Secrecy Outage Probability with Destination Assisted Jamming in Presence of an Untrusted Relay

Anurag Kumar, Shashibhushan Sharma,
Department of ECE, NIT Durgapur, India
anurag4203@gmail.com
sbs1988pks@gmail.com

Sanjay Dhar Roy, Member, IEEE
Sumit Kundu, Senior Member, IEEE
Department of ECE, NIT Durgapur, India
s_dharroy@yahoo.com
sumit.kundu@ece.nitdgp.ac.in

***Abstract*— The study of secrecy capacity of wireless networks, considering variety of powerful attacks is currently of great interest. In this paper, we have considered a possible attack scenario where an eavesdropper is present as a legitimate relay node in disguise in the network. A novel scheme of simultaneous transmission of jamming signal and message signal is proposed to confuse the eavesdropper. Here we consider a source, a destination and two amplify and forward (AF) relays each employed with a single antenna. One of the two relays used in the network is un-trusted and eavesdrop the information signal sent by the source. We analyze secrecy outage probability (SOP) of our proposed scheme under several network parameters such as target secrecy rate, transmit power of source, jamming power by destination and mean powers of fading channel. We also develop a simulation test bed to evaluate secrecy outage probability.**

Keywords--- cooperative relay networks; amplify and forward relay; jamming; secrecy outage.

I. INTRODUCTION

The fundamental requirement for any communication using wireless network is the maintenance of data secrecy. The computational complexities associated with cryptographic approach using secret keys motivated the use of physical layer security in wireless communication. In physical layer security approach, random nature of the communication channel is exploited to maximize the secrecy of data exchanged between two legitimate users, while minimizing the information leakage to the eavesdropper if any.

Wyner [1], showed that when an eavesdropper's channel is a degraded version of the channel between source and destination, communication can be achieved with a secrecy rate greater than zero while reducing spoofing by the eavesdropper. The secrecy capacity is defined as the difference between the capacities of the main channel and eavesdropper's channel [1]. It has been observed that in the presence of fading even if the eavesdropper has a better average signal to noise ratio (SNR) than the legitimate receiver, a non-zero secrecy rate is achieved thereby making an advantage of fading [3]. When fading for the channel to the destination is more than the channel to the eavesdropper, an optimal secrecy rate cannot be guaranteed. This problem can be overcome by using node cooperation with the help of amplify-and-forward relay, or decode-and-forward relay, or by use of cooperative jamming [4]. In cooperative jamming, relays just transmit artificial noise to degrade the channel to the eavesdropper, thereby increasing the secrecy rate. In [5], authors considered that the relay sends jamming when source transmits the message to destination and obtain the maximum secrecy under total transmits power constraint. In [6], it was shown that artificially generated noise can be added to the information signal to achieve secrecy. Here two different scenarios are considered; one in which transmitter generates artificial noise using multiple transmit antennas, and the other in which transmitter is assisted by helper nodes to generate noise. In [7], destination based jamming is considered in the case of an untrusted AF relays system model and it is found that when number of relays is increased, performance degrades. In [8], an upper and a lower bound of the secrecy outage in a dual hop AF system was obtained, where an eavesdropper taps the second hop, but any form of jamming was not considered. In [9], single energy harvested AF relay has been assumed under destination based jamming and SOP has been observed under power splitting based scheme and time switching based scheme of energy harvesting relay.

In this paper, we propose a novel scheme of jamming from destination to combat eavesdropping by an un-trusted relay. We consider a wireless relay channel with a set of two relays out of which one is trusted and other is an un-trusted one. The un-trusted relay eavesdrop the transmitted signal. A source transmits the message and the destination transmits jamming noise to confuse the eavesdropper in order to enhance the secrecy capacity. AF relay scheme has been assumed. We evaluate SOP for the proposed model.

The remaining part of this report is organized as follows. In Section II, we describe system model. In Section III, performance analysis has been discussed. Section IV shows the simulation results. Finally, Section V concludes the paper.

II. SYSTEM MODEL

As shown in Fig. 1, a wireless relay network consists of two amplify and forward relay nodes, a source node, and a destination node. Each node operates in a half-duplex mode. Out of the two relay nodes one say relay2 is un-trusted which eavesdrops the information signal. The direct link between Source and Destination is unavailable. Thus communication completes in two phases of equal time slots. Fig.2 shows that Communication between source and destination happens in two phase each of time duration T/2. In phase I, source node transmits information signal and destination node transmits

978-1-5090-3646-2/16/$31.00 ©2016 IEEE

jamming signal to the relays. In phase II, each relay nodes amplify and forward signals present at its input to the destination node. As shown in fig.1 and fig.2, both the relay nodes receive the transmitted signal with the jamming signals in phase I. They retransmit scaled versions of the jammed signal to the destination node in phase II. Finally, the destination node receives the jammed signal from both the relay nodes. Since jamming signal is known to the destination, it subtracts the jamming signal from the received signal to nullify the effect of jamming. Destination use the maximum ratio combining scheme to add the signal through different channels.

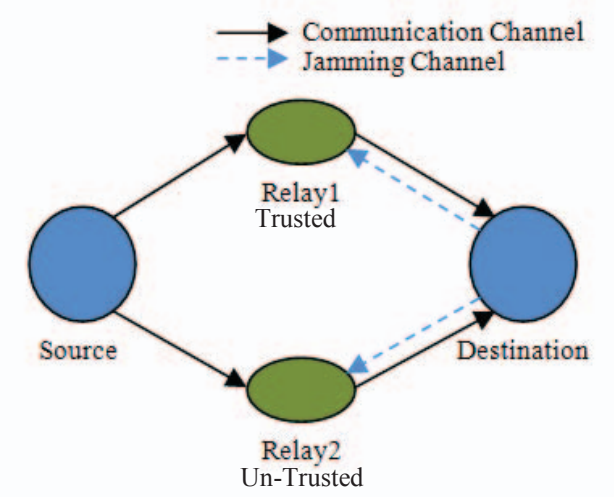

Fig.1: System model

We assume that the channels of all links are flat Rayleigh fading channels. We denote the coefficient of the channel between nodes n and m by h_{nm} . The channel power is given by $|h_{nm}|^2$, which has exponential distribution with mean Ω_{nm} . The probability density function $f_{|h_{nm}|^2}(x)$ of the channel power $|h_{nm}|^2$ is given as

$$f_{|h_{nm}|^2}(x)=\frac{1}{\Omega_{nm}}\exp\left(\frac{-x}{\Omega_{nm}}\right),x>0.$$

Here we denote the channel coefficient of the communication link Source- Relay, Relay-Destination and Destination-Relay as h_{SR_K} , h_{R_KD} and h_{DR_K} , respectively. The subscript K=1and 2 stands for relay nodes 1 and 2, respectively. The mean power of the channel coefficients h_{SR_K} , h_{R_KD} and h_{DR_K} are Ω_{SR_K} , Ω_{R_KD} and Ω_{DR_K} , respectively. We assume that the channel is a complex additive white Gaussian noise (AWGN) channel with zero mean and variance N_0 .The AF relay simply amplifies and forwards the signal received at input with an amplification factor μ .

Source ⇒ Relays	Relay ⇒ Destination
Information Signal	Amplified
Destination ⇒ Relays	Information + jamming
Jamming signal	signal
T/2	T/2

Fig.2: Transmission of Information and Jamming signal for the secure communication via AF relay in the duration T.

The net input SNR at the destination using maximum ratio combining scheme is given as;

$$\gamma_d=\gamma_{d1}+\gamma_{d2} \quad (1)$$

where γ_{d1} and γ_{d2} are SNR at destination through relay1 and relay2, respectively.

III. PERFORMANCE ANALYSIS

We present the necessary analytical framework for evaluating the SOP following our scheme proposed.

1. *Information processing and relaying protocols.*

In stage I, Source transmits the information signal over communication channel and at the same time destination sends jamming signal over the channel. Both the information signal as well as the jamming signal is available at the input of the relays. Thus the input signal at the relay1 and relay2, i.e. Y_{R1} and Y_{R2} is given as [3]

$$Y_{R1}=\sqrt{P_S}x_S h_{SR_1}+\sqrt{P_D}x_D h_{DR_1}+n_0 \quad (2)$$

$$Y_{R2}=\sqrt{P_S}x_S h_{SR_2}+\sqrt{P_D}x_D h_{DR_2}+n_0 \quad (3)$$

Where, P_S is the transmit power from source, x_S is the information transmitted by source and, x_D is the jamming symbol transmitted by destination. n_0 is additive white Gaussian noise (AWGN) voltage level. The SNR γ_E at the input of the eavesdropper is given as [3]

$$\gamma_E=\frac{P_S\left|h_{SR_2}\right|^2}{P_D\left|h_{DR_2}\right|^2+N_0} \quad (4)$$

The amplification factor of relay1 and that of relay2 using equation (2) is given as

$$\mu_1=\sqrt{\frac{P_{R_1}}{P_S\left|h_{SR_1}\right|^2+P_D\left|h_{DR_1}\right|^2+N_0}} \quad (5)$$

$$\mu_2 = \sqrt{\frac{P_{R_2}}{P_S\left|h_{SR_2}\right|^2 + P_D\left|h_{DR_2}\right|^2 + N_0}} \quad (6)$$

Where, P_{R_1} and P_{R_2} are the output power transmitted by the relay1 and relay2, respectively. Using this amplification factor, relays amplify the net signal present at its input and forward to the destination. Destination then receives signal from both the relay over two different links separately. The received signal thus contains both the information signal as well as the jamming signal. The received signal Y_{D1} at the destination through relay1 link is given as [1]

$$Y_{D1} = h_{R_1D}\mu_1 Y_{R1} + n_0$$

Putting value of Y_{R1} from equation (2), Y_{D1} can be written as

$$Y_{D1} = h_{R_1D}\mu_1(\sqrt{P_S}x_S h_{SR_1} + \sqrt{P_D}x_D h_{DR_1} + n_0) + n_0$$

$$Y_{D1} = h_{R_1D}\mu_1\sqrt{P_S}x_S h_{SR_1} + (h_{R_1D}\mu_1 + 1)n_0 + h_{R_1D}\mu_1\sqrt{P_D}x_D h_{DR_1}$$

Where, the last part of the above equation is jamming part and destination being aware of the jamming signal subtracts it from the received signal. Thus Y_{D1} is given as:

$$Y_{D1} = h_{R_1D}\mu_1\sqrt{P_S}x_S h_{SR_1} + (h_{R_1D}\mu_1 + 1)n_0 \quad (7)$$

Similarly, the received signal Y_{D2} at the destination through relay2 link is given as:

$$Y_{D2} = h_{R_2D}\mu_2\sqrt{P_S}x_S h_{SR_2} + (h_{R_2D}\mu_2 + 1)n_0 \quad (8)$$

First part of the Y_{D2} in equation (8) is information signal and the second part constitutes noise. Thus using equations (7) and (8), the SNR at destination through relay1 and relay2 link, is given as [3]

$$\gamma_{D1} = \frac{\mu_1^2 P_S\left|h_{SR_1}\right|^2\left|h_{R_1D}\right|^2}{(\mu_1^2\left|h_{R_1D}\right|^2 + 1)N_0} \quad (9)$$

$$\gamma_{D2} = \frac{\mu_2^2 P_S\left|h_{SR_2}\right|^2\left|h_{R_2D}\right|^2}{(\mu_2^2\left|h_{R_2D}\right|^2 + 1)N_0} \quad (10)$$

Using maximum ratio combining scheme, mentioned in equation (2), the total SNR at the destination is given as

$$\gamma_D = \frac{\mu_1^2 P_S\left|h_{SR_1}\right|^2\left|h_{R_1D}\right|^2}{(\mu_1^2\left|h_{R_1D}\right|^2 + 1)N_0} + \frac{\mu_2^2 P_S\left|h_{SR_2}\right|^2\left|h_{R_2D}\right|^2}{(\mu_2^2\left|h_{R_2D}\right|^2 + 1)N_0} \quad (11)$$

2. *Secrecy capacity and secrecy outage probability*

the secrecy capacity of the complex channel model is given as [2]

$$C_S = C_D - C_E \quad (12)$$

where C_D is destination channel capacity which expressed as:

$$C_D = \frac{1}{2}\log(1+\gamma_D)$$

and eavesdropper's channel capacity C_E expressed as:

$$C_E = \frac{1}{2}\log(1+\gamma_E)$$

Thus instantaneous secrecy capacity C_S is given as

$$C_S = \frac{1}{2}\left[\log\left\{\frac{(1+\gamma_D)}{(1+\gamma_E)}\right\}\right]^+ \quad (13)$$

where, $[x]^+ = \max(x,0)$.

The SOP at the destination is given as [3]:

$$P_{out} = P(C_S < R_S) \quad (14)$$

i.e. the probability of instantaneous secrecy capacity C_S at destination is less than a target secrecy rate $R_S > 0$. We can write equation (15) as

$$P_{out} = P\left(\frac{1}{2}\left[\log\left\{\frac{(1+\gamma_D)}{(1+\gamma_E)}\right\}\right] < R_S\right)$$

$$P_{out} = P\left(\left\{\frac{(1+\gamma_D)}{(1+\gamma_E)}\right\} < 2^{2R_S}\right)$$

$$P_{out} = \int_0^{\infty}\int_0^{\left(2^{2R_S}(1+\gamma_E)-1\right)} P_{\gamma_D\gamma_R}(x,y)dxdy$$

$$P_{out} = \int_0^{\infty}\int_0^{\left(2^{2R_S}(1+\gamma_E)-1\right)} P_{\gamma_R}(y)P_{\gamma_D}\left(\frac{x}{y}\right)dxdy\,. \quad (15)$$

IV. SIMULATION RESULTS AND DISCUSSION

MATLAB simulation results for proposed scheme following the above formulation are provided. All simulation results are obtained assuming one source, one destination and these communicate via two AF relay nodes in which one is trusted and other is untrusted.

Both the relay nodes are assumed to be equidistant from source and also from destination. Therefore channel mean powers are considered as $\Omega_{SR_1} = \Omega_{SR_2}$, $\Omega_{DR_1} = \Omega_{DR_2}$ and $\Omega_{R_1D} = \Omega_{R_2D}$. Also the channel mean power from relays to destination and that of destination to relays are considered to be same i.e. $\Omega_{R_KD} = \Omega_{DR_K}$. The power transmitted by both

the relays has been considered same i.e. $P_{R1} = P_{R2}$ and the power transmitted by the source and the destination has also been considered same i.e. $P_S = P_D$.

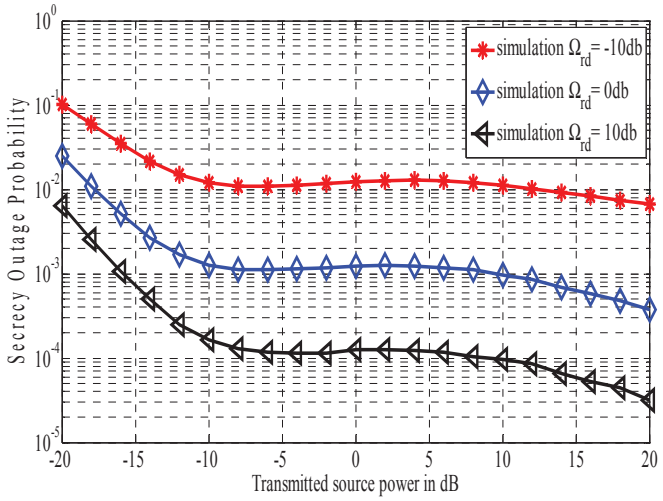

Fig.3: Secrecy outage probability versus transmitted source power P_S , for selected values of Ω_{RD} and for a normalized target secrecy rate (R_S)equal to 0.1. Ω_{SR} is equal to 1 dB.

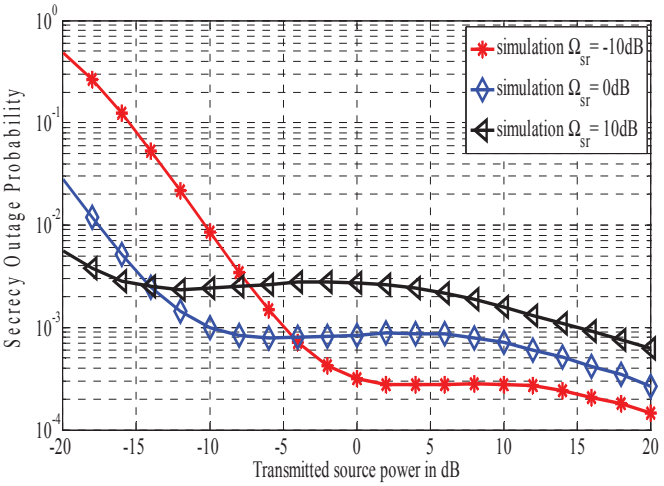

Fig.4: Secrecy outage probability versus transmitted source power P_S , for selected values of Ω_{SR} and for a normalized target secrecy rate (R_S) equal to 0.1. Ω_{RD} is equal to 1 dB.

Fig. 3 depicts the SOP versus P_S , for selected values of Ω_{rd} and for a normalized target secrecy rate equal to 0.1. Further Ω_{sr} is taken as 1 dB. We observe that for a constant Ω_{rd} , with increase in P_S , the SOP curve first decreases then saturates to a value for certain range and finally, decreases from that point onwards. Initial decrease is due to the facts that increase in P_S increases the information signal strength at the relays, thus increasing the SNR at the destination in turn which uses MRC scheme. But at the same time jamming also increases which further decreases the SNR at the eavesdropper. Later with increase in P_S , information signal strength at eavesdropper increases significantly, which compensates the effect of jamming, improving eavesdropper's channel capacity as compared to destination channel capacity. This leads to almost constant nature of SOP curve in that range. Finally, after a certain value of P_S jamming dominates over information signal strength at the eavesdropper, decreasing eavesdropper's SNR but total SNR at the destination keeps on increasing which justifies the further decreasing nature of SOP curve. For a constant value of P_S , increase in Ω_{rd} increases the channel capacity of relay to destination channel which reduces SOP.

Fig.4 depicts the SOP versus P_S , for selected values of Ω_{sr} and for a normalized target secrecy rate equal to 0.1. Further Ω_{rd} is taken as 1 dB. For a constant Ω_{sr} similar nature of the SOP curve is observed as that for the case of a constant Ω_{rd} in fig.3. But as the value of Ω_{sr} is changed to a higher value for a constant P_S , signal strength at eavesdropper improves resulting in increase in eavesdropper's capacity. This causes increase in SOP in this case.

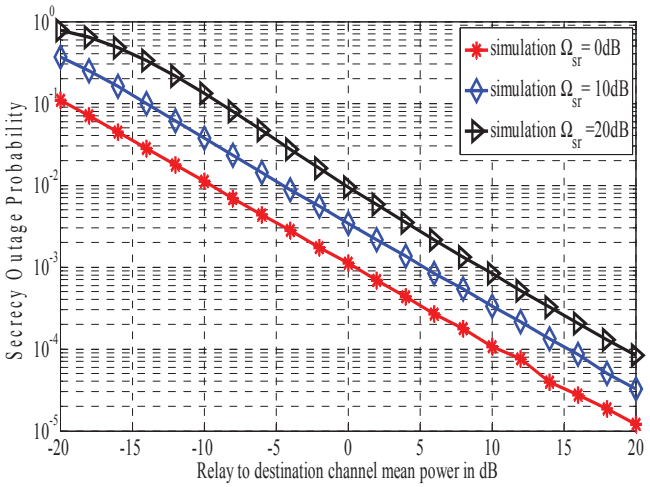

Fig.5: Secrecy outage probability versus Ω_{RD} , for selected values of Ω_{SR} and for a normalized target secrecy rate (R_S) equal to 0.1. $P_S = P_D$ = 1dB.

Fig.5 depicts the SOP versus relay to destination channel mean power Ω_{rd} for selected values of Ω_{sr} and a normalized target secrecy rate equal to 0.1. Each P_S and P_D is equal to1dB. For a constant value of Ω_{sr} , with increase in Ω_{rd} , SOP decreases because, with increase in relay to destination channel mean power, SNR at the destination increases while the SNR at the eavesdropper remains the same. For a constant Ω_{rd} , with increase in Ω_{sr} , SNR at eavesdropper increases while SNR at destination remains constant thereby increasing SOP. Fig.6 depicts the SOP versus source to relay channel mean power Ω_{sr} for selected values of Ω_{rd} and for normalized target secrecy rate equal to 0.1 where P_S and P_D are

equal to 1dB. We observe that, under a constant value of Ω_{rd}, SOP first decreases, reaches to a minimum and increases with further increase in source to relay channel mean power. This behavior of SOP is due to the facts that, at the beginning, increase in Ω_{sr} increases information signal strength at the relay.

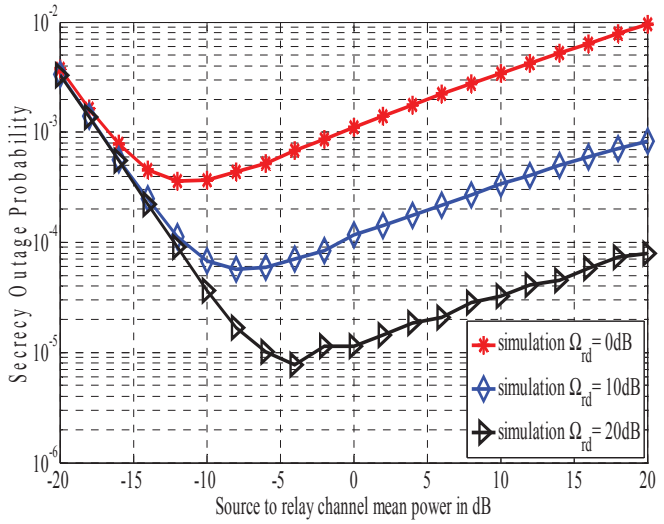

Fig.6: Secrecy outage probability versus Ω_{SR}, for selected values of Ω_{RD} and for a normalized target secrecy rate (R_S) equal to 0.1. $P_S = P_D$ = 1dB.

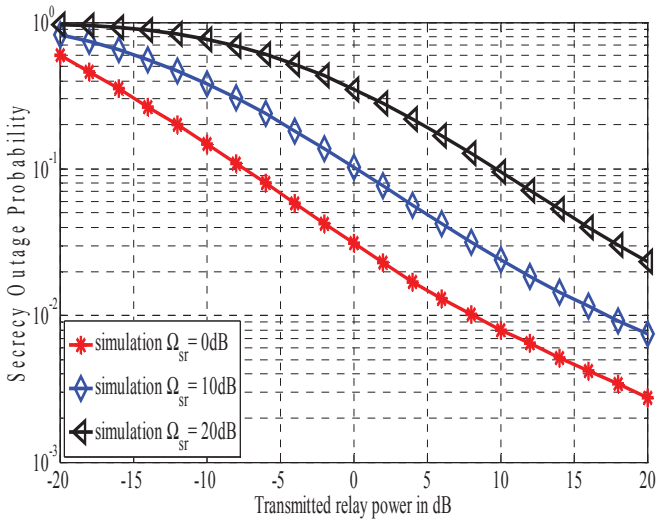

Fig.7: Secrecy outage probability versus transmitted relay power $P_{R1} = P_{R2}$, for selected values of Ω_{SR} and for a normalized target secrecy rate (R_S) equal to 0.1. $P_S = P_D$ = 1dB.

This increases SNR at the destination where MRC scheme is used. Though Information signal strength at the eavesdropper increases, presence of jamming reduce SNR at the eavesdropper. After certain value of Ω_{sr}, increase in signal strength at the eavesdropper dominates over jamming signal, thus increasing the SNR at eavesdropper, which leads to the increase of SOP beyond that point. For a constant Ω_{sr} increase in Ω_{rd} causes increase in SNR at the destination while reducing SNR at the eavesdropper, thereby causing downward shift of SOP curve and right shift of optimal point of Ω_{sr}.

Fig.7 depicts the SOP versus relay transmission power $P_{R1} = P_{R2}$ for selected values of Ω_{sr} and for normalized target secrecy rate of 0.1; where P_S and P_D are equal to 1dB. We observe, that for a constant value of Ω_{sr}, as relay power is increased the signal strength at destination increases which increases the causing reduction in SOP. For constant relay power, increase in Ω_{sr} causes increase in SNR at the eavesdropper which increases SOP.

.

III CONCLUSION

We propose a relay network with cooperative jamming scheme, where destination transmits jamming noise to increase uncertainty in eavesdropping by an un-trusted relay and maximize secrecy rate. We investigate the secrecy outage probability of our scheme under source transmit power variation, communication channel mean power variation (Ω_{SR} and Ω_{RD}) and relay transmit power variation. It has been noticed that increase in source transmit power or relay transmit power is beneficial to the secure communication. Also increase in relay to destination channel mean power Ω_{RD} for a constant value of Ω_{SR} reduces the SOP thus enhancing security. An optimum value of source to channel mean power is observed depending on other network parameters which minimize SOP.

REFERENCES

[1] A. D. Wyner, "The wiretap channel," *Bell System Technical Journal*,vol. 54, no. 8, pp. 1355–1387, 1975.

[2] S. K. Leung- Yan- Cheong and M. E. Hellman, "the gaussian wiretap channel," IEEE Trans. Inf. Theory, Vol. 24, no. 3, pp. 339-348, may 1978.

[3] Jo˜ao Barros, "Secrecy Capacity of Wireless Channels," ISIT 2006, Seattle, USA, July 9 14,2006.

[4] L. Lai and H. El Gamal, "The relay-eavesdropper channel: cooperation for secrecy," *IEEE Trans. Inform. Theory*, vol. 54, pp. 4005–4019, Sept. 2008.

[5] L. Dong, Z. Han, A. P. Petropulu and H. Vincent Poor, "Cooperative jamming for wireless physical layer security," in *Proc. IEEE/SP Workshop on Statistical Signal Processing*, pp. 417–420, 2009.

[6] R. Negi and S. Goel, "Secret communication using artificial noise," in *Proc. IEEE 62nd Vehicular Technology Conference*, vol.3, pp. 1906–1910, 25-28 Sept., 2005.

[7] Li Sun and Yubo Li, "Performance Study of Two-Hop Amplify-and-Forward Systems with Untrustworthy Relay Nodes," IEEE Trans. on Vehicular Technology, Vol. 61, No. 8, pp. 3801-3807, October 2012.

[8] Abhishek Jindal, Chinmoy Kundu and Ranjan Bose, "Secrecy Outage of Dual-hop Amplify-and-Forward System and its Application to Relay Selection," 978-1-4799-4482-8/14/$31.00 ©2014 IEEE

[9] S.S. Kalamkar and A. Banerjee, "Secure communication Via a Wireless Energy Harvesting Untrusted Relay," arXiv: 1509.08262v1 [cs.IT] 28 Sep 2015.