ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 7, July 2015

Secrecy Rate Maximization under Improved Relay Selection with Different Coding Schemes for Cooperative Wireless Network

Akanksha Rai[1], Mrs. Rupali Phatak[2]

Dept. Electronics and Communication Engg., Medicaps Institute of Technology and Management, Indore, India[1,2]

Abstract: Wireless communications system strategies are required that be dependent on the impending of the physical (PHY) layer to consent a transmitter-receiver pair communicate securely in the attendance of one or additional eavesdroppers. Communication is accomplished with the help of numerous trusted relays, via the amplify-and-forward (AF) or decode-and-forward (DF) protocol, and presumptuous knowledge of global channel state information (CSI). As an alternative, of dealing with information-theoretic security, we assume that eavesdroppers have bounded resources, and therefore we need to assure that the transmitted information is computationally secure; this is shown to impose constraints on the maximum power of the signals received by the eavesdroppers. Cooperative structures are a means to increase the performance of secure wireless communications. In this paper, we propose an improved relay selection scheme, based on source-eavesdropper channel SNR restriction, The first scheme tries to reduce the overheard information at the eavesdroppers by choosing the relay having the lowest instantaneous SNR to them both between source to relay (ER) and relay to desitnation (RE). The second is a conventional selection relaying one which seeks the relay having the highest SNR to the destination. Various DF (Convlution Codes, RS codes, Turbo Codes) relaying is used in order to find the best relaying technique. Performance has been studied in terms of secrecy rate, outage probability and average error probability (Symbol and bit error rates). Simulations shows that the proposed scheme outperforms in terms of the secrecy rate and error rate at the destination when compared to techniques in the literature.

Keywords: Cooperative Communication; Cooperative Secrecy; Cooperative diversity; Multiple Eavesdropper; Amplify & Forward; Decode & Forward; Maximum ratio combining algorithm; Best Relay Selection Scheme.

I. INTRODUCTION

In wireless networks, the privacy and security issues have aroused much interest and attention due to the broadcast nature of wireless channels. In recent years, physical(PHY) layer security has attracted considerable attention. By using an information-theoretic point of view, its basic idea is to exploit the physical characteristics of the wireless channel so that the source messages can be transmitted securely. Wyner introduced the wiretap channel in [1], in which a source wishes to transmit confidential messages to a destination while keeping the messages as secret as possible from a wiretapper. The maximum rate at which a source can transmit to its destination in the presence of an eavesdropper, named the secrecy capacity. In [2], Wyner's approach was extended to the transmission of confidential messages over broadcast channels. However, the secrecy capacity is affected by the channel conditions between the source and the destination and that of the source and the eavesdroppers. The secrecy rate is typically zero [1], [2] when the channel conditions between source and destination is worse than that of source and eavesdroppers.

By taking advantage of multiple antenna systems, some recent work, such as multiple-input multiple-output (MIMO) [3], single-input multiple-output (SIMO) [4], and multiple input single-output (MISO) [5] systems, has been proposed to overcome this limitation. Due to the cost and size limitations, multiple antennas may not be available at network nodes. In such scenarios, node cooperation is an effective way to enable single-antenna nodes to enjoy the benefits of multiple-antenna systems.

Thus, a low cost approach to increase the secrecy capacity by exploiting/mitigating channel effects is node cooperation via relays [6]-[10]. In [6], a four-node system model was considered (i.e., source, destination, eavesdropper and relay), in which the relay transmits a noise signal that is independent of the source signals such that the eavesdropper is confounded. In [7]-[9], the authors considered a scenario in which a source communicates with a destination with the help of multiple relays in the presence of one or more eavesdroppers, and the extended version was recently proposed in [10]. Three cooperative schemes, decode-and-forward (DF)[7], amplify and-forward (AF)[8] and cooperative jamming (CJ)[9], were studied to improve the achievable secrecy rate, or minimize the total transmit power. For DF and AF, in Stage 1, a source broadcasts its encoded signal to the trusted relay nodes. In Stage 2, in DF, each relay first decodes the message and then re-encodes it and transmits a weighted version of the reencoded signal, while in AF, each relay forwards a weighted version of the noisy signals that it received in Stage 1. For CJ, while the source transmits the encoded signal, relays transmit a weighted jamming signal with the purpose of confounding the eavesdroppers. All cooperation nodes are divided into two classes: 1)the relay nodes, which receive a signal from the source in stage 1 and relay the signal to the destination in stage 2. 2)the jamming nodes, which transmit a noise signal that is independent of the source signals. However,

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 7, July 2015

in the previous works, either the relay nodes or the jamming nodes were considered in establishing a secure link from the source to the destination in the wireless networks.

In this research work, we investigate the effects of relay selection with multiple eavesdroppers under Rayleigh fading and with security constraints. The proposed work is done under both AF (Amplify and Forward) and DF (Decode and Forward) method to extract appropriate validation of schemes. Three Dcode and forward Schemes are considered: Convolutional Coding scheme, Reed-solomon codes [34] , and Turbo Codes [33]. For the proposed scheme firtsly, the relay to be selected is the one that has the lowest SNR to the eavesdroppers (both between the source and relay and between relay and destination). For the second scheme, it is the relay that provides the highest signal-to-noise ratio (SNR) to the destination. In the third scheme, the best potential relay gets selected according to its secrecy rate.

The first scheme tries to reduce the overheard information at the eavesdroppers by choosing the relay having the lowest instantaneous SNR to them both between source to relay (ER) and relay to desitnation (RE). The second is a conventional selection relaying one which seeks the relay having the highest SNR to the destination. We also study the performance of the Relay selection scheme in terms of the probability of Symbol error rate, Bit error rate, secrecy outage probability and achievable secrecy rate of all AF and DF schemes. These will first be analytically described by investigating the probability density functions (PDF) of the end-to-end system SNR. Then, the asymptotic approximations for the system achievable secrecy rate, which reveal the system behavior, will be provided. We will show that previously known results in [15] and [33] are special cases of our obtained results. MATLAB simulations will finally be conducted for confirming the correctness of the Proposed analysis.

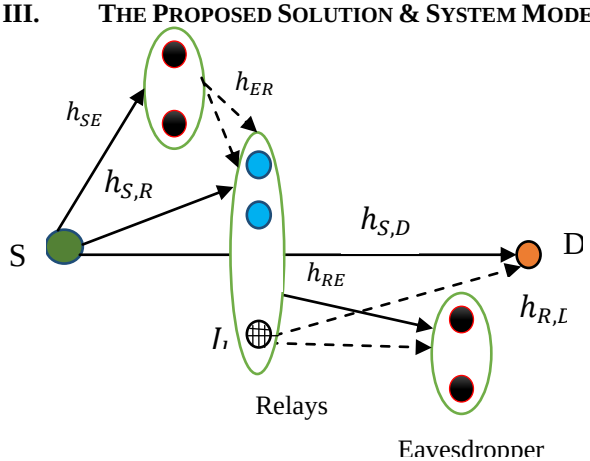
II. BACKGROUND & RELATED WORK

Cooperative communication has been considered as one of the most interesting paradigms in future wireless networks. By encouraging single-antenna equipped nodes to cooperatively share their antennas, spatial diversity can be achieved in the fashion of multi-input multi-output (MIMO) systems [11], [12]. Recently, this cooperative concept has increased interest in the research community as a mean to ensure secrecy for wireless systems [13]–[18].

The basic idea is that the system achievable secrecy rate can be significantly improved with the help of relays considering the spatial diversity characteristics of cooperative relaying.While relay selection schemes have been intensively studied (see, e.g., [19]–[23] and references therein), there has been little research to date that focuses on relay selection with security purposes and related performance evaluation. In particular, Dong et al. investigated repetition-based decode-and-forward (DF) cooperative protocols and considered the design problem of transmit power minimization in [15]. Relay selection and cooperative beamforming were proposed for physical layer security in [24]. For the same system model, destination assisted jamming was considered in [25], showing an increase of the system achievable secrecy rate with the total transmit power budget. Investigating physical layer security in cognitive radio networks was carried out by Sakran et al. in [26] where a secondary user sends confidential information to a secondary receiver on the same frequency band of a primary user in the presence of an eavesdropper receiver. For amplify-and-forward (AF) relaying, the secure performance, based on channel state information (CSI) of the two hops, of different relay selection schemes was investigated in [27].
For orthogonal frequency division multiplexing (OFDM) networks using DF, a closed-form expression of the secrecy rate was derived in [28]. In a large system of collaborating relay nodes, the problem of secrecy requirements with a few active relays was investigated in [29], aimed at reducing the communication and synchronization needs by using the model of a knapsack problem.

To simultaneously improve the secure performance and quality of service (QoS) of mobile cooperative networks, an optimal secure relay selection was proposed in [30] by overlooking the changing property for the wireless channels. Effects of cooperative jamming and noise forwarding were studied in [31] to improve the achievable secrecy rates of a Gaussian wiretap channel. In [32], Krikidis et al. proposed a new relay selection scheme to improve the Shannon capacity of confidential links by using a jamming technique. Then, in [33], by taking into account of the relay-eavesdropper links in the relay selection metric, they also introduced an efficient way to select the best relay. The base work [34] proposed Restricted Best Second Hop (RBSH) and the Worst Relay-Eavesdropper Link (WREL). In which best relay are choosen with respect to best and worst link of relay with respect to destination and eavesdropper. Many problems are considered within base work [34] in order to propose a more efficient method so that we can outperform the base work both in terms of error rate and secrecy.

III. THE PROPOSED SOLUTION & SYSTEM MODEL



Relay Which Has minimum h_{ER} and h_{RE} and Maximum $h_{R,D}$

Fig. 1. The system model with K relays and M eavesdroppers.

DOI 10.17148/IJARCCE.2015.4778

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 7, July 2015

The system model consists of one source S, one destination D, and a set of *K* decode-and-forward (DF-Convolutional coding, RS coding, Turbo Coding) or AF (amplify-and-forward) relays, R_k, (k = 1, . . . , K) which help the transmission between the source and the destination to avoid the overhearing attacks of *M* malicious eavesdroppers, E_m, (m = 1, . . . , M). In order to focus our study on the cooperative slot, we assume that the source has no direct link with the destination and eavesdroppers (E_m) (i.e. the direct links are in deep shadowing) and the communication is performed through a reactive DF-AF protocol. It is worth noting that this assumption is well-known in the literature for cooperative systems with and without taking into account secrecy constraints as well as is to facilitate the analysis. More specifically, this assumption refers to cooperative systems with a secure broadcast phase or clustered relay configurations where the source node communicates with the relays via a local connection with small transmission power.

In the first phase of this proposed work, the source broadcasts the signal to the relay nodes and during the second phase one potential relay node, which is chosen among the relays that successfully decoded the source transmission forwards the reencoded signal towards the destination. Fig. 1 schematically presents the system model and the two phases of the considered cooperative scheme. A slow, flat, block Rayleigh fading environment is assumed, where the channel remains static for one coherence interval (one slot) and changes independently in different coherence intervals. Denote the instantaneous gain of the channel from relay *k* to the destination is $\gamma_{k,D}$, and that from relay *k* to eavesdropper *m* is $\gamma_{k,m}$. Hence, for each relay R_k, the channel capacity from it to D can be given as:

$$C_{k,D} = \frac{1}{2}\log_2(1 + P_R\gamma_{k,D}) \quad \text{....(1)}$$

Where P_R is the transmission power of the relays, the factor 1⁄2 presents for the two phase transmission of the dual-hop network similarly, the Shannon capacity of the channel from relay *k* to eavesdropper *m* can be given as:

$$C_{k,m} = \frac{1}{2}\log_2(1 + P_R\gamma_{k,m}) \quad \text{....(2)}$$

In order to avoid that at least one eavesdropper can overhear the forwarded signal, we must focus on the maximal channel from one relay to the eavesdropper group. The equivalent capacity from the relay *k* to all the eavesdroppers should be defined as:

$$C_{k,E} = \max_m\left[\frac{1}{2}\log_2(1 + P_R\gamma_{k,m})\right] = \frac{1}{2}\log_2(1 + P_R\gamma_{k,E}) \quad \text{.... (3)}$$

Where $\gamma_{k,E} = \max_m\gamma_{k,m}$ denotes as the equivalent channel gain from relay *k* to all the eavesdroppers. Then, the instantaneous secrecy rate at the relay *k* can be defined as:

$$C(k) = C_{k,D} - C_{k,E} = C_{k,D} - max_m\, C_{k,m} = \frac{1}{2}\log_2(1 + P_R\gamma_{k,D}) - \frac{1}{2}\log_2(1 + P_R\gamma_{k,E} \quad \text{....(4)}$$

At high SNRs, the secrecy capacity at relay *k* can be approximated As

$$C(k) \approx \frac{1}{2}\log_2\left(\frac{\gamma_{k,D}}{\gamma_{k,E}}\right) = \frac{1}{2}\log_2\left(\frac{\gamma_{k,D}}{max_m\,\gamma_{k,m}}\right) \quad \text{....(5)}$$

The selection of relays depends on the relay selection criterion and its operating optimization is the main objective of this paper. Noting that to facilitate the relay selection process, we assume a perfect knowledge of the required channel-based parameters available. In this paper, we would like to investigate three selection schemes, namely

1) Choosing relay having the minimum channel gain to the multiple eavesdroppers (choose min) from both the side of cooperative network (between source-relay and between relay-destination). We can say that Choosing the relay having the highest secrecy capacity to the destination and eavesdroppers (choose secrecy).
2) Choosing relay having the maximum channel gain to the destination (choose max).

A. Dual Hop multi-eavesdropper worst eavesdropper link

In this strategy, based on the instantaneous SNR of the links from the relays to all the eavesdroppers between source to relay and relay to destination, the equivalent channel gain from it to the malicious nodes can be can calculated as $\gamma_{k,E} = \max_m\gamma_{k,m}$. Then, the relay which has the lowest equivalent channel (SNR_{ER} *and* SNR_{RE}) will be chosen to forward the signal to the destination. The problem how to select the lowest one can be solved by the timer approach. Then, the secrecy capacity for this relay selection strategy can be written as

$$C_1(k^*) = C_{k^*,D} - \min_{k^*}(\max_m C_{k,m}), \quad \text{....(6)}$$

Where k^* denotes the index of the selected relay.

B. Dual Hop multi-eavesdropper restricted best second hop method

In this strategy, using the same timer-based approach as in the second strategy, the relay from the set of SNR_{ER} *and* SNR_{RE} with the highest SNR to the destination will become the next sender of the next hop. Therefore, the secrecy capacity of this strategy can be calculated as

$$C_2(k^*) = (\max_{k^*} C_{k^*,D}) - (\max_m C_{k^*,m}) \quad \text{....(7)}$$

C. Optimal selection

The proposed selection technique incorporates the quality of the relay-eavesdropper links in the selection decision metric. In its optimal version, we assume that the instantaneous quality of the relay-eavesdropper links is available during the decision process. Based on the expression of the instantaneous secrecy capacity, which is given in (5), the proposed selection technique is written as

$$k^* = arg\max_k\left\{\frac{\gamma_{k,D}}{\gamma_{k,E}}\right\} = arg\max_k\left\{\frac{\gamma_{k,D}}{max_m\,\gamma_{k,m}}\right\} \quad \text{....(8)}$$

and the corresponding secrecy capacity converges to

$$C_3(k^*) = \max_{k^*}(C_{k,D} - \max_m C_{k,m}) \approx \frac{1}{2}\log_2\left[\max_{k^*}\left(\frac{\gamma_{k,D}}{max_m\gamma_{k,m}}\right)\right] \quad \text{....(9)}$$

The new selection metric is related to the maximization of the secrecy capacity and therefore is the optimal solution for reactive AF-DF protocols with secrecy constraints.

DOI 10.17148/IJARCCE.2015.4778

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 7, July 2015

However, its application requires the instantaneous knowledge of the relay-eavesdroppers links and therefore its practical interest is partially limited. It is also noted that turbo codes and convolutional channel coding perform better than any other DF method.

IV. VALIDATION RESULTS

In this section, we investigate the performance of the proposed design algorithms numerically. In the simulation setup, we assume that the average SNR of the direct link is proportional to the average SNR of the second hop as: $SNR_{SD} = \alpha * SNR_{R^*D}$ average SNR between the relays and destination is the same as that between relays and eavesdroppers, and unit transmission power at the source and the relays. QPSK modulation technique is used, and the number of relays and the value of interference threshold are varying as shown in the simulation figures. We tested the proposed work on 10 relays and 4 eavesdropper under fading environment. Eavesdroppers are placed both between the sorce-relay and relay-destination. Initially the proposed work calculate the worst link of eavesdropper at both side of relays and extract a set of relay S from n number of relays and after that from the set S we extract a relay R^* which has best link (SNR) with the destination. The efficiency of relay are validate in terms of symbol error rate (SER) and bit error rate (BER). In digital transmission, the number of bit or symbol errors is the number of received bits or symbols of a data stream over a communication channel that have been altered due to noise, interference, distortion or bit synchronization errors. The bit error rate (BER) and Symbol error rate (SER) is the number of bit or symbol errors per unit time. The bit error ratio or symbol error ratio (also BER or SER) is the number of bit or symbol errors divided by the total number of transferred bits or symbols during a studied time interval. BER and SER is a unitless performance measure, often expressed as a percentage. The bit error probability is the expectation value of the bit error ratio. The bit error ratio can be considered as an approximate estimate of the bit error probability. This estimate is accurate for a long time interval and a high number of bit errors.

Simulations are carried out in **MATLAB R2013b** (Version 8.2.0.703). The Error Rate Calculation block compares input data from a transmitter with input data from a receiver. It calculates the error rate as a running statistic, by dividing the total number of unequal pairs of data elements by the total number of input data elements from one source. Use this block to compute either symbol or bit error rate, because it does not consider the magnitude of the difference between input data elements. If the inputs are bits, then the block computes the bit error rate. If the inputs are symbols, then it computes the symbol error rate.

Figure 2 below divulges that the proposed method offers a lower symbol error rate than the RBSH [34] and other methods. We notice that the SER for proposed work is mimimum approximately over a range of SNR, this is due to the fact that it does not depend on the number of relays. We remark the same behavior for the bit error probability of the methods shown in the figure below. The RBSH [34] method offers a higher outage probability than the Proposed method. This confirm the fact that having the maximum Relay-Eavesdropper (at desntination) SNR ratio does not guarantee the best QoS at the destination.

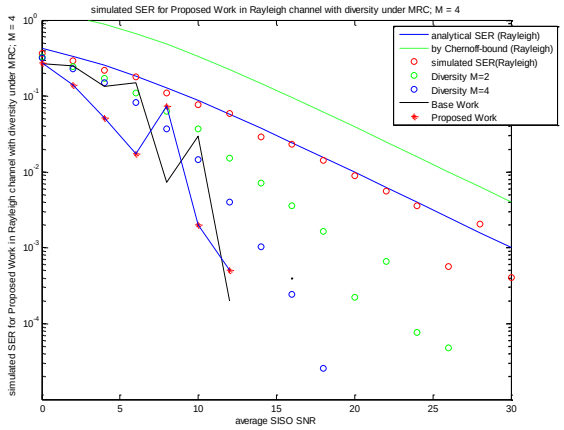


Fig. 2. Shows the comparison of SER in terms of relaying capacity with respect to various values of SNR. It is clear from the figure that symbol error rate is minimum for the relaying in proposed work.

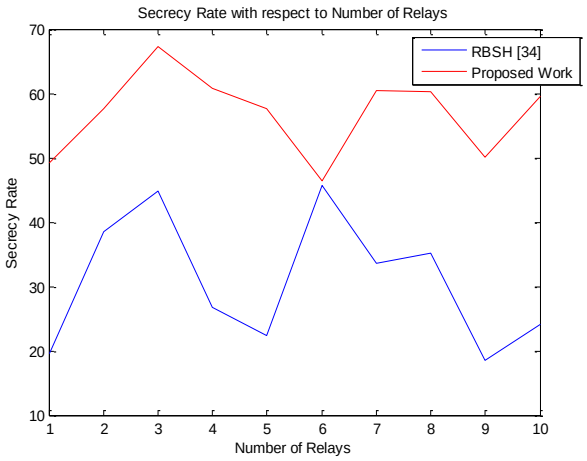


Fig. 3. The secrecy rate between 0 to 100 with respect to number of relays for both the proposed and RBSH [34] techniques. The achievable secrecy is higher in proposed work approximately for all mth relays in network.

Fig. 3 shows the secrecy rates achieved by the proposed work and RBSH [34] with respect to number of relays. It shows that the proposed work has higher secrecy rate on approximately all the conditions and RBSH [34] scheme does not offer better results because none of the relays satisfies the secrecy condition.

In a noisy channel, the BER is often expressed as a function of the normalized carrier-to-noise ratio measure denoted Eb/N0, (energy per bit to noise power spectral density ratio), or Es/N0 (energy per modulation symbol to noise spectral density). For example, in the case of QPSK modulation and AWGN channel, the BER as function of the Eb/N0 is given by:

$$BER = \frac{1}{2} erfc(\sqrt{E_b/N_0})$$

DOI 10.17148/IJARCCE.2015.4778

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 7, July 2015

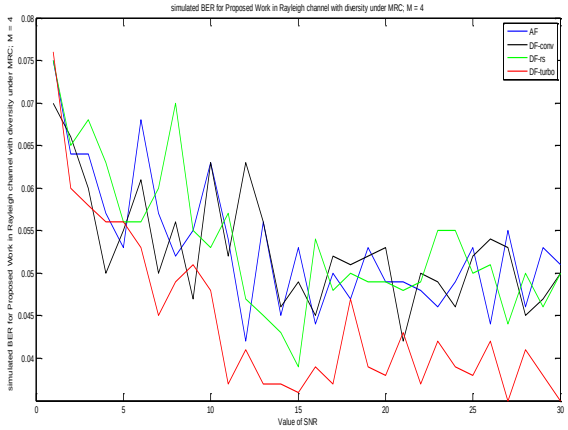


Fig. 4. We consider four relaying. That is, AF, DF-convolutional coding, DF-rs coding, DF-turbo coding. The figure shows the bit error rate performance of all the relaying meothds. It is noted that, Turbo DF method provides more secrecy compare to other methods.

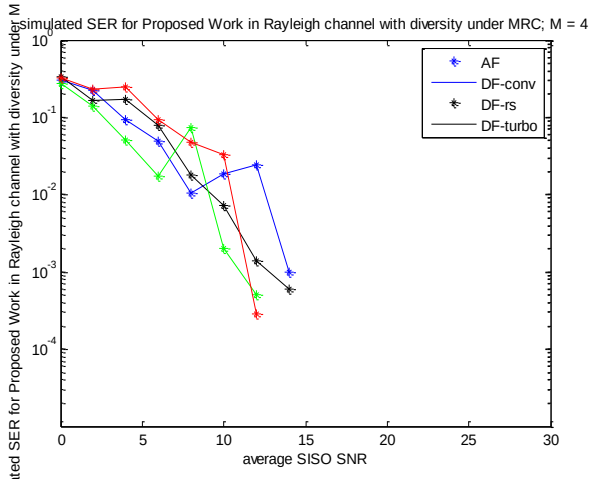


Fig. 5. The figure shows the SER performance of all the relaying meothds. It is noted that, Turbo DF method provides more secrecy compare to other methods.

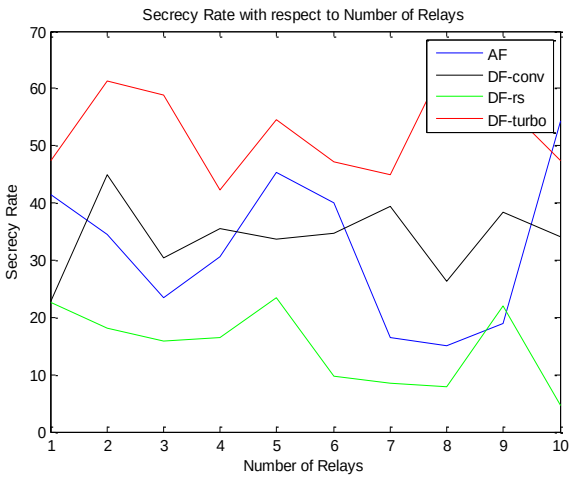


Fig. 6. The figure shows the achievable secrecy rate with all the four relaying methods considered in proposed work. In terms of secrecy turbo coding based DF method proved as most secure method.

We have demonstrated that cooperative network secrecy can be achieved for arbitrary wireless relay networks by utilizing the signal interactions to carry secure information forward cooperatively. We have shown an achievable trade-off between the reliable transmission rate from the source to the legitimate destination and the amount of information leaked to a class of eavesdroppers over an arbitrary wireless relay network. Roughly speaking, the trade-off is related to the information-theoretic min-cuts between the source-destination and source-eavesdropper pairs.

V. CONCLUSION & DISCUSSION

Previously reported relay selection schemes select the best single relay without taking into account confidentiality issues. In this paper, we have introduced relay selection as an efficient way in order to ensure secrecy and protect the source message against eavesdroppers. We have introduced an efficient cooperative communications scheme which maximizes the secrecy rate. We proposed a better relay selection method that maximizes the secrecy rate and benefits from increasing the number of relays under QoS constraint at the destination. The proposed transmission scheme was studied for both AF and DF (Convolution codes, RS codes, Turbo Codes) relaying strategy. Performance has been studied in terms of secrecy rate, and average error probability expressions have been derived. Simulations results are used to confirm the mathematical derivations and an agreement results are observed. The results confirm the better secrecy rate and lower error rate of the introduced transmission scheme compared to well established techniques introduced in the literature.

REFERENCES

[1] A. D.Wyner, The wire-tap channel, Bell Syst. Tech. J., vol. 54, no. 8, pp. 1355C1387, 1975.
[2] I. Csiszr and J. Korner, Broadcast channels with confidential messages, IEEE Trans. Inf. Theory, vol. 24, pp. 339348, May 1978.
[3] F. Oggier and B. Hassibi, The secrecy capacity of the MIMO wiretapchannel, 2008 IEEE international symposium on information theory,Toronto, ON, pp. 524-528, July 2008.
[4] P. Parada and R. Blahut, Secrecy capacity of SIMO and slow fading channels, in Proc. IEEE Int. Symp. Inf. Theory, Adelaide, Australia, Sep. 2005.
[5] S. Shafiee and S. Ulukus, Achievable rates in Gaussian MISO channels with secrecy constraints, in Proc. IEEE Int. Symp. Inf. Theory, France, Jun. 2007.
[6] L. Lai and H. El Gamal, The relay-eavesdropper channel: Cooperation for secrecy, IEEE Trans. Inf. Theory, vol. 54, no. 9, pp. 4005C4019, Sep. 2008.
[7] L. Dong, Z. Han, A. Petropulu and H. V. Poor, Secure wireless communications via cooperation, in 46th Annual Allerton Conference on Communication, Control, and Computing, pp. 1132-1138, Sept. 2008.
[8] L. Dong, Z. Han, A. Petropulu, and H. V. Poor, Amplify-and-forward based cooperation for secure wireless communications, in Proc. IEEE Int. Conf. Acoust., Speech, Signal Process., Taipei, Taiwan, Apr. 2009.
[9] L. Dong, Z. Han, A. Petropulu, and H. V. Poor, Cooperative jamming for wireless physical layer security, in Proc. IEEE Statistical Signal Processing Workshop, Cardiff, Wales, U.K., Aug.CSep. 2009.
[10] L. Dong, Z. Han, A. Petropulu and H. V. Poor, Improving wireless physical layer security via Cooperative relays, IEEE Trans. Signal Processing. vol. 58, no. 3, pp. 1875-1888 march. 2010.

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 7, July 2015

[11] A. Nosratinia, T. E. Hunter, and A. Hedayat, "Cooperative communication in wireless networks," IEEE Commun. Mag., vol. 42, Oct. 2004.
[12] J. N. Laneman, D. N. C. Tse, and G. W. Wornell, "Cooperative diversity in wireless networks: efficient protocols and outage behavior," IEEE Trans. Inf. Theory, vol. 50, no. 12, pp. 3062–3080, Dec. 2004.
[13] L. Lai and H. El Gamal, "The relay-eavesdropper channel: cooperation for secrecy," IEEE Trans. Inf. Theory, vol. 54, no. 9, pp. 4005–4019 , Sept. 2008.
[14] J. Barros and M. Rodrigues, "Secrecy capacity of wireless channels," in Proc. 2006 IEEE International Symposium on Information Theory, pp. 356–360.
[15] L. Dong, Z. Han, A. Petropulu, and H. Poor, "Secure wireless communications via cooperation," in Proc. 2008 Allerton Conference on Communication, Control, and Computing, pp. 1132–1138.
[16] V. Aggarwal, L. Sankar, A. Calderbank, and H. Poor, "Secrecy capacity of a class of orthogonal relay eavesdropper channels," EURASIP J. Wireless Commun., vol. 2009, pp. 1–14, 2009.
[17] P. Popovski and O. Simeone, "Wireless secrecy in cellular systems with infrastructure-aided cooperation," IEEE Trans. Inf. Forensics Security, vol. 4, no. 2, pp. 242–256, Feb. 2009.
[18] H. Alves, R. D. Souza, M. Debbah, and M. Bennis, "Performance of transmit antenna selection physical layer security schemes," IEEE Signal Process. Lett., vol. 19, no. 6, pp. 372–375, June 2012.
[19] A. Bletsas, H. Shin, "Outage analysis for cooperative communication with multiple amplify-and-forward relays," Electron. Lett., Mar. 2007.
[20] I. Krikidis, J. Thompson, S. McLaughlin, and N. goertz, "Amplify-andforward with partial relay selection," IEEE Commun. Lett., vol. 12, Apr. 2008.
[21] J. Lopez Vicario, A. Bel, J. A. Lopez-Salcedo, and G. Seco, "Opportunistic relay selection with outdated CSI: outage probability and diversity analysis," IEEE Trans. Wireless Commun., vol. 8, no. 6, pp. 2872–2876, June 2009.
[22] M. Seyfi, S. Muhaidat, and J. Liang, "Performance analysis of relay selection with feedback delay," IEEE Signal Process. Lett., vol. 18, no. 1, Jan. 2010.
[23] W. Zhang, D. Duan, and L. Yang, "Relay selection from a battery energy efficiency perspective," IEEE Trans. Commun., vol. 59, no. 6, June 2011.
[24] K. Junsu, A. Ikhlef, and R. Schober, "Combined relay selection and cooperative beamforming for physical layer security," J. Commun. Netw., vol. 14, no. 4, pp. 364–373, Aug. 2012.
[25] L. Yupeng and A. P. Petropulu, "Relay selection and scaling law in destination assisted physical layer secrecy systems," in Proc. 2012 IEEE Statistical Signal Processing Workshop, pp. 381–384.
[26] H. Sakran, M. Shokair, O. Nasr, S. El-Rabaie, and A. A. El-Azm, "Proposed relay selection scheme for physical layer security in cognitive radio networks," IET Commun., vol. 6, no. 16, pp. 2676–2687, Nov. 2012.
[27] Y. Shi, P. Mugen, W. Wenbo, D. Liang, and M. Ahmed, "Relay selfselection for secure cooperative in amplify-and-forward networks," in Proc. 2012 International ICST Conference on Communications and Networking in China
[28] C. Chunxiao, C. Yueming, and Y. Weiwei, "Secrecy rates for relay selection in OFDMA networks," in Proc. 2011 International Conference on Communications and Mobile Computing, pp. 158–160.
[29] S. Luo, H. Godrich, A. Petropulu, "A knapsack problem formulation for relay selection in secure cooperative wireless communication," in Proc. 2011 IEEE International Conference on Acoustics, Speech and Signal Processing.
[30] W. Li, K. Tenghui, S. Mei, W. Yifei, and T. Yinglei, "Research on secrecy capacity oriented relay selection for mobile cooperative networks," in Proc. 2011 IEEE International Conference on Cloud Computing and Intelligence Systems.
[31] R. Bassily and S. Ulukus, "Deaf cooperation and relay selection strategies for secure communication in multiple relay networks," vol. 61, no. 6, Dec. 2013.
[32] I. Krikidis, J. S. Thompson, and S. McLaughlin, "Relay selection for secure cooperative networks with jamming," IEEE Trans. Wireless Commun., vol. 8, no. 10, pp. 5003–5011, Aug. 2009.
[33] I. Krikidis, "Opportunistic relay selection for cooperative networks with secrecy constraints," IET Commun., vol. 4, no. 15, Oct. 2010.
[34] Seifeddine BOUALLEGUE, Mazen O. HASNA, Ridha HAMILA, and Kaouthar SETHOM, "Improved Relay Selection for Decode-and-Forward Cooperative Wireless Networks under Secrecy Rate Maximization", IEEE transactions on wireless communications, accepted for publication, 2014.