Global Journal of Pure and Applied Mathematics.
ISSN 0973-1768 Volume 11, Number 5 (2015), pp. 3337-3347

http://www.ripublication.com

Reliable Transmission with Flawless Power Proportion in Low defined signal Disseminate Systems

Dr.A.Rengarajan

Professor, CSE Veltech Multitech Engineering College
Chennai, Tamilnadu, India rengu_rajan@yahoo.com

S.Rajasekaran

Junior Research Fellow, CSE, Veltech Multitech Engineering College
Chennai, Tamilnadu, India rajasekaran009@gmail.com

S.John Justin Thangaraj

Ph.D. Scholar, CSE St.Peter's University
Chennai, Tamilnadu, India john_justin@rediffmail.com

Abstract

The forward untrusted relay network and two hop amplify is used to secure the transmission problem. Ergodic secrecy capacity (ESC) is used in the high signal - to - noise ratio regime. Antenna arrays are used in large scale either in the source or in the destination. If large antenna arrays are in the source ESC is solely between the destination channel and relay. If the large antenna arrays are in the destination ESC is between relay and the source.

Index Terms— Cooperative jamming, optimal power allocation, physical layer security, untrusted relay

I. INTRODUCTION

It is known-fact that the communication coverage can expanded by relay and also provides diversity gains **[1]** .Even in the absence of external eavesdroppers, secrecy may not be guaranteed in untrusted relay network. For example, an untrusted relay may belong to a public network without the same security clearance **[2]**. In wireless network the issues of information-theoretic security has attracted widespread interests **[3], [4]** and physical layer security initiated by Wyner **[5]** is an appealing alternative to resist various malicious abuses and security attacks from eavesdroppers **[6]**. In the

recent literature, the untrusted relay network has been paid considerable attention in Security. For example, cooperative jamming (CJ) was proposed to achieve positive secrecy rate in **[7], [8]** Secrecy outage performance for different relaying schemes was examined in **[9]**. The impact of relay antenna selection on secrecy outage probability was analyzed in **[10]**. Without Optimal Power Allocation (OPA) the lower bound of the Ergodic secrecy capacity (ESC) was derived in **[11]** where single-relay and multiple-relay cases were considered. From the above mentioned works, we can take into account CJ and OPA in two hop amplify-and-forward (AF) untrusted relay networks for securing the transmission. We derive the ESC as the metric for secrecy. In particular, we present compact expressions for the ESC in the high signal-to-noise ratio (SNR) regime. Motivated by the recent works on large scale antenna systems **[12], [13]**. However we gathered as many fundamental insights as the number of antennas grows large. Thus the large number of antennas varies the Ergodic Secrecy Capacity (ESC) as explained. For large number of antennas at the source, we reveal that the ESC is independent of the number of antennas. We also reveal that it is solely determined by the second hop. In this case, we concisely express the ESC in terms of the average channel gain of the second hop and the transmit SNR of the network. On the other hand, for large number of antennas at the destination, we reveal that the ESC is dependent on the number of antennas. However, for very large number of antennas at the destination, i.e., the number of antennas approaches infinity, the ECS is independent of the number of antennas. In this case, it is solely determined by the first hop and is concisely expressed in terms of the average channel gain of the first hop and the transmit SNR of the network.

II. MATHEMATICAL MODEL

In mathematical model we can consider an untrusted AF relay communicated with CJ in a half-duplex two-hop relay network consisting of source (Alice) and a destination (Bob).During the first phase, while Alice transmits the information signal whereas Bob transmits the jamming signal, and the direct link between Alice and Bob is assumed to be existent. . During the second phase, the relay forwards the signals to Bob. The purpose is to quantify the impact of OPA in securing the transmission for two practical networks, whereas two networks have mathematically explained below:

1) Alice is equipped with M_a antennas, whereas both the relay and Bob are equipped with a single antenna (M_a-1-1) and
2) Bob is equipped with M_b antennas, whereas both the relay and Alice are equipped with a single antenna ($1-1-M_b$).

By above two networks the maximum-ratio transmission (MRT) to get signal. For the M_a-1-1 network, Alice uses the maximum-ratio transmission (MRT) beam former to transmit the signal. For the $1-1-M_b$ network, Bob uses the MRT beam former to transmit the jamming signal and maximum-ratio combining (MRC) to maximize the received SNR. This transceiver design at Bob can be easily achieved, particularly in reciprocal channels **[10], [11]**. We note that the MRT beam former has low implementation complexity compared to other more complex beam forming designs

[14]. Let $R_{x,h} \sim CN_{1\times Nx}(0_{1\times Nx}, \Omega_{a,r} I_{Nx})$ denote the complex Gaussian channel vector from Alice to relay and $R_{h,y} \sim CN_{1\times Ny}(0_{1\times Ny}, \Omega_{r,y} I_{Ny})$ denote the channel vector from relay to Bob. We assume a reciprocal channel between the relay and Bob **[10], [11]**.

1) Note that Alice knows the channel knowledge of the two hops, in order to determine the length of codeword.
2) In fact, since the destination operates in half-duplex mode, it cannot receive the transmitted signal from the source while transmitting the jamming signal. The instantaneous received signal-to-interference-plus-noise ratio at the relay is given by

$$\alpha R = \frac{\gamma \alpha x,r}{(1-\gamma)\alpha r,y+\lambda} \quad (1)$$

And the instantaneous end-to-end SNR at Bob is given by

$$\alpha B = \frac{\gamma \alpha x,r\, \gamma r,y}{\gamma \alpha x,r+(2-\gamma)\alpha r,y+\lambda} \quad (2)$$

Where $\boldsymbol{\gamma}$ is the power allocation factor, $\boldsymbol{\gamma} \in (0,1)$. Alice transmits the signal with power $\boldsymbol{\gamma}P$ and Bob transmits the jamming signal with power (1- $\boldsymbol{\gamma}$) P, where P is the total power budget in this network for each transmission.

III. OPTIMAL POWER ALLOCATION

In this section, the performance of the proposed power allocation scheme will be investigated. The allocation scheme is optimum in the sense of minimizing the total average probability of error. The power allocation factors that minimize the total probability of error are discussed. Most of the power allocation factor scenarios investigated in this section. Thus the instantaneous secrecy rate is expressed as

$$Xs = \frac{1}{2}[\log2\,(1+\Upsilon B) - \log2\,(1+\Upsilon R)] \quad (3)$$

Where $[x]^+ = \max\{0, x\}$. In order to facilitate analysis and gather deep insights behind this system, we consider $\lambda = 0$, as mentioned in [15]. Note that the $\lambda = 0$ case asymptotically approaches the $\lambda = 1$ case at high SNRs. The $\lambda = 0$ case also takes into account the maximum probability of eavesdropping at the relay, since the received SINR at the relay given in **(1)** becomes the signal- ratio to-interference (SIR).As such, Let $\frac{\boldsymbol{\gamma a,r}}{\boldsymbol{\gamma r,b}} = \boldsymbol{\mu}$, We write equation **(1)** and **(2)** as

$$\alpha_r = \frac{\Upsilon \mu}{(1-\alpha)} \text{ and } \alpha_b = \frac{\gamma \mu \alpha r,y}{\gamma \mu + 2 - \gamma} \quad (4)$$

Our aim is to maximize the secrecy rate. As such, we focus on OPA. Based on **(3)**, the OPA factor is calculated as

$$\alpha^* = \arg_0 max\{w(\beta)\} \quad (5)$$

Where w (β) = $\frac{1+\gamma y}{1+\gamma r}$, Noting that $\vartheta^2\omega(\alpha)/\vartheta\alpha^2 < 0$, we take the Derivatives of $\omega(\alpha)$ w.r.t α and set it to Zero to obtain the OPA factor as

$$\alpha^* = \begin{cases} 0.5 - \frac{1}{\gamma r,y}, \mu = 1 \\ \frac{2-2\mu-2\gamma r,y+\sqrt{2\gamma r,y\sqrt{\Delta}}}{(\mu-1)^2+(\mu-2)\gamma r,b+\mu^2\gamma r,y}, \mu \neq 1 \end{cases} \quad (6)$$

Where $\Delta = 1 - \mu^2 + \mu\gamma_{r,b} + \mu^2\gamma_{r,b}$. For large ${\gamma_{r,b}}^4$, based on (6), when $\mu = 1$, $\alpha^* \approx 1/2$, and when $\mu \_= 1$, α^* can be approximated as

$$\alpha^* = \frac{\frac{2-2\mu}{\gamma r,y}-2+\sqrt{2\sqrt{\frac{1-\mu^2}{\gamma r,y}+\mu+\mu^2}}}{\frac{(\mu-1)^2}{\gamma r,y}+(\mu-2)+\mu^2}$$

$$\approx \frac{-2+\sqrt{2\sqrt{\mu+\mu^2}}}{(\mu-2)+\mu^2} = \frac{-1+\sqrt{(\mu+\mu^2)/2}}{\frac{\mu+\mu^2}{2}-1}$$

$$= \frac{1}{\sqrt{\frac{\mu+\mu^2}{2}+1}} \quad (7)$$

Since $\mu = 1$ case also satisfies, $\boldsymbol{\alpha^*=\frac{1}{\sqrt{\frac{(\mu+\mu^2)}{2}+1}} = \frac{1}{2}}$, for arbitrary μ, α^* is approximated as

$$\alpha^*=\frac{1}{\sqrt{\frac{(\mu+\mu^2)}{2}+1}} \quad (8)$$

In an effort to assess the secrecy performance, we proceed to derive the ESC with OPA and present fundamental design insights as the number of antennas grows large. To get outage constrained maximized secrecy rate, Let us assume the nodes don't have any channel information with the following exception:

- Alice knows h_0 perfectly.
- Alice has statistical information on k_0 ... (i, e) ... k_0 .. *CN* (0,σ^2 *I*)
- Helper k knows its own links to Bob ,h_k

The outer probability is defined as

$$P_{out}(R) = \min_{Q\geq 0, Tr(Q)<1} \Pr(C, < R) \quad (9)$$

We will determine the maximum R such that the outer probability is below prescribed below in small level, ϵ which is determined by the quality of the service (QoS) requirement. Mathematically the problem is determined by

$$\max_{Q} R \tag{10}$$

$$\text{S.t } P_{out}(R) \leq \epsilon \tag{11}$$

The problem of (10) is equivalent to the problem to maximizing the secrecy rate subject to QoS and power constraints as follows

$$\max_{Q} R \tag{12}$$

$$\text{S.t } Q \geq 0,\ \text{Tr}(Q) \leq 1, \tag{13}$$

$$\Pr(C_1 < R) < \epsilon \tag{14}$$

The outer coverage secrecy rate also maximized by also optimal input covariance matrix structure and also by closed form outage probability and also presents the basic structure through the number of antennas grows large.

IV. ERGODIC SECRECY CAPACITY

The erotic secrecy capacity (ESC) of the wiretap channel is known when the main channel (between the transmitter and the legitimate receiver) state information (CSI) is perfect at the transmitter and the coherence period is sufficiently large to enable random coding arguments in each block. The ESC describes the maximum of the average achievable secrecy rate, which is formulated as **[3]**

$$S_c = E\{S_c\}$$

$$= \int_0^x \int_0^x S_c\, f_{\gamma_{a,r}}(x_1) f_{\gamma_{r,b}}(x_2) dx_1\, dx_2 \tag{15}$$

where E {x} is the expectation of x, $f_{\gamma_{a,r}}(x1)$ is the probability density function (PDF) of $\gamma_{a,r}$, and $f_{\gamma_{r,b}}(x2)$ is the PDF of $\gamma_{r,b}$. Using the integration by substitution the ESC in (9) is re-expressed as

$$S_c = \int_0^\infty \int_0^\infty S_c\, X_2 f_{\gamma_{a,r}}(\mu, x_2) f_{\gamma_{r,b}}(x_2) d\mu dx_2 \tag{16}$$

Substituting equation **(3)** and **(4)** in equation **(16)**, we obtain the erotic secrecy capacity with OPA, Thus the equation is given below:

$$S_c = \frac{1}{2\log 2} \int_0^\infty \int_0^\infty \left[\log\left(1 + \frac{\alpha^* \mu x_2}{\alpha^* \mu + 2 - \alpha^*}\right) - \log\left(1 + \frac{\alpha^* \mu}{(1-\alpha^*)}\right)\right] x_2 f_{\gamma_{a,r}}(\mu, x_2) f_{\gamma_{r,b}}(x_2) d\mu dx_2 \tag{17}$$

We find that it is intractable to further simplify the ESC expression in **(17)**. To gain more insights, we derive new compact expressions for the ESC at high SNRs. We also quantify the impact of large scale antennas on the ESC for the M_a-1-1 and $1-1-M_b$ networks. From this two networks, the signal transmitted by following analysis

- High SNR (Signal to noise) Analysis
- Large N_α Analysis

A. M_a-1-1 Network:

From this network, N_α antennas are equipped by Alice and also uses the MRT beam former, this method is mainly for used for transmit the signal. From this network we using above mention analysis:

1. High SNR Analysis:

By this analysis, we get simple accurate expression for the asymptotic erotic secrecy capacity (ESC) as

$$S_c^{asy}=\frac{1}{2\log 2}[\log\alpha_{x,r}+\varphi(M_x)-M_a\ \frac{\alpha_{x,r}}{\alpha_{r,y}}\ X\ \int_0^\infty \tau(\mu)\ \mu^{N_a-1}\ (\mu+\frac{\gamma_{x,r}}{\gamma_{r,y}})^{-(N_a+1)}\ d\mu \quad (18)$$

Where$\alpha_{x,r}=\Omega_{a,r}\gamma_0$; $\alpha_{r,y}=\Omega_{r,b}$ $\varphi(M_x)=-C+\sum_{N=1}^{N_0-1}\frac{1}{n}$ With Euler's constant. A detailed derivation of equation (18) is given below. Hence based on equation (4) and (3), ESC in (10) can be rewritten as

$$S_c=\frac{1}{2\log 2}(E_1-E_2) \quad (19)$$

Where

$$E_1=\int_0^\infty\int_0^\infty x_2\log\left(1+\frac{\alpha^*\mu x^2}{\alpha^*\mu+2-\alpha^*}\right)f_{\gamma_{a,r}}(\mu,x_2)f_{\gamma_{r,b}}(x_2)d\mu dx_2 \quad (20)$$ And

$$E_2=\int_0^\infty\int_0^\infty x_2\log\left(1+\frac{\alpha^*\mu}{(1-\alpha^*)}\right)f_{\gamma_{a,r}}(\mu,x_2)f_{\gamma_{r,b}}(x_2)d\mu dx_2 \quad (21)$$

In additional,

$$f_{\gamma_{a,r}}(x)=\frac{x^{N_a-1}\,e^{-\frac{x}{\gamma_{a,r}}}}{(N_a-1)!(\gamma_{a,r})}N_a \text{and} \quad (22)$$

And

$$f_{\gamma_{a,r}}(x)=\frac{1}{\gamma_{r,b}}\ e^{-\frac{x}{\gamma_{r,b}}} \quad (23)$$

In high Signal to noise ratio with $\boldsymbol{\gamma_{0\to\infty}}$, E1 is evaluated as

$$E1=\log\gamma_{a,r} + \varphi(N_a)+ N_a \frac{\gamma_{a,r}}{\gamma_{r,b}} \int_0^{\infty} \frac{\mu^{Na-1} \log\left(\frac{\alpha^*}{\alpha^*\mu+2-\alpha^*}\right)}{(\mu+\frac{\gamma_{a,r}}{\gamma_{r,b}})^{(Na-1)}} d\mu \quad (24)$$

Similarly for E2

$$E2= N_a \frac{\gamma_{a,r}}{\gamma_{r,b}} \int_0^{\infty} \frac{\mu^{Na-1} \log\left(\frac{\alpha^*\mu}{1-\alpha^*}\right)}{(\mu+\frac{\gamma_{a,r}}{\gamma_{r,b}})^{(Na-1)}} d\mu \quad (25)$$

From E1 & E2, and the OPA factor given by **(8)** into **(19)** and after some manipulations, we get **(18)**

2. Large Na Analysis:

From this analysis we substituting equation **(8)** and equation **(4)**, we get

$$\gamma_r = \frac{1}{\sqrt{2\left(1+\frac{1}{\mu}\right)+\frac{1}{\mu}}} \text{And} \quad (26)$$

$$\gamma_b = \frac{\gamma_{r,b}}{1+\sqrt{2\left(1+\frac{1}{\mu}\right)+\frac{1}{\mu}}} \quad (27)$$

For large N_a, $\mu = (\|h\_(a,r\|))/(\|h\_(b,r\|))$ >>1, hence $\frac{1}{\mu} \approx 0$

From the equation **(26)** & **(27)** which reduce to

$$\gamma_{r=\sqrt{2}} \text{ And } \gamma_b = \frac{\gamma_{r,b}}{1+\sqrt{2}} \quad (28)$$

By the equation **(28)**, we get

$$C_s = \frac{1}{2} Y\{\ln_2\left(1 + \frac{\gamma_{r,b}}{1+\sqrt{2}}\right) - \ln_2(1+\sqrt{2})\}$$

$$= \frac{1}{2\log 2} \int_0^{\infty} \frac{1-F_{\gamma_{r,b}}(x)}{1+\sqrt{2+x}} dx - \frac{1}{2}\log_2(1+\sqrt{x})$$

$$=-\frac{e^0}{2\log 2} Yi(-v)-\frac{1}{2} \ln_2(1+\sqrt{2}) \quad (29)$$

Where, $F_{\gamma_{r,b}}(x) = 1 - e^{-x/\gamma_{r,b}}$ is the cumulative? Distribution function (CDF) of $\gamma_{r,b}$, v= $(1+\sqrt{2})/\gamma_{r,b} = (1+\sqrt{2})/\left(\Omega_{r,b}\gamma_0\right)$ and Ei(x) is an exponential integral function, as we said In equation (29), the Erogdic secrecy ratio is entirely determined by the average channel gain of the second hop and the transmit SNR of the network.

We can also find that the increasing number of antennas at Alice has no impact on the ESC when N_a is large.

B. 1-1-M_b technique:

By this network, M_b antennas is equipped by Bob and use the maximum ratio transmission beamformer to transmit the jamming signal to the relay, Bob first cancels the jamming signal , then uses MRC to maximize the received SNR. Using two analyses below:

1. High SNR Analysis:

From this we get a compact expression for the asymptotic in Erogdic secrecy ratio as:

$$S_c^{asy} = \frac{1}{2\log 2}[\log\alpha_{x,r} - C) - \frac{\gamma_{r,bN_b}}{\gamma_{r,y}} X \int_0^{\infty} \varphi(\mu)\ (\mu + \frac{\gamma_{x,r}}{\gamma_{r,y}} + 1)^{-(N_a+1)}\ d\mu \qquad (30)$$

2. Large N_b Analysis:

As we know that $\mu = [\|h\_(a,r\|)]\text{^}2/[\|h\_(r,b\|)]\text{^}2$
From (13) and (14), we obtain

$$\gamma_r = \frac{\sqrt{2\mu}}{\sqrt{1+\mu}} \approx \sqrt{2\mu} \text{ And } \gamma_b = \frac{\mu\gamma_{r,b}}{\mu+\sqrt{a(\mu^2+\mu+1}} \approx \mu\gamma_{r,b} = \gamma_{a,}$$

We have,

$$C_s = \frac{1}{2} Y\{\ln_2(1+\gamma_{a,r}) - \ln_2(1+\sqrt{2\mu}) \quad \} = \frac{1}{2\log 2}\int_0^{\infty} \ln(1+x)\, f_{\gamma_{a,r}}(x)dx - \frac{1}{2\ln 2} X \int_0^{\infty}\int_0^{\infty} x_2 \ln(1+\sqrt{2\mu}\, f_{\gamma_{a,r}}(\mu, x_2) f_{\gamma_{r,b}}(x_2) d\mu dx_2$$

$$= -\frac{e^{\frac{1}{\gamma_{a,r}}}}{2\log 2} Yi(-1/\gamma_{a,r}) - \frac{1}{2\log 2} X \int_0^{\infty} (\frac{\gamma_{r,b}\, t^2}{2\gamma_{a,r}} + 1)\ (+t)^{-1} dt \qquad (31)$$

From the equation **(31)**, we see that the erodgic secrecy capacity has increases with number of antennas at Bob. For very large antennas (i.e.)

$N_b \to \infty$, $\gamma_r \approx 0$, now

$$C_s = -\frac{e^{\frac{1}{\gamma_{a,r}}}}{2\log 2} Yi(-1/\gamma_{a,r}) \qquad (32)$$

It is indicated by **(32)** the ESC only depends on the average channel gain of the first hop and the transmit SNR of the network when N_b is very large.

V.NUMBERICAL RESULTS:

We now present some numerical illustrations for the ergodic secrecy capacity region. We select$M_a - 1 - 1$, and 1-1-$M_b$network. Consequently, the powers of the channel gains, i.e., Ei(x) and Ei(y), are exponential random variables with mean values N_a andN_b, respectively. The difference between these mean values can be viewed as a measure of the relative strengths of the users' channels on average. Thus, we expect that the user that has a larger mean value would have larger secrecy rates. In **Fig.1**, ergodic secrecy capacity region is given for two different sets ofγ_0, γ_1. For the first set, we have $\gamma_0 = \gamma_1 = 1$ which results in a symmetric ergodic secrecy capacity region. For the second set, we select $\gamma_2 = 1$, $\gamma_3 = 0.5$. Since user 2's average signal-to-noise ratio is lower in this case, the maximum secrecy rate of user 1 is larger while the maximum secrecy rate of user 2 is lower. To observe the effect of optimal power allocation, we compute the achievable secrecy region obtained by using a uniform power allocation, i.e., $M_a - 1 - 1$ is selected to be constant over 1-1-M_b The corresponding plot is given in **Fig.2**. We note that the optimal power allocation offers a significant advantage over the suboptimal uniform power allocation. The asymptotic curves obtained from **(28)** are in precise agreement with Monte Carlo simulation in the high SNR regime. The theoretical result in **(31)** tightly predicts the ESC with large N_b.

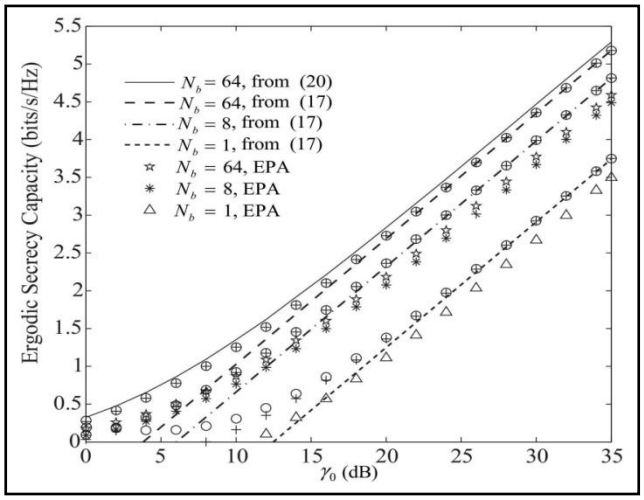

Fig.1. Ergodic secrecy capacity verses γ_0 for N_a -1-1

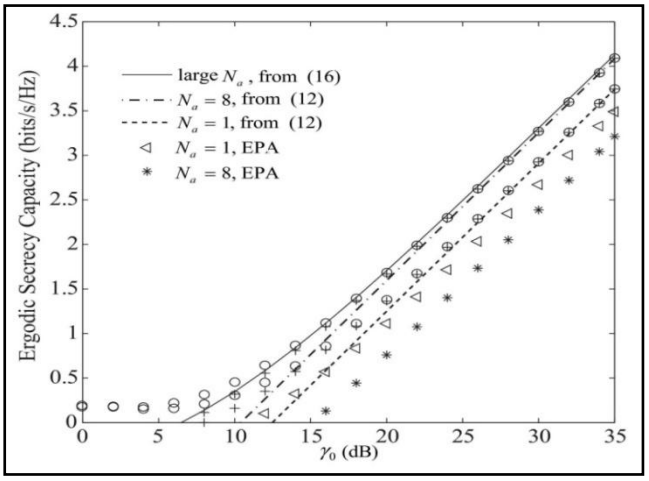

Fig.2. Ergodic secrecy capacity verses γ_0 for 1-1-N_b

V. CONCLUSION

We first obtained the secrecy capacity region of a general parallel channel, where in each one of the L sub channels; one of the users is less noisy with respect to the other user. We took into account CJ and OPA to secure the communication in the two-hop untrusted relay network. We derived the ergodic secrecy capacity for the networks. some interesting $M_a - 1 - 1$ and 1-1-M_b network and conclusions are drawn from our large system analysis as N_a ->∞ and N_b ->∞.for large N_a,we showed that the ESC only depends on the average channel gain of the second hop and the transmit SNR. For very largeN_b, ESC only depends on the average channel gain of the first hop and the transmit SNR.

ACKNOWLEDGEMENT

Authors deliver their graduate to SERB (Young Scientist Scheme, No. SP/FTP/ETA-51/2013) Govt. of India for Financial Assistance and FIST F.NO:SR/FST/College-189/2013

REFERENCE

[1] J. N. Laneman, D. N. C. Tse, and G. W. Wornell, "Cooperative diversity in wireless networks: efficient protocols and outage behavior," IEEE Trans. Inf. Theory, vol. 50, no. 12, pp. 3062–3080, Dec. 2004.

[2] J. Huang, A. Mukherjee, and A. L. Swindlehurst, "Secure communication via an untrusted non-regenerative relay in fading channels," IEEE Trans. Signal Process., vol. 61, no. 10, pp. 2536–2550, May 2013.

[3] M. Bloch, J. Barros, M. R. D. Rodrigues, and S. W. McLaughlin, "Wireless information-theoretic security," IEEE Trans. Inf. Theory, vol. 54, no. 6, pp. 2515–2534, 2008.

[4] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor, "Improving wireless physical layer security via cooperating relays," IEEE Trans. Signal Process., vol. 58, no. 3, pp. 1875–1888, Mar. 2010.

[5] A. D. Wyner, "The wire-tap channel," Bell Syst. Technol. J., vol. 54, no. 8, pp. 1355–1387, Oct. 1975.

[6] Q. Li and W.-K. Ma, "Optimal and robust transmit designs for MISO channel secrecy by semidefinite programming," IEEE Trans. Signal Process., vol. 59, no. 8, pp. 3799–3812, Aug. 2011.

[7] X. He and A. Yener, "Two-hop secure communication using an untrusted relay: a case for cooperative jamming," in Proc. 2008 IEEE Global Telecommun. Conf., pp. 1–5.

[8] "Cooperation with an untrusted relay: a secrecy perspective," IEEE Trans. Inf. Theory, vol. 56, no. 8, pp. 3807–3827, 2010.

[9] J. Huang, A. Mukherjee, and A. L. Swindlehurst, "Outage performance for amplify-and-forward channels with an unauthenticated relay," in Proc. 2012 IEEE Int Commun. Conf., pp. 893–897.

[10] "Secrecy analysis of unauthenticated amplify-and-forward relaying with antenna selection," in Proc. 2012 IEEE Acoustics, Speech and Signal Processing, pp. 2481–2484.

[11] L. Sun, T. Zhang, Y. Li, and H. Niu, "Performance study of two-hop amplify-and-forward systems with untrustworthy relay nodes," IEEE Trans. Veh. Technol., vol. 61, no. 8, pp. 3801–3807, Oct. 2012.

[12] G. Geraci, R. Couillet, J. Yuan, M. Debbah, and I. B. Collings, "Large system analysis of linear precoding in MISO broadcast channels with confidential messages," IEEE J. Sel. Areas Commun., vol. 31, no. 9, pp. 1660–1671, Sep. 2013.

[13] H. Q. Ngo, E. G. Larsson, and T. L. Marzetta, "Energy and spectral efficiency of very large multiuser MIMO systems," IEEE Trans. Commun., vol. 61, no. 4, pp. 1436–1449, Apr. 2013.

[14] C. Jeong, I.-M. Kim, and D. I. Kim, "Joint secure beamforming design at the source and the relay for an amplify-and-forward MIMO untrusted relay system," IEEE Trans. Signal Process., vol. 60, no. 1, pp. 310–325, Jan. 2012.

[15] R. H. Y. Louie, Y. Li, H. A. Suraweera, and B. Vucetic, "Performance analysis of beamforming in two hop amplify and forward relay networks with antenna correlation," IEEE Trans. Wireless Commun., vol. 8, no. 6, pp. 3132–3141, June 2009.

[16] I. S. Gradshteyn and I. M. Ryzhik, Table of Integrals, Series and Products, 7th ed. Academic Press, 2007.