Novel Physical Layer Security Schemes for Two-Way Cooperative Network with Multiple Eavesdroppers

Fatemeh-Sadat. Saeidi-Khabisi [1], Dariush. Abbasi-Moghadam [2]
1-Department of Electrical Engineering, Faculty of Electrical Engineering, Isfahan University of Technology, Isfahan, Iran.
saeedi.fs@gmail.com
2-Electrical Engineering Department, Shahid Bahonar University of Kerman, Kerman, Iran.
Abbasimoghadam@uk.ac.ir

ABSTRACT
Physical layer security has been taken a considerable attention for several years due to the broadcasting nature of the wireless networks. In this work, the relay and jammers selection in two-way cooperative networks are considered to improve the physical layer security. Three different categories of selection schemes are proposed including selection schemes without jamming, selection schemes with conventional jamming and selection schemes with controlled jamming. After that, two techniques are proposed to increase the secrecy rate in two-way cooperative networks: firstly, artificial noise is used to confuse eavesdropper: This signal is sent from intermediate nodes. As a result, the total secrecy rate is increased. Secondly, we propose a sub-optimal power allocation solution for jammer nodes. Sub-optimal power of the jammer nodes vary according to the type of scenario, location of the eavesdroppers and the second source. The sub-optimal power allocation to the jammer nodes causes more eavesdroppers confusion. As a result, the total secrecy rate is increased too. Plus these two techniques, we compare secrecy rate in one-way cooperative networks of other papers with proposed two-way cooperative network. Therefore improving in secrecy rate in two-way relay networks are observed clearly. In total simulation and analytical results demonstrate the performance improvement of the proposed techniques.

KEYWORDS: Physical layer security, Multi-eavesdropper networks, Cooperative jamming, Artificial noise, Power allocation, Secrecy rate.

1. INTRODUCTION

Security is a fundamental problem in wireless communications due to the broadcasting nature of the wireless medium. Traditionally, secure communication is achieved by using cryptographic technologies such as encryption. On the other hand, the studies from an information-theoretic viewpoint have found conditions for reliable secure communication without using secret keys.

1.1. Related works

In the pioneering works on information theoretic security, Wyner introduced the wiretap channel model in which the eavesdropper's channel is a degraded version of the receiver's channel [1]. Csisz´ar and K¨orner considered a general non-degraded channel condition and studied the transmission of both a common message to two receivers and a confidential message to only one of them [2]. The results in these early works showed that a positive secrecy capacity can be achieved if the intended receiver has a better channel than the eavesdropper. Therefore, to cope with these limitations, physical layer security (or information-theoretic security) has gained considerable attention in the last few years. From an information theoretic standpoint, the achieved source–destination confidential rate is called an achievable secrecy rate.

In [3], some relay selection metrics have been proposed with different levels of feedback overhead. In [4, 5], different relay selection strategies were introduced for improving the secrecy rate in [3]. In [6], an assignment game approach is proposed for relay selection and stimulating the cooperative behaviors of the relays in wireless networks. The sources should pay the relays for their cost energy in cooperative transmissions. The relays compete with each other to earn virtual currency from the assisted sources.

In [7–9], jamming schemes, which produce an artificial interference at the eavesdropper node in order to reduce the capacity of the related link, seem to be an interesting approach for practical applications. In [10], relay and jammer selection optimization scheme has the dual objective of maximizing the secrecy rate under

تاریخ دریافت: ۱۳۹۸/۰۹/۱۷ تاریخ پذیرش: ۱۳۹۹/۰۶/۱۶

power constraint and satisfying the requisite signal-to-interference-plus-noise ratio need of co-channel cellular user equipment. In [11] the interaction between relay and jammer is introduced as a non-cooperative game where both nodes have conflicting objectives and the Nash equilibrium (NE) of the system was derived. In [12], the Shannon capacity of secret links was improved using jamming method. Considering the relay-eavesdropper links, selection of the best relay in terms of secrecy outage probability has been proposed in [13] .The authors in [14] have proposed a scheme that is an extension of the work presented in [13] where there are multiple eavesdroppers in the system and the source has also a direct link with the destination. The proposed selection schemes have been analyzed in terms of the achievable secrecy rate and secrecy outage probability under the assumption of global channel state information [15,16].

The one-way relay channels AF and DF protocols have been extended to the general full-duplex discrete two-way relay channel and half duplex Gaussian two-way relay channel, respectively. Joint relay and jammer selection schemes have been studied in [17] to ensure secure communication in DF two-way cooperative networks where there is no direct link between the two sources. Furthermore, the signal transmission consists of three phases and the authors only deal with secrecy outage probability metric. In [18], different relay and jammer selection schemes in DF two-way relay networks have been investigated in terms of ergodic secrecy rate metric only and with a perfect instantaneous knowledge of each link in the presence of one eavesdropper. Several relay and jammer selection schemes in AF two way cooperative networks with physical-layer security consideration have been studied with the assumption that jamming signal is unknown at the other intermediate nodes and considering one eavesdropper network model has been suggested in [19]. The authors in [20] have focused on the investigation of diversity techniques to improve the physical layer security, differing from the conventional artificial noise generation and beamforming techniques which typically consume additional power for generating artificial noise and exhibit high implementation complexity for beamformer design.

The authors in [21] have studied opportunistic relay selection in cooperative networks with secrecy constraints, where a number of eavesdropper nodes may overhear the source message. To deal with this problem, in this paper they consider three opportunistic relay selection schemes. A novel secure transmission scheme for multiple-input multiple-output (MIMO) Two-Way relay channels, where multi-pair communication partners exchange information securely with the help of relay, has been proposed in [22]. In [23], a joint cooperative beamforming, jamming, and power-allocation scheme with the aim of enhancing the security of an amplify-and-forward (AF) cooperative relay network has been suggested, in this paper it is showed that the secrecy rate is a quasi-concave function of the power of the source node so that allocating its total power may not be optimal. In [24] is enhanced the physical layer security (PLS) of amplify-and-forward (AF) relaying with the aid of joint relay and jammer selection (JRJS), despite the deleterious effect of channel state information (CSI) feedback delays. In [25] is considered secure communications of one source-destination pair in wireless multi-hop decode-and-forward (DF) relay networks. In the presence of an eavesdropper, and is derived an optimal power allocation strategy to maximize achievable secrecy rates under an overall transmit power constraint assuming that a single relay is located at each individual hop. In [26] In order to benefit the relays in forwarding the signals for defending against the eavesdropping attacks, the interactions between the source and the multiple relays are modeled as a single-leader multiple-followers Stackelberg game.

In [27], is investigated a source-destination link with an energy-harvesting full-duplex relay and a jammer (to degrade the eavesdropper channel) in the presence of an eavesdropper. Thus, to exploit energy harvesting and to improve security, the authors have proposed a full-duplex jammer (FDJ) protocol and its half-duplex version (HDJ). The authors have proposed robust resource allocation in [28] a framework to improve the physical layer security in the presence of an active eavesdropper. In [29], the authors have studied secure transmission in a four-node (source, destination, mobile relay, and eavesdropper) system and have focused on maximizing the secrecy rate via jointly optimizing the relay trajectory and the source/relay transmits power. They have proposed an alternating optimization approach, where in the trajectory designing and the power allocating are tackled in an alternating manner. This paper investigates the relay selection (RS) problem for multi-hop full-duplex relay networks where multiple source-destination (SD) pairs compete for the same pool of relays, under the attack of multiple eavesdroppers [30].in [31], the authors have studied the physical layer security of a downlink hybrid satellite-terrestrial relay network (HSTRN), where a multi-antenna satellite communicates with multiple terrestrial destinations via multiple cooperative relays in the presence of multiple eavesdroppers. As well as there are some new papers in this field that include the following papers.

The authors in [32] have introduced two modes that in the first mode, coined passive user mode, the users receive signals from both the BS and the untrusted relay and combine them to decode their messages. In the second mode, termed the active user mode, the users transmit a cooperative jamming signal

simultaneously with the BS's transmission to further confuse the relay. In [33] the authors have studied physical layer security for two-way relay non-orthogonal multiple access systems. They have analyzed the effective secrecy diversity order and demonstrated that the eavesdropper severely degrades the secrecy performance, and even reduces the diversity order to zero. In [34] is investigated beamforming design for cooperative secure transmission in cognitive two-way relay networks, where the cognitive transmitter (CT) with multiple antennas helps to forward the signals of two primary transmitters (PTs) and tries to protect the PTs from wiretapping by a single-antenna eavesdropper. In [35] , the authors have propose a novel decode-and-forward (DF)-based secure 3D mobile unmanned aerial vehicle (UAV) relaying for hybrid satellite-terrestrial networks (HSTNs) in the presence of an aerial eavesdropper lying around a serving UAV relay in a circular plane. Herein, they adopted a stochastic mixed mobility (MM) model for mobilizing the UAV relays in a 3D cylindrical cell with a ground user equipment (UE).

1.2. Contribution

Based on the authors' knowledge, none of these works have not examined the case of multiple cooperating and non-cooperating eavesdroppers' model in two-way cooperative networks along with novel idea to improve physical layer security. The main contributions of this paper are proposing the relay and jammers selection in two-way cooperative networks to improve their physical layer security with multiple eavesdroppers. Plus two new ideas are proposed for improving the physical layer security in two-way relay network. In the first idea, artificial noise signal is used to confuse the eavesdropper; therefore, the secrecy rate is increased. In the second idea, a sub-optimal power allocation solution is proposed to jammer nodes. Sub-optimal power of the jammer nodes is variable according to the type of scenario, the eavesdroppers and the second source location. The sub-optimal power allocation to the jammer nodes leads to more confusion for the eavesdroppers; as a result, the secrecy rate is increased.

In this paper we present advantage of using two way relays in different scenario and models. In our previous paper [36], our research topic was about physical layer security which has a remarkable difference with current research. In that research our focus was on one way relay networks which was used different ideas such as a new criterion which decreases the rate at the eavesdroppers, a new relay selection schemes and a sub-optimal power allocation solution for jammer nodes in one way relay networks. While in this paper our special attention is on two way relay networks, plus their advantages rather than one way ones. Moreover, in this paper we have proposed new ideas such as artificial noise broadcasting and sub-optimal power allocation in two way relay networks.

The rest of the paper is organized as follows: in section 2 the system model is introduced. The relay and jammers selection schemes and the proposed techniques are described in sections 3. Numerical results are shown and discussed in section 4. Finally, we conclude the paper in section 5.

2. SYSTEM MODEL

The system model consists of two sources S_1 and S_2 in addition to an middle node set S_{relay}= {1, 2,…,N} with N nodes as shown in Fig. 1, which help the transmission between the $S_1$and the $S_2$to avoid overhearing attacks of M malicious eavesdroppers, E_m { m=1,...,M}. Fig. 1 schematically presents the system model. Relays cannot transmit and receive simultaneously; therefore, communication is performed in two orthogonal channels and the communication process is performed in two phases. During the first phase, S_1 and S_2 transmit their data to the intermediate nodes (R) and due to the broadcasting nature of the transmission, the eavesdroppers overhear the transmitted information. In addition, according to the security protocol, one node J_1 is selected from S_{relay} set to operate as a "jammer" and transmit intentional interference to degrade the sources-eavesdroppers links in this phase. During the second phase, according to the security protocol, an intermediate node R is selected to operate as a conventional relay; it forwards the sources messages to the corresponding sources (R belongs to a decoding set $C_d \subseteq S_{relay}$, which includes the relays that can successfully decode two sources messages). Beside when one protocol is safe that present at least secrecy rate along with malicious nodes. The proper choice of relay node can increase secrecy rate .as a result access to this principle can be more comfortable. Thus relay node effect security protocol directly.

Also a second jammer J_2 is selected from S_{relay}, for the same reason as J_1. In fact, the task of J_1 ,J_2 is just sending of jamming signal, not decoding any signal. Therefor J_1 ,J_2 must choose from S_{relay} not C_d.

It should be notified that the artificial interference from the jamming nodes is unknown at $S_1$and S_2; thus, they are not able to mitigate it and this is referring to applications with critical secrecy constraints. In this system model, it is assumed that the direct links ($S_1 \leftrightarrow S_2$, $S_1 \rightarrow E$ and $S_2 \rightarrow E$) are available and the broadcasting and cooperative phases are insecure.

Thus, the eavesdroppers can overhear the transmitted signal. The channel remains static for one coherence interval and changes independently in different coherence intervals with a variance $\sigma_{i,j}^2 = d_{i,j}^{-\beta}$, where $d_{i,j}$ is the Euclidean distance between node i and node j, and β is the path-loss exponent. In overall phases, a slow, flat, and block Rayleigh fading environment has been assumed, i.e.[24]. Also, additive white Gaussian noise (AWGN) is considered with zero mean and unit variance. The middle nodes act in half duplex mode. Therefore, they cannot transmit and receive simultaneously.

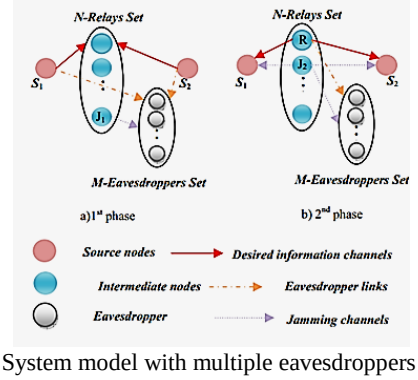

Fig. 1. System model with multiple eavesdroppers in two-way Relay network.

3. THE PROPOSED METHODS

The aim of relay selection is to select the nodes R, J_1 and J_2 to maximize the achievable secrecy rate. First, a cooperative network with multiple eavesdroppers is considered that can individually decipher the source information. The most important scenarios in [14] are also investigated in this section. In the table 1, we present the most important schemes are used in this paper [14].

NC	non-cooperative eavesdroppers without jamming
NCJ	non-cooperative eavesdroppers with jamming
NCCJ	non-cooperative eavesdroppers with controlled jamming
CW/OJ	cooperative eavesdroppers without jamming
CJ	cooperative eavesdroppers with jamming
CCJ	Cooperative eavesdroppers with controlled jamming

Table 1. The investigated schemes in this paper

3.1. Jammer selection in Two-Way Relay System

In this section, the mentioned selection process is analyzed for scenarios with and without eavesdropper cooperation. With cooperation, the eavesdropper nodes cooperate (create a malicious network) to overhear the source information where each of these sections contains different designs such as selection schemes without jamming, selection schemes with conventional jamming (i.e. the jamming signal is unknown at the sources) and selection schemes with controlled jamming (i.e. the jamming signal is known at the destinations) are discussed in the following sub sections. For without cooperation in the eavesdropper nodes, these mentioned schemes are investigated too.

The overall secrecy performance of the system in the all mentioned scheme in the different scenario is characterized by the ergodic secrecy rate which is the sum of the two sources' secrecy rates that is given as:

$$C_S^{|C_d|} = C_{S_1}^{|C_d|} + C_{S_2}^{|C_d|} \qquad (1)$$

(1) is used in all schemes and the secrecy rate for each of the sources is obtained separately.

In practice, in the first step relays receive signals from two sources and in the second step send them to opposite sources. In fact the basic method for calculating secrecy rate in two way relay networks in this paper is based on superposition principle [17-20]. Actually based on this principle, two phases for calculating total secrecy rate has been done. In the first phase, the mount of signal that is sent from S_2 considered zero. Beside S_1 , S_2 are considered as S (the system source) and D (the system destination) respectively (like one way relay network). Then the secrecy rate related to the first phase is calculated. Also In the second phase, the mount of signal that is sent from S_1 is considered zero. Beside S_1 , S_2 are considered as D and S respectively. Then the secrecy rate related to the second phase is calculated. Finally two calculating secrecy rates are summed.

- *Selection schemes with non-cooperative eavesdroppers*

In this subsection, we consider non-cooperative eavesdroppers that try to decode the source information individually. In this case, the instantaneous achievable secrecy rate for each source shown in Fig. 1, with a decoding set C_d is given as follows [36]:

$$C_{S_1}^{|C_d|}(R,J_1,J_2)= \tag{2}$$
$$\begin{cases}\left[\frac{1}{2}\log_2\left(1+\frac{\gamma_{S_1,S_2}}{1+\gamma_{J1,S_2}}\right)-\frac{1}{2}\log_2\left(1+\max_{E_m\in S_{evs}}\left(\frac{\gamma_{S_1,E_m}}{1+\gamma_{J1,E_m}}\right)\right)\right]^+, & |C_d|=0\\ \left[\frac{1}{2}\log_2\left(1+\frac{\gamma_{S_1,S_2}}{1+\gamma_{J1,S_2}}+\frac{\gamma_{R,S_2}}{1+\gamma_{J2,S_2}}\right)-\frac{1}{2}\log_2\left(1+\max_{E_m\in S_{evs}}\left(\frac{\gamma_{S_1,E_m}}{1+\gamma_{J1,E_m}}+\frac{\gamma_{R,E_m}}{1+\gamma_{J2,E_m}}\right)\right)\right]^+, & |C_d|>0\end{cases}$$

$$C_{S_2}^{|C_d|}(R,J_1,J_2)= \tag{3}$$
$$\begin{cases}\left[\frac{1}{2}\log_2\left(1+\frac{\gamma_{S_2,S_1}}{1+\gamma_{J1,S_1}}\right)-\frac{1}{2}\log_2\left(1+\max_{E_m\in S_{evs}}\frac{\gamma_{S_2,E_m}}{1+\gamma_{J1,E_m}}\right)\right]^+, & |C_d|=0\\ \left[\frac{1}{2}\log_2\left(1+\frac{\gamma_{S_2,S_1}}{1+\gamma_{J1,S_1}}+\frac{\gamma_{R,S_1}}{1+\gamma_{J2,S_1}}\right)-\frac{1}{2}\log_2\left(1+\max_{E_m\in S_{evs}}\frac{\gamma_{S_2,E_m}}{1+\gamma_{J1,E_m}}+\frac{\gamma_{R,E_m}}{1+\gamma_{J2,E_m}}\right)\right]^+, & |C_d|>0\end{cases}$$

In these equals one time S_1 is considered as source and S_2 is considered as destination. Another time S_2 is considered as source and S_1 is considered as destination. Then secrecy rate is calculated like [14] separately in two phases. After that the secrecy rate is summed according to (1). where $R\in C_d$ $J_1\in S_{relay}$ and $J_2\in \{S_{relay}-R^*\}$, $\gamma_{i,j}=P^{(i)}|h_{i,j}|^2$ is the instantaneous signal-to-noise ratio (SNR) for the link i →j modeled as a zero-mean, independent, circularly symmetric complex Gaussian random variable with variance $\sigma_{i,j}^2$. The distribution of the channel coefficient between the nodes i and j ($h_{i,j}$) is given as $h_{i,j}\sim CN(0,\delta_{i,j}^2)$. Also, $P^{(S_{1,2})}$, $P^{(R)}$ and $P^{(J)}$ represent the transmitted power for the sources node, the relay node and the jammer nodes, respectively. In order to protect the sources from the intentional interference and maximize the advantages of the proposed schemes, the jammer nodes transmit with a lower power than the relay nodes and thus their transmitted power is defined as $P^{(J)}=P^{(R)}/L$ (with $P^{(S_{1,2})}=P^{(R)}$), where L>1 represent the ratio of the relay power to the jammer power. Since the jamming signal is harmful for eavesdropper nodes. If the power of jammer is increased, the eavesdropper will recognize and removed it [23, 36].

The purpose is to select the proper nodes R, J_1 and J_2 in order to maximize the instantaneous secrecy capacity for various feedback channels. The optimization problem can be formulated as:

$$(J_1^*,R^*,J_2^*)=\arg\max_{\substack{J_1\in S_{relay}\\ R\in C_d\\ J_2\in\{S_{relay}-R^*\}}}\left\{C_{S_{1,2}}^{|C_d|}(R,J_1,J_2)\right\} \tag{4}$$

In the new scheme of NC, the instantaneous secrecy capacity for each source is:

$$C_{S_1}^{NC}(R) = \left[\frac{1}{2}\log_2\left(\frac{1+\gamma_{\gamma_{S_1,S_2}}+\gamma_{R,S_2}}{\max_{E_m\in S_{evs}}1+\gamma_{S_1,E_m}+\gamma_{R,E_m}}\right)\right]^+ \tag{5}$$

$$C_{S_2}^{NC}(R,) = \left[\frac{1}{2}\log_2\left(\frac{1+\gamma_{\gamma_{S_2,S_1}}+\gamma_{R,S_1}}{\max_{E_m\in S_{evs}}1+\gamma_{S_2,E_m}+\gamma_{R,E_m}}\right)\right]^+ \tag{6}$$

The relay selection process that maximizes the secrecy rate given in (1) is:

$$(R^*)=\operatorname{argmax}_{R\in C_d}\left\{C_{S_{1,2}}^{|C_d|}(R,J_1,J_2)\right\} \tag{7}$$

In the new scheme of NCJ, the instantaneous secrecy capacity for each source is:

$$C_{S_1}^{NCJ}(J_1,R,J_2)= \tag{8}$$

$$\left[\frac{1}{2}\log_2\left(\frac{1+\frac{\gamma_{S_1,S_2}}{1+\gamma_{J1,S_2}}+\frac{\gamma_{R,S_2}}{1+\gamma_{J2,S_2}}}{1+\max\limits_{E_m\in S_{evs}}\left\{\frac{\gamma_{S_1,E_m}}{1+\gamma_{J1,E_m}}+\frac{\gamma_{R,E_m}}{1+\gamma_{J2,E_m}}\right\}}\right)\right]$$

$$C_{S_2}^{NCJ}(J_1,R,J_2)= \tag{9}$$

$$\left[\frac{1}{2}\log_2\left(\frac{1+\frac{\gamma_{S_2,S_1}}{1+\gamma_{J1,S_1}}+\frac{\gamma_{R,S_1}}{1+\gamma_{J2,S_1}}}{1+\max\limits_{E_m\in S_{evs}}\left\{\frac{\gamma_{S_2,E_m}}{1+\gamma_{J1,E_m}}+\frac{\gamma_{R,E_m}}{1+\gamma_{J2,E_m}}\right\}}\right)\right]^+$$

The selection policy that maximizes the secrecy rate given in NCJ scheme is similar to (4).

In the non-cooperative eavesdroppers with controlled jamming (NCCJ) scheme, this signal can be decoded at the destination (S_1 or S_2) although it is unknown for eavesdroppers. The secrecy capacity in this scheme is

$$C_{S_1}^{|C_d|}(R,J_1,J_2)= \tag{10}$$

$$\begin{cases}\left[\frac{1}{2}\log_2\left(1+\frac{\gamma_{S_2,S_1}}{1+\gamma_{J1,S_1}}\right)-\frac{1}{2}\log_2\left(1+\frac{\gamma_{S_2,S_2}}{1+\gamma_{J1,S_2}}\right)\right]^+, & |C_d|=0\\ \left[\frac{1}{2}\log_2\left(1+\frac{\gamma_{S_2,S_1}}{1+\gamma_{J1,S_1}}+\frac{\gamma_{R,S_1}}{1+\gamma_{J2,S_1}}\right)-\frac{1}{2}\log_2\left(1+\frac{\gamma_{S_2,S_2}}{1+\gamma_{J1,S_2}}+\frac{\gamma_{R,S_2}}{1+\gamma_{J2,S_2}}\right)\right]^+, & |C_d|=0\\ \left[\frac{1}{2}\log_2\left(1+\sum_{m=1}^{M}\frac{\gamma_{S_2,E_m}}{1+\gamma_{J1,E_m}}\right)-\frac{1}{2}\log_2\left(1+\sum_{m=1}^{M}\frac{\gamma_{S_2,E_m}}{1+\gamma_{J1,E_m}}\right)\right]^+, & |C_d|>0\\ \left[\frac{1}{2}\log_2\left(1+\sum_{m=1}^{M}\frac{\gamma_{S_2,E_m}}{1+\gamma_{J1,E_m}}+\frac{\gamma_{R,E_m}}{1+\gamma_{J2,E_m}}\right)-\frac{1}{2}\log_2\left(1+\sum_{m=1}^{M}\frac{\gamma_{S_2,E_m}}{1+\gamma_{J1,E_m}}+\frac{\gamma_{R,E_m}}{1+\gamma_{J2,E_m}}\right)\right]^+, & |C_d|>0\end{cases} \tag{11}$$

The terms of γ_{S_1,E_m} ,γ_{S_2,E_m} in (10, 11) present the interference caused by eavesdroppers on the signals that is sent from S_1 and S_2. Also table 1 include set of selection schemes that maximize the secrecy capacity in (1) and the optimization problems are similar to the previous section except that the eavesdroppers have the ability to exchange their obtained information to decode the source information.

3.2. Improving the secrecy rate by using artificial noise in two way relay

Using artificial noise is one of the main techniques for confusing the eavesdroppers. Artificial noise is well known for the authorized sources; therefore this signal should be transmitted from a known node. Relay nodes can be a good choice to transmit artificial noise signal.

In order to evaluate the effect of artificial noise, we distinguish between these two cases: conventional jamming (i.e. the jamming signal is unknown at the sources) and controlled jamming (i.e. the jamming signal is known at the sources). In these cases, the total transmit power of each relay for sending artificial noise in the decoding set is constrained to $P_{NA}=P_R/100$ and the power of original signal is P_R.

similar to NCJ scheme except that in this scheme,γ_{J1,S_1}, γ_{J2,S_1}, γ_{J1,S_2} and $\gamma_{J1,S_2}$are zero. Also, the selection policy that maximizes the secrecy rate with respect to NCCJ definition is given in (4).

- *Selection schemes with cooperative eavesdroppers*

In cooperative eavesdropping model, the eavesdroppers have the ability to exchange their obtained information to decode the source information. The instantaneous secrecy rate for this model with decoding set C_d is given as:

- *Selection schemes with non-cooperative eavesdroppers*

In the proposed NCJ (the jamming signal is unknown at the source) scheme, the secrecy rate expression for each source is follow:

$$C_{S_1}^{NA.NCJ}(J_1,R,J_2)= \tag{12}$$

$$\left[\frac{1}{2}\log_2\left(\frac{1+\frac{\gamma_{S_1,S_2}}{1+\gamma_{J1,S_2}}+\frac{\gamma_{R,S_2}}{1+\gamma_{J2,S_2}}}{1+\max\limits_{E_m\in S_{evs}}\left\{\frac{\gamma_{S_1,E_m}}{1+\gamma NA_{1,E_m}+\gamma_{J1,E_m}}+\frac{\gamma_{R,E_m}}{1+\gamma_{NA_2,E_m}+\gamma_{J2,E_m}}\right\}}\right)\right]^+$$

$$C_{S_2}^{NA.NCJ}(J_1,R,J_2)= \tag{13}$$

$$\left[\frac{1}{2}\log_2\left(\frac{1+\frac{\gamma_{S_2,S_1}}{1+\gamma_{J1,S_1}}+\frac{\gamma_{R,S_1}}{1+\gamma_{J2,S_1}}}{1+\max\limits_{E_m\in S_{evs}}\left\{\frac{\gamma_{S_2,E_m}}{1+\gamma_{NA_1E_m}+\gamma_{J1,E_m}}+\frac{\gamma_{R,E_m}}{1+\gamma_{NA_2,E_m}+\gamma_{J2,E_m}}\right\}}\right)\right]^+$$

Where $\gamma_{NA_1,\mathrm{E_m}}, \gamma_{NA_2,\mathrm{E_m}}$ denote signal to noise ratio for the case that relay sends artificial noise to the eavesdroppers. The secrecy rate and the best node selection policy related to NCCJ scheme is similar to the NCJ scheme except that the parameters $\gamma_{\mathrm{J1},S_{1,2}}$ and $\gamma_{\mathrm{J2},S_{1,2}}$ are zero.

In these equations once S_1 and S_2 are considered as source node (transmitter node) and destination node (receiver node) sequentially. Again S_1 and S_2 are considered as destination node (receiver node) and source node (transmitter node) sequentially. After that the secrecy rates are summed according to (1). In this scheme the objective is to obtain the following optimization problem.

$$(J_1^*, R^*, J_2^*, NA_1^*, NA_2^*) = \arg \max_{\substack{J_1\in S_{relay}\\ R\in C_d\\ NA_1\in C_d\\ J_2\in\{S_{relay}-R^*\}\\ NA_2\in C_d}} \left\{C_S^{|C_d|}(R, J_1, J_2, NA_1, NA_2)\right\} \quad (14)$$

Instantaneous SNR related to eavesdropper -jammer link is malicious agent both for eavesdropper and for destination (S1, S2). Therefore this SNR is brought in denominator of these logarithms [14, 16, 17, 19]. Also artificial noise has the functional similar to jamming signal, thus this signal is brought along with the term related to the jammer.

Where $\mathrm{NA}_1^*, \mathrm{NA}_2^*$ denote selected nodes among intermediate nodes that send artificial noise to eavesdroppers in the first and the second phases respectively.

In the relay selection schemes had emphasized on choice of the best relay. Therefore at least one relay can decode and forward a special signal. As a result, we assume $\mathrm{C_d}>0$.

In the selection schemes with cooperative eavesdropper, all of the selection policies and equations are similar to selection schemes with non-cooperative eavesdropper, but it should be notified that in these schemes, the eavesdroppers cooperate together to decode original data.

3.3. Sub-optimal power allocation to the jammers in two-way relay network

The suboptimal power allocation for jammer nodes is an effective method for improving secrecy rate or physical layer security in two way relay networks. In the papers about two way relay networks with multi eavesdropper, the power of jammer nodes have been fixed and this issue is one of the blind spots in these papers.

In this proposed technique, when the location of the second source and eavesdropper changed, the sub optimal power allocation changed too. We mean, when the locations of eavesdroppers are closer to the jammer node than the second source, the sub-optimal power allocation for jammer must have been increased.
Moreover, when the location of the second source is closer to the jammer node than eavesdroppers, the sub optimal power allocation for jammer node must have been decreased. As a result this issue lead to more confusing of eavesdroppers and more safe for second source. Thus the total secrecy rate increases.

In this technique, we just investigate two schemes CCJ and NCCJ because in these scheme jamming signal is known and is removed .thus power increasing of node jammer doesn't destroy information in the second source. But excessive increasing of jammer node power cause the jammer node recognizes this signal and removes it. Also if this signal be less than the specified amount, the eavesdropper won't confuse. As a result the secrecy rate decreases. Therefore the sub-optimal power allocation for jammer node is determined by L parameter in (15). Thus the best range for L parameter is selected between 10 to 100.as well as, L was chosen from a limited range of integers for simplify.

$$P^{(J)}=P^{(R)}/\mathrm{L} \quad (15)$$

In (16) and (17), the secrecy rate is expressed for non-cooperative eavesdropper's models in S_1, S_2 respectively.

The secrecy rate expressed in cooperative eavesdropper's models is similar to (16-18) by considering the fact that in this model, the eavesdroppers cooperate with each other to decrypt the data.

$$C_{s_1}^{|C_d|}(R,J_1,J_2) = \quad (16)$$

$$\begin{cases} \left[\frac{1}{2}\log_2\left(1+\frac{P_{S_1}|h_{S_1,S_2}|^2}{1+\gamma_{J_1,S_2}}\right)-\frac{1}{2}\log_2\left(\max_{E_m\in S_{evs}}\left\{1+\frac{\gamma_{S_1,E_m}}{1+\gamma_{J1,E_m}}\right\}\right)\right]^+ & |C_d|=0 \\ \left[\frac{1}{2}\log_2\left(1+\frac{P_{S_1}|h_{S_1S_2}|^2}{1+\left(\frac{P_{S_1}}{L}\right)*|h_{J_1,S_2}|^2}+\frac{P_R|h_{R,S_2}|^2}{1+\left(\frac{P_{S_1}}{L}\right)*|h_{J_2,S_2}|^2}\right)-\frac{1}{2}\log_2\left(\max_{E_m\in S_{evs}}\left\{1+\frac{P_S|h_{S_1,E_m}|^2}{1+\left(\frac{P_{S_1}}{L}\right)*|h_{J_1,E_m}|^2}+\frac{P_R|h_{R,E_m}|^2}{1+\left(\frac{P_{S_1}}{L}\right)*|h_{J_2,E_m}|^2}\right\}\right)\right]^+ & |C_d|>0 \end{cases}$$

$$C_{s_2}^{|C_d|}(R,J_1,J_2)= \quad (17)$$

$$\begin{cases} \left[\frac{1}{2}\log_2\left(1+\frac{P_{S_2}|h_{S_2,S_1}|^2}{1+\gamma_{J_1,S_1}}\right)-\frac{1}{2}\log_2\left(\max_{E_m\in S_{evs}}\left\{1+\frac{\gamma_{S_2,E_m}}{1+\gamma_{J1,E_m}}\right\}\right)\right]^+ & |C_d|=0 \\ \left[\frac{1}{2}\log_2\left(1+\frac{P_{S_2}|h_{S_2S_1}|^2}{1+\left(\frac{P_{S_1}}{L}\right)*|h_{J_i,S_1}|^2}+\frac{P_R|h_{R,S_2}|^2}{1+\left(\frac{P_{S_1}}{L}\right)*|h_{J_i,S_1}|^2}\right)-\frac{1}{2}\log_2\left(\max_{E_m\in S_{evs}}\left\{1+\frac{P_S|h_{S_2,E_m}|^2}{1+\left(\frac{P_{S_2}}{L}\right)*|h_{J_i,E_m}|^2}+\frac{P_R|h_{R,E_m}|^2}{1+\left(\frac{P_{S_2}}{L}\right)*|h_{J_i,E_m}|^2}\right\}\right)\right]^+ & |C_d|>0 \end{cases}$$

In these equations once $S_1$and S_2 are considered as source node (transmitter node) and destination node (receiver node) sequentially. Again S_1 and S_2 are considered as destination node (receiver node) and source node (transmitter node) sequentially.. After that the secrecy rate is summed according to (1).

Our ultimate objective is to select appropriate nodes R, J_1 , J_2 and L in order to maximize the instantaneous secrecy rate for two schemes CCJ and NCCJ in non-cooperative eavesdropper's models. The optimization problem can be formulated as:

$$(J_1^*,R^*,J_2^*,L^*)= \quad (18)$$

$$\arg\max_{\substack{J_1\in S_{relay} \\ R\in C_d \\ J_2\in\{S_{relay}-R^*\} \\ L\in\{10:1000\}}} \left\{C_S^{|C_d|}(R,J_1,J_2,L)\right\}$$

4. NUMERICAL RESULTS

In this section, we present the advantage of our proposed technique by using simulation. Our system model has been explained in section 2 and has been shown in Fig. 1. We assume that we have four relays (N) and two eavesdroppers (M) which are located in a two-dimensional unit-square area. The position of relays and eavesdroppers are fixed and these locations are $\{x_{S_1},y_{S_1}\}$= {0,0.5} and $\{x_{R_i},Y_{R_i}\}_{i=1}^4$={(0.5,0.2),(0.5,0.4),(0.5,0.6),(0.5,0.8)}, respectively, as is shown in Fig. ۲.

We investigate our techniques in three scenario A,B and C. the location of eavesdroppers in these three scenarios are $\{x_{E_i},Y_{E_i}\}_{i=1}^2$={(1,0.3),(1,0.7)}, $\{x_{E_i},Y_{E_i}\}_{i=1}^2$={(1,0.3),(1,0.7)} and $\{x_{E_i},Y_{E_i}\}_{i=1}^2$={(0.7,0.3),(0.7,0.7)} respectively. Also the location of the second source in A, B and C scenario are $\{x_{S_2},y_{S_2}\}$= {1, 0.5}, $\{x_{S_2},y_{S_2}\}$= {0.7, 0.5} and $\{x_{S_2},y_{S_2}\}$= {1, 0.5} respectively.

The SNR related to in the simulation is defined as SNR=P/N0, where P≜ P_S ≜ P_R.also has been assumed that the power allocated to the jammer nodes is much lower than the power of the source and the selected relay. In addition, we have considered the power ratio $P_{j_i} = P/L$, i=1,2, in which L= 100 except for the sub-optimal power allocation in section ۴.3 where the value of L will be achieved. Moreover, the path-loss exponent is set to β=3.

The considered selection schemes are: Non-cooperative eavesdroppers without jamming (NC) Non-cooperative eavesdroppers with Jamming (NCJ), Non-cooperative eavesdroppers with Controlled Jamming (NCCJ), Cooperative eavesdroppers without jamming (Cw/oJ) cooperative eavesdroppers with jamming (CJ) and cooperative eavesdroppers with controlled jamming (CCJ). Results of the proposed technique are shown in the following parts.

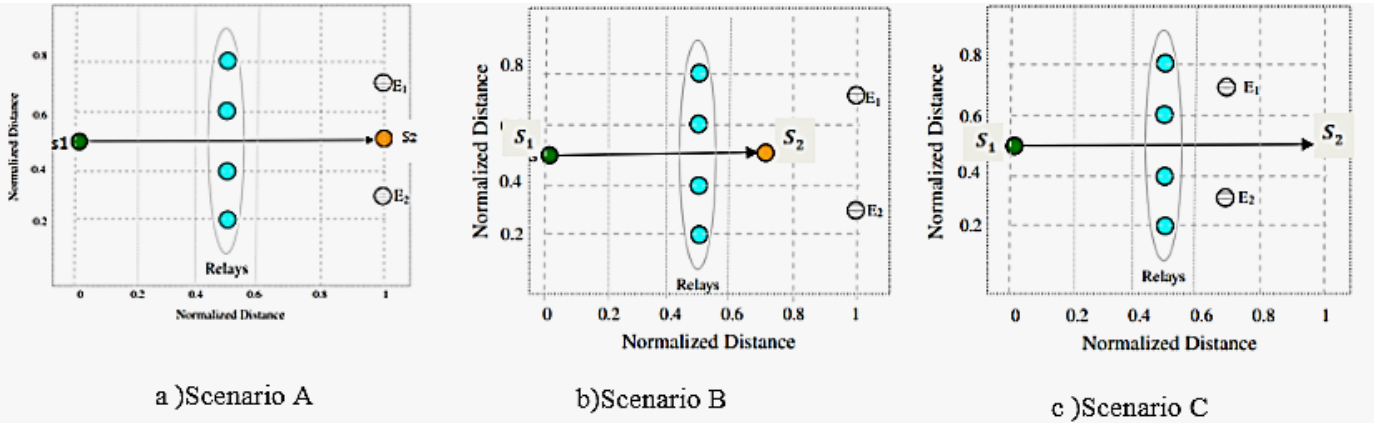

Fig. 2. The simulation environment with square unit are, N=4, M=2, α=3, (a) Scenario A: the second source and the eavesdroppers are of equal distances from the relays. (b) Scenario B, the second source is closer to the relays than the eavesdroppers. (c) Scenario C, where the eavesdroppers are closer to the relays.

- *Selection with Jamming in Two-way Relay System*

There is comparison of proposed schemes and the schemes presented in [14] in terms of the achievable secrecy rate. The obtained results show that by using this idea, the secrecy rate between the whole schemes is greater than the system using one way relays. We consider scenario A along with the previously described selection schemes namely, NC, NCJ, NCCJ, Cw/oJ, CJ and CCJ schemes. Fig. ۳ presents the whole schemes is greater than the system using one way relays. As is shown in Fig.۳ and ۴, when the jamming signal is known in S_2(NCCJ and CCJ), the secrecy rate is more than the other schemes. Also, in all of schemes, scenario B presents more secrecy rate rather than scenario A and this happens because the second source in scenario A has less distance from eavesdroppers.

Fig.۵ shows that the secrecy rate in all proposed schemes improve in comparison with one way relays. It is mentionable that in this scenario, eavesdroppers have less distance from the first source; therefore, the secrecy rate decreases in this source and as a result, in all schemes of this scenario, the secrecy rate is lower than scenario B.

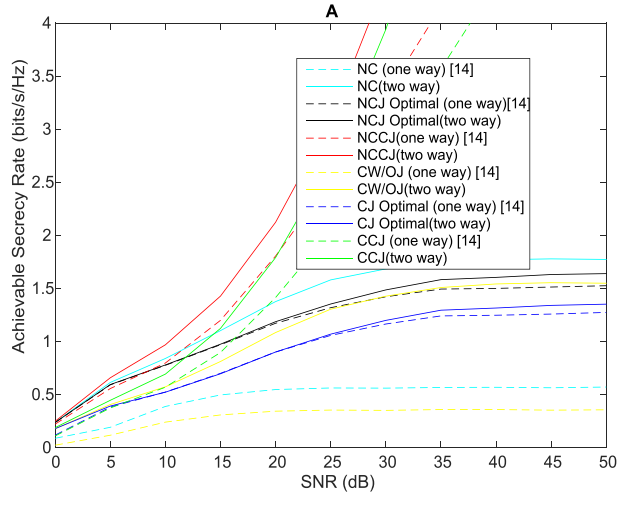

Fig. ۳. Achievable secrecy rate versus SNR in the Selection with Jamming in Two-way Relay System scheme for scenario A with N=4, and M=2

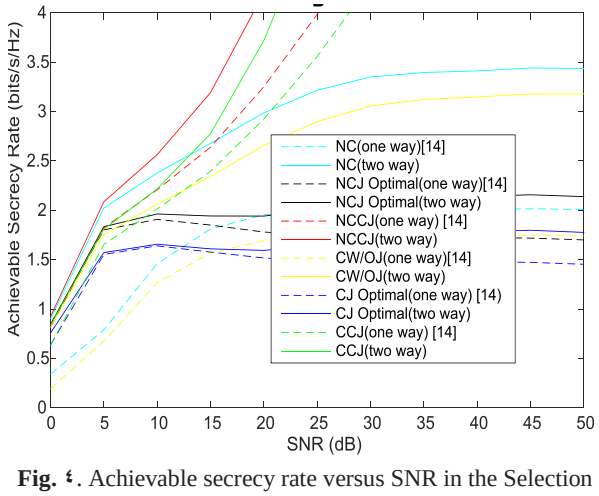

Fig. ۴. Achievable secrecy rate versus SNR in the Selection with Jamming in Two-way Relay system scheme for scenario B with N=4, and M=2

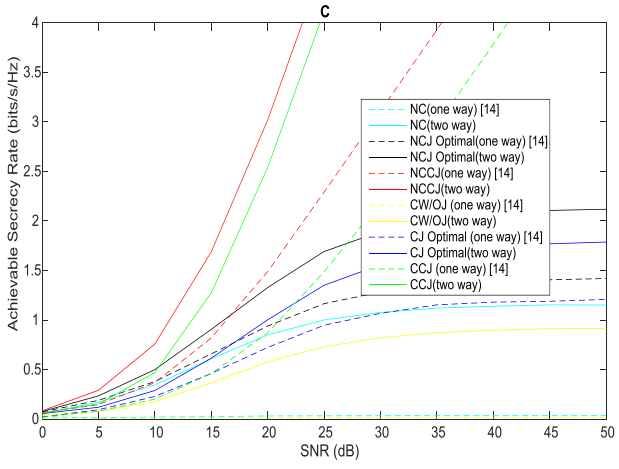

Fig. ٥. Achievable secrecy rate versus SNR in the Selection with Jamming in Two-way Relay System scheme for scenario C with N=4, and M=2

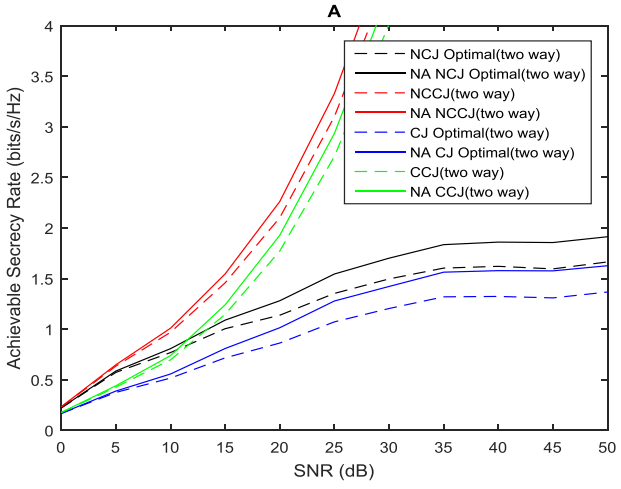

Fig. ٦. Achievable secrecy rate versus SNR in the improving secrecy rate with using artificial noise in the two way relay scheme for scenario A with N=4, and M=2

- *Improving the secrecy rate with using artificial noise in two way relay*

  In this idea, artificial noise signal is sent from known nodes such as relays to confuse the eavesdropper. This signal will be removed by the first and the second sources, so the secrecy rate is improved. This idea is investigated in three scenarios A, B and C and in NCJ, NCCJ, CJ and NCCJ schemes. As Fig.٦ showed, in some schemes such as CCJ, NCCJ due to the combined use of jamming signal and artificial noise in addition to identifying and removing these two signals in the first and the second sources, an acceptable secrecy rate is achieved. In Fig.8 the eavesdroppers in scenario B compared to the scenario A has a greater distance from the second sources; thus, the secrecy rate in all schemes of this scenario compared to the scenario A is greater. Fig.٨ shows that in all schemes, secrecy rate significantly increases when the artificial noise signal is used along with jamming signals for confusing the eavesdropper.

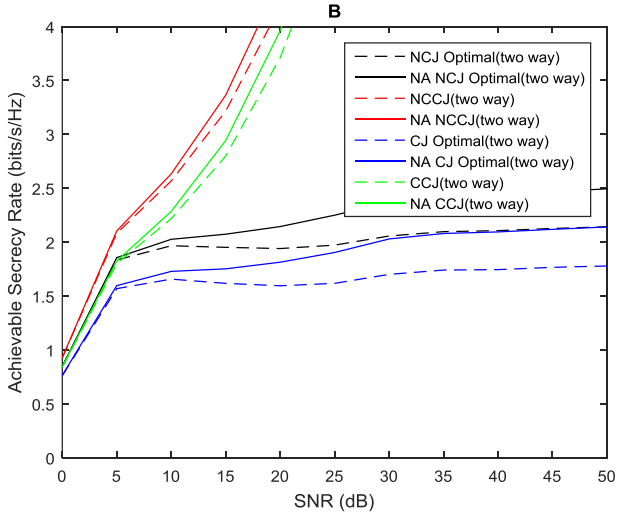

Fig. ٧.Achievable secrecy rate versus SNR in the improving secrecy rate with using artificial noise in the two way relay scheme for scenario B with N=4, and M=2

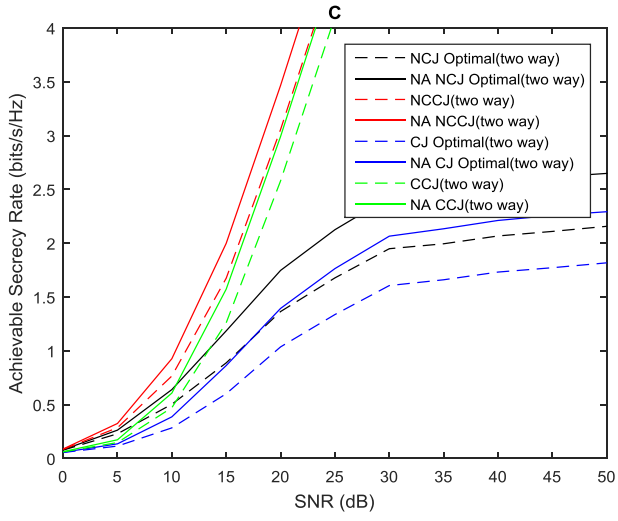

Fig. ٨. Achievable secrecy rate versus SNR in the new criterion for calculating the rate of security scheme for scenario C with N=4, and M=2

- *Sub-optimal power allocation to the jammers nodes*

Because only in the CCJ and NCCJ scheme, changing the power of the jamming signal significantly improves the secrecy rate in the tree scenarios, we only investigate these two schemes. In the CCJ and NCCJ scheme, jamming signal is known and removed. Thus we can increase the power of jammer node with consideration of the limitations mentioned in section ٣.3. Because the number of candidate answers is low, we use search method to find optimal answer [36-38]. Hence, for the two mentioned schemes, optimal value for L has been obtained to be 10.

In Fig.9 when power allocated to jamming signal is increasing, it causes more confusion to the eavesdroppers and makes them achieve less information, so the secrecy rate increases.

In Fig.١٠, when eavesdroppers are close to the intermediate node, the effects of increasing the power of jamming signal is more than the scenario A. By use of this idea in the mentioned scenario, we can see increasing rate of security in NCCJ and CCJ schemes. In Fig.١١, the secrecy rate has raised up too. Because eavesdroppers have more distance rather than intermediate nodes, this idea is less effective rather than scenario B.

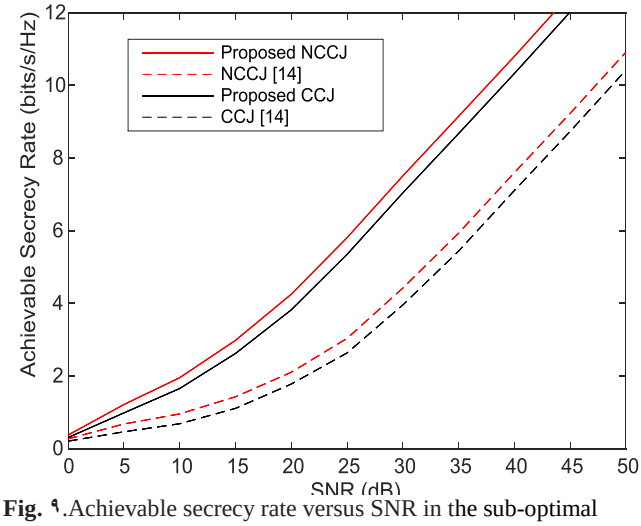

Fig. ٩.Achievable secrecy rate versus SNR in the sub-optimal power allocation to the jammers nodes scheme for scenario A with N=4, and M=2

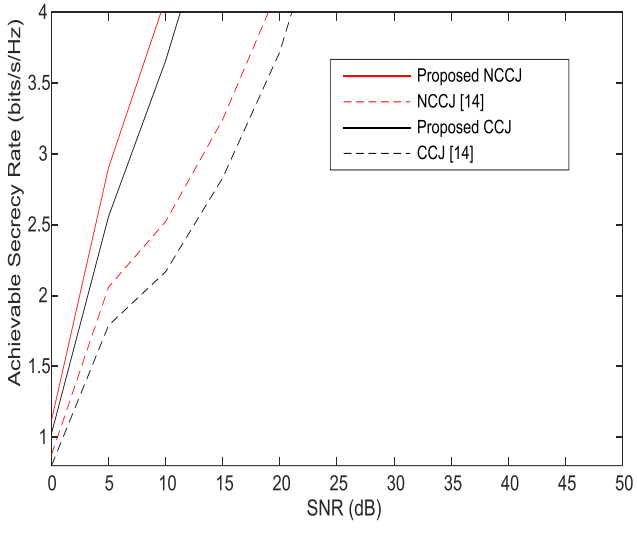

Fig. 1٠. Achievable secrecy rate versus SNR in the sub-optimal power allocation to the jammers nodes scheme for scenario B with N=4, and M=2

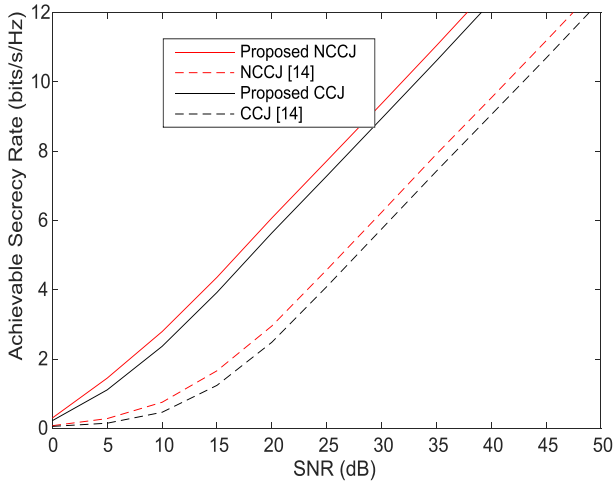

Fig. 11. Achievable secrecy rate versus SNR in the sub-optimal power allocation to the jammers nodes scheme for scenario C with N=4, and M=2

5. CONCLUSIONS

We have shown the effectiveness of the proposed two-way relay selection schemes over the one-way relay selection schemes to improve the physical layer security. Then two methods are proposed in this paper to improve the physical layer security of two-way cooperative networks.

In the first method, to confuse the eavesdropper and to improve the secrecy rate, we have used sending artificial noise signal by intermediate nodes to eavesdropper. In the second method, we have proposed a sub-optimal power allocation solution for jammer nodes in two-way cooperative networks. In these schemes, two main categories are considered: non-cooperative eavesdroppers and cooperative eavesdroppers. For each case, one jammer is selected in the first phase and one jammer is chosen in the second phase to enhance the security against the eavesdroppers. Our simulation results have proved that the proposed schemes can significantly improve the system performance in terms of the total achievable secrecy rate.

REFERENCES

[1] A. D. Wyner, "The wire- tap channel," Bell system technical journal, vol. 54, no. 8, pp. 1355-1387, 1975.

[2] I. Csiszár and J. Korner, "Broadcast channels with confidential messages," IEEE transactions on information theory, vol. 24, no. 3, pp. 339-348, 1978.

[3] I. Krikidis, "Opportunistic relay selection for cooperative networks with secrecy constraints," IET communications, vol. 4, no. 15, pp. 1787-1791, 2010.

[4] E. Beres and R. Adve, "Selection cooperation in multi-source cooperative networks," IEEE Transactions on Wireless Communications, vol. 7, no. 1, pp. 118-127, 2008.

[5] A. S. Ibrahim, A. K. Sadek, W. Su, and K. R. Liu, "Cooperative communications with relay-selection: when to cooperate and whom to cooperate with?," IEEE Transactions on wireless communications, vol. 7, no. 7, pp. 2814-2827, 2008.

[6] D. Li, Y. Xu, and J. Liu, "Distributed relay selection over multi-source and multi-relay wireless cooperative networks with selfish nodes," Computer Communications, vol. 33, no. 17, pp. 2145-2153, 2010.

[7] O. Simeone and P. Popovski, "Secure communications via cooperating base stations," IEEE Communications Letters, vol. 12, no. 3, pp. 188-190, 2008.

[8] P. Popovski and O. Simeone, "Wireless secrecy in cellular systems with infrastructure-aided cooperation," IEEE Transactions on Information Forensics and Security, vol. 4, no. 2, pp. 242-256, 2009.

[9] L. Wang, C. Cao, and H. Wu, "Secure inter-cluster communications with cooperative jamming against social outcasts," Computer Communications, vol. 63, pp. 1-10, 2015.

[10] E. Tekin and A. Yener, "The general Gaussian multiple-access and two-way wiretap channels: Achievable rates and cooperative jamming," IEEE Transactions on Information Theory, vol. 54, no. 6, pp. 2735-2751, 2008.

[11] T. Wang and G. B. Giannakis, "Mutual information jammer-relay games," IEEE Transactions on Information Forensics and Security, vol. 3, no. 2, pp. 290-303, 2008.

[12] I. Krikidis, J. S. Thompson, and S. McLaughlin, "Relay selection for secure cooperative networks with jamming," IEEE Transactions on Wireless Communications, vol. 8, no. 10, pp. 5003-5011, 2009.

[13] I. Krikidis, "Opportunistic relay selection for cooperative networks with secrecy constraints," IET communications, vol. 4, no. 15, pp. 1787-1791, 2010.

[14] A. Y. Al-nahari, I. Krikidis, A. S. Ibrahim, M. I. Dessouky, and F. E. Abd El-Samie, "Relaying techniques for enhancing the physical layer secrecy in cooperative networks with multiple eavesdroppers," Transactions on Emerging Telecommunications Technologies, vol. 25, no. 4, pp. 445-460, 2014.

[15] J. Li, A. P. Petropulu, and S. Weber, "On cooperative relaying schemes for wireless physical layer security," IEEE transactions on signal processing, vol. 59, no. 10, pp. 4985-4997, 2011.

[16] 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.

[17] J. Chen, L. Song, Z. Han, and B. Jiao, "Joint relay and jammer selection for secure decode-and-forward two-way relay communications," in 2011 IEEE Global Telecommunications Conference-GLOBECOM 2011, 2011: IEEE, pp. 1-5.

[18] J. Chen, R. Zhang, L. Song, Z. Han, and B. Jiao, "Joint relay and jammer selection for secure two-way relay networks," IEEE Transactions on Information Forensics and Security, vol. 7, no. 1, pp. 310-320, 2011

[19] Chen, R. Zhang, L. Song, Z. Han, and B. Jiao, "Joint relay and jammer selection for secure two-way relay networks," IEEE Transactions on Information Forensics and Security, vol. 7, no. 1, pp. 310-320, 2011.

[20] Y. Zou, J. Zhu, X. Wang, and V. C. Leung, "Improving physical-layer security in wireless communications using diversity techniques," IEEE Network, vol. 29, no. 1, pp. 42-48, 2015.

[21] V. N. Q. Bao, N. Linh-Trung, and M. Debbah, "Relay selection schemes for dual-hop networks under security constraints with multiple eavesdroppers," IEEE transactions on wireless communications, vol. 12, no. 12, pp. 6076-6085, 2013.

[22] Q. Liu, G. Gong, Y. Wang, and H. Li, "A novel physical layer security scheme for MIMO two-way relay channels," in 2015 IEEE Globecom Workshops (GC Wkshps), 2015: IEEE, pp. 1-6.

[23] H.-M. Wang, F. Liu, and M. Yang, "Joint cooperative beamforming, jamming, and power allocation to secure AF relay systems," IEEE Transactions on Vehicular Technology, vol. 64, no. 10, pp. 4893-4898, 2014.

[24] L. Wang, Y. Cai, Y. Zou, W. Yang, and L. Hanzo, "Joint relay and jammer selection improves the physical layer security in the face of CSI feedback delays," IEEE Transactions on Vehicular Technology, vol. 65, no. 8, pp. 6259-6274, 2015.

[25] J.-H. Lee, "Optimal power allocation for physical layer security in multi-hop DF relay networks," IEEE Transactions on Wireless Communications, vol. 15, no.

1, pp. 28-38, 2015.

[26] H. Fang, L. Xu, and X. Wang, "Coordinated multiple-relays based physical-layer security improvement: A single-leader multiple-followers Stackelberg game scheme," IEEE transactions on information forensics and security, vol. 13, no. 1, pp. 197-209, 2017.

[27] Z. Mobini, M. Mohammadi, and C. Tellambura, "Wireless-powered full-duplex relay and friendly jamming for secure cooperative communications," IEEE Transactions on Information Forensics and Security, vol. 14, no. 3, pp. 621-634, 2018.

[28] M. R. Abedi, N. Mokari, H. Saeedi, and H. Yanikomeroglu, "Robust resource allocation to enhance physical layer security in systems with full-duplex receivers: Active adversary," IEEE Transactions on Wireless Communications, vol. 16, no. 2, pp. 885-899, 2016.

[29] Q. Wang, Z. Chen, H. Li, and S. Li, "Joint power and trajectory design for physical-layer secrecy in the UAV-aided mobile relaying system," IEEE Access, vol. 6, pp. 62849-62855, 2018.

[30] S. Atapattu, N. Ross, Y. Jing, Y. He, and J. S. Evans, "Physical-layer security in full-duplex multi-hop multi-user wireless network with relay selection," IEEE Transactions on Wireless Communications, vol. 18, no. 2, pp. 1216-1232, 2019.

[31] V. Bankey and P. K. Upadhyay, "Physical layer security of multiuser multirelay hybrid satellite-terrestrial relay networks ," IEEE Transactions on Vehicular Technology , vol. 68, no. 3, pp. 2488-2501, 2019.

[32] A. Arafa, W. Shin, M. Vaezi, and H. V. Poor, "Secure relaying in non-orthogonal multiple access: Trusted and untrusted scenarios," IEEE Transactions on Information Forensics and Security, vol. 15, no. 1, pp. 210 222,2019.

[33] M. K. Shukla, H. H. Nguyen, and O. J. Pandey, "Secrecy Performance Analysis of Two-Way Relay Non-Orthogonal Multiple Access Systems," IEEE Access, 2020.

[34] Q. Li and L. Yang, "Beamforming for cooperative secure transmission in cognitive two-way relay networks," IEEE Transactions on Information Forensics and Security, vol. 15, pp. 130-143, 2019.

[35] P. K. Sharma and D. I. Kim, " P. K. Sharma and D. I. Kim, "Secure 3D Mobile UAV Relaying for Hybrid Satellite-Terrestrial Networks," IEEE Transactions on Wireless Communications, 2020.

[36] F. Saeedi, V. T. Vakili, D. Abbasi-Moghadam, "Improving the Physical Layer Security in Cooperative Networks with Multiple Eavesdroppers", Wireless Personal Communications, Vol 55, No 3, pp. 3295-3320, 2017.

[37] H. Koga, H. Goto and E. Chiba, "Resolution of resource conflicts in the CCPM framework using a local search method," IEEE International Conference on Industrial Engineering and Engineering Management, Bandar Sunway, pp. 94-98,2014.

[38] J. Kim, C. Choi and M. W. Spong, "Passive dynamic walking with knee and fixed flat feet," IEEE International Conference on Systems, Man, and Cybernetics (SMC), Seoul, pp. 2744-2750, 2012.