Maximized Secrecy Rate Based Power Allocation for Wireless Cooperative Network with Control Jamming

Kiran Kumar Gurrala
Ph.d Scholar, Department of Electrical Engineering
NIT Rourkela, India
e-mail:gkk.chityala@gmail.com

Susmita Das
Department of Electrical Engineering
NIT Rourkela, India
email:sdas@nitrkl.ac.in

Abstract— In this paper, we propose efficient power allocation techniques using both convex optimization (using Lagrange multiplier method) and a soft evolutionary approach (using Differential Evolution (DE) algorithm) to optimize both the relay and jammer powers in addition to an increase in the system performance in terms of secrecy rate. Here, we consider a cooperative wireless network with control jamming comprising of a source-destination pair with a set of relay nodes in the presence of single and multiple eavesdroppers. Optimal relay node is selected based on the SNR received at each relay, which transmits the data to the destination using decode and forward strategy. Amongst the remaining nodes, selection of jammer is done based on the SNR value of the relay to eavesdropper link. The proposed power allocation schemes are compared with equal power allocation policy for using the Monte-Carlo simulation study and these schemes are found to be superior in terms of average secrecy rate.

Keywords—Physical layer security, cooperative jamming, power allocation, DE algorithm

I. INTRODUCTION

The secure communication between the source and the destination in the presence of unauthorized receivers which are called eavesdroppers is of great importance. The information theoretic secrecy is introduced by Shannon in [1]. Wireless secure communication issue is addressed at the upper layers of the protocol stack using cryptography algorithms are discussed in [2]. Recently, implementing information security at the physical layer is the emerging research area. The performance metric for physical layers security is secrecy rate which is defined as the difference of direct link (between source and destination) capacity and the eaves droppers link capacity. The secrecy rate represents the rate at which the source securely transmits the data to the destination in the presence of eaves droppers [3].

The main purpose is to enhance the capacity of main confidential link while the capacity of eavesdropper link decreased. The relays help the source by noise forwarding to confuse the eavesdropper in order to improve the system performance in terms of secrecy rate [4-6]. The authors in [7] proposed relay selection schemes in cooperative networks such that they can act as relay, cooperative jammer and a new jamming and non jamming switched based hybrid scheme.

Power allocation for physical security to maximize the secrecy rate in wireless cooperative network is a promising research area. The recent work related to issue of power allocation schemes for cooperative jamming are introduced in [7-13]. From the considered literature it is observed that the power allocation for control jamming in secure wireless cooperative network is not introduced earlier which was mentioned in this work. This present research work focuses on the power allocation schemes of control jamming for a wireless cooperative network in the presence of single eavesdropper to maximize the secrecy rate. Initially, relay power allocation issue to maximize the secrecy rate of control jamming based on total relay power constraint is solved by using convex optimization and evolutionary approaches. The performance of the proposed power allocation schemes are compared with the conventional equal power allocation. Finally the efficacy of the proposed power allocation schemes is given.

The organization of paper is as follows. The system model and conventional relay and jammer selection schemes are given in Section II. The problem formulation and proposed power allocation schemes are introduced in Section III. The simulation results are shown and discussed in Section IV. Finally Section V provides the conclusion.

II. SYSTEM MODEL

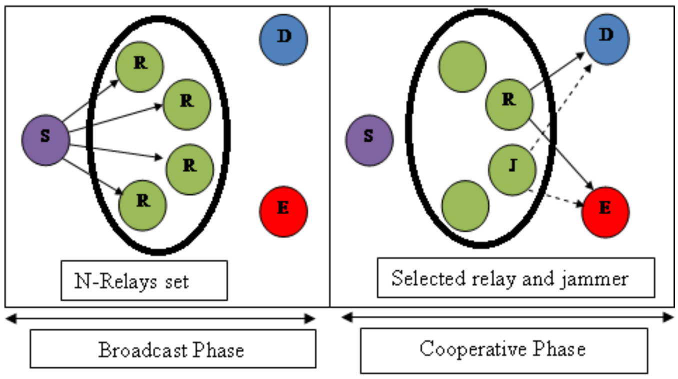

Fig. 1. System model

A cooperative wireless network model consists of single source destination pair, in which source (S) sends its data to the destination node (D) with the help of half duplex mode multiple Decode and Forward (DF) relays nodes R1, R2, . . . , RN) is considered in the presence of single eavesdropper nodes (E) case [7]. The channel conditions subject to flat Rayleigh fading which are mutually independent and orthogonal. It is also considered that given network is employed with TDMA protocol where source transmits its information during the first time slot and relays transmit information during the second time slot. The communication process is performed in two phases named broadcasting phase and cooperative phase as shown in Fig. 1.

Broadcast phase: The source transmits data to the destination via N number of relays. Here there no direct links available between source to destination and source to eavesdroppers. On the other hand, the broadcast phase is secured means eavesdropper cannot has impact on source to relay transmission.

$$y_{sr_i} = \sqrt{P_s}\, h_{sr_i} x + n_{sr_i} \quad for\ i = 1,2,..., N \tag{1}$$

where x and y_{sr_i} are the transmitted information signal from source, signals received at i^{th} relay node respectively. P_S is the transmitted source power, $h_{sr_i} \sim CN(0, \sigma^2_{sr_i})$ are the channel coefficients of source to relay links. The noise terms n_{sr_i} which are zero mean complex Gaussian random variables with variance N_o.

Cooperative phase: Among the relay set, based on the considered secure relay and jammer selection schemes, two relays are selected in which one relay which can decode the received signal correctly will operate in DF relay mode and another relay act as jammer. The jammer node generates interference for the relay transmission by noise forwarding. In control jamming, interference caused by jammer is known at the destination but not at the eavesdropper. So the destination can decode the interference provided by the jammer. Hence, the received signals at the destination and eaves dropper for the selected relay and jammer are given by

$$y_{rd} = \sqrt{P_r}\, h_{rd}\, \hat{y}_{sr} + n_{rd} \tag{2}$$

$$y_e = y_{re} + y_{je} \tag{3}$$

where $y_{re} = \sqrt{P_r}\, h_{re} y_{sr} + n_{re}$; $y_{je} = \sqrt{P_j}\, h_{je} y_{sr} + n_{je}$.

Here P_r is the power of selected relay node and P_j is the jammer power. $\hat{y}_{sr}$ is the estimation of the transmitted signal by the selected relay. $h_{rd} \sim CN(0, \sigma^2_{rd})$ is the channel coefficient for the selected relay to destination link. The noise term n_{rd} is zero mean complex Gaussian random variables with variance N_o. The channel variance is given as $\sigma^2_{xy} \propto d^{-l}_{xy}$ where d_{xy} is the Euclidean distance between nodes $x \in \{s, r, j\}$ and $y \in \{e, r, d\}$. In this paper, the value of the path loss exponent is assumed as $l = 4$. The relation between source, relay and jammer powers is considered as follows $P_s = P_r = L \times P_j$, where $L = 100$.

Conventional selection techniques without and with jamming: The effect of control jamming can be well understood by considering three different relay and jammer selection schemes which are given as in [8].

Conventional Selection (Without Jamming)

This selection does not involve any jamming process hence in cooperative phase only conventional relay accesses the channel and sends information to the destination. it selects the best relay based on the maximum instantaneous relay-destination link and source-destination link and is expressed as

$$R^* = \max_{R \in C_d} \left(1 + SNR_{rd}\right) \tag{4}$$

Secrecy rate for conventional selection is expressed as

$$C_S^{|C_d|}(R) = \max\left(0, 0.5 * \log_2\left(\frac{1 + SNR_{rd}}{1 + SNR_{re}}\right)\right) \tag{5}$$

Optimal Selection with Jamming (OSJ): While selecting the cooperative relay and jammer, it assumes that relay-eavesdropper links are available and the destination is unaware of the jamming nodes. The selection of relay and jammer is done based on the following equations

$$R^* = \arg\max_{R \in C_d} \left(\frac{SNR_{rd}}{SNR_{re}}\right)$$

$$J^* = \arg\max_{J \in S_{relay}} \left(\frac{SNR_{je}}{SNR_{jd}}\right) \tag{6}$$

Secrecy rate for OSJ is expressed as

$$C_S^{|C_d|}(R, J) = \max\left(0, 0.5 * \log_2\left(\frac{1 + \frac{SNR_{rd}}{1 + SNR_{jd}}}{1 + \frac{SNR_{re}}{1 + SNR_{je}}}\right)\right) \tag{7}$$

Optimal Selection with Control Jamming (OSCJ):

This selection scheme is proposed on the basis of assumption that the destination knows about the jamming nodes and the eavesdropper is unaware of it. Hence only destination can decode the jamming signal but not eavesdropper. Cooperative relay and jammer is selected based on the following equations

$$R^* = \arg\max_{R \in C_d} \left(\frac{SNR_{rd}}{SNR_{re}}\right)$$

$$J^* = \arg\max_{J \in S_{relay}} \left(SNR_{je}\right) \tag{8}$$

Secrecy rate for OSCJ can be expressed as

$$C_S^{|C_d|}(R, J) = \max\left(0, 0.5 * \log_2\left(\frac{1 + SNR_{rd}}{1 + \frac{SNR_{re}}{1 + SNR_{je}}}\right)\right) \tag{9}$$

The instantaneous signal to noise ratio for the channel link $i \rightarrow j$ is given by $SNR_{ij} = P_i\, \sigma^2_{i,j}$.

III. Problem Formualtion and Proposed Power Allocation Schemes

A. Problem formulation for convex optimization

The optimization problem is defined as

$$Max\left(log_2\left(1+SNR_{rd}\right)-\log_2\left(1+\frac{SNR_{re}}{1+SNR_{je}}\right)\right)$$

such that $P_s+P_r+P_j\le P_T\,;P_s>0;\Pr>0;Pj>0;$ (10)

Theorem.1: (Maximized secrecy rate based optimal relay power allocation in presence of single eavesdropper) : With the perfect CSI , SNR_{re}, SNR_{rd} and SNR_{je} , the optimal relay power to maximize the secrecy rate of control jamming using Lagrange multiplier method is given by

$$P_r=\max\left(0,\left(\left(-x_2+\sqrt{x_2^2-4x_1(1+\frac{x_3}{\lambda}}\right)/2x_1\right)\right) \qquad (11)$$

$x_1=\frac{xy}{z}\,;x_2=x+\frac{y}{z}\,;x_3=\frac{y}{z}-x$.

where $x=\sigma_{rd}^2\,;y=\sigma_{re}^2\,;z=1+P_j\sigma_{je}^2$.

Theorem 1 is proved in Appendix. The value of λ is obtained using sub gradient method as follows.

Sub gradient algorithm to find λ

1. Initialize $k=1$, $\lambda(1)=0.1$, $f(1)=-P_t$
2. While (abs(f)>0.0001)
3. Calculate

$$P_r=\max\left(0,\left(\left(-x_2+\sqrt{x_2^2-4x_1(1-\frac{x_3}{\lambda}}\right)/2x_1\right)\right)$$

where $x_1=\sigma_{rd}^2\,;x_2=\sigma_{re}^2\,;x_3=1+P_j\sigma_{je}^2$

4. $f(k)=P_r(2+(1/L))-P_t$
5. $\lambda(k+1)=\lambda(k)-(1/k)\,f(k)$
6. $k=k+1$
7. end

B. Problem formualtion for DE based Optimization

Differential Evolution algorithm is an efficient stochastic search optimization technique like genetic algorithm using the similar operators: crossover, mutation, and selection. It finds the true global minimum irrespective of initial parameters which converges fast with only few control parameters [15]. In optimum power allocation using Lagrange multiplier method, the relay power depends on the Lagrange multiplier value λ in which the value of Lagrange multiplier is obtained using iterative methods. To avoid this computational burden, we use evolutionary approach like differential evolution.

Problem definition

In the presence of single eavesdropper

Maximize

$$C_{\sec_1}\left|C_d\right|=\left(log_2\left(1+SNR_{rd}\right)-\log_2\left(1+\frac{SNR_{re}}{1+SNR_{je}}\right)\right)$$

subject to $P_s+P_r+P_j\le P_T$

Cost function: $f_{\sec_1}=\arg\min\left(-C_{\sec_1}\left|C_d\right|\right)$

where $SNR_{rd}=P_r\sigma_{rd}^2$, $SNR_{re}=P_r\sigma_{re}^2$,

$SNR_{je}=P_j\sigma_{je}^2\,;P_r=\alpha P_T\,;P_j=P_r/100\,;$

Subject to $0\le\alpha\le\frac{1}{(2+1/L)}$

The detailed algorithm for the proposed power allocation schemes using Differential evolution algorithm is shown in the following flowchart. The parameters in the flowchart shown in Fig. 4 are defined as follows Gd represents the total number of generations; g represents the individual generation; NP and D represent the number of population members and the number of parameters of objective function respectively.

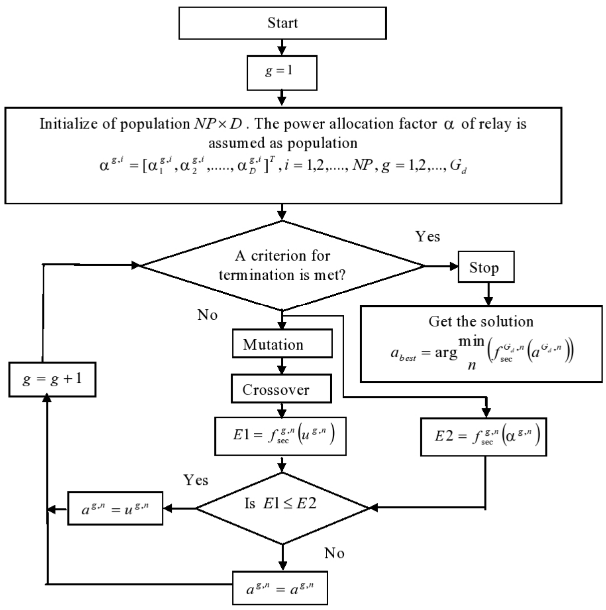

Fig.2. Differential Evolution (DE) algorithm for proposed power allocation

Initialization: The n^{th} individual of the population in the g^{th} generation is expressed as

$$\alpha^{g,i}\; for\; i=1,2,....,NP,\, g=1,2,...,G_d$$

Cost function evolution:

$E1 = f_{\text{sec}}^{g,n}\left(u^{g,n}\right)$ is the cost function of the n^{th} individual in the g^{th} generation of $u^{g,n}$ which is represented as

$$E1 = f_{\text{sec}}^{g,n}\left(u^{g,n}\right) = f_{\text{sec}_1}\left(u^{g,n}\right) = -C_{\text{sec}_1}{}^{|C_d|}\left(u^{g,n}\right)$$

$E2 = f_{\text{sec}}^{g,n}\left(a^{g,n}\right)$ is the cost function of the n^{th} individual in g^{th} of $\alpha^{g,n}$ which is represented as

$$E2 = f_{\text{sec}}^{g,n}\left(a^{g,n}\right) = f_{\text{sec}_1}\left(a^{g,n}\right) = -C_{\text{sec}_1}{}^{|C_d|}\left(a^{g,n}\right)$$

where $a^{g,n}$ and $u^{g,n}$ are the target and the trail vectors which are obtained after mutation and cross over operations respectively.

Optimal search: The best individual which has the minimum cost function value is considered as the optimal power allocation factor α. The optimal solution for power allocation factor is obtained as

$$\alpha_{best} = \arg\min_{n}\left(f_{\text{sec}}^{G_d,n}\left(a^{G_d,n}\right)\right),\ n = 1,2,\ldots, NP$$

Here $f_{\text{sec}}^{G_d,n}\left(a^{G_d,n}\right)$ is the optimal solution after meeting the termination criteria.

IV. Simulation Results and Analysis

The proposed power allocation schemes are validated through computer simulations using Matlab. The simulation model for the system as shown in Fig.1 is assumed as 2-D square topology in which the source, destination and the eavesdropper are located as $S(0,0)$, $D(1,0)$ and $E(0,1)$ respectively and also the area of this network is supposed as a 1×1 square unit. Here it is also assumed that the direct paths i.e., source-to-eaves dropper and source-to-destination links are not available so the effect of eavesdropping rise in cooperative phase only.

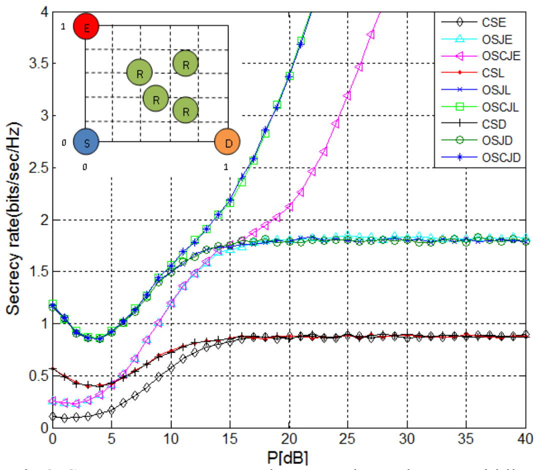

Fig.3. Secrecy rate versus total power when relays at middle

For the simulation results, the number of relays in the considered secure cooperative network are four $(N = 4)$ for which location are mentioned for each case. In addition, it also contemplated that both source and relay should transmit with the same power $(P_s = P_r)$. The jammer node power is a fraction L of relay power $(L = 100)$. The transmission spectral efficiency is considered as 2 bits per channel use (BPCU) [8].

From the Fig.3, the secrecy rate of proposed power allocation schemes outperforms with control jamming than the non jamming relay selection schemes. The both Lagrange multiplier method and DE based power allocation method achieve nearly same secrecy rate of 3.3 bits/sec/Hz while the equal power allocation scheme achieves a secrecy rate of 2.1bist/sec/Hz at total power 20dB for the control jamming case.

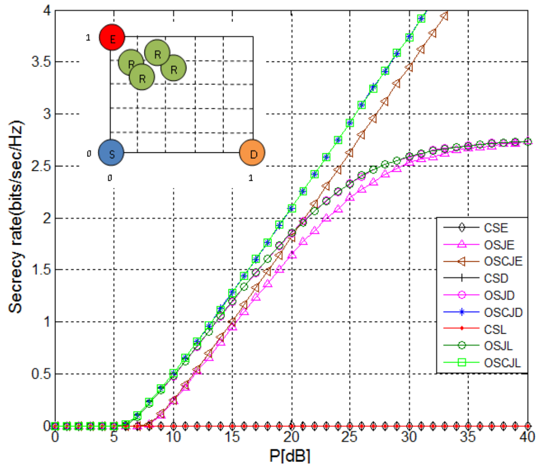

Fig.4. Secrecy rate versus total power when relays close to eavesdropper

From Fig.4, the performance of the non jamming schemes is very poor compared to the jamming schemes. The both proposed power allocation schemes achieves nearly same secrecy rate. Proposed power allocation schemes achieve a secrecy rate of 2.1bits/sec/Hz where as conventional equal power allocation achieves a secrecy rate of 1.8 bits/sec/Hz for OSCJ. On the other hand, proposed schemes achieve a secrecy rate of 1.8bit/sec/Hz for OSJ where as equal power allocation achieves a secrecy rate of 1.6bits/sec/Hz.

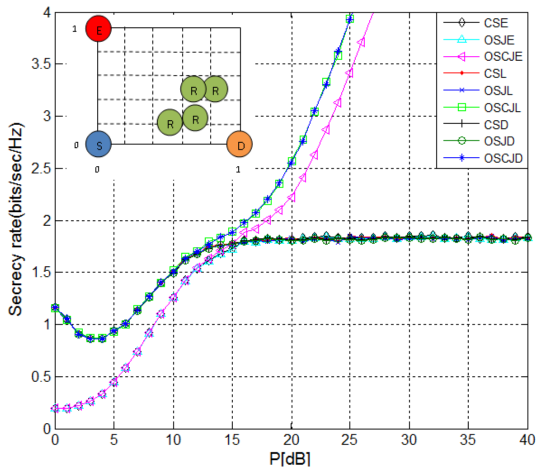

Fig.5. Secrecy rate versus total power when relays close to destination

From Fig.5, the proposed power allocation schemes achieve a secrecy rate of 2.6 bits/sec/Hz where as equal power allocation get secrecy rate of 2.2bits/sec/Hz for OSCJ. The proposed schemes achieve a secrecy rate of 1.5 bits/sec/Hz where as for equal power allocation achieves a secrecy rate of 1.3 bits/sec/Hz for low SNR values and for high SNR value both equal power allocation and proposed schemes achieves the same secrecy rate. Fig.7 depicts that the secrecy rate is high for non jamming schemes because the relay to destination link is very strong. With the optimized power the jamming schemes introduce interference at the destination which reduces the secrecy rate compare to OSCJ.

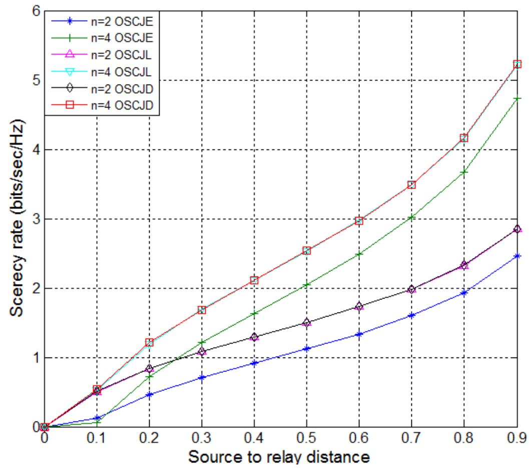

Fig.6 Secrecy rate versus source-to-relay distance

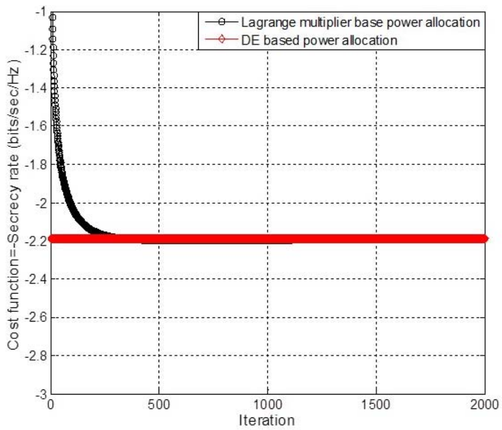

Fig.7 Convergence analysis of proposed power allocation schemes

From the Fig.6, it is observed that as the path loss exponent increases from 2-4, the performance is also increases in terms of secrecy rate. The optimized relay powers and corresponding jamming powers using the proposed power allocation schemes are compared with equal power allocation in terms of secrecy rate when the relay location at middle when is shown in Fig 7. From which it is concluded that as the proposed power allocation schemes achieve a secrecy rate of the relay and jammer powers are increases the secrecy rate also increases.

In results, OSCJE-optimal selection with control jamming with equal power allocation

OSCJL- optimal selection with control jamming with Lagrangian Multiplier method based power allocation.

OSCJD- optimal selection with control jamming with Differential Evolution (DE) algorithm based power allocation.

V. Conclusion

In this paper, efficient power allocation schemes are proposed by using convex optimization and evolutionary approach for physical layer security of single source destination pair secure wireless cooperative network with control jamming. We defined and solved the constrained optimization problems using Lagrange multiplier method and Differential evolution algorithm aiming to allocate the relay and jammers powers such that the secrecy rate is to be maximized subject to total power constraint. The performance of proposed power allocation schemes are validated using Monte Carlo simulations and compared with the conventional equal power allocation for both jamming and non jamming relay selection cases. Among all relay locations, the performance of the system is poor when the relays close to eavesdropper case. The non jamming schemes get poor secrecy rate when the eavesdropper is close to source and close to destination. From all the observations, it is confirmed that the proposed power allocation schemes outperforms than conventional equal power allocation in all jamming and non jamming cases.

References

[1]. C. E. Shannon.: ‘Communication theory of secrecy systems’, *Bell Syst. Tech. J.*, 1949, 28, pp: 656 -715.

[2]. M. Bloch , J. Barros , M. R. D. Rodrigues and S. W. McLaughlin: ‘Wireless information-theoretic security’, *IEEE Trans. Inf. Theory,* 2008, 54**,** (6), pp: 2515 -2534.

[3]. S. K. Leung-Yan-Cheong and M. E. Hellman.: ‘The Gaussian wiretap channel’, *IEEE Trans. Inf. Theory*, 1978, **24,** (4), pp: 451 -456.

[4]. L. Lai and H. El Gamal.: ‘The relay-eavesdropper channel: Cooperation for secrecy’, *IEEE Trans. Inf. Theory* 2008, **54,** (9), pp : 4005 -4019.

[5]. L. Dong , Z. Han , A. P. Petropulu and H. V. Poor.: ‘Secure wireless communications via cooperation’, *Proc. 46th Ann. Allerton Conf. Communication, Control, and Computing, UIUC*, 2008, pp:1132-1138.

[6]. L. Dong , Z. Han , A. P. Petropulu and H. V. Poor.: ‘Improving wireless physical layer security via cooperative relays’, *IEEE Trans. Signal Process.,* 2010, **58,** (3), pp: 1875 -1888.

[7]. I. Krikidis , J. Thompson and S. Mclaughlin., ‘Relay selection for secure cooperative networks with jamming’, *IEEE Trans. Wireless Commun.* 2009, **8,** (10), pp: 5003 -5011.

[8]. Ibrahim, DH, Hassan, ES, El-Dolil, SA: ‘A new relay and jammer selection schemes for secure one-way cooperative networks’, *Wireless Personal Communications*,2014,**75,** (1), pp: 665-685.

[9]. L. Dong , H. Yousefi&; zadeh and H. Jafarkhani: 'Cooperative jamming and power allocation for wireless relay networks in presence of eavesdropper', 2011 *IEEE International Conference on Communications (ICC 2011)*, Kyoto, Japan, June 2011, pp:1-5.
[10]. G. Zheng , L.-C. Choo and K. K. Wong: 'Optimal cooperative jamming to enhance physical layer security using relays', *IEEE Trans. Signal Process,* 2011, **59,** (3), pp:1317 - 1322.
[11]. L.wang, M.Elkashlan, J. Huang, N.H. Tran and T.Q. Duong: 'Secure transmission with optimal power allocation in untrusted relay networks', *IEEE Wireless Commun. Letters*, 2014, **3,** (3), pp: 289-292.
[12]. Wang, Li, et al.: 'Security-oriented cooperation scheme in wireless cooperative networks', *IET Commu.*, 2014, **8,** (8), pp: 1265-1273.
[13]. L Wang, C Cao, M Song: 'Joint Cooperative Relaying and Jamming for Maximum Secrecy Capacity in Wireless Networks', *IEEE International Conference on Communications (ICC)*, Sydney, NSW, June 2014, pp: 4448-4453.
[14]. S. Boyd and L. Vandenberghe,: 'Convex *Optimization'*, 2004: Cambridge Univ. Press.
[15]. R. Storn and K. V. Price: 'Differential evolution-A simple and efficient heuristic for global optimization over continuous Spaces', *J. Global Optim.,* 1997, **11**, pp:341 -359.

Appendix

Proof of Theorem.1:

Maximized secrecy rate based relay power allocation problem in the case of single eavesdropper is solved using Lagrange multiplier method as follows. The optimization problem is defined as

$$Max\left(log_2(1+SNR_{rd}) - \log_2\left(1+\frac{SNR_{re}}{1+SNR_{je}}\right)\right)$$

Such that $P_s + P_r + P_j \le P_T$;

$P_s > 0; \Pr > 0; Pj > 0;$

The Lagrangian function is defined as follows

$$J = \log_2\left(\frac{1+a}{1+b}\right) - \lambda\left(P_s + P_r + P_j - P_T\right)$$

By solving the defined Lagrangian function,

$$\partial J/\partial P_r = 0 \Rightarrow \left(\frac{1+b}{1+a}\right)\frac{\partial}{\partial P_r}\left(\frac{1+a}{1+b}\right) - \lambda = 0$$

$$\frac{1}{(1+a)}\frac{\partial a}{\partial P_r} - \frac{1}{(1+b)}\frac{\partial b}{\partial P_r} = \lambda$$

where $\frac{\partial a}{\partial P_r} = x$; $\frac{\partial b}{\partial P_r} = y/z$; $\frac{x}{(1+a)} - \frac{y/z}{(1+b)} = \lambda$

$$x(1+b) - (y/z)(1+a) = \lambda(1+a+b+ab)$$

The quadratic equation in terms of P_r

$$\left(\frac{xy\lambda}{z}\right)P_r^2 + \left(\left(x+\frac{y}{z}\right)\lambda\right)P_r + \left(\left(\frac{y}{z}-x\right)+\lambda\right) = 0$$

The roots of the binomial equation are given by

$$P_r = \max\left(0, \left(\left(-x_2 + \sqrt{x_2^2 - 4x_1(1+\frac{x_3}{\lambda}}\right)/2x_1\right)\right)$$