Secrecy Performance of Novel Destination Assisted Jamming in Cooperative Networks under the influence of Trusted and Untrusted Relays

Pravat Biswas[1], Chandrima Thakur[2], Ajit Haldar[3] and Sudipta Chattopadhyay[4]

Department of Electronics & Telecommunication Engineering

Jadavpur University, Kolkata, India

E-mail: - *pravatbiswas98@gmail.com[1], chandrima31.ece@gmail.com[2], ajithaldar2080@gmail.com[3], sudiptachat@yahoo.com[4]*

DOI: - https://doi.org/10.47531/MANTECH/ECC.2021.01

Abstract

In this paper, we have proposed a novel scheme of destination-based jamming in a cooperative relay network where a source communicates with the destination via multiple untrusted half-duplex amplify and forward relays in the absence of a direct link. For this purpose, two novel models have been proposed. We have observed the secrecy performances of the network under possible attack scenarios where eavesdropper may be present as a legitimate node in disguise. We have also developed a simulation testbed to evaluate the secrecy outage probability. Moreover, the secrecy outage probabilities of our proposed schemes have been analyzed with respect to several network parameters such as target secrecy rate; transmit power of the source, jamming power by destination and mean power of the fading channel. This paper gives us a guideline to choose an optimized model from a network with multiple trusted and untrusted relays.

Keywords: - *Amplify and forward relay, Fading, Jamming, Relay networks, Secrecy outage, Wireless channel.*

INTRODUCTION

Secrecy [1] has a great impact related to any wireless network. In [2], the authors have presented a system where the information is transmitted using a discrete, memoryless channel subjected to a wiretap at the receiver side. Another model has been developed in [3] where two legitimate users are communicating with each other in the presence of the eavesdropper. Here the important role of fading is characterized in terms of average secure communication rates and outage probability. Various cryptographic algorithms [4] provide secrecy of data under the presence of an eavesdropper. The results for the discrete memoryless wire-tap channel has been extended to the Gaussian wire-tap channel [5]. In [6], the authors have characterised a network where confidential data are being communicated and an eavesdropper present in the network. Here, secrecy capacity has been taken as a parameter to analyze the performance which is defined in terms of outage probability and has given complete information for the maximum transmitted rate at which the eavesdropping of information is zero. In [7], the authors have characterized the secrecy capacity of a network consisting of an eavesdropper under different assumptions on the available channel state information (CSI). Further, this shows the positive impact of fading of a channel that is helping in the better performance of secrecy capacity. The authors [8] have found out the value of capacity of an AWGN channel with Rayleigh fading and proposed an approximation capacity and compared it with numerically computed one. Further their approximation results have a better performance in approximating Rayleigh fading channel than the bounds which have been set before.

To get a secrecy rate greater than zero Amplify and Forward (AF) relay or Decode and Forward (DF) relay or cooperative jamming can be used [9]. In [10], authors have established the utility of user cooperation in secure wireless communication. They have studied that Novel noise forwarding relay helps in secure wireless communication while it has nothing to do with the source message. It sends noise signal to the eavesdropper to confuse it about the original message. Work presented in [11] shows two different ways to increase the secrecy using the

concept of cooperative jamming. In the first approach, the transmitter generates noise with the multiple antennas in it. The second approach incorporates helper nodes which generates noise to help the transmitter. In [12], destination assisted based jamming has been used when the system has an untrusted AF relay. It is also shown that as the number of relays in the system increases, the overall performance of the model decreases. In [13], the authors have determined the upper and lower bounds of secrecy outage probability of a dual hope amplify and forward relay system where the eavesdropper is connected to the second hop. It is proposed to use AF or DF relays in the system model to secure cooperative communication [14]. In [15], it has been shown that Secrecy capacity (CS) can be defined in terms of maximum transmission rate but then we will have to make sure that the eavesdropper does not overhear the channel. In case of spoofing of information, secrecy capacity is defined as the difference between main channel capacity and the eavesdropper channel capacity. The major contributions of this work are:

1. Two novel models of destination assisted jamming cooperative relay network are proposed here.
2. The secrecy performances of the proposed models have been studied.
3. The comparative analysis of the proposed models with the existing model has been presented.

The organization of the paper is as follows: The proposed system models have been discussed in section II. In Section III, the performance analysis of the proposed work has been developed through mathematical modeling. Simulation results have been presented in Section IV. Finally, the paper has been concluded in Section V.

SYSTEM MODEL

1. In this section, two proposed models have been described. The existing model [15] has also been included here for better understanding. The list of assumptions based on which the models are developed is listed below:
2. The channels of all links are Rayleigh fading in nature. There is no direct connection between source and destination.
3. Each of the Models consists of one source, one destination with variable relays.
4. All the trusted relays are identical to each other.
5. All the untrusted relays are identical to each other.
6. The channel coefficient is same for source to any relay and also from any relay to destination.
7. Existing Model [15] consists of a wireless relay network, with one trusted and one untrusted relay.
8. Proposed Model 1 contains a wireless relay network, with two trusted and one untrusted relays
9. Proposed Model 2, includes a wireless relay network, with two trusted and two untrusted relays.

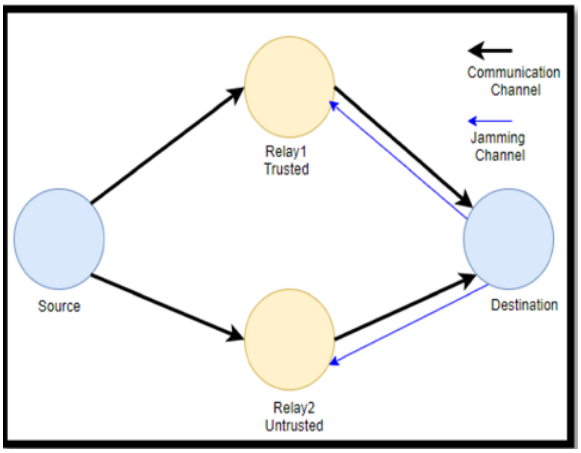

Fig.1: Existing Model

In the Existing Model, each node operates in a half-duplex mode. Out of two relay nodes, Relay2 is un-trusted in nature which eaves drop the information signal.

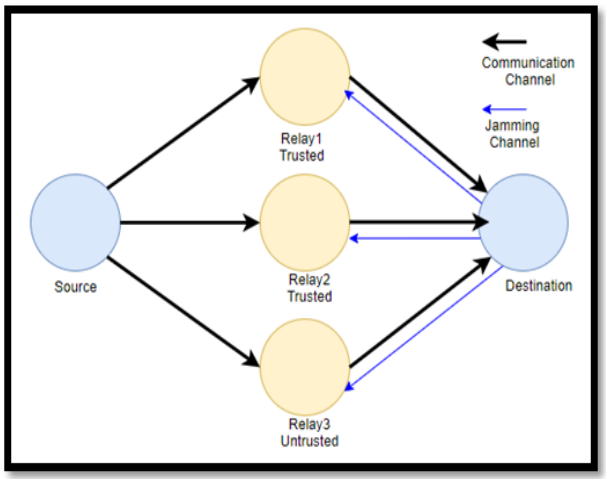

Fig.2: Proposed Model 1

In Proposed Model 1, out of the three relay nodes, Relay3 is untrusted which eaves drops the information signal.

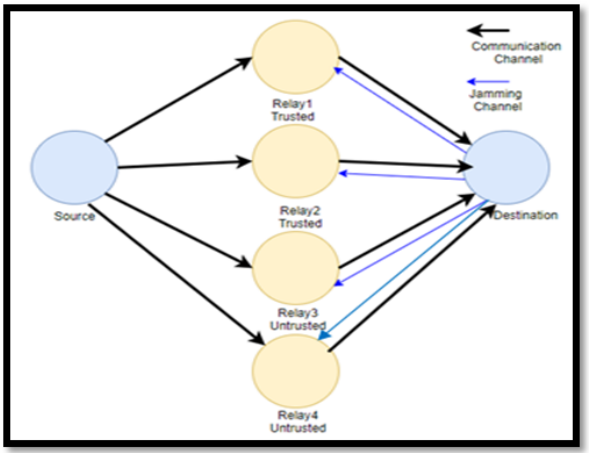

Fig. 3: Proposed Model 2

In Proposed Model 2, out of the four relay nodes, Relay3 and Relay4 are untrusted which eavesdrop the information signal.

The communication gets completed in two phases of equal time slots. In the first phase, the information signal is transferred from source to the relay nodes and the jamming signal is also transmitted from the destination to the relays. Thereafter in the second time slot, the scaled version of the information signal is transmitted from the relays to destination. As the receiver knows the jamming signal, hence it subtracts the jamming signal from the received signal to nullify the effects of jamming and retrieves the original signal. Maximum ratio combining scheme is mainly used at the receiver to combine the signals that are being received from the multiple channels. The coefficient for the channel with nodes n and m is given by h_{nm}. The channel power is given by $|h_{nm}|^2$, which has an exponential distribution with mean Ω_{nm}. The probability density function f (x) of the channel power $|h_{nm}|^2$ is given as,

$$f(x)=\frac{1}{\Omega nm}\exp(\frac{-x}{\Omega nm}),x > 0 \text{[15]} \quad (1)$$

Here, all the relays are equidistant from the source and destination, hence, $\Omega_{SRi} = \Omega_{SRj}$; $\Omega_{DRi} = \Omega_{DRj}$; $\Omega_{R\,D} = \Omega_{R}$; for i ≠ j. Similarly, the channel mean power from the relay to destination and from destination to relay are same, i.e $\Omega_{R\,D} = \Omega_{DRk}$ [15].

PERFORMANCE ANALYSIS

A. Information processing for Proposed Model 1

In proposed model 1, three relay nodes are present. Relay 1 and Relay 2 are assumed to be trusted; whereas, Relay 3 is assumed to the untrusted one. Following the evaluation given in [15] for the existing model, the total SNR at the destination (γ_D) for the Proposed Model 1 can be obtained as listed below:

$$\gamma D = \gamma D1 + \gamma D2 + \gamma D3$$

$$= \mu_1^2 P_S |h_{SR1}|^2 |h_{R1D}|^2 / [(\mu_1^2 |h_{R1D}|^2 + 1)N_0] + \mu_2^2 P_S |h_{SR2}|^2 |h_{R2D}|^2 / [(\mu_2^2 |h_{R2D}|^2 + 1)N_0] + \mu_3 PS |h_{SR3}|^2 |h_{R3D}|^2 / [(\mu_2^2 |h_{R3D}|^2 + 1)N_0]. \quad (2)$$

As Relay3 is untrusted one, the SNR γE at the input of the eavesdropper is given as

hence $$\gamma_E = \frac{P_S |h_{SR_3}|^2}{P_D |h_{DR_3}|^2 + N_0} \quad (3)$$

The secrecy capacity of the channel is further given as $C_S = C_D - C_E$ [15] where C_D and C_E is the destination channel and eavesdropper's channel capacity respectively

These expressed as [15], $C_D = \frac{1}{2}\log(1 + \gamma_D)$ (4)

$C_E = \frac{1}{2}\log(1 + \gamma_E)$ (5)

Hence, $C_S = [\frac{1}{2}\log\{\frac{(1+\gamma_D)}{(1+\gamma E)}\}]^+$ where $x^+ \max(x, 0)$ (6)

The SOP at the destination is, $P_{out} = P (C_S < R_S)$ (7)

B. Information processing for Proposed Model 2

In the Proposed Model 2, two trusted along with two untrusted relays are assumed to be present between the source and destination. Relay1 and relay 2 are only trusted relay. As relay 3 and relay 4 are untrusted relays, following the evaluation in [15], the SNR γE at the input of the eavesdropper is given as

$$\gamma_E = \frac{P_S |h_{SR_3}|^2}{P_D |h_{DR_3}|^2 + N_0} + \frac{P_S |h_{SR_4}|^2}{P_D |h_{DR_4}|^2 + N_0} \quad (8)$$

Further, total SNR at the destination is given as,

$$\gamma D = \gamma D1 + \gamma D2 + \gamma D3 + \gamma D4 \quad (9)$$

where γDi is the SNR due to ith relay at the destination. The respective value of γDi can be determined following the analysis shown in[15]. In a similar manner, the SOP at the destination, $P_{out} = P (C_S < R_S)$ [15] (10)

SIMULATION RESULTS AND DISCUSSIONS

The performance of the proposed models has been evaluated through simulation results. Simulation has been carried out using MATLAB version R2018a. The parameters have been set according to Table – 1.

Table I: Parameter Settings

Case: 1.	SOP vs. P_S with Ω_{SR} = Constant = 1 dB for three selective values of Ω_{RD} = - 10, 0, 10 (in dB), R_S = 0.1, $P_D = P_S$.
Case: 2.	SOP vs. P_S with Ω_{RD} = Constant = 1 dB for three selective values of Ω_{SR} = - 10, -5, 0 (in dB), R_S = 0.1, $P_D = P_S$.

Case: 3.	SOP vs. Ω_{SR} with $P_D = P_S$ = Constant = 1 dB for three selective values of Ω_{RD} = 0, 10, 20(in dB), R_S = 0.1.
Case: 4.	SOP vs. Ω_{RD} with $P_D = P_S$ = Constant = 1 dB for three selective values of Ω_{SR} = 0, 10, 20(in dB), R_S = 0.1.

CASE 1

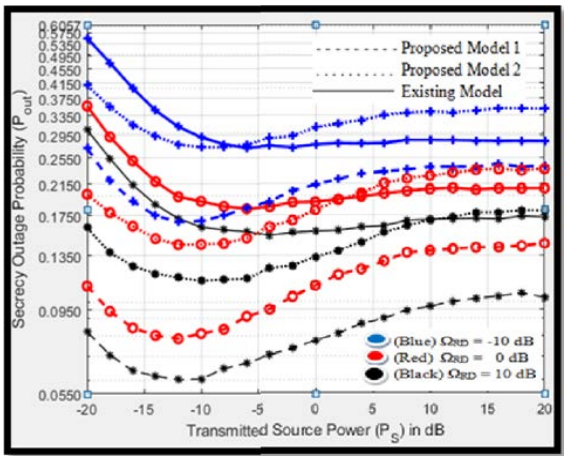

Fig.4: Plot of SOP versus Transmitted Source Power (PS)

In Fig. 4, three models are shown together. Initially, with the increase of the transmitted source power, irrespective of the models, the secrecy outage probability (SOP) decreases as the SNRs of all the relays increase. But after a certain point, with the increase of source power PS, the jamming at the eavesdropper also increases, reducing the SNR contributed by the relays; hence the SOP starts to increase. Thereafter, with the increase in PS, the signal strength at the eavesdropper increases significantly, which further compensates for the jamming at the eavesdropper. As a result, the SOP almost remains constant for a specific range. Then again, for further high values of PS, the overall SNR at the destination increase slightly to reduce the SOP. With the increase of the selected values of the relay to destination mean power, the overall SOP decreases for each and every model separately. Observing all the models, the SOP for the Proposed Model 1 is the lowest for a selected value of ΩRD The Proposed Model 1 has more number of trusted relays than the existing Model (though the same number of the untrusted relay) and less number of untrusted relay than the Proposed Model 2 (though the same number of trusted relays). Hence this results in the minimum SOP. So, the best performance for secrecy can be seen from the Proposed Model 1.

Among the other two models, the Existing Model and Proposed Model 2 have the same ratio of trusted and untrusted relays, but the number of relays is different. Initially, the SOP of the Proposed Model 2 is less than the existing model for respective selected values of ΩRD as the numbers of trusted relays are higher in Proposed Model 2 than Existing Model.

With the increase of PS, the SOP of the Proposed Model 2 starts to increase due to the presence of more untrusted relays, as it eavesdrops on the information more, as a result of which the overall SNR at the destination decreases. Hence, for higher PS, the SOP for Proposed Model 2 is higher than the Existing Model. So it observed that for a lower range of PS, the Existing Model would be more suitable than Proposed Model 2, and for a higher range of PS, Proposed Model 2 will be preferred.

It can be concluded that for models with the same ratio of trusted and untrusted relays, the number of relays would decide the best-suited model for a certain range of PS, and it can be decided as illustrated above.

A model with the ratio of trusted and untrusted relays is greater than the others will always be preferred over every range of PS. The lower range of PS for which the SOP is lower in Proposed Model 2 than that of the Existing Model will increase with the increment of selected $\Omega_{RD.}$

CASE 2

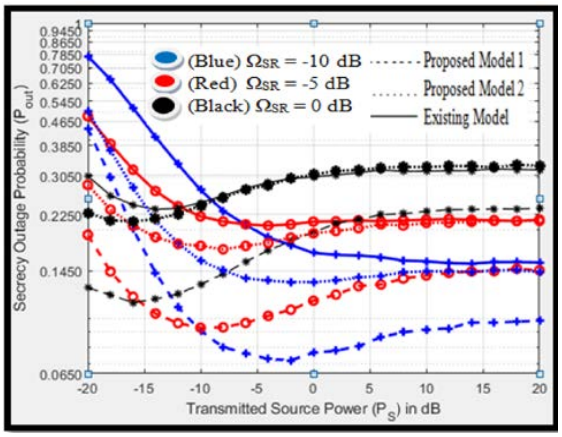

Fig.5: Plot of SOP versus Ω_{RD}

In Fig. 5, for a constant $\Omega_{SR,}$ similar nature of the SOP curve can be observed as that for the case of a constant Ω_{RD}. However, as the value of Ω_{SR} is changed to a higher value for a constant P_S, signal strength at eavesdropper improves, resulting in an increase in eavesdropper's capacity, reducing the overall SNR contributed towards the destination. This causes an increase in the SOP.

In all the models similar kind of nature can be observed. Now, for a selected value of Ω_{SR}, the SOP for the Proposed Model 1 is always lesser than other models as the ratio of trusted and

untrusted relays is higher. Similar to the previous case, for the initial and lower range of P_S, the SOP for the existing model is higher than that of Proposed Model 2. Further increase in P_S results in high eavesdropping of the information from the untrusted relays, and hence the SOP starts to increase in proposed model 2, converging with the existing model and at a higher range of PS, it becomes higher than the existing model.

So, depending on the ratio of trusted and untrusted relays along with the total number of relays, a suitable model can be given higher priority than others, making the information transmission more secure.

CASE 3

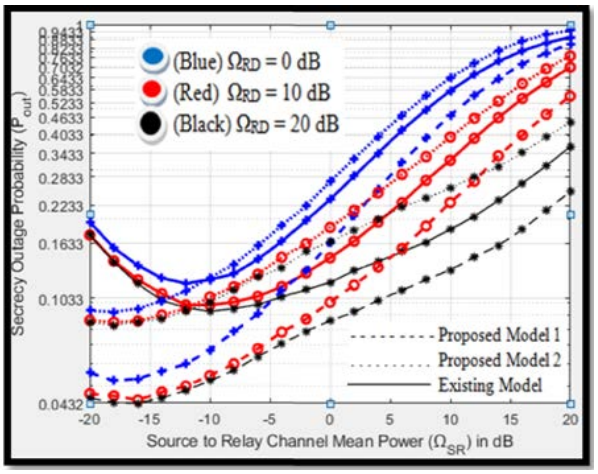

Fig.6: Plot of SOP versus Ω_{SR}

In Fig. 6, for a selected value of ΩRD, initially, with the increase of ΩSR, the overall SNR at the destination increases and the increased signal information at eavesdropper is compensated by the jamming signal.

Hence the initial decrement in SOP can be observed in all the models for a selected value of ΩRD. But from a certain point beyond, due to the higher increase in information, the jamming signal is not able to compensate, and the information at eavesdropper increase, increasing the SOP. Now for the same model, with the increase in ΩRD, the chances of eavesdropping on information reduce, hence the SOP decreases.

The Proposed Model 1 with the highest number of trusted relays and the lowest number of untrusted relays perform better where the SOP is the lowest than the Existing Model and the Proposed Model 2 under all the ranges of ΩSR for a specific selected value of ΩRD.

Likewise, all the aforementioned observation can be further justified through Fig. 6.

CASE 4

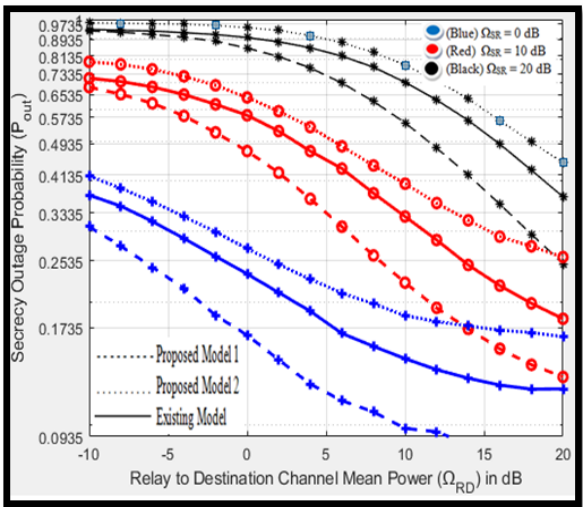

Fig. 7: Plot of SOP versus Ω_{RD}

In Fig.7, with the increase of Ω_{RD} for a selected value of Ω_{SR}, the overall SNR at the destination increases and the chances of eavesdropping of information also reduces as more information is transferred from relays to destination. Each model with the increase of Ω_{SR}, the information at the eavesdropper increases which further increases SOP. It can be justified that the performance of the Proposed Model 1 is better than others for a selected value of Ω_{SR} (Fig. 7).

The critical analysis of these results (Fig. 4 & Fig. 5) is summarized in Table 2-6.

Table: 2: Variation of SOP with P_S keeping Ω_{SR} constant

Models	Value of SOP			
Existing Model	P_S(dB)	Ω_{RD1} = -10 dB	Ω_{RD2} = 0 dB	Ω_{RD3} = 10 dB
	P_{S1} = 0	0.2750	0.1900	0.1550
	P_{S2} = 10	0.2850	0.1950	0.1650
	P_{S3} = 20	0.2800	0.1950	0.1650
Proposed Model: 1	P_{S1} = 0	0.2150	0.1100	0.0750
	P_{S2} = 10	0.2300	0.1400	0.0950
	P_{S3} = 20	0.2300	0.1450	0.1000
Proposed Model: 2	P_{S1} = 0	0.3000	0.1850	0.1350
	P_{S2} = 10	0.3350	0.2250	0.1650
	P_{S3} = 20	0.3400	0.2350	0.1750

Table: 3: Variation of SOP with P_S keeping Ω_{RD} constant

Mode	Value of SOP			
Existing Model	P_S(dB)	Ω_{SR1} = - 10 dB	Ω_{SR2} = -5dB	Ω_{SR3} = 0 dB
	P_{S1} = 0	0.1850	0.2150	0.2950
	P_{S2} = 10	0.1650	0.2150	0.3050
	P_{S3} = 20	0.1550	0.2150	0.3150
Proposed Model: 1	P_{S1} = 0	0.0850	0.1350	0.1950
	P_{S2} = 10	0.1050	0.1400	0.2250
	P_{S3} = 20	0.1150	0.1450	0.2350
Proposed Model: 2	P_{S1} = 0	0.1250	0.1950	0.2950
	P_{S2} = 10	0.1450	0.2150	0.3150
	P_{S3} = 20	0.1450	0.2250	0.3200

Table: 4: % Improvement of secrecy (or % Degradation in SOP) of Proposed Model 1 over Existing Model

P_S (dB)	% improvement					
	Ω_{RD}(dB)			Ω_{SR}(dB)		
	Ω_{RD1}= -10	Ω_{RD2}= 0	Ω_{RD3}= 10	Ω_{SR1}= -10	Ω_{SR2}= -5	Ω_{SR3} = 0
P_{S1}=0	21.81	42.10	51.61	54.05	37.20	33.89
P_{S2}=10	19.29	28.20	42.42	36.36	34.88	26.22
P_{S3}=20	17.85	25.64	39.39	25.80	32.55	25.39

Table: 5: % Improvement of secrecy (or % Degradation in SOP) of Proposed Model 2 over Existing Model

P_S (dB)	% improvement					
	Ω_{RD}(dB)			Ω_{SR}(dB)		
	Ω_{RD1}= -10	Ω_{RD2}= 0	Ω_{RD3}= 10	Ω_{SR1}= -10	Ω_{SR2}= -5	Ω_{SR3}= 0
P_{S1}=0	-9.09	2.63	12.90	32.43	9.30	0
P_{S2}=10	-17.54	-15.38	0	12.12	0	-3.27
P_{S3}=20	-21.42	-20.51	-6.06	6.45	-4.65	-1.58

Table: 6: % Improvement of secrecy (or % Degradation in SOP) of Proposed Model 1 over Proposed Model 2

P_S (dB)	% improvement					
	Ω_{RD}(dB)			Ω_{SR}(dB)		
	Ω_{RD1}= -10	Ω_{RD2} = 0	Ω_{RD3}= 10	Ω_{SR1}= -10	Ω_{SR2}= -5	Ω_{SR3} = 0
P_{S1}=0	28.33	40.54	44.44	32.0	30.76	33.89
P_{S2}=10	31.34	37.77	42.42	27.58	34.88	28.57
P_{S3}=20	32.35	38.29	42.85	20.68	35.55	26.56

CONCLUSION

In this paper, a novel scheme of destination-based jamming in a cooperative relay network is targeted. In this context, two novel models have been proposed, and their secrecy performances are observed, analyzed and further compared with the existing model under the influence of different parameters. The designed models are shown in Fig. 1 – Fig. 3, and the simulation results of all the models have been discussed through Fig. 4– Fig. 7. Through Table 2 – Table 6, the critical analyses are performed to come to a conclusion that the Proposed Model 1 always performs better than other considered system models and the dependency of the secrecy outage probability is observed under various parameters like the number of relays, the nature of relays (trusted or untrusted), the mean power of communication channel and transmitted source power. In general, when the ratio between trusted and untrusted relay increases, the secrecy outage probability decreases and when the ratio remains the same for two networks but the number of relays increases, the secrecy outage probability decreases. The comparative study of the models that are presented in this work may be extended to monitor the overall performance of a system consisting of multiple relay nodes. Further, the effect of different relay selection (trusted or untrusted) on the system can then be properly investigated. Thus, the outcome of this work will make the secrecy analysis in such a network environment more robust and compatible.

REFERENCES

1. N. Sklavos and X. Zhang (Ed.), Wireless Security and Cryptography: Specifications and Implementations.CRC Press, Boca Raton, FL, 2007
2. A.Wyner, “The wiretap channel,” Bell System Technical Journal, vol. 54, no. 8, pp. 1355–1387, 1975
3. M. Bloch, J. Barros, M. R. D. Rodrigues, and S. McLaughlin, “Wire- less information-theoretic security,” IEEE Transactions on Information Theory, vol. 54, no. 6, pp. 2515–2534, 2008.
4. N. Sklavos and X. Zhang (Ed.), Wireless Security and Cryptography: Specifications and Implementations.CRC Press, Boca Raton, FL, 2007.
5. S. Leung-Yan-Cheong and M. Hellman, “The gaussian wire-tap channel,” IEEE Transactions on Information Theory, vol. 24, no. 4, pp. 451–456, 1978.
6. Jo˜ao Barros, “Secrecy Capacity of Wireless Channels,” ISIT 2006, Seattle, USA, July 9 14, 2006.
7. Praveen Kumar Gopala, Lifeng Lai and Hesham El Gamal OH43210arXiv:cs/0610103v1[cs.IT]17Oct 2006
8. Rayleigh Flat Fading Channels’ Capacity Jun Li, Amitava Bose, and Yiqiang Q. Zhao School of Mathematics & Statistics,
9. Y. Oohama, “Relay channels with confidential messages,” IEEE Trans. on Information Theory, Nov. 2006. Submitted
10. The Relay-Eavesdropper Channel: Cooperation for Secrecy Lifeng Lai and Hesham El Gamalar Xiv: cs/0612044v1 [cs.IT] 7 Dec 2006
11. 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.
12. 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.
13. 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

14. 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.
15. Secrecy Outage Probability with Destination Assisted Jamming in Presence of an Untrusted Relay, Anurag Kumar, Shashibhushan Sharma, Department of ECE, NIT Durgapur, India.