ISSN: 2229-6948(ONLINE)
DOI: 10.21917/ijct.2014.0133

PERFORMANCE ANALYSIS OF COOPERATION SCHEMES IN EAVESDROPPER ASSISTED RELAY CHANNEL

Vaibhav Kumar Gupta[1] and Poonam Jindal[2]
Department of Electronics and Communication Engineering, National Institute of Technology Kurukshetra, India
E-mail: [1]gupta.vaibhav25@gmail.com, [2]poonamjindal81@yahoo.co.in

Abstract

The prominence of the wireless communication has been urging the monotonically increasing demand of security and privacy. In wireless systems, the notion of perfect secrecy of information with respect to illegitimate nodes can be ensured via physical layer security (PLS) techniques. Unfortunately, they can be made less effective if source-eavesdropper wiretap channel is better than the main source-receiver channel. The various node cooperation schemes can be employed to combat this limitation where a relay node assists the communication to improve the performance significantly. In this paper, a four node wireless communication system consisting of a source, a destination, a relay and an eavesdropper as wire-tapper has been considered. The performance of the traditional cooperation schemes in terms of secrecy rate has been investigated with a different scenario where relay node helps the eavesdropper to deteriorate the secrecy rate. In addition, since legitimate receiver can overhear the transmission of relay, it favours the achievable secrecy rate. We formulate an analytical expression of conditional secrecy outage probability for the investigated system. From the obtained simulation results, it has been observed that secrecy rate is monotonically increases with path loss index. Furthermore, the proper selection of the system parameters leads to enhance the secrecy performance of the system even if relay pertains to degrade the performance. Amplify-and-forward, cooperation, decode-and-Forward, secrecy rate, relay.

Keywords:

Amplify-and-Forward, Cooperation, Decode-and-Forward, Secrecy Rate, Relay

1. INTRODUCTION

Confidentiality of data is a fundamental and crucial requirement for any wireless network due to significant growth in wireless applications in contemporary times. The performance of wireless communication has been degraded significantly due to open and shared medium and makes the system vulnerable to security threats. With the drastically increasing demand of wireless communication in civilian, critical applications and personal data transfer such as in military, on-line transactions etc. at global level, PLS has been aroused as a new paradigm now a days to tackle the security issues. On the basis of characteristic attributes, the various prevalent approaches to improve secrecy at physical layer can be grouped into five categories namely information-theoretic secrecy capacity, and the code, power, channel, and signal detection techniques. Earlier, cryptographic algorithms were used for security at higher network layers [1]. But, they are computationally complex and depend upon the private key encryption-decryption. An information-theoretic approach at the physical layer can be used for secure communication without using key encryption and can't be hampered even if sufficient computational power is available at the adversary. PLS exploits the channel state information (CSI) or characteristics of transmission medium to improve the intended receiver's channel quality. The most commonly used PLS schemes are cooperative jamming (CJ) and cooperation schemes. Decode-and-forward (DF), amplify-and-forward (AF) and compress-and-forward (CF) are generally used node cooperation schemes for PLS. In the cooperative jamming scheme, an artificial jamming signal that is independent of source is transmitted to create interference at eavesdropper. The overall communication process takes place in a single stage. When source transmits its message, the relay node acting as jammer interferes in order to confuse the eavesdropper without influencing the destination signal. In 1971, Meulen has introduced the relay channel and further, Cover and Gamal have proposed a number of relaying schemes and evaluated the secrecy capacity of degraded version of relay channel in [2], [3]. In 1975, Wyner worked in the direction of PLS for single point-to-point communication. A system model was considered having perfect confidential communication between the source and legitimate destination node pair in presence of an eavesdropper who is kept ignorant of the transmitted information between intended pair of nodes. However, the traditional physical layer based security can be compromised by channel conditions; if the main channel is worse than eavesdropper's channel, the secrecy capacity is typical zero as it cannot be negative [4], [5]. Csiszar and Korner generalized the transmission of confidential messages over broadcast channels to the wireless medium and multiuser environment in [6]-[8]. A single antenna system fails if signal degradation is observed after a certain distance. In that case, multiple antenna system but with transmit power constraints have to be considered. A solution has been investigated to mitigate this limitation by taking advantage of multiple antenna systems, e.g. multiple input and multiple output system (MIMO) in [9], [10]. But, due to high cost and large size, network nodes with multiple antennas are hardly available. To overcome these limitations, system with single-antenna nodes can be used as multiple-antenna systems by making use of node cooperation scheme [11]. The secrecy aspect of relay channel was investigated considering relay can not only send message to assist the transmission but also can learn some knowledge about the transmitted information to wire-tap the relay channel in [12]. In [13], a novel hybrid cooperation scheme has been proposed to analyse secrecy of the semi-deterministic relay channel. In [14], secrecy rate was evaluated using rate splitting technique with the full-duplex source node with DF scheme and having feedback from the trusted relay node with CF scheme. In [7], cooperation for secrecy of relay-eavesdropper channel was discussed in which relay assist the intended transmission but was kept ignorant of transmitted information. Further, Yuksel and Erkip investigated the secrecy with untrusted relay node assisting the eavesdropper channel not the main channel in [15]. However, it was shown that as the relay node has some knowledge about the transmitted

signal between legitimate nodes, it is favourable to secrecy rate as destination also can overhear the transmission of relay.

In this paper, the secrecy rate of relay channel from a different perspective has been analysed. Most of the previous studies have consider a system spans over a model constituting four nodes a source, a destination, an eavesdropper and a trusted relay which outperforms to enhance the perfect secrecy. In this scenario, the relay focuses to aid the wire-tapper to impair the achievable secrecy since the relay has knowledge about the source information. Different cooperation schemes can be employed at the relay node to hamper the communication secrecy. All the channels are assumed to be AWGN with thermal noise variance σ^2. The comparative analysis of the system performance in terms of secrecy rate with respect to system parameters has been presented for various cooperation protocols i.e. DF, AF and CF. Traditionally, when relay assist the source-destination transmission, DF protocol provides better secrecy then CF if relay is situated in the proximity of source node and vice-versa [16]. But, the above result is not convincing if the relay helps the eavesdropper instead of the destination. We derived a close-form analytical expression for conditional secrecy outage probability for DF protocol in the addressed wire-tapper assisted scenario.

The rest of the paper is organised as follows. Section 2 introduces physical layer security and cooperative communication approaches. Section 3 involves the addressed system description and the assumptions. In section 4, we study about the AF, DF and CF cooperative strategies and their secrecy rates. In section 5, the mathematical formula for conditional secrecy outage probability has been derived for the investigated system. Finally, simulation outcomes are presented in section 6, and section 7 includes the possible conclusions.

2. PHYSICAL LAYER SECURITY AND COOPERATIVE COMMUNICATION

Secure transmission of data through wireless medium is a rigorous issue. Physical layer security (PLS) has been emerging as recent paradigm to tackle these issues at physical layer instead of ancient cryptographic approach at upper layers. Cryptography, a laborious approach, demands complex calculation. It pertains solely on encryption-decryption of data using secret pseudorandom key. However, the adversary can obtain transmission information if it has large computational power. PLS is an information theoretic based approach for perfect security. PLS explores the characteristics of wireless transmission medium which are commonly treated as impairments such as fading, path loss and noise to achieve perfect secrecy. PLS approach can be divided in five wide categories as depicted in Fig.1 [17].

Historically, Shannon devised the concept of theoretical secure capacity in communication networks. In pessimistic scenario, both the legitimate receiver and the adversary can access to the transmitted information from the source. Then, the achievable secrecy capacity is given by $max[I(S;D) - I(S;E)]$, where $I(S;D)$ denotes the mutual information between source and intended destination and $I(S;E)$ is the mutual information between source and adversary. The coding based technique for PLS are used to prevent eavesdropping and jamming of transmitted signal by making use of spread spectrum coding and error correction coding respectively. The power based techniques are beneficial to tackle the jamming as well as security issues. In the presence of jammer, it can be possible to detect the signal by employing directional antenna. If intended receiver channel has degraded response than that of eavesdropper channel, perfect secrecy can be entertained implementing artificial noise approach. An artificial noise signal is transmitted to reduce the power level of received signal at eavesdropper without affecting the destination signal.

The channel based schemes have been invented to improve security of data by exploiting salient features of wireless channel. Each legitimate source has its unique RF fingerprint. The RF fingerprinting system compares the fingerprint extracted from each received signal with the fingerprints available in its database. It issues a contender alert if any discrepancy is detected.

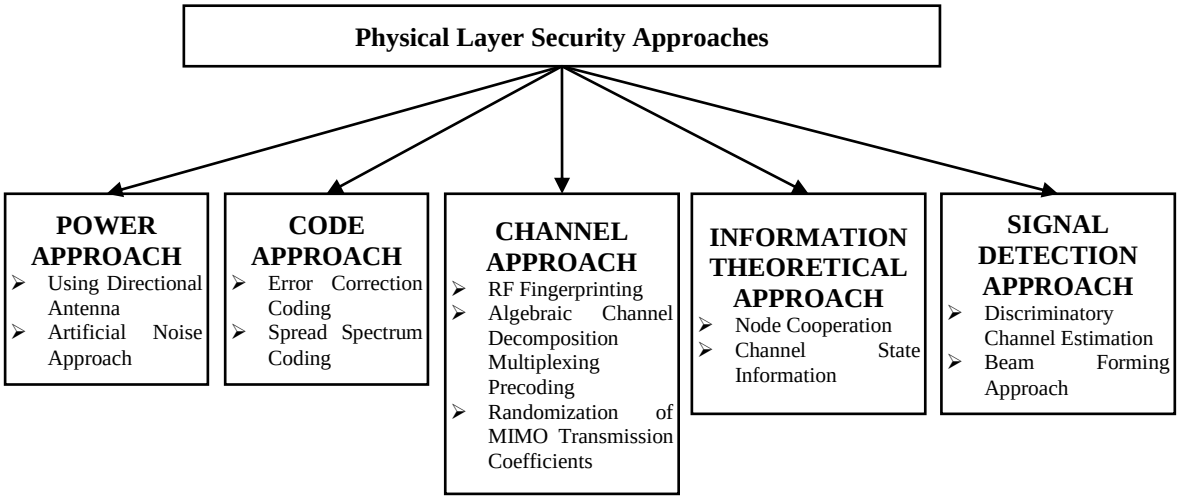

Fig.1. Physical Layer Security Approaches

In fact, the research on cooperative communication has been proliferated since a decade. The reliable transfer of message signal between intended pair of nodes can be assured with the utility of node cooperation schemes as multiple terminals helping each other in communication. It can be made feasible to achieve perfect secrecy in suspicious situation where intruder's channel is better than receiver's channel via cooperation strategies [7]. The cooperative communication occurs in two phases. In first phase, the source sends message signal to the relay and then in second phase, the relay sends source signal to the intended destination. So, there is a chance that the transmitted signal can be eavesdropped in either of the two phases. On the basis of methodology used, the cooperative strategies can be broadly classified in two groups as shown in Fig.2.

- Oblivious Cooperation
- Active Cooperation

A. Oblivious Cooperation: In this cooperation mechanism, the relay does not have any knowledge about the transmitted signal from the source. In this procedure, the relay node deteriorates the eavesdropper's channel without interfering the destination channel sending dummy signal or artificial noise. Hence, noise and interference, which are treated as unwanted effects for wireless environment, can be advantageous for privacy and secrecy requirements.

B. Active Cooperation: As per the literal meaning of cooperation, it can be experienced in traditional sense, i.e., the relay assists the legitimate destination by strengthening the intended receiver channel. In this cooperation mechanism, the relay has knowledge about the transmitted signal from the source.

3. SYSTEM DESCRIPTION AND ASSUMPTIONS

In this section, we describe a network model to represent the wireless system under investigation. As depicted in Fig.3, the system consist of a source (S) that communicates with a destination (D) and a relay node (R) which intends to assist the eavesdropper (E) treated as the wire-tapper.

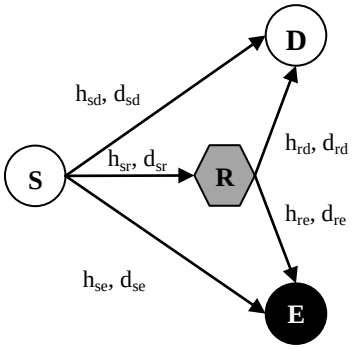

Fig.3. System model framework

We represent the channel gain from source to destination, source to relay, source to eavesdropper, relay to destination and from relay to eavesdropper by h_{sd}, h_{sr}, h_{se}, h_{rd}, $h_{re.}$ respectively. The distance between different pairs of nodes as source and destination, source and eavesdropper, jammer and destination and jammer and eavesdropper are $d_{SD,}$ $d_{SE,}$ $d_{RD,}$ d_{RE} respectively. Some assumptions are taken in to consideration as the source has constant transmission power *Ps* and the relay has a variable transmission power $P_r \in [0, P_s]$. Each node is having a single omnidirectional antenna element. For all the nodes, the additive white Gaussian noise is distributed with zero mean and variance σ^2. All the channels undergo Rayleigh quasi-static fading. Only distance dependent term and path loss index have been considered in the channel gain coefficient h_{xy} having Gaussian distribution:

$$h_{xy} \sim CN\left(0,1/d_{xy}^{n/2}\right)$$

where, n denotes the path loss index and d_{xy}, $x = S, R$ & $y = R, D, E$, $x \neq y$, represents the Euclidian distance between node x and node y. Also, the network is employed with a time division access protocol that bounds the source to transmit message only during the first time slot and the relay has to transmit message during the second slot only.

The length of the first and the second time slots are equal. All the legitimate nodes have full channel state information of all the communication channels. Moreover, it is globally known that which cooperative strategy is going to be implemented by the relay.

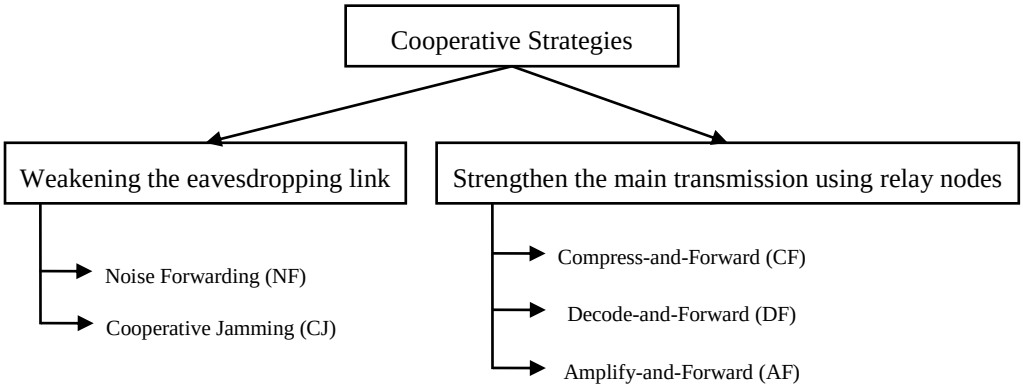

Fig.2. Classification of Cooperative Strategies

During the first time slot, signal received at different nodes are,

$$y_k^{(1)} = \sqrt{P_s h_{sk} s(t)} + n_k^{(1)} \quad (1)$$

where, $s(t)$ is the signal transmitted by source node, $n_k^{(1)}$ is the noise at k^{th} node in first time slot for $k = R, E, D$.

In the second time slot, it is noteworthy that the source remains idle. Hence, signal received at different nodes are,

$$y_k^{(2)} = \sqrt{P_r h_{Rk} r(t)} + n_k^{(2)} \quad (2)$$

where, $r(t)$ is the signal transmitted by relay, $n_k^{(2)}$ is the noise at k^{th} node in second time slot for $k = E, D$.

When node x communicates with node y through the channel, the exponentially distributed instantaneous SNR with mean $\bar{\gamma}_{xy}$ can be formulated as,

$$\gamma_{xy} = \frac{P_x |h_{xy}|^2}{\sigma^2} \quad (3)$$

where, P_x is the available power of node x to transmit the signal and $\bar{\gamma}_{xy} = \frac{P_x}{\sigma^2 . d_{xy}^n}$. The probability density function of random valued SNR is expressed as,

$$f_\gamma(\gamma_{xy}) = \frac{1}{\bar{\gamma}_{xy}} e^{-\frac{\gamma_{xy}}{\bar{\gamma}_{xy}}} \quad (4)$$

4. COOPERATIVE SCHEMES AND THEIR INSTANTANEOUS SECRECY RATES

In this section, the achievable secrecy rates of the cooperation schemes particularly DF, AF and CF, in pessimistic scenario where relay helps the eavesdropper to deteriorate the secrecy, along with direct transmission without relay (DTWR) approach. The instantaneous SNR for the links from S to D, S to R, S to E, R to D and from R to E are denoted by γ_{sd}, γ_{sr}, γ_{se}, γ_{rd} and γ_{re} respectively throughout the paper. For the case of single eavesdropper, analytically achievable secrecy rate is given by,

$$R_S = \max\{0, I_d - I_e\} = (I_d - I_e)^+ \quad (5)$$

where, I_d is the achievable information rate of the source-destination channel and I_e is the achievable information rate of the source-eavesdropper channel.

4.1 DIRECT TRANSMISSION WITH RELAY OFF (DTRO)

In DTRO, the relay does not participate in communication and can be treated as traditional wire-tap transmission [4]-[6]. We consider it as a special case of all the relaying strategies as the source terminal sends encoded message using its codebook directly to the intended destination with maximum available transmission power. The DTRO relaying achieves a secrecy rate,

$$R_s^{Dir} = \left[I_d^{Dir} - I_e^{Dir} \right]^+ \quad (6)$$

where,

$$I_d^{Dir} = \frac{1}{2}\log_2(1+\gamma_{sd}) \quad (7)$$

$$I_e^{Dir} = \frac{1}{2}\log_2(1+\gamma_{se}) \quad (8)$$

It is noteworthy, the factor ½ accounts for the node participation only in one phase out of two phases.

4.2 DECODE AND FORWARD

In DF relaying, the source terminal sends encoded information signal towards the relay in first time slot. Then, this signal is successfully decoded by the relay and again encodes it with different code from codebook that is similar to the source and forwards the message. Moreover, it is considered that DF is applicable significantly only for the condition $d_{sd,} > d_{sr}$.

The achievable secrecy rate when relay is employed with DF relaying can be stated as follows [15],

$$R_s^{DF} = \begin{cases} \min_\alpha \frac{1}{2}\left[I_d^{DF} - I_e^{DF} \right]^+, & d_{sr} < d_{sd} \\ R_s^{Dir}, & d_{sr} \geq d_{sd} \end{cases}$$

where, the relay power scaling factor for DF, $\alpha \in [0, 1]$ as the relay favours the wire-tapper to pertain unreliable system via scaling its power, and

$$I_d^{DF} = \min\left\{ \frac{1}{2}\log_2(1+\gamma_{sr}), \frac{1}{2}\log_2(1+\gamma_{sd})(1+\alpha\gamma_{rd}) \right\} \quad (9)$$

$$I_e^{DF} = \min\left\{ \frac{1}{2}\log_2(1+\gamma_{sr}), \frac{1}{2}\log_2(1+\gamma_{se})(1+\alpha\gamma_{re}) \right\} \quad (10)$$

4.3 AMPLIFY AND FORWARD

In the AF relaying, source broadcasts in first slot and the scaled version of received signal is forwarded by relay in second time slot. The input- output signal relation for relay can be described as,

$$S_r^{(out)} = \sqrt{P_r S_r^{(in)}} \quad (11)$$

With $P_r \in \left[0, \frac{P_R}{1+\gamma_{sr}}\right]$ and scaling factor $\mu \in \left[0, \frac{1}{1+\gamma_{sr}}\right]$.

For AF scheme, the secrecy rate can be formulated as below [15]

$$R_s^{AF} = \min_\mu \frac{1}{2}\left[I_d^{AF} - I_e^{AF} \right]^+ \quad (12)$$

where, $I_d^{AF} = \frac{1}{2}\log_2\left(1 + \gamma_{sd} + \frac{\mu\gamma_{rd}.\gamma_{sr}}{1+\gamma_{sr}+\mu\gamma_{rd}}\right)$

$$I_e^{AF} = \frac{1}{2}\log_2\left(1 + \gamma_{se} + \frac{\mu\gamma_{re}.\gamma_{sr}}{1+\gamma_{sr}+\mu\gamma_{re}}\right)$$

4.4 COMPRESS AND FORWARD

In CF scheme, the relay re-encodes the received signal after quantization (compression) and forwards it to the eavesdropper

with such a power level that contender receives it perfectly. When the relay employed with CF, the secrecy rate [15],

$$R_S^{CF} = \min_{\lambda\in[0,1]} \frac{1}{2}\left[I_d^{CF} - I_e^{CF}\right]^+ \quad (13)$$

where,

$$I_d^{CF} = \begin{cases} \frac{1}{2}\log_2\left(1+\gamma_{sd}+\frac{\gamma sr}{1+M}\right), & if\ (d_{sd} < d_{se}\ and\ d_{rd} < d_{re}) \\ \frac{1}{2}\log_2(1+\gamma_{sd}), & otherwise \end{cases}$$

$$I_e^{CF} = \frac{1}{2}\log_2\left(1+\gamma_{se}+\frac{\gamma_{sr}}{1+M}\right) \quad (14)$$

and

$$M = \frac{1+\gamma_{se}+\gamma_{sr}}{(1+\gamma_{se})\lambda.\gamma_{re}} \quad (15)$$

In particular, the secrecy rate will be minimized optimally for $\lambda = 1$.

5. SECRECY OUTAGE PERFORMANCE FOR DF RELAYING IN PESSIMISTIC SCENARIO

In this section, the secrecy outage performance in terms of conditional secrecy outage probability has been analyzed from a distrustful perspective where the relay helps the eavesdropper. The close form expression for conditional secrecy outage probability has been evaluated particularly for DF cooperation scheme in given network environment with feasible assumption that the main link is of worse quality and the source-relay channel has better performance characteristics. These assumptions can be combined analytically in form of an equation,

$$\gamma_{sr} > (\gamma_{sd} + \alpha\gamma_{rd}) \quad (16)$$

The secrecy outage probability (SOP) is defined as the probability of message cannot be secured properly against eavesdropping which occurs when maximal information rate over the eavesdropper link is less than the capacity of the link.

The SOP for DF scheme can be stated as [18],

$$P_{SOP}^{(DF)}(R) = P_r\begin{bmatrix} \min\{\log_2(1+\gamma_{sr}), \log_2(1+\gamma_{sd}+\gamma_{rd})\} \\ < \log_2(1+\gamma_{se}+\gamma_{re}) + R \end{bmatrix}. \quad (17)$$

Similarly, we can express the SOP for the considered case with α ∈ [0, 1]

$$P_{SOP}^{(DF)}(R) = P_r\begin{bmatrix} \min\{\log_2(1+\gamma_{sr}), \log_2(1+\gamma_{sd}+\alpha\gamma_{rd})\} \\ < \log_2(1+\gamma_{se}+\alpha\gamma_{re}) + R \end{bmatrix} \quad (18)$$

The conditional secrecy outage probability (CSOP) is defined as SOP for given values of γ_{sr}, γ_{sd} and γ_{rd}. Therefore, CSOP can be written as,

$$P_{CSOP}^{(DF)}\left(R\big|_{\gamma_{sr},\gamma_{sd},\gamma_{rd}}\right) = P_r\begin{bmatrix} \min\{\log_2(1+\gamma_{sr}), \log_2(1+\gamma_{sd}+\alpha\gamma_{rd})\} \\ < \log_2(1+\gamma_{se}+\alpha\gamma_{re}) + R\big|_{\gamma_{sr},\gamma_{sd},\gamma_{rd}} \end{bmatrix} \quad (19)$$

Define, $\gamma_d^{'} = \gamma_{sd} + \alpha\gamma_{rd}$ and $\gamma_e^{'} = \gamma_{se} + \alpha\gamma_{re}$

Then, we can write from Eq.(19),

$$P_{CSOP}^{(DF)}\left(R\big|_{\gamma_{sr},\gamma_{sd},\gamma_{rd}}\right) = P_r\begin{bmatrix} 2^{-R}\left(1+\min\left(\gamma_{sr},\gamma_d^{'}\right)\right) \\ -1 < \gamma_e^{'}\big|_{\gamma_{sr},\gamma_{sd},\gamma_{rd}} \end{bmatrix} \quad (20)$$

Since, our assumption in Eq.(16) implies that $\min\left(\gamma_{sr},\gamma_d^{'}\right) = \gamma_d^{'}$. Hence,

$$P_{CSOP}^{(DF)}\left(R\big|_{\gamma_{sr},\gamma_{sd},\gamma_{rd}}\right) = P_r[2^{-R}\left(1+\gamma_d^{'}\right) - 1 < \gamma_e^{'}\big|_{\gamma_{sr},\gamma_{sd},\gamma_{rd}}]$$

$$= \int_2^{\infty} 2^{-R}\left(1+\gamma_d^{'}\right) - 1 f\gamma_e^{'}\left(\gamma_e^{'}\right) d\gamma_e^{'}$$

$$= \frac{1}{\alpha\bar{\gamma}_{re} - \bar{\gamma}_{se}}\left[\alpha\bar{\gamma}_{re}e^{\frac{-\left(2^{-R}\left(1+\gamma_d^{'}\right)-1\right)}{\alpha.\bar{\gamma}_{re}}} - \bar{\gamma}_{se}e^{\frac{-\left(2^{-R}\left(1+\gamma_d^{'}\right)-1\right)}{\bar{\gamma}_{se}}}\right]$$

$$P_{CSOP}^{(DF)}\left(R\big|_{\gamma_{sr},\gamma_{sd},\gamma_{rd}}\right) =$$

$$\frac{1}{\alpha\bar{\gamma}_{re} - \bar{\gamma}_{se}}\left[\alpha\bar{\gamma}_{re}e^{\frac{-\alpha\left(2^{-R}\left(1+\gamma_{sd}+\alpha\gamma_{rd}\right)-1\right)}{\bar{\gamma}_{re}}} - \bar{\gamma}_{se}e^{\frac{-\left(2^{-R}\left(1+\gamma_{sd}+\alpha\gamma_{rd}\right)-1\right)}{\bar{\gamma}_{se}}}\right]$$

6. SIMULATION OUTCOMES

In this section, the simulation outcomes are discussed which were performed to investigate the effect of the cooperation strategies on secrecy performance of network with respect to different system parameters.

To illustrate the effect of cooperation schemes, a one-dimensional model in which a source, a destination, an eavesdropper and a relay are placed linearly for line-of-sight communication between various nodes. It is assumed that intended source sends a confidential message to the legitimate destination in presence off contender eavesdropper node and a relay which assists the contender. The fixed distance between source and destination is 1m and the source power is fixed at $P_S = 3.16$W.

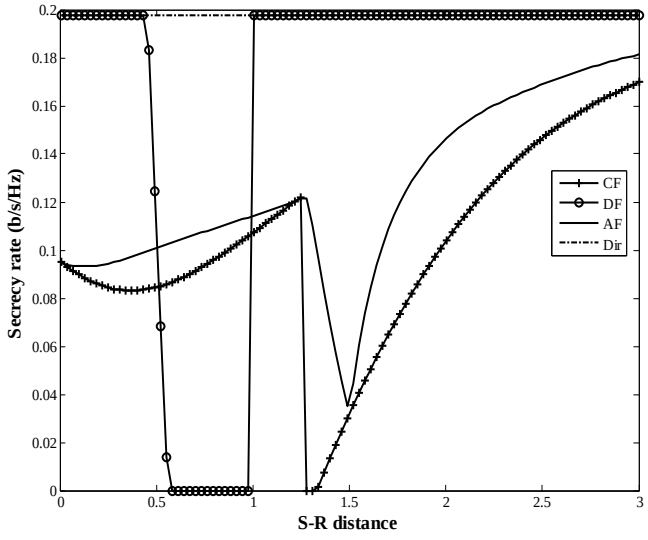

Fig.4. Secrecy rate as a function of distance between the source and the relay for AF, DF, CF and DR

Firstly, the secrecy rate of DF, AF and CF are compared with the secrecy rate of direct transmission when position of relay is varied up to 3m. The relay has fixed power $P_r = P_S$, the path loss index is $n = 2$ and the distance between source and eavesdropper is fixed at 1.5m. Secrecy rate as a function of distance between the source and relay is shown in Fig.4. From the obtained result, it is observed that the secrecy performance of CF scheme is most severely except, when the relay is situated in the proximity of D between S and D, the secrecy rate with DF scheme is zero. Otherwise, DF protocol provides best performance out of the three protocols.

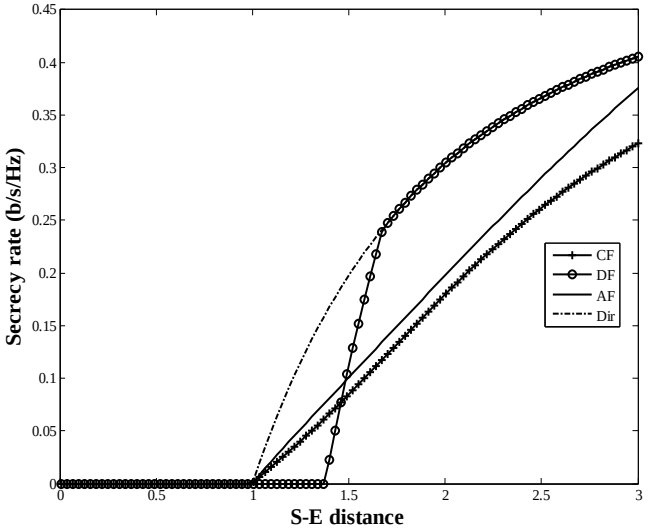

Fig.5. Secrecy rate as a function of eavesdropper position from the source

In the second case, the relay is located at the centre in between S and D and the position of the eavesdropper is changed up to 3m from S. The relay has fixed power $P_r = P_S$, the path loss index is $n = 2$. It is depicted in Fig.5 that no scheme provide positive secrecy rate if eavesdropper is in between the S and D as relay assist the eavesdropper , relay-eavesdropper link is better than relay-destination link. The secrecy rate using DF protocol at the relay is maximum and equal to direct transmission if $d_{SE} > 1.5$m.

Next, the variation of the secrecy rate with the relay power has been plotted for three different location of relay i.e. $d_{SR} = 0.3$, $d_{SR} = 0.8$, $d_{SR} = 1.3$ in Fig.6. The relay power is varied up to $P_S = 3.16$W, the path loss index is $n = 2$ and the distance between source and eavesdropper is fixed at 1.5m. It can be deduced that secrecy rate is highest for AF and lowest for DF with no effect of the relay power for $d_{SR} = 1.3$. With the increasing relay power, the secrecy rate for AF and CF decreases exponentially but remains constant for DF.

Finally, we investigated the effect of path loss index on the secrecy rate of the DF, AF and CF cooperative schemes respectively as shown in Fig.7, Fig.8 and Fig.9. The secrecy rate as a function of relay distance has been plotted for different values of path loss index $n = 2, 3, 4$. The other system parameters are $d_{SR} = 1$, $d_{SE} = 1.5$, $P_r = P_S = 3.16$W. The performance of the system increases as path loss index increases in terms of secrecy rate which contradicts the behaviour of cooperative strategies in classical scenario.

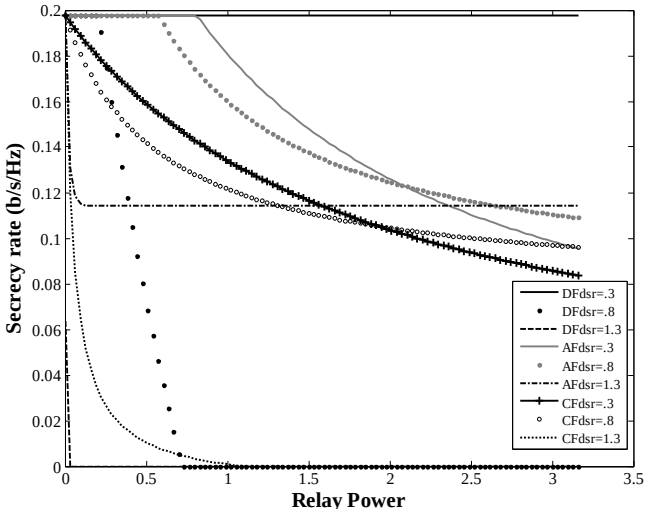

Fig.6. The variation of secrecy rate of DF, AF and CF with the Relay Power

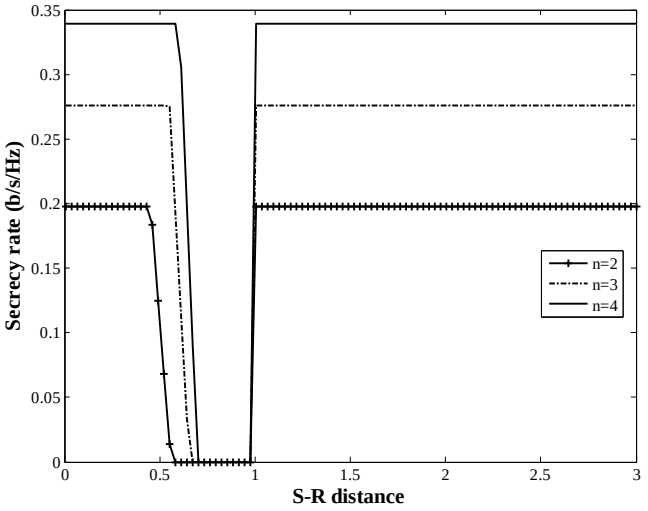

Fig.7. Secrecy rate of DF vs S-R distance, with path loss index as parameter

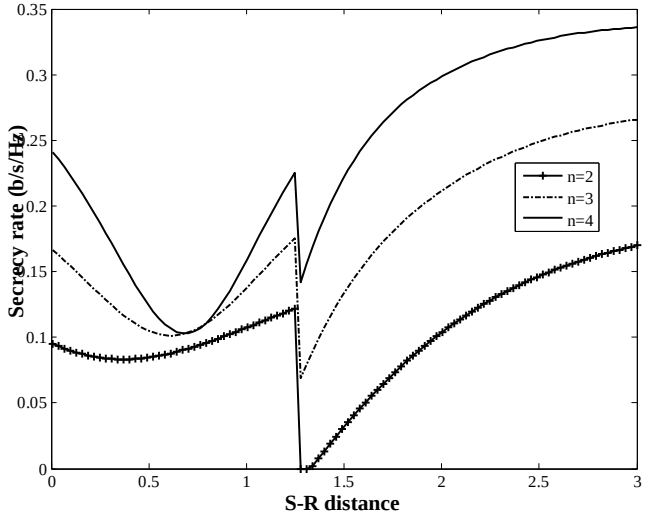

Fig.8. Secrecy rate of AF vs S-R distance, with path loss index as parameter

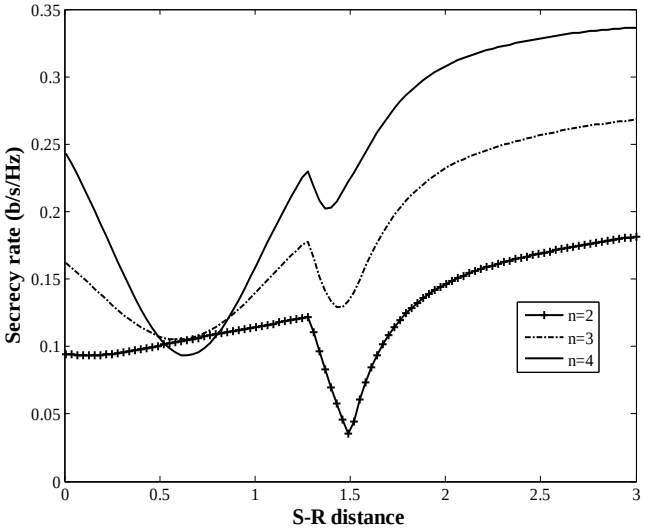

Fig.9. Secrecy rate of CF vs S-R distance, with path loss index as parameter

7. CONCLUSION

Physical layer security technique based on cooperation scheme has been explored in the present work. The performance analysis of AF, DF, CF and direct transmission in terms of attainable secrecy rate has been investigated, considering a four-node network model with different scenario where the relay favours the wire-tapper to reduce the reliability of transmission. An interesting fact was observed that secrecy rate increases with path loss index in the considered relay link. Also, a close-form expression for conditional secrecy outage probability for DF scheme is derived for the addressed system. The impact of the schemes, in considered scenario, is not like that of in traditional scenario where relay assisted main channel. Furthermore, we deduced that DF outperforms of the three schemes if relay is located in the vicinity of the source. However, we can optimise the secrecy performance with proper selection of system parameter such as location of adversary, relay and scaling of relay power.

REFERENCES

[1] Nicolas Sklavos and Xinmiao Zhang, "*Wireless Security and Cryptography: Specifications and Implementations*", CRC Press, 2007.

[2] Edward C. Van Der Meulen, "Three-Terminal Communication Channels", *Advances in Applied Probability*, Vol. 3, pp. 120-154, 1971.

[3] T. M. Cover and A. E. Gamal, "Capacity Theorems for the Relay Channel", *IEEE Transactions on Information Theory*, Vol. 25, No. 5, pp. 572-584, 1979.

[4] D. Wyner, "The Wire-Tap Channel", *Bell System Technical Journal*, Vol. 54, No. 8, pp. 1355-1387, 1975.

[5] S. K. Leung-Yan-Cheong and M. E. Hellman, "The Gaussian wire tap channel", *IEEE Transactions on Information Theory*, Vol. 24, No. 4, pp. 451-456, 1978.

[6] I. Csiszár and J. Körner, "Broadcast channels with confidential message", *IEEE Transactions on Information Theory*, Vol. 24, No. 3, pp. 339-348, 1978.

[7] L. Lai and H. El Gamal, "The Relay-Eavesdropper Channel: Cooperation for Secrecy", *IEEE Transactions on Information Theory*, Vol. 54, No. 9, pp. 4005- 4019, 2008.

[8] Yingbing Liang, H. V. Poor and S. Shamai, "Secure Communication over fading channels", *IEEE Transactions on Information Theory*, Vol. 54, No. 6, pp. 2470-2492, 2008.

[9] Martin Haenggi, "The secrecy graph and some of its properties", *Proceedings of IEEE International Symposium on Information Theory*, pp. 539-543, 2008.

[10] Pedro C. Pinto, Joao Barros and Moe Z. Win, "Secure Communication in Stochastic Wireless Networks", *Computing Research Repository*, 2010.

[11] S. Goel, V. Aggarwal, A. Yener and R. Calderbank, "Modeling Location Uncertainty for Eavesdroppers: A Secrecy Graph Approach", *Proceedings of IEEE International Symposium on Information Theory*, pp. 2627-2631, 2010.

[12] Y. Oohama, "Coding for relay channels with confidential messages", *Proceedings of IEEE Information Theory Workshop*, pp. 87-89, 2001.

[13] A. Sonee and S. Salimi, "A New Achievable Rate Equivocation Region for the Relay-Eavesdropper Channel", *Proceedings of 18th Iranian Conference on Electrical Engineering*, pp. 188-193, 2010.

[14] Ma Yayan, Bao Jing, Zhao Junxi and Wang Bao-Yun, "Achievable secrecy rate of the relay-eavesdropper channel with generalized feedback", *Proceedings of International Conference on Wireless Communications and Signal Processing*, pp. 1-4, 2011.

[15] M. Yuksel and E. Erkip, "Secure Communication with a Relay Helping the Wire-tapper", *IEEE Information Theory Workshop*, pp. 595-600, 2007.

[16] G. Kramer, M. Gastpar and P. Gupta, "Cooperative Strategies and Capacity Theorems for Relay Networks", *IEEE Transactions on Information Theory*, Vol. 51, No. 9, pp. 3037-3063, 2005.

[17] Yi-Sheng Shiu, et. al., "Physical Layer Security in Wireless Networks: A Tutorial", *IEEE Wireless Communications*, Vol. 18, No. 2, pp. 66-74, 2011.

[18] F. Gabry, R. Thobaben and M. Skoglund, "Outage performance and power allocation for decode and forward relaying and cooperative jamming for the wiretap channel", *Proceedings of IEEE International Conference on Communications Workshops*, pp. 1-5, 2011.