ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization, Volume 3, Special Issue 1, February 2014

International Conference on Engineering Technology and Science-(ICETS'14)

On 10th & 11th February Organized by

Department of CIVIL, CSE, ECE, EEE, MECHNICAL Engg. and S&H of Muthayammal College of Engineering, Rasipuram, Tamilnadu, India

Secured Power Allocation for Decode and Forward Relay in Wireless Relay Networks

P.Mangayarkarasi[1], R.Revathi[2], Dr.S.Jayashri[3]

Assistant Professor, Department of ECE, Adhiparasakthi Engineering College, Melmaruvathur, India[1]

PG Scholar, Department of ECE, Adhiparasakthi Engineering College, Melmaruvathur, India[2]

Professor, Department of ECE, Adhiparasakthi Engineering College, Melmaruvathur, India[3]

***Abstract*—In wireless networks, security issues have taken a critical role in today's communications. In the proposed work, two hop wireless relay network in the presence of an eavesdropper is considered. The interest spans over a four node network model including a source, destination, trusted relay and an untrusted eavesdropper, in which the relay forwards the source message in a decode-and forward manner. When transmitting the messages from source to relay, eavesdropper intercept and try to capture that messages. The destination transmits an artificial jamming noise to the relay, to prevent that eavesdropper interception. This approach is analyzed for different jamming power allocation schemes to minimize the outage probability of the secrecy rate and improve the SNR rate, based on the channel state information available at the destination.**

***Index Terms*—Physical layer security, Decode and forward relay, Jamming power allocation scheme, Cooperative jamming, Outage probability.**

I. INTRODUCTION

Wireless networks are susceptible to numerous security threats due to the open nature of the wireless medium. Due to the broadcast nature of the wireless medium, transmitting confidential information securely in presence of possible eavesdroppers is of increasing importance.Wireless communication based on the assistance of relay has received considerable attention among researchers in recent years.Wireless relay networks are increasingly becoming an important part of next generation network infrastructure. The objective of these networks is to provide with anytime, anywhere secure data access.Power consumption has become an important concern when it comes to the implementation phase of wireless devices. Therefore, power management is one of the challenging problems in wireless communication, and recent research has addressed this problem by using various power allocation algorithms.

In wireless relay networks, based on secure communications where a source transmits a secret data to receiver over wireless wiretap channel [1]. The main drawback of the encryption systems is that they provide less security.

Relay selection for secure cooperative networks with jamming was proposed in [2], to maintain a secure communication against eavesdropper node. In which the network consists of two relay. The primary relay act as a straight mode to transmit a data from source to destination through decode and forward relay. The next relay, is usedto generatethe intended interference and transmit at the eavesdropper node.

Joint decode-and-forward and jamming for wireless physical layer security with destination assistance was proposed in [3], multipledecode-and-forwardrelaying schemes have been proposed to increase the signal to noise ratio efficiency of the relaying protocols. In this scheme, relay transmits the secured message to the destination and optimum relay selection scheme is also considered.

Petropulu et al. proposed on cooperative relaying schemes for wireless physical layer security in [4]in which a cooperative networks consists of single relay and one or more eavesdropper system, is used to maximize the average signal to noise ratio at the destination. Here node cooperation is exploited for achieving security in physical layer.

Cooperativejamming for secure communications in multiple input and multiple output relay networks was proposed in [5]. An optimal power allocation scheme for relayed transmissions over a Rayleigh fading channel is considered. In a conventional relay systems, one or more data streams

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization, Volume 3, Special Issue 1, February 2014

International Conference on Engineering Technology and Science-(ICETS'14)

On 10th & 11th February Organized by

Department of CIVIL, CSE, ECE, EEE, MECHNICAL Engg. and S&H of Muthayammal College of Engineering, Rasipuram, Tamilnadu, India

are transmitted based on the linear precoding schemes, under the assumption that channel state information (CSI) is available.

Outage probability based power distribution between data and artificial noise for physical layer security was proposed in [6]. It provides the physical layer security with many sources, one relay, and one destination is considered. Here two types of strategies are used to make a secured communications namely spatial beam forming and artificial noise broadcasting. In this two strategies provides the quality of service and also improve the probability of secret rate at the destination node.

A power allocation scheme was proposed in [7] for a single relay system to maximize the average SNR at the destination. To protect the source messages from being intercept and capture against by the eavesdropper. The cooperative transmissions are utilized with half duplex relay communication in this model. It develops the amplify and forward strategies for relay networks with single antenna nodes and multiple antenna nodes. The outage probability and diversity multiplexing was investigated here, and the outage probability is also achieved the level of zero.

Cooperation for secrecy in relay- eavesdropper channel was proposed in [8]. It develops the four-terminal relay eavesdropper channel and also Noise-forwarding (NF) scheme is considered. The noise forwarding scheme is used for relay node transmit the code words of source message to confuse the eavesdropper node, and also increase the secrecy rate for secured communication. Here the secrecy rate maximization problem is exploited by the additive white Gaussian noise channel.

Quality of service based transmit beam forming in the presence of eavesdroppers is considered in[9].Here, two design approaches was investigated. First approach, the eavesdropper allows the maximum amount of signal-to-interference-and-noise ratio (SINR) and the second approach is intended receiver provides the artificial noise with a satisfactory SINR. To avoid the design problems, here semi definite relaxation (SDR) is used.

The two hop wireless relay networks of half duplex communication with different jamming power allocation schemes under the Gaussian channel was investigated in [10]-[12]. This paper refers an extension of the work offered in [13] for cooperative ad-hoc environments with jamming. In contrast, where only one relay node is selected to guarantee security, here the problemconsidered involves the selection of a relay and a jammer node.Optimal power allocation for improving the amplify-and-forward(AF) relaying network is proposed in [14]. Jamming techniques which produce an artificial interference at the eavesdropper node inorder to reduce the outage probability of the related link seem to be an interesting approach for practical applications[15].

In our proposed work, we consider a two hop wireless relay networks in the presence of an eavesdropper with decode-and-forward Quadrature phase shift keying relaying protocol is used. Jamming power allocation scheme is used here whichefficiently minimizes the outage probability and improve the signal to noise ratio rate (SNR). Quality of service is provided for all the users participating in the network with secured communication.

The paper is organized as follows: section II describes about the system model, section III discusses the jamming power allocation method , section IV gives the numerical results with discussions and finally section V concludes the work.

II. SYSTEM MODEL AND RECEIVED SNR

A. System Model

We consider a two-hop wireless system which consists of one source node(S), one decode-and-forward relay node(DF), one destination node(D), and one eavesdropper node(E) terminals as shown in Fig.1.Here the relay node forwards the source message in a decode-and-forward manner to the destination node. When transmitting the messages from source to relay, eavesdropperintercept and capture that relay node messages. The destination transmits a artificial jamming noise to the relay, to prevent that eavesdropper interception. Power allocation is done for this network using different jamming power allocation scheme in which, noise allocated to channels are taken into account and based on that power allocation is done. For conveying the information to destination, decode-and- forward relay is used. This protocol first fully decodes the received source signal, re-encodes it, and retransmits the signal to destination.

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization, Volume 3, Special Issue 1, February 2014

International Conference on Engineering Technology and Science-(ICETS'14)

On 10th & 11th February Organized by

Department of CIVIL, CSE, ECE, EEE, MECHNICAL Engg. and S&H of Muthayammal College of Engineering, Rasipuram, Tamilnadu, India

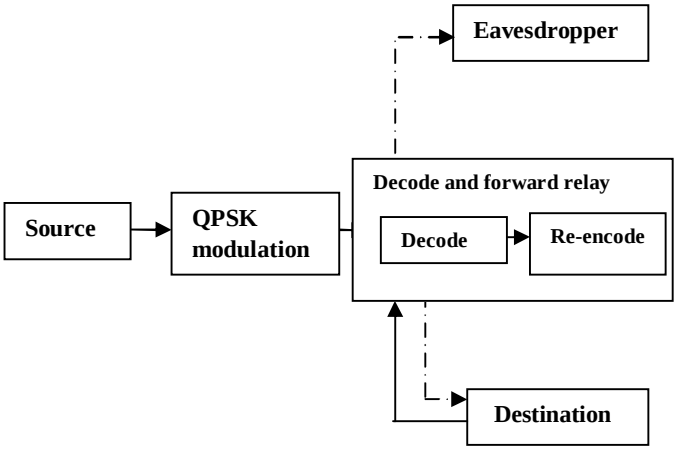

Fig.1. Block diagram of the proposed dual-hop half-duplex communication.

Power allocation can be done based on the outage probability and signal to noise ratio(SNR).If SNR thresholds are set properly, unnecessary power allocation can be avoided. Jamming power allocation scheme is used here to allocate power to the network terminals based on the channel state information available at the destination. This approach is analyzed for different jamming power allocation schemes to minimize the outage probability of the secrecy rate and improve the SNR rate,based on the channel state information available at the destination. Source can be a base station and the destination can be a mobile station. In between these two stations relay nodes are placed. In order to allocate power to the network terminals, we first transmit the message from source to relay terminals.

The received signal at the relay, $Y_{sr}$is then given by

$$Y_{sr} = \sqrt{P}h_{sr}X + \sqrt{P} + \eta_{sr} \quad (1)$$

$\sqrt{P}$-Transmitted power.

X -Transmitted signal from source to relay.

Z - Intended noise.

η -Additive white Gaussian noise.

Where $h_{sr}$and$h_{rd}$the channel fades between the source, relay and destination respectively. It can be modeled as Rayleigh flat fading channels. Rayleigh flat fading channel can bemathematically modeled as complex Gaussian randomvariable. Gaussian channel are zero mean independent and identically distributed channel. The Additive white Gaussian noise terms are modeled as zero-mean complex Gaussian randomvariables with varianceis N_0.

The received signal at the destination is then given by,

$$Y_{rd} = h_{rd}\beta Y_{sr} + \eta_{rd}$$

$$Y_{rd} = h_{rd}\beta[\sqrt{P}h_{sr}X + \sqrt{P}h_{rd}Z + \eta_{sr}] + \eta_{rd}$$

$$Y_{rd} = h_{rd}\beta\sqrt{P}h_{sr}X + h_{rd}\beta\sqrt{P}h_{rd}Z + h_{rd}\beta\eta_{sr} + \eta_{rd} \quad (2)$$

Whereβ is the relay gain. Toprevent the eavesdropper interception, destinationis engender by theartificial jamming noise and it can be injected to the relay. Relay having the ability tocancelled the self-interference at the destination. Then, the received signal is rewritten as,

$$Y_{rd} = h_{rd}\beta\sqrt{P}h_{sr}X + h_{rd}\beta\eta_{sr} + \eta_{rd} \quad (3)$$

The received signal at the eavesdropper is given by,

$$Y_{re} = h_{re}\sqrt{P}\beta h_{sr}X + h_{re}\sqrt{P}\beta h_{rd}Z + h_{re}\beta\eta_{sr} + \eta_{re} \quad (4)$$

To analyze the performance of the network, noise is added and checked how power is allocated based on it. Here Additive white Gaussian noise is considered. The additive noise at the source, relay, and destination are assumed to be complex Gaussian random variables with zero mean.

B. Received SNR

In decode-and-forward relaying, the relays decode the received signal and forward the scaled signals to the destination. During the first interval, the transmitter sends its signal to the relays and the second interval forwards it to the destination. In this process, noise is decodedat the relay. The mutual information for decode-and-forward relay transmission in terms ofthe channel fades can be given by,

$$I_{DF} = \frac{1}{2}\min\{\log(1 + \Gamma|h_{sr}|^2), \log(1 + \Gamma|h_{sd}|^2 + \Gamma|h_{rd}|^2)\}$$

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization, Volume 3, Special Issue 1, February 2014

International Conference on Engineering Technology and Science-(ICETS'14)

On 10th & 11th February Organized by

Department of CIVIL, CSE, ECE, EEE, MECHNICAL Engg. and S&H of Muthayammal College of Engineering, Rasipuram, Tamilnadu, India

Where the min operator in the above equation takes into account the fact that the relayonly transmits if decoded correctly, and hence the performance is limited by the weakestlink between the sourcedestination and source–relay. This equation gives the amount signal to noise ratio level received at the destination and eavesdropper.
The relay does that by simply scaling the received signal by a factor that is inversely proportional to the received power, which is denoted by,

$$\beta = \frac{\sqrt{P}}{\sqrt{P|h_{sr}|+N_0}} (5)$$

The signal transmitted from the relay is thus given byβ and has power P equal to the power of the signal transmitted from the source.Where N_0represents additive white Gaussian noise.It is an optimal independent AWGN channels. The signalis reached at the relay, after demodulation is done using QPSK technique.

III. POWER ALLOCATION

Jamming power allocation method is used here to minimize the outage probability and improve the signal to noise ratio rate in the network, according to the channel state information available at the destination. The increased SNR rate provides the maximum secrecy rate in a network. The perfect secrecy, which means the eavesdropper channel capacity is lower than legitimate channel capacity, can be achieved by properly injecting artificial noise. To adding artificial noise can be used to achieve perfect secrecy. In this method, artificial noise is generated by the coordination of helping nodes. Artificial noise is utilized to decrease the receptivity of legitimate receiver, but has only a small influence or none influence on legitimate receiver. The benefit of artificial noise injection is that even if the eavesdropper occupies a better channel condition than legitimate channel, by adding artificial noise into the transmission, it is still possible to guarantee an acceptable secrecy for a secured transmission. The secrecy channel is characterized as the capacity difference between the legitimate channeland eavesdropper channel.
The notion can be explained in a way that if the maximum of information transmitted in legitimate channel is higher than the maximum of information transmitted in the eavesdropper channel, the eavesdropper can never receive enough information to break through the legitimate transmission. This is also called as Perfect Secrecy. A positive secrecy rate is achieved while insuring that the eavesdropperreceives no information. Therefore, the transmitter sends the confidential message only if the legitimate receiver obtains a better transmission rate than the eavesdropper; otherwise, it remains idle. In order to guarantee perfect secure transmission, the signal-to-noise ratio (SNR) received at the eavesdropper is degraded compared to that at the legitimate receiver. To obtain the jamming power level, it can be minimize the outage probability of the secrecy rate.

A. Destination based on $\gamma_{sr}, \gamma_{rd}, \gamma_{re}$ of CSI

In this case, channel state information is based on the all nodes of source to relay, relay to destination node, relay to eavesdropper node. To send the messages with secure communications and reliability, improving the instantaneous secrecy rate and also minimize the outage probability of secrecy rate, which is given by,

$$C_s = (C_d - C_e)^+$$

$$C_s = \left(\frac{1}{2}\log\left(1+\frac{P_s}{\sigma_d^2}\right) - \frac{1}{2}\log\left(1+\frac{P_s}{\sigma_e^2}\right)\right)^+ (6)$$

C_s - Secrecy rate.

C_d - Destination node secrecy rate.

C_e - Eavesdropper node secrecy rate.

Theorem 1 RJPA method:

The Rate jamming power allocation method is based on the all nodes of channel state information γ_{sr}, γ_{rd}, and γ_{re}.The secrecy rate of the RJPA method is given by,

$$\alpha^* = \begin{cases} \min(\alpha_1^+, 1), & \gamma_{rd} > \gamma_{re}, \alpha_2 \le 1 \\ \text{No allocation}, & \text{otherwise}, \end{cases} (7)$$

Whereα^*isthe scaling factor, that is used tomaximize the instantaneous secrecy rate. If the relay to destination link is partially weak compared to the relay to eavesdropper link, that time destination should transmit the jamming noise with full power. If the relay to destination link is very strong it cannot be degrade that eavesdropper node and also reduces the secrecy rate. Therefore the interference level is

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization, Volume 3, Special Issue 1, February 2014

International Conference on Engineering Technology and Science-(ICETS'14)

On 10th & 11th February Organized by

Department of CIVIL, CSE, ECE, EEE, MECHNICAL Engg. and S&H of Muthayammal College of Engineering, Rasipuram, Tamilnadu, India

increased at the destination compared to the eavesdropper node.

B. Destination based on γ_{sr}, γ_{rd} of CSI

In this case, channel state information is based on the nodes of source to relay, relay to destination node. The eavesdropper node, channel state information is difficult to obtain at the destination node. Therefore it can be eliminates that the relay for the eavesdropper node information. The outage probability of the secrecy rate is given by,

$$P_{out}(SNR, R) = P_r(I_{DF} < R) \approx \frac{2^{2R}-1}{\sigma_{sr}^2 \beta} (8)$$

Theorem 2 outage OJPA method:

The outage optimal jamming power allocation method is based on the nodes of channel state information is γ_{sr}, and γ_{rd}.The secrecy rate of the outage OJPA method is the optimum α hitting $P_0 = 0$ can be determined when the source to relay and relay to destination link SNRs are strong so that $\Delta \geq 0$.

C. Destination based on γ_{re} node of CSI

In this case, channel state information is based on the node ofstatistical CSI instead of instantaneous node CSI. This method is also called as statisticalOJPA method of CSI.

To find α that minimizes the outage probability ofthe secrecy rate. This three jamming power allocationmethod can be estimated by using a software such as MATLAB.Hence using this scheme optimum power allocation can be explicitly found.

IV. Numerical Results and Discussion

In this section, simulations are done and the following figures show the performance of Jamming power allocation algorithm. Fig.2 shows theperformance of the Jamming power allocation scheme based Decode and forward relay networks and the simulation results are plotted.Taking advantage of the better secrecy rate, power allocation is done here.

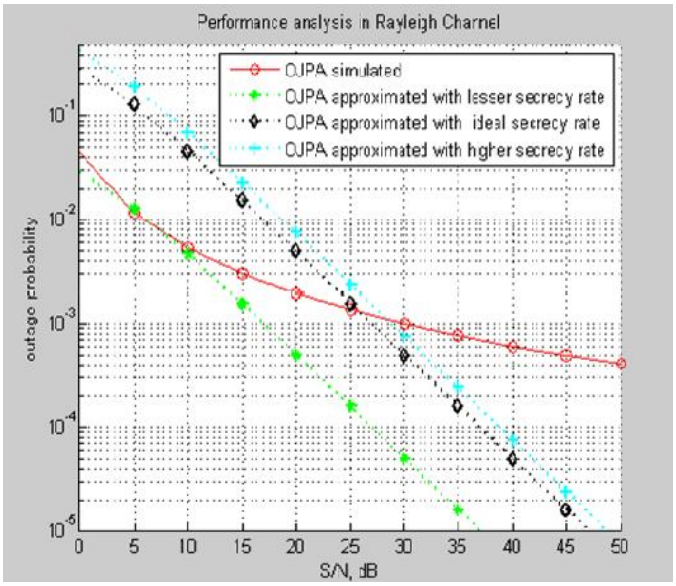

Fig. 2.Outage probability Vs Signal to noise ratio.

Figure shows the comparison of the outage probability of the secrecy rate among simulation and analytical results for Rayleigh fading channels. It is observed that by increasing the signal to noise ratio, and decreasing outage probability, the secrecy rate of the system have been improved.

Outage occurs when the channel variations does not support the required rate. Fig.3 shows the outage probability performance of Decode and Forward relay scheme based two-hop relay network with different jamming power allocation scheme.

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization, Volume 3, Special Issue 1, February 2014

International Conference on Engineering Technology and Science-(ICETS'14)

On 10th & 11th February Organized by

Department of CIVIL, CSE, ECE, EEE, MECHNICAL Engg. and S&H of Muthayammal College of Engineering, Rasipuram, Tamilnadu, India

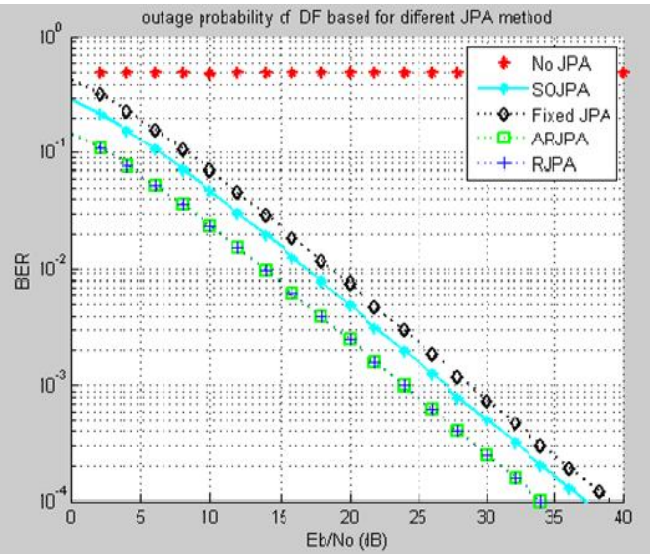

Fig. 3.Comparison of the outage probability of the secrecy rate among different JPA methods for Rayleigh fading channels.

It can be observed from the system for increasing values of signal to noise ratio, the performance of the system gets improved. The relay demodulates and decodes the received signal and then retransmits to destination. Decode and forward relay method offers enhanced performance over Amplify and forward relay method. The decoding operation at the decode and forward relay helps remove noise from the destination, while the noise is amplified by the relay when Amplify and forward relay is used.

V. CONCLUSION AND FUTURE WORK

This project work gives the analysis of jamming power allocation method that effectivelyachieve the secrecy rate in the network. The performance of the jamming power allocation method has been analyzed by the simulation results and then compared over different JPA methods. Maximum Signal to noise ratio rate was achieved by decode and forward relay method. To improve the secrecy rate modulation was carried out in QPSK modulation scheme. It is clear from the simulation results that for higher values of signal to noise ratio and the outage probability is minimized.This work can further be extended by increasing the number of relays and also the system can be further improved with various modulation schemes. Secrecy is a major concern in wireless networks, such as mobile phone wallet and military network applications.

REFERENCES

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

[2] I. Krikidis, J. S. Thompson, and S. McLaughlin, "*Relay selection for secure cooperative networks with jamming*," IEEE Trans. WirelessCommun., vol. 8, no. 10, pp. 5003–5011, Oct. 2009.

[3] Y. Liu, A. P. Petropulu, and H. V. Poor, "*Joint decode-and-forward and jamming for wireless physical layer security with destination assiatance*," in Proc. Asilomar Conference on Signals, Systems andComputer (ASILOMAR'11), Pacific Grove, USA, Nov. 2011.

[4] J. Li, A. P. Petropulu, and S. Weber, "*On cooperative relaying schemes for wireless physical layer security*," IEEE Trans. Signal Process.,vol. 59, no. 10, pp. 4985–4997, Oct. 2011.

[5] J. Huang and A. L. Swindlehurst, "*Cooperative jamming for secure communications in MIMO relay networks*," IEEE J. Sel. Areas Commun., vol. 59, no. 10, pp. 4871–4884, Oct. 2011.

[6] N. Romero-Zurita, M. Ghogho, and D. McLernon, "*Outage probability based power distribution between data and artificial noise for physicallayer security*," IEEE Signal Process. Lett., vol. 19, no. 2, pp. 71–74,Feb. 2012.

[7] Z. Ding, K. K. Leung, D. L. Goeckel, and D. Towsley, "*On the application of cooperative transmission to secrecy communictions*,"IEEE J. Sel. Areas Commun., vol. 30, no. 2, pp. 359–368, Feb. 2012.

[8] L. Lai and H. El Gamal, "*The relay-eavesdropper channel: Cooperation for secrecy*," IEEE Trans. Inf. Theory, vol. 54, no. 9, pp. 4005–4019, Sep. 2008.

[9] W. C. Liao, T. H. Chang, W. K. Ma, and C. Y. Chi, "*QoS-based transmit beamforming in the presence of eavesdroppers: An optimized artificial noise- aided approach*," IEEE Trans. Signal Process., vol. 59, no. 3, pp.1202–1216, Mar. 2011.

[10] S. Goel and R. Negi, "*Guaranteeing secrecy using artificial noise*," IEEE Trans. Wireless Commun., vol. 7, no. 6, pp. 2180–2189, Jun. 2008.

[11] S. Adams, D. Goeckel, Z. Ding, D. Towsley, and K. Leung;, "*Multi-user diversity for secrecy in wireless networks*," in Proc. Information Theoryand Applications Workshop (ITA), Feb. 2010.

[12] A. Mukherjee and A. L. Swindlehurst, "*Robust beamforming for security in MIMO wiretap channels with imperfect CSI*," IEEE Trans. SignalProcess., vol. 59, no. 1, pp. 351–361, Jan. 2011.

[13] O.Simeone and P. Popovski, "*Secure communications via cooperating base stations*," IEEE Commun. Lett., vol. 12, pp. 188-190, Mar. 2008.

[14] L.Dong, Z. Han, A. P. Petropulu, and H. V. Poor,

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization, Volume 3, Special Issue 1, February 2014

International Conference on Engineering Technology and Science-(ICETS'14)

On 10th & 11th February Organized by

Department of CIVIL, CSE, ECE, EEE, MECHNICAL Engg. and S&H of Muthayammal College of Engineering, Rasipuram, Tamilnadu, India

"*Improving wireless physical layer security via cooperating relays*," IEEE Trans. Signal Process., vol. 58, no. 3, pp. 1875–1888, Mar. 2010.

[15] 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.