Available online at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/cose

Computers & Security

Relay and jammer selection schemes for improving physical layer security in two-way cooperative networks

Doaa H. Ibrahim, Emad S. Hassan, Sami A. El-Dolil*

Dept. of Electronics and Electrical Comm., Faculty of Electronic Eng., Menoufia Univ., 32952 Menouf, Egypt

ARTICLE INFO

Article history:
Received 6 June 2014
Received in revised form
8 January 2015
Accepted 9 February 2015
Available online 18 February 2015

Keywords:
Relay and jammer selection
Cooperative networks
Physical layer security
Decode-and-forward (DF) strategy
Ergodic secrecy rate
Secrecy outage probability

ABSTRACT

This paper is concerned with the relay and jammers selection in two-way cooperative networks to improve their physical layer security. Three different categories of selection schemes are proposed which are; selection schemes without jamming, selection schemes with conventional jamming and selection schemes with controlled jamming. The selection process is analyzed for two different network models; single eavesdropper model and multiple cooperating and non-cooperating eavesdroppers' model. The proposed schemes select three intermediate nodes during two communication phases and use the Decode-and-Forward (DF) strategy to assist the sources to deliver their data to the corresponding destinations. The performance of the proposed schemes is analyzed in terms of ergodic secrecy rate and secrecy outage probability metrics. The obtained results show that the selection schemes with jamming outperform the schemes without jamming when the intermediate nodes are distributed dispersedly between sources and eavesdropper nodes. However, when the intermediate nodes cluster gets close to one of the sources, they are not superior any more due to the strong interference on the destination nodes. Therefore, a hybrid scheme which switches between selection schemes with jamming and schemes without jamming is introduced to overcome the negative effects of interference. Finally, a comparison between relay and jammers selection schemes in both one-way and two-way cooperative networks is given in terms of both secrecy metrics. The obtained results reveal that, despite the presence of cooperating eavesdroppers, the proposed selection schemes are still able to improve both the secrecy rate and the secrecy outage probability of the two-way cooperative networks.

1. Introduction

Due to the broadcast nature of wireless communication networks, the adversarial "eavesdroppers" nodes can intercept transmissions in their coverage area and try to recover parts of the transmitted message. This issue makes security solutions quite challenging to implement in wireless communications. Recently, security technologies that are designed for the physical (PHY) layer have gained considerable attention (Wyner, 1975). The basic idea of these PHY-based approaches is to exploit the characteristics of wireless medium, like

* *Corresponding author*. Faculty of Electronic Engineering, Menoufia Uni., Egypt.
E-mail addresses: doaa_dreams@yahoo.com (D.H. Ibrahim), emad.hassan@el-eng.menofia.edu.eg (E.S. Hassan), msel_dolil@yahoo.com (S.A. El-Dolil).
http://dx.doi.org/10.1016/j.cose.2015.02.002
0167-4048/

channel fading and inherent randomness of the noise, to allow legitimate nodes (source and destination) to communicate securely at a nonzero rate in the presence of eavesdroppers, provided that the source-eavesdropper channel is a degraded version of the main channel. The security is quantified by the secrecy capacity, which is defined as the maximum rate at which information is transmitted with a perfect secrecy from the source to the destination. In Csiszar and Korner (1978), Liang et al. (2008), the secrecy capacity of the Gaussian wiretap channel, was extended to signal transmission over the broadcast and wireless fading channels, respectively.

Several works have been proposed to increase secrecy capacity of wireless networks with both cooperative relaying and cooperative jamming protocols (Dong et al., 2009; Dong et al., 2008; Liang et al., 2008; Lai and El Gamal, 2008; Krikidis, 2010; Krikidis, 2009; Ibrahim et al., 2013; Ibrahim et al., 2008; Beres and Adve, 2008; Al-nahari et al., 2012; Simeone and Popovski, 2008; Popovski and Simeone, 2009; Tekin and Yener, 2008). In Dong et al. (2009), Dong et al. (2008), the authors proposed effective amplify-and-forward (AF) and decode-and-forward (DF)-based cooperative relaying protocols for physical-layer security, respectively. In Liang et al. (2008), the authors address the reliability, stability and physical layer security for wireless broadcast networks. Furthermore, joint optimal power control and optimal scheduling schemes were proposed to enhance the secrecy rate of the intended receiver against cooperative and non-cooperative eavesdroppers'. In Lai and El Gamal (2008), the authors show that even if the source-destination rate is zero a positive secrecy rate can be achieved if the relay is closer to the destination than the eavesdropper. Moreover, an efficient secrecy rate for networks with several potential relays and multiple eavesdroppers can be verified via relay selection by keeping the complexity relatively low. In Krikidis (2010), two relay selection techniques have been proposed with different levels of feedback overhead. The authors in Krikidis (2009) extended the work presented in Krikidis (2010) for cooperative networks with jamming protection without considering the direct links. The authors in Ibrahim et al. (2013) extended the work presented in Krikidis (2009) with the presence of direct links, the assumption that broadcast phase is unsecured, and when one or more eavesdroppers are present in the system. In Ibrahim et al. (2008), Beres and Adve (2008), different strategies for relay selection were introduced for improving the secrecy rate in Krikidis (2010). In Al-nahari et al. (2012), the authors proposed multiple relay selection schemes which improve the secrecy rate and enhance the outage performance for secrecy-constrained cooperative networks with multiple eavesdroppers. In Simeone and Popovski (2008), Popovski and Simeone (2009), Tekin and Yener (2008), the authors showed that, the capacity of the eavesdropper link can be reduced via jamming schemes which produce an artificial interference at the eavesdropper node.

1.1. *Related work*

The two-way relay channel has attracted much interest because of its bandwidth efficiency and potential application to cellular networks and peer-to-peer networks (Rankov and Wittneben, 2006; Rankov and Wittneben, 2007; Chen et al., 2011; Zhou et al., 2013; Chen et al., 2012). In Rankov and Wittneben (2006), Rankov and Wittneben (2007), the one-way relay channels AF and DF protocols were extended to the general full-duplex discrete two-way relay channel and half-duplex Gaussian two-way relay channel, respectively. In Chen et al. (2011), joint relay and jammer selection schemes have been studied to ensure secure communication in DF two-way cooperative networks when there is no direct link between the two sources. Furthermore, the signal transmission consists of three phases and the authors deal with secrecy outage probability metric only. In Zhou et al. (2013), 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. In Chen et al. (2012), 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. However, none of these works have examined the case of multiple cooperating and non-cooperating eavesdroppers' model in two-way cooperative networks. Therefore, this paper addresses this case.

1.2. *Paper contributions*

The main contribution of this paper is to propose three different categories of relay and jammers selection schemes to improve the physical layer security of two-way cooperative networks. These categories are; selection schemes without jamming, selection schemes with conventional jamming (where the jamming signal is unknown at the destinations), and selection schemes with controlled jamming (where the jamming signal is known at the destinations). The considered network consists of two sources, multiple intermediate nodes, and one or more eavesdroppers. The proposed schemes select three intermediate nodes during two communication phases. In the first phase, a friendly jammer is selected to create intentional interference at the eavesdroppers' nodes. In the second phase, two relay nodes are selected; one node is selected to operate as a conventional relay and assists the sources to deliver their data to the corresponding destinations via the DF strategy. While the other node behaves as a jammer node in order to confuse the eavesdroppers in this phase. The proposed schemes are analyzed with two different channel knowledge sets; a global instantaneous knowledge of all links and an average knowledge of the eavesdroppers' links.

The performance of the proposed schemes is analyzed in terms of ergodic secrecy rate and secrecy outage probability. The obtained results show that the selection schemes with jamming outperform the schemes without jamming when the intermediate nodes are distributed dispersedly between sources and eavesdropper. However, when the intermediate nodes cluster gets close to one of the sources, they are not superior any more due to the strong interference on the destination nodes. Therefore, a hybrid scheme which switches between jamming and non-jamming selection schemes is proposed to overcome jamming limitations and

seems to be an efficient solution for practical applications with critical secrecy constraints. Moreover, the impact of changing both the eavesdroppers and the intermediate nodes location on the system performance is discussed in this paper. Finally, we discuss the impact of the presence of multiple cooperating and non-cooperating eavesdroppers on system performance metrics. The obtained results reveal that, despite the presence of cooperating eavesdroppers, the proposed selection schemes are still able to improve both the secrecy rate and the secrecy outage probability of the two-way cooperative networks.

The rest of this paper is organized as follows. In Section 2 we describe the network model, and formulate the problem. In Section 3 the different proposed selection schemes are introduced. Numerical results and discussion are shown in Section 4, and finally the main conclusions are drawn in Section 5.

2. Network model and assumptions

2.1. Single eavesdropper model

2.1.1. Network model

We assume a simple network configuration consisting of two sources S_1 and S_2, one eavesdropper E, and an intermediate node set $S_{relay} = \{1, 2, \ldots, N\}$ with N nodes as shown in Fig. 1. The intermediate nodes operate in half duplex mode therefore, they cannot transmit and receive simultaneously and the communication process performed in two phases. During the first phase S_1 and S_2 transmit their data to the intermediate nodes and due to the broadcasting nature of the transmission; the eavesdropper overhears 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 transmits intentional interference to degrade the sources-eavesdropper links in this phase. During the second phase, an intermediate node R is selected to operate as a conventional relay which forwards the sources messages to the corresponding destinations. Node R belongs to a decoding set, C_d ($C_d \subseteq S_{relay}$) which includes the relays that can successfully decode the sources messages. A second jammer J_2 is selected from S_{relay}, for the same reason as J_1. Note that the artificial interference from the jamming nodes is unknown at S_1 and S_2 and thus they are not able to mitigate it and this is referring to applications with critical secrecy constraints.

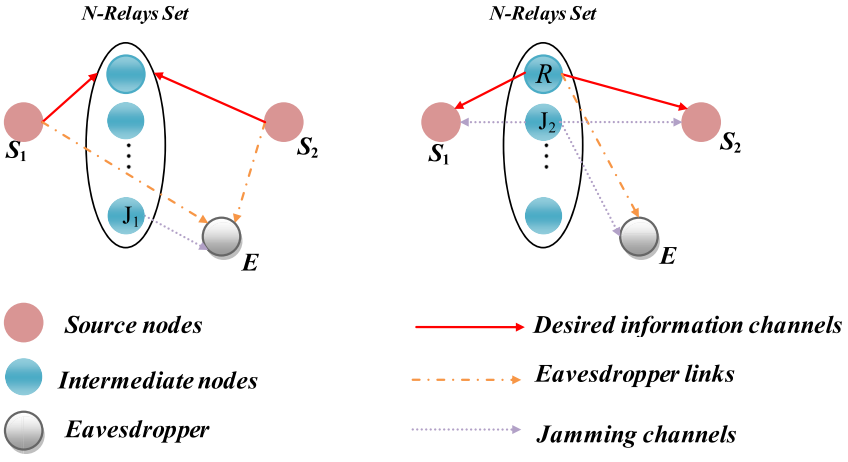
In this work we made the following assumptions:

- There is no direct link between the two sources.
- The jamming signal is known at the rest nodes of S_{relay}, the interference will not degrade the performance of the sources-relay links.
- Selection in the proposed schemes made with the secrecy constraints.
- In both two phases, a slow, flat and block Rayleigh fading environment is assumed, i.e., the channel remains static for one coherence interval and changes independently in different coherence intervals with a variance $\sigma^2_{m,n} = d^{-\beta}_{m,n}$, where $d_{m,n}$ is the Euclidean distance between node m and node n, and β is the path-loss exponent (Hassan, 2012).
- Furthermore, additive white Gaussian noise (AWGN) is assumed with zero mean and unit variance.

Let $P^{(S)}$, $P^{(R)}$ and $P^{(J)}$ denote the transmitted power for the source nodes, the relay node and the jamming nodes, respectively. In order to maximize the benefits of the proposed schemes and protect the destinations from the artificial interference, the jamming nodes transmit with a lower power than the relay node and thus their transmitted power is defined as $P^{(J)} = P^{(R)}/L$ (with $P^{(S)} = P^{(R)}$), where $L > 1$ denotes the power ratio of relay to jammer (Krikidis, 2009).

2.1.2. Problem formulation

The instantaneous secrecy rate with the decoding set C_d for source S_i is given as Liang et al. (2008);



a) 1st phase. b) 2nd phase.

Fig. 1 – Network model with one eavesdropper.

$$R_{S_i}^{|C_d|}(R,J_1,J_2)=\left[\frac{1}{2}\log_2(1+\Gamma_i)-\frac{1}{2}\log_2\left(1+\Gamma_{E_j}\right)\right]^+ \quad for|C_d|>0 \tag{1}$$

where $[x]^+ \triangleq \max\{0, x\}$, Γ_i and Γ_{Ej} denote the signals to interference-plus-noise ratios (SINRs) of link $S_j \rightarrow S_i$ ($i, j = 1, 2, i \neq j$) and link $S_j \rightarrow E$, respectively and they are given by:

$$\Gamma_i=\frac{\gamma_{R,S_i}}{\gamma_{J_2,S_i}+1} \tag{2}$$

$$\Gamma_{E_j}=\frac{\gamma_{S_j,E}}{\gamma_{S_i,E}+\gamma_{J_1,E}+1}+\frac{\gamma_{R,E}}{\gamma_{J_2,E}+1} \tag{3}$$

where $\gamma_{m,n} \triangleq P^{(m)}|f_{m,n}|^2$ denotes the instantaneous signal-to-noise ratio (SNR) for the link $m \rightarrow n$ modeled as a zero-mean, independent, circularly-symmetric complex Gaussian random variable with variance $\sigma^2_{m,n}$. The overall secrecy performance of the system is characterized by the ergodic secrecy rate which is the expectation of the sum of the two sources' secrecy rates, $E[R_S^{|C_d|}(R,J_1,J_2)]$ where,

$$R_S^{|C_d|}(R,J_1,J_2)=R_{S_1}^{|C_d|}(R,J_1,J_2)+R_{S_2}^{|C_d|}(R,J_1,J_2) \tag{4}$$

Sometimes secrecy performance of the system is characterized by the secrecy outage probability, which is defined as the probability that the system secrecy rate is less than a target secrecy rate $R_T > 0$. Secrecy outage probability is written as:

$$P_{out}=\sum_{n=1}^{N}P_r\{R_S^n(R,J_1,J_2)<R_T\}P_r\{|C_d|=n\} \tag{5}$$

Our ultimate objective is to select appropriate nodes R, J_1, and J_2 in order to maximize the instantaneous secrecy rate for different types of channel feedback. The optimization problem can be formulated as Ibrahim et al. (2013):

$$(R^*,J_1^*,J_2^*)=\arg\max_{\substack{J_1\in S_{relay}\\ R\in C_d\\ J_2\in\{S_{relay}-R^*\}}}\left\{R_S^{|C_d|}(R,J_1,J_2)\right\} \quad ,s.t.\psi_u(for\ u=0,1) \tag{6}$$

where R^*, J_1^*, J_2^* denote the selected relay and jamming nodes, respectively. Note that, the selected jammers J_1^* and J_2^* in the two phases may be the same node, which is determined by the instantaneous secrecy rate. Ψ_0 denotes a global instantaneous knowledge for all the links and Ψ_1 denotes an average channel knowledge for the eavesdropper links.

2.2. Multiple eavesdroppers model

2.2.1. Network model

Here we consider the presence of M-eavesdroppers set, $S_{eves} = \{1, 2,\ldots, M\}$as shown in Fig. 2.

2.2.2. Problem formulation

In the network with multiple eavesdroppers, the eavesdroppers may cooperate or non-cooperate with each other in two different scenarios as follows:

1st scenario: when the eavesdroppers are non-cooperative (i.e. each eavesdropper tries to decode the sources information individually). The instantaneous secrecy rate with the decoding set C_d for source S_i is given as (Al-nahari et al., 2012)

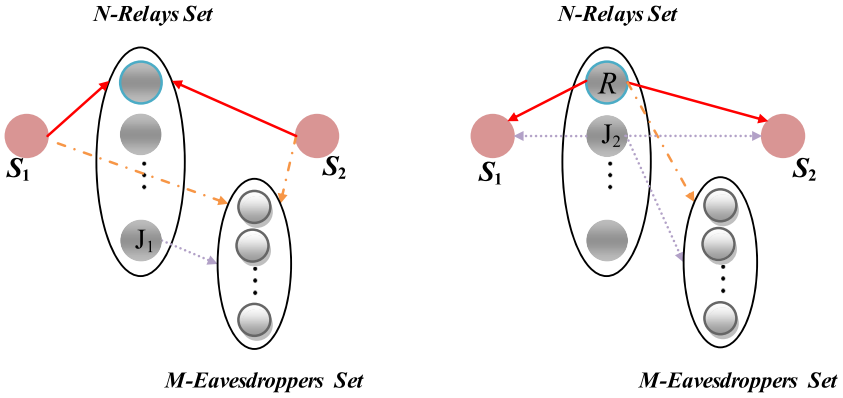
$$R_{S_i}^{|C_d|}(R,J_1,J_2)=\left[\frac{1}{2}\log_2(1+\Gamma_i)-\frac{1}{2}\log_2\left(1+\max_{E_m\in S_{eves}\forall m}\left\{\Gamma_{E_{m_j}}\right\}\right)\right]^+ \quad for|C_d|>0 \tag{7}$$

where Γ_i is given by (2) and $\Gamma_{E_{m_j}}$ can be expressed as follows

$$\Gamma_{E_{m_j}}=\frac{\gamma_{S_j,E_m}}{\gamma_{S_i,E_m}+\gamma_{J_1,E_m}+1}+\frac{\gamma_{R,E_m}}{\gamma_{J_2,E_m}+1} \tag{8}$$

Note that in (7) we have considered the worst case, in which the eavesdropper can achieve the maximum rate. In other words, the secrecy rate achieved at the destination node is limited by the maximum rate achieved at the eavesdroppers.

2nd scenario: when the eavesdroppers are cooperative (i.e. malicious eavesdroppers cooperate together in order to overhear the sources information). The instantaneous secrecy rate with the decoding set C_d for source S_i is given as (Lai and El Gamal, 2008);



a) 1st phase b) 2nd phase

Fig. 2 – Network model with multiple eavesdroppers.

$$R_{S_i}^{|C_d|}(R,J_1,J_2)=\left[\frac{1}{2}\log_2(1+\Gamma_i)-\frac{1}{2}\log_2\left(1+\sum_{m=1}^{M}\left(\Gamma_{E_{m_j}}\right)\right)\right]^{+} \quad for|C_d|>0 \tag{9}$$

where Γ_i and $\Gamma_{E_{m_j}}$ are given by (2), (8), respectively.

It is clear from (9) that the cooperation between the eavesdroppers adds more constraints on the achievable secrecy rate by the source nodes.

3. The proposed relay and jammers selection schemes

Three different categories of relay and jammers selection schemes including; selection schemes without jamming, selection schemes with conventional jamming (where the jamming signal is unknown at the destinations) and selection schemes with controlled jamming (where the jamming signal is known at the destinations) will be discussed in the following subsections.

3.1. *Selection schemes in the presence of one eavesdropper*

3.1.1. *Selection schemes without jamming*

In a conventional cooperative network, the relay scheme does not have a jamming process and therefore only one relay accesses the channel during the second phase of the protocol. The existing selections are summarized as follows:

- *Conventional Selection (CS)*

This solution does not take the eavesdropper channels into account, and the relay node is selected according to the instantaneous SNR of the channel between node S_1 and node S_2 (Krikidis, 2010). Therefore, the SINR given in (2) can be written as follows

$$\Gamma_i^{CS}=\gamma_{R,S_i} \tag{10}$$

Hence, the conventional selection scheme can be expressed as:

$$\begin{aligned}R^*&=\arg\max_{R\in C_d}\left\{R_{S_1}^{|C_d|}(R)+R_{S_2}^{|C_d|}(R)\right\}\\&=\arg\max_{R\in C_d}\left\{\frac{1}{2}\log_2(1+\Gamma_1^{CS})+\frac{1}{2}\log_2(1+\Gamma_2^{CS})\right\}\\&=\arg\max_{R\in C_d}\left\{(1+\Gamma_1^{CS})\cdot(1+\Gamma_2^{CS})\right\}\end{aligned} \tag{11}$$

Although the selection in (11) is an effective solution for non-eavesdropper environments, it cannot support the secrecy constraints for eavesdropper environments.

- *Optimal Selection (OS)*

This solution takes the relay-eavesdropper link into account and decides the relay node according to the knowledge set Ψ_0.The SINRs given in (2) and (3) can be rewritten as:

$$\Gamma_i^{OS}=\Gamma_i^{CS}=\gamma_{R,S_i} \tag{12}$$

$$\Gamma_{E_j}^{OS}=\frac{\gamma_{S_j,E}}{\gamma_{S_i,E}+1}+\gamma_{R,E} \tag{13}$$

The optimal selection scheme is given as (Zhou et al., 2013):

$$\begin{aligned}R^*&=\arg\max_{R\in C_d}\left\{R_{S_1}^{|C_d|}(R)+R_{S_2}^{|C_d|}(R)\right\}=\arg\max_{R\in C_d}\left\{\frac{1}{2}\log_2(1+\Gamma_1^{OS})\right.\\&\left.-\frac{1}{2}\log_2\left(1+\Gamma_{E_2}^{OS}\right)+\frac{1}{2}\log_2(1+\Gamma_2^{OS})-\frac{1}{2}\log_2\left(1+\Gamma_{E_1}^{OS}\right)\right\}\\&=\arg\max_{R\in C_d}\left\{\frac{1+\Gamma_1^{OS}}{1+\Gamma_{E_2}^{OS}}\cdot\frac{1+\Gamma_2^{OS}}{1+\Gamma_{E_1}^{OS}}\right\}\end{aligned} \tag{14}$$

- *Optimal Selection with Max-Min Instantaneous Secrecy Rate (OS-MMISR)*

It is common that the sum of the two sources secrecy rates, i.e.,$\{R_{S_1}^{|C_d|}(R)+R_{S_2}^{|C_d|}(R)\}$ may be driven down to a low level by the source with the lower secrecy rate. As a result, for a low complexity, the relay node, which maximizes the minimum secrecy rate of the two sources, can be selected to achieve a near-optimal performance. In addition, in some scenarios, the considered secrecy performance takes into account not only the total secrecy rate of both sources, but also the individual secrecy rate of each one. If one source has a low secrecy rate, the whole system is regarded as secrecy inefficient. The *OS-MMISR* scheme maximizes the worse instantaneous secrecy rate of the two sources with the assumption of knowledge set Ψ_0, and we can get

$$\begin{aligned}R^*&=\arg\max_{R\in C_d}\min\left\{R_{S_1}^{|C_d|}(R),\ R_{S_2}^{|C_d|}(R)\right\}\\&=\arg\max_{R\in C_d}\min\left\{\frac{1+\Gamma_1^{OS}}{1+\Gamma_{E_2}^{OS}},\ \frac{1+\Gamma_2^{OS}}{1+\Gamma_{E_1}^{OS}}\right\}\end{aligned} \tag{15}$$

where Γ_i^{OS} and $\Gamma_{E_j}^{OS}$ are given by (12) and (13), respectively.

- *Suboptimal Selection (SS)*

This scheme avoids the *OS* scheme instantaneous estimation of the relay eavesdropper link by deciding the appropriate relay based on the knowledge set Ψ_1. The suboptimal selection scheme can be written as (Krikidis, 2010):

$$R^*=\arg\max_{R\in C_d}\left\{\frac{1+\Gamma_1^{SS}}{1+\Gamma_{E_2}^{SS}}\cdot\frac{1+\Gamma_2^{SS}}{1+\Gamma_{E_1}^{SS}}\right\} \tag{16}$$

where

$$\Gamma_i^{SS}=\Gamma_i^{OS}=\gamma_{R,S_i} \tag{17}$$

$$\Gamma_{E_j}^{SS}=\frac{E\left[\gamma_{S_j,E}\right]}{E\left[\gamma_{S_i,E}\right]+1}+E\left[\gamma_{R,E}\right] \tag{18}$$

Comparing *OS* scheme in (14) and *SS* scheme in (16), *SS* scheme is more useful in practice as it depends on average channel knowledge for the eavesdropper links.

- *Suboptimal Selection with Max-Min Instantaneous Secrecy Rate (SS-MMISR)*

The *SS-MMISR* scheme maximizes the worse instantaneous secrecy rate of the two sources with the assumption of the knowledge set Ψ_1, and we can get

$$\begin{aligned} R^* &= \arg \max_{R\in C_d} \min\left\{R_{S_1}^{|C_d|}(R),\ R_{S_2}^{|C_d|}(R)\right\} \\ &= \arg \max_{R\in C_d} \min\left\{\frac{1+\Gamma_1^{SS}}{1+\Gamma_{E_2}^{SS}},\ \frac{1+\Gamma_2^{SS}}{1+\Gamma_{E_1}^{SS}}\right\} \end{aligned} \tag{19}$$

where Γ_i^{SS} and $\Gamma_{E_j}^{SS}$ are given by (17) and (18), respectively.

3.1.2. *Selection schemes with conventional jamming*

In this subsection, we present several node selection schemes based on the optimization problem given by (6) in order to maximize the expectation of the sum of the two sources' secrecy rates.

- *Optimal Selection with Jamming (OSJ)*

The optimal selection with jamming assumes the knowledge of the Ψ_0 set and ensures a maximization of the sum of instantaneous secrecy rates of node S_1 and node S_2 given in (4), which gives credit to:

$$\begin{aligned} (R^*,J_1^*,J_2^*) &= \arg \max_{\substack{J_1\in S_{relay}\\ R\in C_d\\ J_2\in\{S_{relay}-R^*\}}} \left\{R_S^{|C_d|}(R,J_1,J_2)\right\} \\ &= \arg \max_{\substack{J_1\in S_{relay}\\ R\in C_d\\ J_2\in\{S_{relay}-R^*\}}} \left\{\frac{1+\Gamma_1}{1+\Gamma_{E_2}}.\frac{1+\Gamma_2}{1+\Gamma_{E_1}}\right\} \end{aligned} \tag{20}$$

where Γ_i and Γ_{E_j} are given by (2) and (3), respectively. The cooperative relay and jammers selection in (20) tends to promote the system's secrecy performance by maximizingΓ_i, which promotes the assistance to the sources and minimizingΓ_{E_j}, which is equivalent to enhance the interference to the eavesdropper.

- *Optimal Selection with Jamming with Max-Min Instantaneous Secrecy Rate (OSJ-MMISR)*

In *OSJ-MMISR* scheme, the selected relay and jamming nodes aim to maximize the worse instantaneous secrecy rate of the two sources with the assumption of the knowledge set Ψ_0, and we can get

$$\begin{aligned} (R^*,J_1^*,J_2^*) &= \arg \max_{\substack{J_1\in S_{relay}\\ R\in C_d\\ J_2\in\{S_{relay}-R^*\}}} \min\left\{R_{S_1}^{|C_d|}(R,J_1,J_2),\ R_{S_2}^{|C_d|}(R,J_1,J_2)\right\} \\ &= \arg \max_{\substack{J_1\in S_{relay}\\ R\in C_d\\ J_2\in\{S_{relay}-R^*\}}} \min\left\{\frac{1+\Gamma_1}{1+\Gamma_{E_2}},\ \frac{1+\Gamma_2}{1+\Gamma_{E_1}}\right\} \end{aligned} \tag{21}$$

where Γ_i and Γ_{E_j} are given by (2) and (3), respectively.

- *Suboptimal Selection with Jamming (SSJ)*

In practice, an average knowledge of eavesdropper links available from long-term supervision of the eavesdropper transmission provides suboptimal selection metrics. The selection metric is modified as

$$(R^*,J_1^*,J_2^*) = \arg \max_{\substack{J_1\in S_{relay}\\ R\in C_d\\ J_2\in\{S_{relay}-R^*\}}} \left\{\frac{1+\Gamma_1}{1+\Gamma'_{E_2}}.\frac{1+\Gamma_2}{1+\Gamma'_{E_1}}\right\} \tag{22}$$

where Γ_i is given by (2) andΓ'_{E_j} can be calculated as follows

$$\Gamma'_{E_j} = \frac{E\left[\gamma_{S_j,E}\right]}{E\left[\gamma_{S_i,E}\right]+E\left[\gamma_{J_1,E}\right]+1} + \frac{E\left[\gamma_{R,E}\right]}{E\left[\gamma_{J_2,E}\right]+1} \tag{23}$$

- *Suboptimal Selection with Jamming with Max-Min Instantaneous Secrecy Rate (SSJ-MMISR)*

In *SSJ-MMISR* scheme, the selection policy maximizes the worse instantaneous secrecy rate of the two sources with the assumption of the knowledge set Ψ_1. The selection metric is modified as:

$$(R^*,J_1^*,J_2^*) = \arg \max_{\substack{J_1\in S_{relay}\\ R\in C_d\\ J_2\in\{S_{relay}-R^*\}}} \min\left\{\frac{1+\Gamma_1}{1+\Gamma'_{E_2}},\ \frac{1+\Gamma_2}{1+\Gamma'_{E_1}}\right\} \tag{24}$$

where Γ_i andΓ'_{E_j} are given by (2) and (23), respectively.

3.1.3. *Selection schemes with controlled jamming*

In this subsection, an optimal selection with controlled jamming (*OSCJ*) scheme is proposed. Unlike the previous conventional jamming schemes, where the jamming signal is unknown at destinations and eavesdropper, *OSCJ* scheme assumes that the jamming signal can be decoded at destinations but not at eavesdropper. In this case, the SINR of the link from S_j (for $j = 1, 2$) to E remains the same as given by (3). The SINR of the link from S_j to S_i (for $i, j = 1, 2$, $i \neq j$) is modified as follows:

$$\Gamma_i^{OSCJ} = \gamma_{R,S_i} \tag{25}$$

3.1.4. *Hybrid selection schemes*

- *Optimal Switching (OW)*

The original idea of using jamming nodes is to introduce interference on the eavesdropper links. However, based on the assumption that jamming signal is unknown at destinations, the continuous jamming from J_2 in the second phase may decrease the secrecy rate of both sources seriously, specifically when J_2 is close to one destination. In order to overcome this "negative jamming" effect which leads to excessive interference at destinations, we propose an intelligent hybrid selection scheme which switches between optimal selection with jamming and optimal selection without jamming. The required condition for the participation of the jamming nodes is

$$\left\{R_{S_1}^{|C_d|}(R,J_1,J_2)+R_{S_2}^{|C_d|}(R,J_1,J_2)\right\}_{OSJ} > \left\{R_{S_1}^{|C_d|}(R)+R_{S_2}^{|C_d|}(R)\right\}_{OS}$$

i.e.,

$$\left\{\frac{1+\Gamma_1}{1+\Gamma_{E_2}}\cdot\frac{1+\Gamma_2}{1+\Gamma_{E_1}}\right\} > \left\{\frac{1+\Gamma_1^{OS}}{1+\Gamma_{E_2}^{OS}}\cdot\frac{1+\Gamma_2^{OS}}{1+\Gamma_{E_1}^{OS}}\right\} \quad (26)$$

where Γ_i, Γ_{E_j}, Γ_i^{OS} and $\Gamma_{E_j}^{OS}$ are given by (2), (3), (12) and (13), respectively.

If the condition in (26) was achieved, the *OSJ* scheme provides higher instantaneous secrecy rate than *OS* does and is preferred. Otherwise the *OS* scheme is more efficient in promoting the system's secrecy performance and should be employed. Because of the uncertainty of the channel coefficient $h_{m,n}$ for each channel $m \to n$, *OW* should outperform either the continuous jamming scheme or the non-jamming one.

$$R^* = \arg \max_{R\in C_d} \left\{\frac{1+\Gamma_1^{OS}}{1+\max_{E_m\in S_{eves}\forall m}\left(\Gamma_{E_{m_2}}^{OS}\right)}\cdot\frac{1+\Gamma_2^{OS}}{1+\max_{E_m\in S_{eves}\forall m}\left(\Gamma_{E_{m_1}}^{OS}\right)}\right\} \quad (28)$$

where Γ_i^{OS} is given by (12) and $\Gamma_{E_{m_j}}^{OS}$ can be expressed as follows

$$\Gamma_{E_{m_j}}^{OS} = \frac{\gamma_{S_j,E_m}}{\gamma_{S_i,E_m}+1}+\gamma_{R,E_m} \quad (29)$$

3.2.1.2. Selection schemes with conventional jamming. As in Al-nahari et al. (2012) the selection policy which maximizes the instantaneous secrecy rate given in (7) and therefore maximizes the sum of the two sources secrecy rates given in (4), assuming that $|C_d| > 0$ is given as

$$(R^*,J_1^*,J_2^*) = \arg \max_{\substack{J_1\in S_{relay}\\ R\in C_d\\ J_2\in\{S_{relay}-R^*\}}} \left\{\frac{1+\Gamma_1}{1+\max_{E_m\in S_{eves}\forall m}\left(\Gamma_{E_{m_2}}\right)}\cdot\frac{1+\Gamma_2}{1+\max_{E_m\in S_{eves}\forall m}\left(\Gamma_{E_{m_1}}\right)}\right\} \quad (30)$$

- ***Suboptimal Switching (SW)***

Given the fact that jamming is not always a positive process for the performance of the system, the suboptimal switching (SW) scheme uses the available knowledge set Ψ_1 to make intelligent switching between *SSJ* and *SS* schemes. More specifically, the required condition for switching from *SS* to *SSJ* is

where Γ_i and $\Gamma_{E_{m_j}}$ are given by (2) and (8), respectively.

3.2.1.3. Selection schemes with controlled jamming. In this scheme, the selection policy which maximizes the instantaneous secrecy rate given in (7) and therefore maximizes the sum of the two sources secrecy rates given in (4) assuming that $|C_d| > 0$ is given as (Al-nahari et al., 2012)

$$(R^*,J_1^*,J_2^*) = \arg \max_{\substack{J_1\in S_{relay}\\ R\in C_d\\ J_2\in\{S_{relay}-R^*\}}} \left\{\frac{1+\Gamma_1^{OSCJ}}{1+\max_{E_m\in S_{eves}\forall m}\left(\Gamma_{E_{m_2}}\right)}\cdot\frac{1+\Gamma_2^{OSCJ}}{1+\max_{E_m\in S_{eves}\forall m}\left(\Gamma_{E_{m_1}}\right)}\right\} \quad (31)$$

$$\left\{R_{S_1}^{|C_d|}(R,J_1,J_2)+R_{S_2}^{|C_d|}(R,J_1,J_2)\right\}_{SSJ} > \left\{R_{S_1}^{|C_d|}(R)+R_{S_2}^{|C_d|}(R)\right\}_{SS}$$

i.e.,

$$\left\{\frac{1+\Gamma_1}{1+\Gamma'_{E_2}}\cdot\frac{1+\Gamma_2}{1+\Gamma'_{E_1}}\right\} > \left\{\frac{1+\Gamma_1^{SS}}{1+\Gamma_{E_2}^{SS}}\cdot\frac{1+\Gamma_2^{SS}}{1+\Gamma_{E_1}^{SS}}\right\} \quad (27)$$

where Γ_i, Γ'_{E_j}, Γ_i^{SS} and $\Gamma_{E_j}^{SS}$ are given by (2), (23), (17) and (18), respectively.

where Γ_i^{OSCJ} and $\Gamma_{E_{m_j}}$ are given by (25) and (8), respectively.

3.2. *Selection schemes in the presence of multiple eavesdroppers*

3.2.1. Selection schemes with non-cooperating eavesdroppers

3.2.1.1. Selection schemes without jamming. As in Al-nahari et al. (2012) the optimal relay selection is given by

3.2.2. Selection schemes with cooperating eavesdroppers

3.2.2.1. Selection schemes without jamming. As in Ibrahim et al. (2013) the optimal relay selection is given by

$$R^* = \arg \max_{R\in C_d} \left\{\frac{1+\Gamma_1^{OS}}{1+\sum_{m=1}^{M}\left(\Gamma_{E_{m_2}}^{OS}\right)}\cdot\frac{1+\Gamma_2^{OS}}{1+\sum_{m=1}^{M}\left(\Gamma_{E_{m_1}}^{OS}\right)}\right\} \quad (32)$$

where Γ_i^{OS} and $\Gamma_{E_{m_j}}^{OS}$ are given by (12) and (29), respectively.

3.2.2.2. Selection schemes with conventional jamming. As in Ibrahim et al. (2013) the selection policy which maximizes the instantaneous secrecy rate given in (9) and therefore maximizes the sum of the two sources secrecy rates given in (4) assuming that $|C_d| > 0$ is given as

$$(R^*, J_1^*, J_2^*) = \arg \max_{\substack{J_1 \in S_{relay} \\ R \in C_d \\ J_2 \in \{S_{relay} - R^*\}}} \left\{ \frac{1+\Gamma_1}{1+\sum_{m=1}^{M}\left(\Gamma_{E_{m_2}}\right)} \cdot \frac{1+\Gamma_2}{1+\sum_{m=1}^{M}\left(\Gamma_{E_{m_1}}\right)} \right\} \tag{33}$$

where Γ_i and $\Gamma_{E_{m_j}}$ are given by (2) and (8), respectively.

3.2.2.3. *Selection schemes with controlled jamming*. In this scheme, the selection policy which maximizes the instantaneous secrecy rate given in (9) and therefore maximizes the sum of the two sources secrecy rates given in (4) assuming that $|C_d| > 0$ is given as (Ibrahim et al., 2013)

$$(R^*, J_1^*, J_2^*) = \arg \max_{\substack{J_1 \in S_{relay} \\ R \in C_d \\ J_2 \in \{S_{relay} - R^*\}}} \left\{ \frac{1+\Gamma_1^{OSCJ}}{1+\sum_{m=1}^{M}\left(\Gamma_{E_{m_2}}\right)} \cdot \frac{1+\Gamma_2^{OSCJ}}{1+\sum_{m=1}^{M}\left(\Gamma_{E_{m_1}}\right)} \right\} \tag{34}$$

where Γ_i^{OSCJ} and $\Gamma_{E_{m_j}}$ are given by (25) and (8), respectively.

4. Numerical results and discussion

In this section, we provide computer simulations to show the effectiveness of the proposed selection schemes in improving ergodic secrecy rate and secrecy outage probability of the two-way cooperative networks. For simplicity, the sources and the relay transmit with the same power, i.e. $P^{(S)} = P^{(R)}$. The relay and the jammers transmit with a relay-jammer power ratio $L = 100$. The transmission spectral efficiency is equal to $R_0 = 2$ bits per channel use (BPCU) and the target secrecy rate is equal to $R_T = 0.1$ BPCU. The secrecy performance is discussed for two different network models as follows;

4.1. *Secrecy performance for single eavesdropper model*

The simulation environment of this model was presented in Fig. 1 and consists of two sources S_1, S_2, one eavesdropper E and an intermediate nodes cluster with $N = 4$ nodes. All the nodes are located in a 2-D square topology within a 1×1 unit square. The sources and the eavesdropper are fixed at $\{X_{S1}, Y_{S1}\} = \{0, 0\}$, $\{X_{S2}, Y_{S2}\} = \{1, 0\}$ and $\{X_E, Y_E\} = \{0.5, 1\}$, respectively. While the relays are located randomly in the 2-D space considered and their exact location is given for each example separately.

4.1.1. *Secrecy performance when changing the N-Relays set location in the considered area*
We have three different topologies as follows;

4.1.1.1. *Topology 1: when the N-Relays are distributed dispersedly between* S_1, S_2 *and* E *nodes*. Fig. 3 shows the considered topology, as well as the ergodic secrecy rate of the different selection schemes. It is clear that the selection

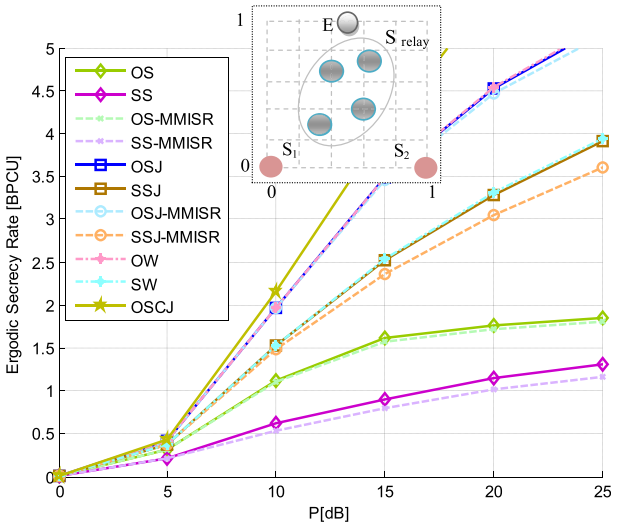


Fig. 3 – Ergodic secrecy rate versus transmitted power (*P*) of different selection schemes when the relays are distributed dispersedly between S_1, S_2 and *E*.

schemes with jamming outperform their non-jamming counterparts along the transmitted power range. For example at $P = 20$ dB, the ergodic secrecy rate of *OSJ* is approximately higher than that of *OS* by 3 BPCU and the ergodic secrecy rate of *SSJ* is approximately higher than that of *SS* by 2 BPCU. In addition, we can see that in this topology, the selection schemes which maximize the minimum instantaneous secrecy rates of the two-sources (e.g., *OS-MMISR*, *SS-MMISR*, *OSJ-MMISR* and *SSJ-MMISR*) have a slightly lower ergodic secrecy rate than the corresponding optimal ones (e.g., *OS*, *SS*, *OSJ* and *SSJ*). Therefore, they can be used in order to get the appropriate relay and the jamming nodes. Regarding to the hybrid schemes, it can be seen that *OW* and *SW* schemes perform almost the same as *OSJ* and *SSJ* schemes, respectively, as the jamming schemes are the best in promoting system's secrecy performance than the non-jamming ones. It is also clear that, the performance of *OSCJ* scheme outperforms all the other selection schemes and achieves the highest ergodic secrecy rate when the transmitted power increases due to the ability of the destinations to decode the artificial interference in this scheme.

Fig. 4 shows the secrecy outage probability metric of the considered selection schemes using the above topology. The presented results are in line with the above ergodic secrecy rate results and show that the integration of jamming provides lower secrecy outage probability for both *OS* and *SS* schemes. Furthermore, all the near optimal selection schemes have a slightly higher secrecy outage probability than the corresponding optimal ones along the transmitted power range, except *OSJ-MMISR* scheme which shows a considerable higher outage probability than *OSJ* for $P > 20$ dB. Regarding the hybrid schemes, the *OW* follows the *OSJ* performance and *SW* has a lower outage probability than *SSJ* when the transmitted power increases. We also note that the *OSCJ* scheme gives the best performance because the effect of jamming signals is removed at the destination nodes.

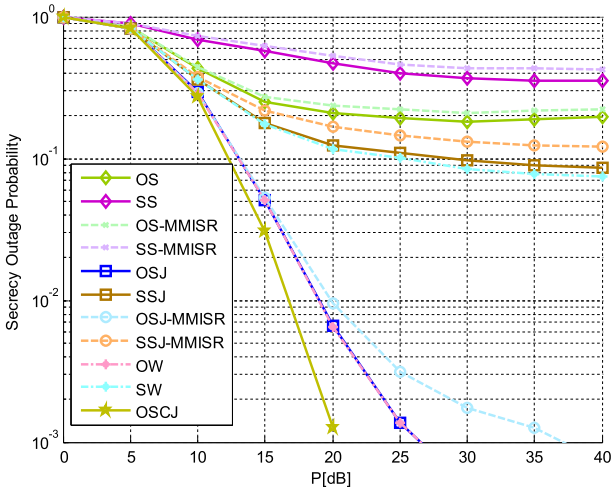


Fig. 4 – Secrecy outage probability versus P of the different selection schemes with $R_T = 0.1$ BPCU and $R_0 = 2$ BPCU.

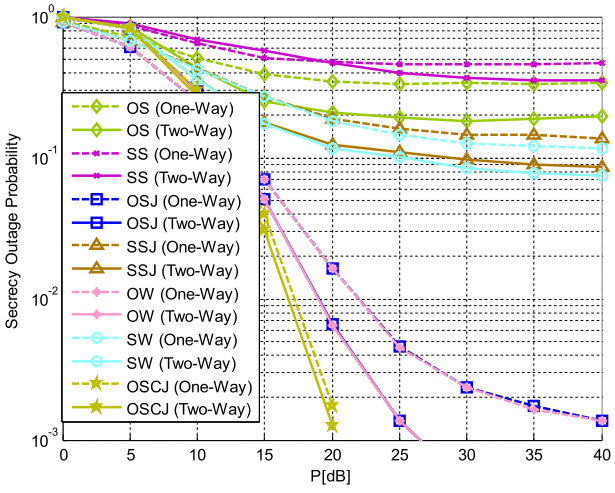


Fig. 6 – Secrecy outage probability versus P for the two-way proposed selection schemes and the one-way schemes presented in Ibrahim et al. (2013).

Figs. 5 and 6 present a comparison between proposed two-way relay and jammers selection schemes and one-way schemes presented in Ibrahim et al. (2013) in terms of ergodic secrecy rate and secrecy outage probability, respectively. The obtained results show that when the relays are distributed dispersedly between S_1, S_2 and E all the proposed schemes outperform the schemes presented in Ibrahim et al. (2013), especially when the transmitted power is increased.

4.1.1.2. Topology 2: when the N-Relays are located close to the eavesdropper (E) node. Fig. 7 shows the considered topology, as well as the ergodic secrecy rate of the different selection schemes. It is clear that the performance of non-jamming approaches is very bad as the relays have a strong link with the eavesdropper. On the other hand, the jamming schemes confuse the eavesdropper and increase significantly the ergodic secrecy rate. For this configuration, the *OS-MMISR*, *SS-MMISR*, *OSJ-MMISR* and *SSJ-MMISR* selection schemes have almost the same performance as *OS*, *SS*, *OSJ* and *SSJ* selection schemes, respectively. Furthermore, the hybrid schemes (*OW*, *SW*) have a similar performance to the jamming schemes (*OSJ*, *SSJ*) as jamming is always beneficial in this case. We also note that the *OSCJ* scheme gives the best performance because the effect of jamming signals is removed at the destination nodes.

Fig. 8 shows the secrecy outage probability metric for the considered selection schemes using the above topology. The obtained results show that *OSJ* and *SSJ* provide a lower secrecy outage probability than *OS* and *SS* selection schemes, respectively. *OSJ-MMISR* and *SSJ-MMISR* schemes have a higher outage probability than *OSJ* and *SSJ* schemes for

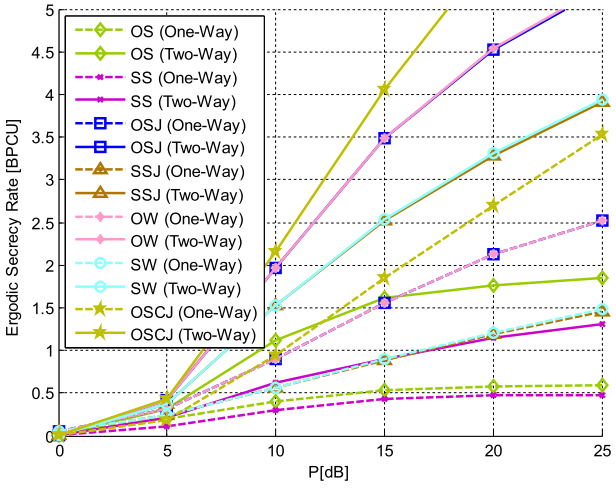


Fig. 5 – Ergodic secrecy rate versus P for the two-way proposed selection schemes and the one-way schemes presented in Ibrahim et al. (2013).

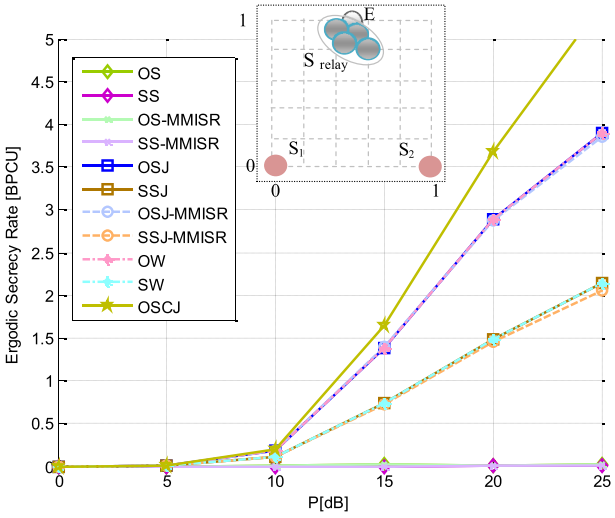


Fig. 7 – Ergodic secrecy rate versus P of different selection schemes when the relays located close to E.

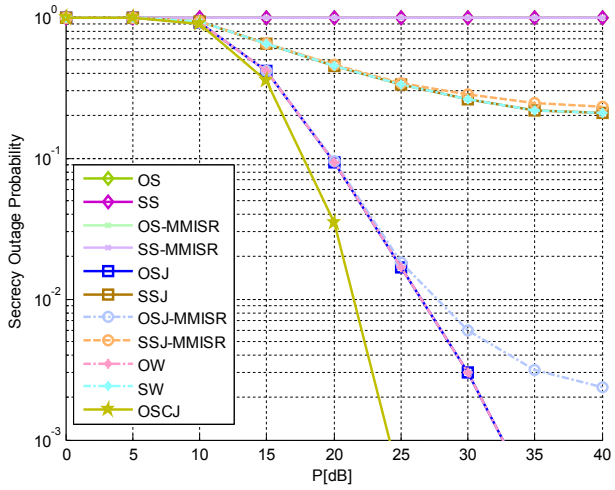


Fig. 8 – Secrecy outage probability versus P for the different selection schemes with $R_s = 0.1$ BPCU and $R_0 = 2$ BPCU.

$P > 25$ dB. Regarding the hybrid schemes, the *OW* and *SW* schemes follow the performance of jamming schemes *OSJ* and *SSJ*, respectively. We also note that the *OSCJ* scheme achieves the lowest outage probability.

4.1.1.3. *Topology 3: when the N-Relays are located close to one of the source nodes, for example* S_2. Fig. 9 shows the considered topology, as well as ergodic secrecy rate of the different selection schemes. As can be seen, for this scenario, continuous jamming schemes introduce high interference at the source node S_2 and become less efficient. The main reason for this result is that for strong source-relay links, jamming becomes stronger at high SNRs and can decrease the secrecy performance achieved. On the other hand, non-jamming schemes increase significantly the ergodic secrecy rate. It is clear that, in this topology there is a difference in the ergodic secrecy rate

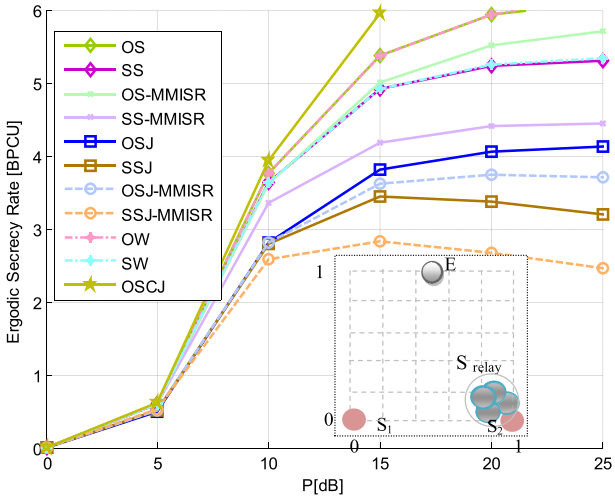


Fig. 9 – Ergodic secrecy rate versus P of different selection schemes when the relays located close to S_2.

of *OS-MMISR*, *SS-MMISR*, *OSJ-MMISR* and *SSJ-MMISR* selection schemes and that of *OS*, *SS*, *OSJ* and *SSJ* schemes, respectively so they cannot be used instead of them. As far as the hybrid schemes are concerned, both the *OW* and *SW* schemes follow the same non-jamming schemes *OS* and *SS* behavior, respectively. For *OSCJ* scheme still achieves the highest ergodic secrecy rate.

From Figs. 3, 7 and 9 we can conclude that, the hybrid switching schemes; *OW* and *SW* follow either the jamming schemes behavior as in Figs. 3 and 7 or the non-jamming schemes behavior as in Fig. 9 based on what either promotes system's secrecy performance.

Tables 1 and 2 present the ergodic secrecy rate and secrecy outage probability comparison of the proposed selection schemes for different topologies at $P = 20$ dB, respectively.

From Tables 1 and 2, we can conclude the following:

- In **topology 1**, where S_{relay} distributed dispersedly between S_1, S_2 and E nodes, the jamming schemes have a considerable effect in improving both system's secrecy metrics. *OS-MMISR*, *SS-MMISR*, *OSJ-MMISR* and *SSJ-MMISR* selection schemes show a slight degradation in system performance compared with *OS*, *SS*, *OSJ* and *SSJ* schemes, respectively. The hybrid switching schemes *OW* and *SW* almost follow the jamming schemes *OSJ* and *SSJ* behavior, respectively as jamming schemes are preferred in this case.
- In **topology 2**, where S_{relay} is close to E node, the non-jamming schemes are inefficient but the jamming schemes confuse the eavesdropper and significantly improve the secrecy performance. The *OS-MMISR*, *SS-MMISR*, *OSJ-MMISR* and *SSJ-MMISR* selection schemes have almost the same performance as *OS*, *SS*, *OSJ* and *SSJ* schemes, respectively. For the hybrid schemes, they follow the jamming schemes behavior.
- In **topology 3**, where S_{relay} is close to S_2 source node, in this topology the non-jamming schemes give better performance than jamming schemes. *OS-MMISR*, *SS-MMISR*, *OSJ-MMISR* and *SSJ-MMISR* selection schemes show a noticeable degradation in secrecy performance compared with *OS*, *SS*, *OSJ* and *SSJ* schemes, respectively. For hybrid schemes, they follow non-jamming schemes behavior due to their efficiency.
- In the three topologies, the *OSCJ* scheme outperforms all the other selection schemes as it provides the highest ergodic secrecy rate and the lowest secrecy outage probability.

4.1.2. *Secrecy performance when changing the eavesdropper location with respect to the two sources* (S_1 *and* S_2)

Fig. 10 shows the considered topology, as well as ergodic secrecy rate of the different selection schemes. It is clear that the non-jamming approaches are inefficient due to the strong link between the sources and the eavesdropper. On the other hand, jamming schemes confuse the eavesdropper and increase significantly the ergodic secrecy rate. For this configuration, the *OS-MMISR*, *SS-MMISR*, *OSJ-MMISR* and *SSJ-MMISR* selection schemes have almost the same performance as *OS*, *SS*, *OSJ* and *SSJ* selection schemes respectively. Furthermore, the hybrid schemes (*OW*, *SW*) have a similar performance to the jamming schemes (*OSJ*, *SSJ*) as jamming is always

Table 1 – Ergodic secrecy rate comparison of proposed selection schemes for the three different topologies at $P = 20$ dB.

Topologies	Schemes without jamming				Conventional jamming				Controlled jamming	Hybrid schemes	
	OS	*SS*	*OS-MMISR*	*SS-MMISR*	*OSJ*	*SSJ*	*OSJ-MMISR*	*SSJ-MMISR*	*OSCJ*	*OW*	*SW*
Topology 1	1.7688	1.1455	1.7239	1.0091	4.5282	3.2885	4.4652	3.0411	5.7078	4.5330	3.3135
Topology 2	0.0146	0.0010	0.0146	0.0014	2.8902	1.4822	2.8785	1.4514	3.6745	2.8902	1.4822
Topology 3	5.9340	5.2313	5.5106	4.4099	4.0674	3.3855	3.7527	2.6818	7.2704	5.9467	5.2521

Table 2 – Secrecy outage probability comparison of proposed selection schemes for the three different topologies at $P = 20$ dB.

Topologies	Schemes without jamming				Conventional jamming				Controlled jamming	Hybrid schemes	
	OS	*SS*	*OS-MMISR*	*SS-MMISR*	*OSJ*	*SSJ*	*OSJ-MMISR*	*SSJ-MMISR*	*OSCJ*	*OW*	*SW*
Topology 1	2.1e-1	4.7e-1	2.4e-1	5.3e-1	6.6e-3	1.2e-1	9.5e-3	1.7e-1	1.3e-3	6.5e-3	1.2e-1
Topology 2	9.9e-1	9.9e-1	9.9e-1	9.9e-1	9.4e-2	4.5e-1	9.4e-2	4.6e-1	3.5e-2	9.4e-2	4.5e-1
Topology 3	5e-4	6e-4	3.9e-3	1.3e-2	3.6e-3	4.7e-2	2.9e-2	1.4e-1	4e-4	5e-4	6e-4

beneficial in this case. We also note that the *OSCJ* scheme gives the best performance because the effect of jamming signals is removed at the destination nodes.

From Figs. 3 and 10 we can conclude that the performance of all the selection schemes is degraded when the eavesdropper node approaching to S_1 and S_2 nodes.

4.2. *Secrecy performance for multiple eavesdroppers model*

The simulation environment for this model follows the model presented in Fig. 2. Assuming the presence of two eavesdroppers which are fixed at $\{x_{E_i}, y_{E_i}\}_{i=1}^{2} = \{(0.5, 1), (0, 0.5)\}$. Figs. 11 and 12 present the ergodic secrecy rate and secrecy outage probability comparison for $N = 4$ and $M = 2$ cooperating and non-cooperating eavesdroppers, respectively. The obtained results show that eavesdroppers' cooperation degrades both secrecy metrics.

Fig. 13 shows the ergodic secrecy rate versus P for $N = 4$ and $M = 3$ cooperating eavesdroppers which are fixed at $\{x_{E_i}, y_{E_i}\}_{i=1}^{3} = \{(0.5, 1), (0, 0.5), (1, 0.5)\}$.

Comparing Figs. 3, 11 and 13 we can conclude that, increasing the number of cooperating eavesdroppers in the system results in:

- Degrade the performance of different selection schemes.
- Optimal selection scheme without jamming (*OS*) becomes inefficient and should not be used in these systems.
- Increase the demand for using optimal selection scheme with jamming (*OSJ*) in these systems due to the ability of jamming nodes to confuse eavesdroppers and increase significantly the ergodic secrecy rate.

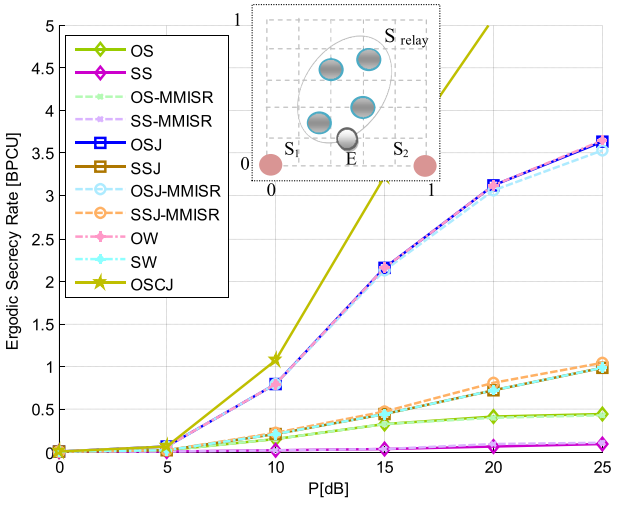


Fig. 10 – Ergodic secrecy rate versus P of different selection schemes when E located close to S_1 and S_2.

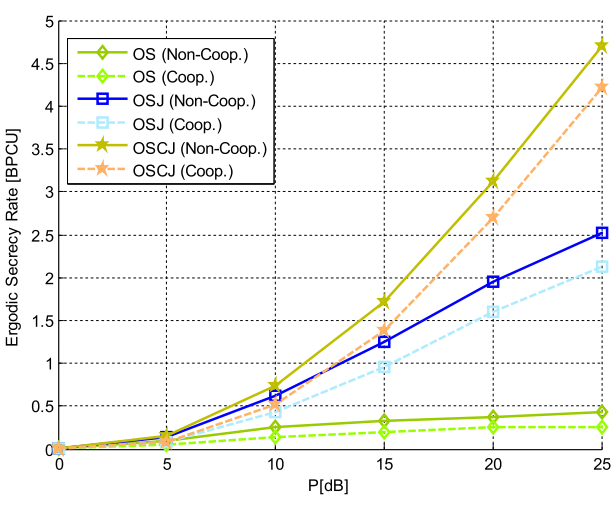


Fig. 11 – Ergodic secrecy rate versus P for $M = 2$ non-cooperating and cooperating eavesdroppers.

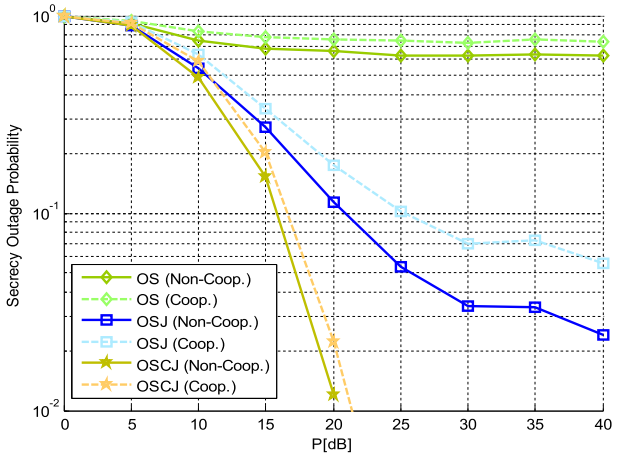


Fig. 12 – Secrecy outage probability versus P for M = 2 non-cooperating and cooperating eavesdroppers.

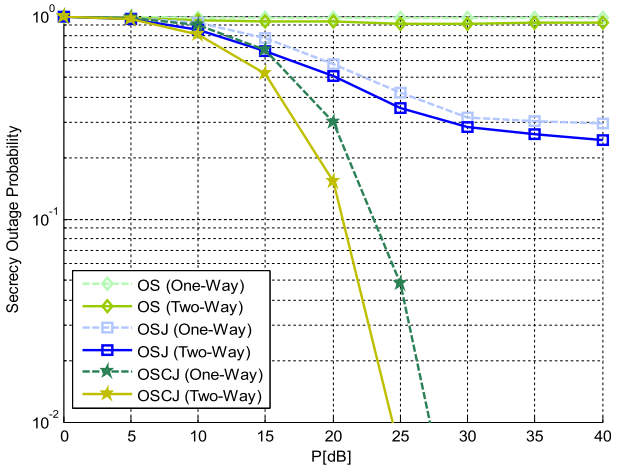


Fig. 14 – Secrecy outage probability versus P for the two-way proposed selection schemes and the one-way schemes presented in (Ibrahim et al., 2013) in the presence of M = 3 cooperating eavesdroppers.

Fig. 14 shows secrecy outage probability metric comparison of the proposed two-way selection schemes and the one-way schemes presented in Ibrahim et al. (2013) in the presence of $M = 3$ cooperating eavesdroppers. The obtained results show that, the proposed two-way selection schemes have a lower secrecy outage probability than one-way schemes presented in Ibrahim et al. (2013).

5. Conclusion

Three categories of relay and jammers selection schemes were proposed in this paper to improve the physical layer security of two-way cooperative networks. These categories are; selection schemes without jamming, selection schemes with conventional jamming and selection schemes with controlled jamming. Moreover, a hybrid scheme which switches between selection schemes with jamming and schemes without jamming was introduced to overcome the negative effects of interference. The obtained results showed the effectiveness of hybrid switching schemes (e.g., *OW*, *SW*) which follow the behavior of *OSJ* and *SSJ* jamming schemes when *N*-relays are distributed dispersedly between system nodes and when they are located close to eavesdropper, and follow the behavior of *OS* and *SS* (without jamming) schemes when *N*-relays are located close to one of source nodes. Despite the eavesdroppers' cooperation which further degrades secrecy performance, the proposed selection schemes are still able to improve both the secrecy rate and the secrecy outage probability especially the *OSJ* scheme. Finally, we showed the effectiveness of the proposed two-way relay selection schemes over the one-way relay selection schemes in promoting the system's secrecy performance.

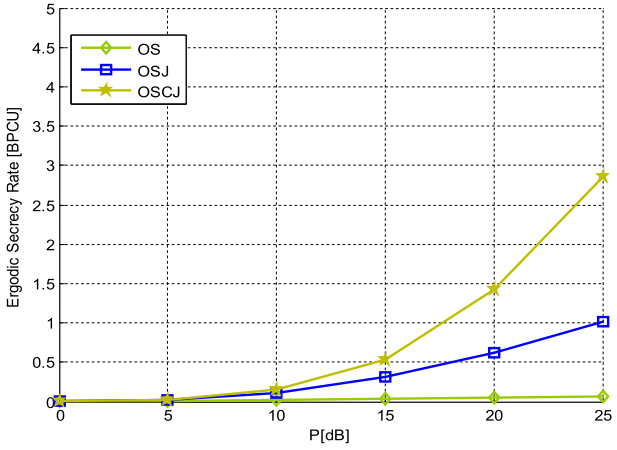


Fig. 13 – Ergodic secrecy rate versus P for N = 4 and M = 3 cooperating eavesdroppers.

REFERENCES

Al-nahari AY, Krikidis I, Ibrahim AS, Dessouky MI, Abd El-Samie FE. Relaying techniques for enhancing the physical layer secrecy in cooperative networks with multiple eavesdroppers. Trans Emerg Telecommun Technol Nov. 2012. http://dx.doi.org/10.1002/ett.2581.

Beres E, Adve R. Selection cooperation in multi-source cooperative networks. IEEE Trans Wirel Commun Jan. 2008;7:118–27.

Chen J, Zhang R, Song L, Han Z, Jiao B. Joint relay and jammer selection for secure decode-and-forward two-way relay networks. In: In proc. of communications (ICC), IEEE international conference; 2011.

Chen J, Zhang R, Song L, Han Z, Jiao B. Joint relay and jammer selection for secure two-way relay networks. Inf Forensics Secur IEEE Trans Feb. 2012;7(1):310–20.

Csiszar I, Korner J. Broadcast channels with confidential messages. IEEE Trans Inf Theory July 1978;24:451–6.

Dong L, Han Z, Petropulu AP, Poor HV. Amplify-and forward based cooperation for secure wireless communications. In: Proc.

IEEE int. conf. acoustics, speech, and signal processing, Taipei, Taiwan; Apr. 2009.
Dong L, Han Z, Petropulu AP, Poor HV. Secure wireless communications via cooperation. In: Proc. Allerton conf. commun. cont. comp., Urbana-Champaign, IL, USA; Sept. 2008.
Hassan ES. Energy-efficient hybrid opportunistic cooperative protocol for single-carrier frequency division multiple access-based networks. IET Commun 2012;6(16):2602–12.
Ibrahim AS, Sadek AK, Su W, Liu KJ. Cooperative communications with relay selection: when to cooperate and whom to cooperate with. IEEE Trans Wirel Commun Jul. 2008;7:2814–27.
Ibrahim Doaa H, Hassan Emad S, El-Dolil Sami A. A new relay and jammer selection schemes for secure one-way cooperative networks. Wirel Personal Commu 2013;72(no. 2). http://dx.doi.org/10.1007/s11277-013-1384-5.
Krikidis I. Opportunistic relay selection for cooperative networks with secrecy constraints. IET Commun 2010;4:1787–91.
Krikidis I. Relay selection for secure cooperative networks with jamming. IEEE Trans Wirel Commun Oct. 2009;8:5003–11.
Lai L, El Gamal H. The relay-eavesdropper channel: cooperation for secrecy. IEEE Trans Inf Theory Sept. 2008;54:4005–19.
Liang Y, Poor HV, Ying L. Wireless broadcast networks: reliability, security, and stability. In: Proc IEEE inf theory appl work, San Diego, CA, USA; Feb. 2008. p. 249–55.
Liang Y, Poor HV, Shamai S. Secure communication over fading channels. IEEE Trans Inf Theory Jun. 2008;54(6):2470–92.
Popovski P, Simeone O. Wireless secrecy in cellular systems with infrastructure-aided cooperation. IEEE Trans Inf Foren Sec June 2009;4:242–56.
Rankov B, Wittneben A. Spectral efficient protocols for half duplex fading relay channels. IEEE J Sel Areas Commun Feb. 2007;25(2):379–89.
Rankov B, Wittneben A. Achievable rate regions for the two-way relay channel. In: Proc. IEEE int. symp. information theory, Seattle, WA; Jul. 2006.
Simeone O, Popovski P. Secure communications via cooperating base stations. IEEE Commun Lett Mar. 2008;12:188–90.
Tekin E, Yener A. The general Gaussian multiple access and two-way wire-tap channels: achievable rates and cooperative jamming. IEEE Trans Inf Theory June 2008;54:2735–51.
Wyner AD. The wire-tap channel. Bell Syst Tech J Jan. 1975;54:1355–87.
Zhou N, Chen X, Li C, Lai Q. Relay selection for physical layer security in decode-and-forward two-way relay networks. J Inf Comput Sci Dec. 2013:5821–8. http://dx.doi.org/10.12733/jics20102372.

Emad S. Hassan received the B.Sc. (Honors), M.Sc., and Ph.D. from the Faculty of Electronic Engineering, Menoufia University, Egypt, in 2003, 2006, and 2010, respectively. He joined the teaching staff of the Department of Electronics and Electrical Communications, Faculty of Electronic Engineering, Menoufia University, Egypt, in 2010. In 2008, he joined the Communications Research Group at Liverpool University, Liverpool, UK, as a Visitor Researcher. His current research areas of interest include image processing, digital communications, cooperative communication, cognitive radio networks, OFDM, SC-FDE, MIMO and CPM based systems.

Doaa H. Ibrahim received the B.Sc. (Honors) in Electronics and Electrical Communications Engineering from Faculty of Electronic Engineering, Department of Electronics and Electrical Communications, Menoufia University, Egypt, in 2009. She works as a design engineer at Benha Company for Electronic Industries, Benha, Qalubeia, Egypt, from 2010. Now she working toward the MSc. degree at the Department of Electronics and Electrical Communications, Faculty of Electronic Engineering, Menoufia University, Egypt. Her current research areas of interest include image processing, digital communications, cooperative communications and cognitive radio networks.

Sami A. El-Dolil received his B.Sc., M.Sc., and Ph.D.degrees in Electronic Engineering from Menoufia University, Menouf, Egypt, in 1977, 1981, and 1989 respectively. In 1986 he joined the communications Research Group at Southampton University, Southampton, England, as a Research Student. He was a Post Doctor Research Fellow at the Department of Electronics and Computer Science, University of Southampton, 1991–1993. He is working as a Professor at the Department of Electronics and Electrical Communications, Faculty of Electronic Engineering, Menoufia University, Menouf, Egypt. His current research interests are in high-capacity digital mobile systems and multimedia networks.