches. If the function to be optimized has at least a continuous second derivative, Brent's method finds the optimum value quicker i.e., its convergence is super linear. This algorithm requires more performance evaluations than derivative method [16].

3.4.2 Exhaustive Search Method (ES):

The algorithm that tries every possible solution of an objective function is known as exhaustive search. After finding the function values for all the possible combinations of dependent variables, the maximum function value is identified and the parameters that provide the maximum function value are considered as optimal values. Though it is the simplest of all search methods, this method is a time consuming one and hence it is computationally inefficient [17].

4. RESULTS AND ANALYSIS

In this section, numerical results are presented to verify the secrecy performance of AF and DF transmission schemes by Monte Carlo simulations. A two-dimensional linear topology as

shown in Fig.2, in which S and D are located at (0,0) and (10,0) respectively, with intermediate nodes randomly placed between them is considered. The eavesdropper is moved from (0, 10) to (10,10). OPA using Brent's method and exhaustive search methods and EPA (a = 0.5) are used for the analysis. The other simulation parameters used for the analysis are P = 30dBm, path loss exponent L = 3, and number of intermediate relays N = 20.

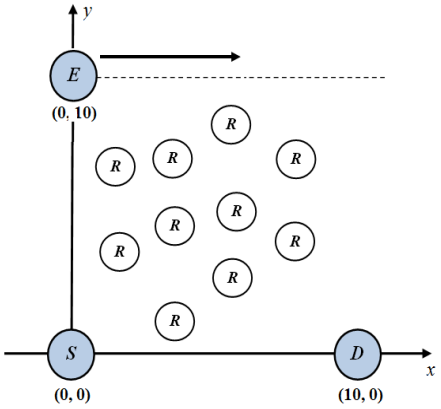


Fig.2. Network topology

The Fig.3 presents the secrecy performance of AF and DF transmission protocols with traditional and proposed RS schemes for $\alpha = \beta = 2$. For both schemes, Eq.(17) and Eq.(18), taking the concept of (19) are used for computing the secrecy rate of AF and DF respectively. For proposed scheme, Eq.(12) and Eq.(14) are used for finding the relay for AF and DF protocols, whereas, for traditional schemes, Eq.(13) and Eq.(15) are used respectively. For $\alpha = \beta$, i.e., for equal values of relevance parameters, the curves for the proposed and traditional RS methods coincides as the selected relay is logically identical in both [8] [9]. From the Fig.3, it is also obvious that secrecy increases when the source to eavesdropper distance increases. It is the reduction in the received signal power at the eavesdropper that improves the secrecy. For DF transmission scheme, the channel for the selected relay has good channel properties and the selected relay produces less decoding errors when compared to other relays. Therefore DF protocol shows better secrecy performance compared to AF.

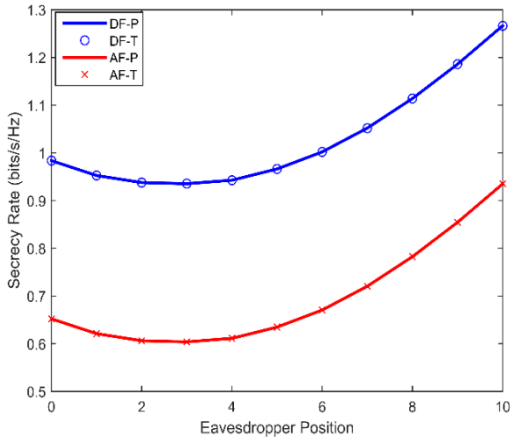


Fig.3. Secrecy performance of AF and DF protocols

The proposed RS algorithm finds the performance of three wireless models and is illustrated in Fig.4. For this, three values of α and β are considered. With $\alpha = \beta = 2$, the scenario maps to a traditional wireless scheme; with $\alpha = 2$ and $\beta = 0$, it resembles a path loss scheme and with $\alpha = 0$ and $\beta = 2$, it maps to a fading scheme. If we consider the same channel coefficients for all the wireless models, the secrecy performance is highest for equal values of α and β, and the system shows the same secrecy performance as traditional BRS scheme. For the other two cases where α or $\beta = 0$, only non-zero values are considered and therefore secrecy reduces. As explained, DF shows better performance in three cases.

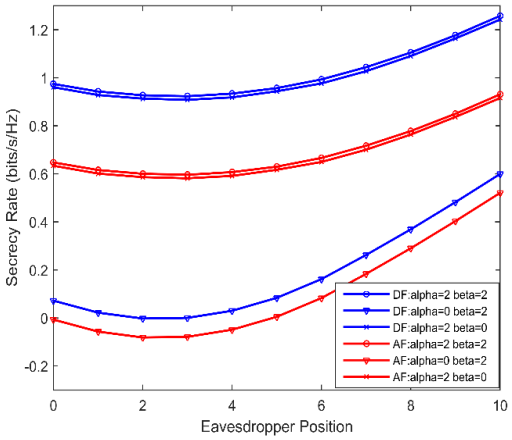


Fig.4. Secrecy performance of AF and DF protocols for different α and β values.

The Table.1 presents the comparison of the power allocation based on Brent's method with one dimensional exhaustive search algorithm and EPA scheme; for symmetric and asymmetric relay positions. Eavesdropper near to source and an SNR of 10dB is assumed. R_1 is the symmetric case where relay is positioned at the center of the network model whereas, R_2 and R_3 represent asymmetric relay positions, where relay near to source and near to destination are considered respectively. It is understood from the table that OPA outperforms EPA at all relay positions and the variation between OPA and EPA is predominant in asymmetric cases. The non-derivative Brent's method shows better secrecy performance in symmetric case for both AF/DF schemes. The DF BM for symmetric case shows the highest secrecy with large source power (a) and for the asymmetric cases, exhaustive search method is better. ES method evaluates the objective function at a predetermined number of equally spaced points δ. Accuracy of the results can be improved with smaller step size δ. The results for δ =0.05 obtained by Matlab simulation are illustrated in Fig.5.

Table 1. Comparison of OPA and EPA results for symmetric and asymmetric relay positions

Relay position	**Optimization method**	**AF**		**DF**	
		a	***Rs***	***a***	***Rs***
R1-Symmetric $\gamma_{sr} = \gamma_{rd}$	BM	0.5054	0.65732	0.5379	0.99089
	ES, δ=0.05	0.5	0.6512	0.55	0.9808
	EPA	0.5	0.6487	0.5	0.9713
R2-Asymmetric $\gamma_{sr} >> \gamma_{rd}$	BM	0.2481	0.40836	0.0840	0.56511
	ES, δ=0.05	0.25	0.4158	0.1	0.7513
	EPA	0.5	0.353	0.5	0.3985
	BM	0.8614	0.6074	0.9899	0.4271

R3-Asymmetric $\gamma_{sr} << \gamma_{rd}$	ES, δ=0.05	0.85	0.6112	0.95	0.6066
	EPA	0.5	0.4615	0.5	0.1932

The Fig.5 illustrates the exhaustive search method, where the secrecy is plotted against power allocation factor for symmetric and asymmetric relay positions. R_1 is the symmetric case; R_2 and R_3 represent asymmetric relay positions. Power requirement in cooperative networks is dependent on the relay and eavesdropper positions. The maximum secrecy is reached when a = 0.5 for R_1; i.e., when $P_s = P_r$ = 0.5W. For relay near to source as in R_2, system requires less source power or less a; and for relay near to destination (R_3) more source power or more a is required and it is obvious from the Fig.5. DF shows better performance only for symmetric case and is not preferred for the asymmetric cases. For analysis, eavesdropper closer to source is considered as it is the worst case of insecurity; since it gets more chance to intercept the signal.

The Fig.6 shows the effect of number of relay nodes on secrecy for AF and DF protocols. It is clear that the secrecy increases with relay nodes for both AF/DF schemes. This is because the probability of choosing a better helper increases when more number of intermediate nodes is deployed. This in turn shows the benefits of using multiple relays against eavesdropping.

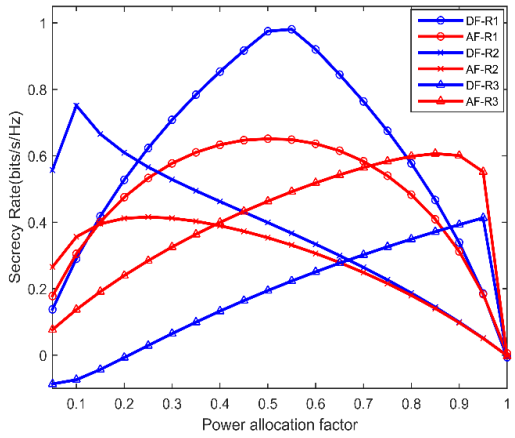


Fig.5. Power allocation factor versus secrecy for symmetric/asymmetric relay positions

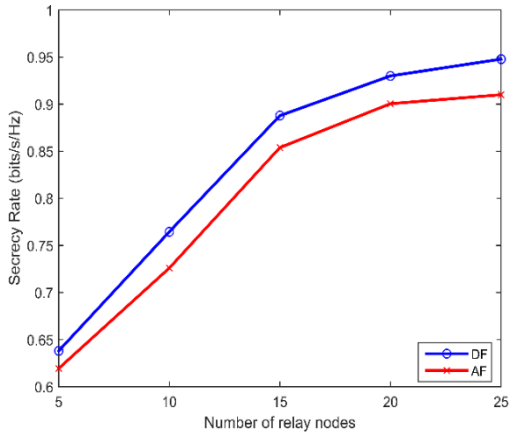


Fig.6. Number of relay nodes versus secrecy for proposed AF/DF transmission schemes

5. CONCLUSION

A performance comparison of ACO based relay selection scheme among AF and DF cooperative relay networks is formulated in this paper. The secrecy is evaluated in three wireless models namely traditional, fading and path loss models. OPA strategy based on non-derivative Brent's method and exhaustive search methods are derived and their performance is compared with EPA. The simulation results show the advantages of the proposed RS scheme. It is found that, for the assumptions made, DF cooperative relay network shows better secrecy performance compared to AF in different wireless scenarios and also OPA shows better performance than EPA. It is also observed that the secrecy increases with the number of intermediate nodes for both AF and DF schemes.

REFERENCES

[1] L. Lai and H. El Gamal, "The Relay-Eavesdropper Channel Cooperation for Secrecy", *IEEE Transactions on Information Theory*, Vol. 54, No. 9, pp. 4005-4019, 2008.

[2] J.N. Laneman, D.N.C. Tse and G.W. Wornell, "Cooperative Diversity in Wireless Networks: Efficient Protocols and Outage Behavior", *IEEE Transactions on Information Theory*, Vol. 50, No. 12, pp. 3062-3080, 2004.

[3] A D. Wyner, "The Wire-Tap Channel", *Bell Labs Technical Journal*, Vol. 54, No 8, pp. 1355-1387, 1975.

[4] Lu Lv, Jian Chen, Long Yang and Yonghong Kuo, "Improving Physical Layer Security in Untrusted Relay Networks: Cooperative Jamming and Power Allocation", *IET Communications*, Vol. 11, No. 3, pp. 393-399, 2017.

[5] Y. Zhao, R. Adve and T. J. Lim, "Improving Amplify-and-Forward Relay Networks: Optimal Power Allocation Versus Selection", *IEEE Transactions on Wireless Communications*, Vol. 6, No. 8, pp. 3114-3123, 2007.

[6] Chaudhuri Manoj Kumar Swain and Susmita Das, "Effects of Threshold Based Relay Selection Algorithms on the Performance of an IEEE 802.16j Mobile Multi-Hop Relay (MMR) WiMAX Network", *Digital Communications and Networks*, Vol. 4, pp. 58-68, 2018.

[7] 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, No. 10, pp. 2099-2111, 2013.

[8] P.M. Shemi, M.G. Jibukumar and M.K. Sabu, "A Novel Relay Selection Algorithm using Ant Colony Optimization with Artificial Noise for Secrecy Enhancement in Cooperative Networks", *International Journal of Communication Systems*, Vol. 31, No. 14, pp. 1-18, 2018.

[9] P.M. Shemi, M.G. Jibukumar and M.A. Ali, "Ant Colony Optimization based Relay Selection for Secrecy Enhancement in Decode-and-Forward Relay Networks", *Proceedings of IEEE International Conference on Wireless Communications and Mobile Computing*, pp. 2345-2354, 2018.

[10] Mischa Dohler and Yonghui Li, "*Cooperative Communications: Hardware*", John Wiley and Sons, 2010.

[11] K.J. Ray Liu, "*Cooperative Communications and Networking*", Cambridge University Press, 2009.

[12] Wei Wang, Kah Chan Teh and Kwok Hung Li, "Generalized Relay Selection for Improved Security in Cooperative DF Relay Networks", *IEEE Wireless Communications Letters*, Vol. 5, No. 1, pp. 1-16, 2016.

[13] Marco Dorigo and Thomas Stutzle, "*Ant Colony Optimization*", Prentice Hall, 2006.

[14] A Bletsas, A. Khisti, D. Reed and A. Lippman, "A Simple Cooperative Diversity Method based on Network Path Selection", *IEEE Journal on Selected Areas in Communications*, Vol. 24, No. 3, pp. 659-672, 2006.

[15] A. Mohammadi and A. Kuhestani, "Destination-Based Cooperative Jamming in Untrusted Amplify-and-Forward Relay Networks: Resource Allocation and Performance Study", *IET Communications*, Vol. 10, No. 1, pp. 17-23, 2016.

[16] R. Brent, "*Algorithms for Minimization without Derivatives*", Prentice Hall, 1973.

[17] J Nievergelt, "Exhaustive Search, Combinatorial Optimization and Enumeration: Exploring the Potential of Raw Computing Power", *Proceedings of International Conference on Current Trends in Theory and Practice of Informatics*, pp. 18-35, 2000.