Wireless Personal Communications (2019) 104:949–977
https://doi.org/10.1007/s11277-018-6062-1

On the Security of Relay Assisted Cognitive Radio Networks in the Presence of Primary Transceiver Network

Waleed Saad[1,3] · Mona Shokair[1] · Shady M. Ibraheem[1,2]

Published online: 1 November 2018

Abstract
In this paper, the benefit of distinguishable diversity order within a co-operative relay system is exploited to overcome the problem of secure communication in an underlay wiretap cognitive radio network. This network is in a coexistence with a primary transceiver network and it is subjected to multiple eavesdropping attacks which employ a specific interception strategy. To improve the physical layer security, simple relay selection schemes will be proposed that aims at maximizing the minimum of the dual hop communication secrecy rates under primary network constraints. For Rayleigh fading channels, exact and asymptotic closed form expressions will be derived for the secondary system outage and secrecy rate. Furthermore, based on the network topology, tight inner and outer bounds will subsequently be derived on the system secrecy outage probability. By employing analytical and simulation results, the gain of the system diversity order is obviously investigated and emphasized.

Keywords Relay selection · Multiple eavesdroppers · Co-operative eavesdroppers · Outage probability · Secrecy rate · Power constraints

1 Introduction

Cognitive radio network (CR) is a useful tool for solving the problem of scarcity of spectral resources and to provide a spectral efficiency by licensed/unlicensed spectrum sharing [1]. In cognitive radio networks, it is permissible to unlicensed secondary users (SUs) to

✉ Shady M. Ibraheem
shadymam@gmail.com

Waleed Saad
waleed.saad@el-eng.menofia.edu.eg

Mona Shokair
mona.sabry@el-eng.menofia.edu.eg

[1] Electronic and Electrical Communication Department, Faculty of Electronic Engineering, Menofia University, Shebin El_Kom, Egypt

[2] Telecom Egypt, Tanta, Egypt

[3] Electrical Engineering Department, College of Engineering, Shaqra University, Dawadmi, Ar Riyadh, Kingdom of Saudi Arabia

access the spectrum of licensed primary users (PUs) without interfere the PUs. To preserve a certain quality of service (QoS) for unlicensed/secondary users while leveraging a limited (uninfluenced) interference to licensed/primary users, the assistance of co-operative relays in cognitive radio networks were utilized extensively [2].

Mainly, co-operative relays were proposed to promote the system performance and obtain signaling and diversity gains. This paradigm was devoted to get rid of the problem of extending the coverage of wireless networks [3–8]. Specifically, promising relay protocols had been studied to forward the secondary source message in a cognitive radio system to the destination [9–14]. However, due to wireless broadcasting, the physical layer security (PLS) is vulnerable to illegitimate benefits. Securing and protecting issues of the physical layer against eavesdroppers were extensively investigated [15–20].

In fact, cognitive radio networks may be classified with respect to spectrum sharing or access techniques into: (1) overlay CR [21], [22] and (2) underlay CR.

In an overlay CR, the SUs have to detect the spectrum holes to maintain their own communication which can be hardly performed in the dense areas due to the lack of empty resources.

Alternatively, underlay cognitive radio network is a crucial network topology for both the academicals and industrial network designers as it provides concurrent cognitive/non-cognitive communications [23, 24]. To achieve secure and reliable communication within such a network, conflict objectives of interest should be maintained:

1. Making the secondary network coverage as large as possible while protecting both primary and secondary networks from interference.
2. Satisfying adoptable (QoS) requirements for both primary and secondary users.
3. Preventing external attackers from overhearing secure and confidential information.

Anywhere, there exist some recent researches in the context of secure underlay CR that aims at enhancing the secrecy performance by exploiting the statistical characteristics of the wireless channels regarding interference constraint requirements [25–29]. For instance, in [25] the authors derived a closed form expression of some performance metrics, i.e., outage probability and secrecy outage probability, for multicasting system in the presence of multiple eavesdroppers. In [26] single and multi-relay selection schemes were investigated where security and reliability tradeoff issues were examined. In [27] the case of unknown channel state information CSI about the attackers (sub-optimal relay selection) was assumed. Regenerative multi-relay system was introduced in [28]. Reference [29] investigated licensed/unlicensed users with dual sources of interference in both directions. Unfortunately, it did not consider the security issue.

Very recently, in [30] the authors considered a secure dual-hop communication where an eavesdropper can overhear the transmission from both the direct and the relayed links. Thus, the eavesdropper performs maximal radio combining (MRC) or selection combining (SC) of the signals. Still, this has not been discussed in terms of secure underlay cognitive radio networks. In [31] the authors proposed three relay selection schemes to improve PLS in an underlay CR in the presence of multiple PUs. Unfortunately, they did not consider the effect of interference from the PUs to SUs.

To the best of our knowledge, in all of the above mentioned works (and the references therein) the mutual interference between PUs and SUs have not been highlighted especially in the presence of multiple secondary eavesdroppers. In particular, the impact of joint constraints of interference and security on the performance of both primary and secondary networks

involves a tradeoff. Motivated by these considerations, a novel secure secondary communication system that incorporates cooperative diversity will be investigated. In particular, the fading characteristics will be exploited to provide useful insights regarding the main factors that regulate the secrecy performance when both direct and relayed links are overheard under all possible interference constraints. The contributions of this paper are summarized as follows:

- We propose relay selection criteria for the per-hop and the dual-hop communications to improve the PLS under the primary/secondary interference constraints.
- We evaluate the secrecy performance and derive new closed form expressions for some important metrics, i.e., achievable secrecy rate, outage probability and asymptotic outage probability.
- The impact of cooperative diversity of relay selection is characterized when perfect or statistical CSI of eavesdroppers are known.
- Thereafter, system inner and outer bounds are also derived. Those bounds become tight at high transmitted signal to interference noise ratio (SINR) in the considered system.

The rest of the paper is organized as follows. In Section II the system analysis and the optimal relay selection conditions are statistically investigated. Also, the effect of the primary user's constraints and impact of diversity order are clarified. In Section III we evaluate the performance metrics. Simulation results are depicted in Section IV. Section V concludes the paper.

2 System and Channel Models

Here, we consider a wiretap cognitive radio network. It is a dual-hop decode and forward relay assisted network. It consists of the following nodes; one secondary user source, S, set of N decode and forward (DF) relays, $(R_i, 1 \leq i \leq N)$, one secondary user destination, D, one primary user transmitter, P_{Tx}, one primary user receiver, P_{Rx}, and multiple M eavesdroppers, $(E_j, 1 \leq j \leq M)$. All nodes are equipped with a single antenna.

2.1 The System Model

We rely on a worse-case model, where the secondary source transmitter transmits a confidential information to the secondary receiver in the presence of multiple eavesdroppers with the aid of N trusted DF relays, while the eavesdroppers try to overhear and attack all of the communication paths between the secondary source, S, and destination, D.

Such an underlay spectrum sharing cognitive radio network in coexistence with a primary user network is shown in Fig. 1. It is assumed that the secondary network communication follows an interference power constraint condition which represents the maximum allowable transmit power of both the secondary source and relays. Thus, the interference power does not exceed a threshold limit P at the primary receiver end.

It is further assumed that all of the receiving nodes are confirmed to know global channel state information (CSI) and either instantaneous information about eavesdroppers or statistical CSI is available at the end of the secondary user source, S.[1] Moreover, the

[1] This assumption is reasonable when the well-known user represents a legitimate user for some applications and an eavesdropper for others.

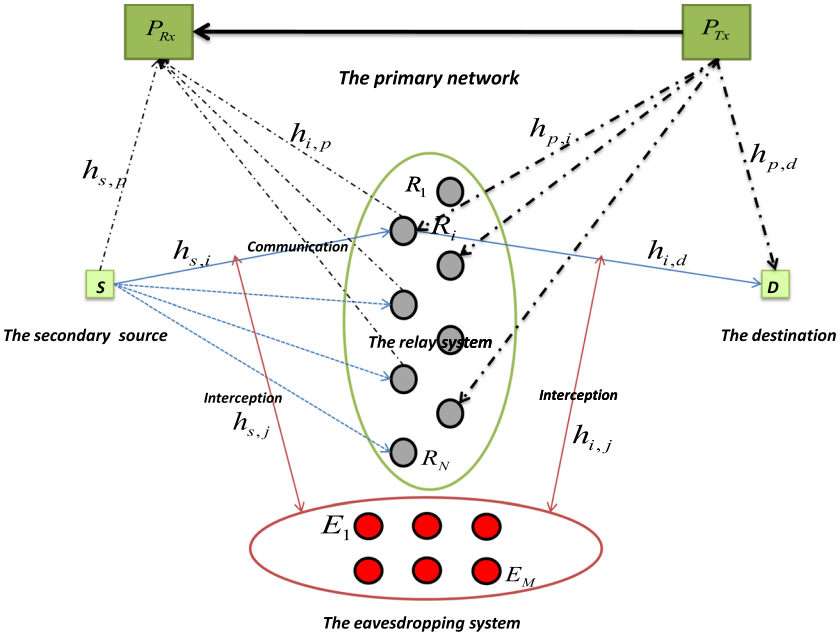

Fig. 1 A class of wiretap underlay cognitive radio networks

secondary user destination, D, and relays are subjected to interference signals from the primary transmitter, P_{Tx}. All communication channels are quasi-static and flat fading Rayleigh channels. No direct path from S to D is found due to deep fading conditions. Communication takes place in a half duplex mode through two phases.

In the first phase S transmits a power constraint signal while the relays listen, type of non-colluding eavesdroppers,[2] i.e., multiple or co-operative eavesdroppers, try to overhear through wiretap channels.

In the second phase, the relays listen in a co-operative scheme. Then, one potential relay node is selected out of the set that successfully decodes the source message to forward the re-encoded messages toward the destination such that this relay satisfies a certain optimization condition. However, the eavesdroppers' system tries to again overhear the second path through another dedicated wiretap channel.

A co-operative communication method based on optimal selection scheme is proposed to select the relay that has the best maximum to forward the source message to the destination.

2.2 The Communication Channels

Since it is assumed that all communication channels follow Rayleigh fading distributions, let us generally define that the fading coefficients $\gamma_{q,r} = \left|h_{q,r}\right|^2, q, r \in \{s, i, p, j, d\}$ satisfy

[2] It is nonsense considering a colluding system as it reduces the opportunity to occupy a legitimate channel.

Rayleigh fading conditions and undergo independent exponential distributions, i.e., be exponential random variables (exponential R.V.s) *with means* $\lambda_{q,r}$, where their cumulative density functions and probability density functions, i.e., CDF and PDF, can be expressed by

$$F_{\gamma_{q,r}}(x) = 1 - exp\left(-\frac{x}{\lambda_{q,r}}\right). \tag{1}$$

$$f_{\gamma_{q,r}}(x) = \frac{1}{\lambda_{q,r}} exp\left(-\frac{x}{\lambda_{q,r}}\right). \tag{2}$$

In the first phase, S sends its message signal to R_i with the constraint power

$$P_s = \frac{P}{\left|h_{s,p}\right|^2}. \tag{3}$$

Where $h_{s,p}$ is the $S-P$ channel fading coefficient and P is the constraint power at P_{Rx}. In the vicinity of R_i, the received signal can be expressed as

$$y_{s,i} = \sqrt{P_s} h_{s,i} x_{s,i} + \sqrt{P_p} h_{p,i} x_{p,i} + n_i. \tag{4}$$

Where $h_{s,i}$ is the $S-R_i$ channel fading coefficient and $x_{s,i}$ is the S transmitted symbol of the $S-R_i$ link, $h_{p,i}$ is the channel fading coefficient of the $P_{Tx}-R_i$ interference signal, $x_{p,i}$ is the corresponding transmitted interference symbol with power P_p and $n_i \sim CN\left(0, N_0\right)$ is an additive white Gaussian noise (AWGN) signal.

In the second phase, R_i forwards its signal to D after successful decoding[3] with the constraint power

$$P_i = \frac{P}{\left|h_{i,p}\right|^2}. \tag{5}$$

Where $h_{i,p}$ is the $R_i - P$ channel fading coefficient. The received signal at D can be expressed as

$$y_{i,d} = \sqrt{P_i} h_{i,d} x_{i,d} + \sqrt{P_p} h_{p,d} x_{p,d} + n_d. \tag{6}$$

Where $h_{i,d}$ is the $R_i - D$ channel fading coefficient and $x_{i,d}$ is the transmitted relay, R_i, symbol of the $R_i - D$ link with power P_i, $h_{p,d}$ is the channel fading coefficient of the $P_{Tx} - D$ interference signal, P_p is the primary transmitted interference power and $n_d \sim CN\left(0, N_0\right)$ is an additive white Gaussian noise (AWGN) signal.

Considering the worst-case scenario, eavesdropper j can recover the interference from the primary user and the received signals in the first and the second phases can be given by

$$y_{\mu,j} = \sqrt{P_\mu} h_{\mu,j} x_{\mu,j} + n_j, \mu \in \{s, i\}. \tag{7}$$

[3] It is supposed that all relay nodes decode the source message correctly.

Where $h_{\mu,j}, \mu \in \{s,i\}$, is the channel fading coefficient of the overheard signals from both S and R_i to E_j, $x_{\mu,j}$ is the corresponding overheard symbol and $n_j \sim CN\left(0, N_0\right)$ is an AWGN with respect to the jth eavesdropper end.

2.3 The Secrecy Capacity

Let us first define the concept of maximum achievable secrecy rate (secrecy capacity) as [32]

$$C_s = \begin{cases} \left[C_M - C_E\right]^+ & if\ \gamma_R > \gamma_E \\ 0 & if\ \gamma_R \leq \gamma_E \end{cases}. \tag{8}$$

Where $[x]^+$ represents $max(0,x)$, $C_M = \frac{1}{2}\log_2\left(1+\gamma_M\right)$,[4] $C_E = \frac{1}{2}\log_2\left(1+\gamma_E\right)$, γ_M, γ_E are the capacity of the main channel, the capacity of the wiretap channel, the SINR of the main channel and the SINR of the wiretap channel, respectively.

Hence, the achievable transmission rate of the $S-R_i$ and R_i-D channels can be given by

$$C_M = \frac{1}{2}\log_2\left(1+\gamma_M\right), M \in \{(s,i),(i,d)\}. \tag{9}$$

Where $\gamma_{s,i}$ and $\gamma_{i,d}$ can be formulated as

$$\gamma_{s,i} = \frac{\frac{P}{N_0}\frac{\left|h_{s,i}\right|^2}{\left|h_{s,p}\right|^2}}{\frac{P_p}{N_0}\left|h_{p,i}\right|^2 + 1}, \tag{10}$$

$$\gamma_{i,d} = \frac{\frac{P}{N_0}\frac{\left|h_{i,d}\right|^2}{\left|h_{i,p}\right|^2}}{\frac{P_p}{N_0}\left|h_{p,d}\right|^2 + 1}. \tag{11}$$

Correspondingly, the achievable wiretap transmission rate of the $S-E$ and R_i-E channels (intercepted by the eavesdropping system J) can be given by

$$C_{E_J} = \frac{1}{2}\log_2\left(1+\gamma_{E_J}\right), E_J \in \{(s,J),(i,J)\}. \tag{12}$$

Where $\gamma_{s,j}$ and $\gamma_{i,J}$ can be formulated as

$$\gamma_{s,J} = \frac{P}{N_0}\frac{\left|h_{s,J}\right|^2}{\left|h_{s,p}\right|^2}. \tag{13}$$

[4] The term $\frac{1}{2}$ indicates the dual split communication protocol (the time slot is divided into two fractions of communication sub-slots).

$$\gamma_{i,J} = \frac{P}{N_0} \frac{\left|h_{i,J}\right|^2}{\left|h_{i,p}\right|^2}. \tag{14}$$

Comparatively, the achievable secrecy rate which is intercepted by the eavesdropping system J can be rewritten for the two communication phases as

$$\begin{aligned} C_{sJ,\omega} &= \frac{1}{2}\log_2\left(\frac{1+\gamma_M}{1+\gamma_{E_J}}\right) \\ &= \frac{1}{2}\log_2\left(\frac{1+\frac{Z_{1,\omega}}{Z_{2,\omega}}\Big/Z_{4,\omega}}{1+Z_{3,\omega}\Big/Z_{4,\omega}}\right). \end{aligned} \tag{15}$$

Where γ_{E_J}, $E_J \in \{(s,J),(i,J)\}$, is the SINR at the eavesdropping system J, the superscript ω, $\omega \in \{1\}$ or $\omega \in \{2\}$, denotes the first phase or the second phase, $Z_{1,\omega} = \frac{P}{N_0}\psi_{1,\omega}$, $Z_{2,\omega} = \frac{P_p}{N_0}\psi_{2,\omega} + 1$, $Z_{3,\omega} = \frac{P}{N_0}\psi_{3,\omega}$, $Z_{4,\omega} = \psi_{4,\omega}$, $\psi_{1,1} \sim \left|h_{s,i}\right|^2, \psi_{1,2} \sim \left|h_{i,d}\right|^2$, $\psi_{2,1} \sim \left|h_{p,i}\right|^2, \psi_{2,2} \sim \left|h_{p,d}\right|^2$, $\psi_{3,1} \sim \left|h_{s,J}\right|^2, \psi_{3,2} \sim \left|h_{i,J}\right|^2$, $\psi_{4,1} \sim \left|h_{s,p}\right|^2$ *and* $\psi_{4,2} \sim \left|h_{i,p}\right|^2$ of the first phase or the second phase, respectively.

In the following, we derive formulas for the cumulative and probability density functions, i.e., CDF and PDF, of the SINR of the two communication phases, considering the proposed selection schemes and the interception strategies, then, we use them to obtain closed form expressions for important performance metrics such as the secrecy outage probability and the non-zero achievable secrecy rate.

3 Relay Selection Schemes and Performance Metrics

Our analysis will be started with the per-hop relay selection scheme. It is remarkable that the per-hop selection may replace the dual-hop one, if perfect CSI information about the location of the eavesdropping system indicates that the eavesdroppers reside within one of the two communication phases.

3.1 Per-hop Relay Selection Schemes

In this sub-section, we propose per-hop relay selection schemes regarding one side of the secondary network transmission. If it is confirmed that the eavesdropping system reside within one of the two communication phases, it is better to derive the cooperative relay to select the one that maximizes the secrecy rate within the phase of the eavesdroppers' residence. Let the per-hop relay selection be defined as

$$i_{per-hop} = \arg\max_i C_{sJ,\omega}, \quad \omega \in \{1,2\}. \tag{16}$$

Where $i_{per-hop}$ is the index of the selected relay.

3.1.1 Relay Selection Scheme at the First Phase Side

At this side, the selected relay depends only on the SINR of the main channel where $C_{sj,1} = \frac{1}{2}\log_2\left(\frac{1+\gamma_M}{1+\gamma_{E_J}}\right)$, $M \in \{(s,i)\}$, $E_J \in \{(s,J)\}$, as investigated by the following theorem.

Theorem 1 *The relay selection rule according to* (16) *is determined statistically by selecting i that maximizes The CDF of the achievable secrecy rate* $\left(i.e.C_{sJ,1}\right)$ *of the first communication phase as,*

$$i_{per-hop(1)} = \arg\max_i\left(\gamma_{s,i}\right) \Rightarrow \arg\Pr\left(\max_i\left(\frac{\frac{P}{N_0}\left|h_{s,i}\right|^2}{\frac{P_p}{N_0}\left|h_{p,i}\right|^2+1}\right) \le \gamma\right) \Rightarrow \arg\left(\prod_{i=1}^{N}\left(\frac{\Omega_{s,i}\gamma\exp\left(\Omega_{p,i}\right)}{\Omega_{s,i}\gamma+\Omega_{p,i}}\right)\right) \tag{17}$$

where $\Omega_{p,i} = \left(\lambda_{p,i}\frac{P_p}{N_0}\right)^{-1}, \Omega_{s,i} = \left(\lambda_{s,i}\frac{P}{N_0}\right)^{-1}$, *and* γ *is the threshold SINR.*

Proof Let $h_{s,i}$ and $h_{p,i}$ be Rayleigh R.V. s, then, the PDF and the CDF of $X_{s,i} = \frac{P}{N_0}\left|h_{s,i}\right|^2$ will take the forms

$$f_{X_{s,i}}(x) = \Omega_{s,i}\exp\left(-\Omega_{s,i}x\right), \tag{18}$$

$$F_{X_{s,i}}(x) = 1-\exp\left(-\Omega_{s,i}x\right), \tag{19}$$

respectively, and after some algebraic manipulation the PDF of $Y_{p,i} = \frac{P_p}{N_0}\left|h_{p,i}\right|^2 + 1$ can be expressed as

$$f_{Y_{p,i}}(x) = \Omega_{p,i}\exp\left(\Omega_{p,i}\right)\exp\left(-\Omega_{p,i}x\right). \tag{20}$$

Thus, the CDF of the R.V. $Z_i = \frac{\mathrm{X}_{s,i}}{Y_{p,i}}$ is given by

$$F_{Z_i}(x) = \exp\left(\Omega_{p,i}\right)\left(1-\frac{\Omega_{p,i}}{\Omega_{s,i}x+\Omega_{p,i}}\right) = \frac{\Omega_{s,i}x\exp\left(\Omega_{p,i}\right)}{\Omega_{s,i}x+\Omega_{p,i}}, \tag{21}$$

where the previous Eq. follows after applying the following integral

$$F_{Z_i}(x) = \int_0^\infty f_{Y_{p,i}}(z_i)F_{X_{s,i}}(xz_i)dz_i. \tag{22}$$

Consequently, (17) immediately follows after some algebraic manipulations by using

$$F_{Z_i}(\gamma) = \Pr\left(\max_i \left(F_{Z_1}(\gamma), \ldots F_{Z_N}(\gamma)\right) \leq \gamma\right) = \prod_{i=1}^{N} \left(F_{Z_i}(\gamma)\right). \tag{23}$$

It can be concluded that, this relay selection is briefly a conventional selection rule.□

3.1.2 Relay Selection Scheme at the Second Phase Side

At the second phase side, the selected relay depends on $C_{sJ,2} = \frac{1}{2}\log_2\left(\frac{1+\gamma_M}{1+\gamma_{E_J}}\right)$, $M \in \{(i,d)\}$, $E_J \in \{(i,J)\}$, where the $R_i - E_J$ channel fading coefficient has a great impact on the decision of the relay selection. Thus, two applicable cases of eavesdropping are adopted and investigated as follows.

Case 1: Maximum of the eavesdroppers:

In this case, the strongest attacker is picked up. Thus, the group SINR is considered by the one that has the highest SINR and is given by,

$$\gamma_{i,J} = \max_j \gamma_{i,j} \Rightarrow \left|h_{i,J}\right|^2 = \max_j \left|h_{i,j}\right|^2. \tag{24}$$

Let $\left|h_{i,j}\right|^2$ be an exponential R.V., then, the CDF of $Z_{3,2} = \frac{P}{N_0}\left|h_{i,J}\right|^2$ can be denoted as follows

$$F_{\left|h_{i,j}\right|^2}(x) = 1 - \exp\left(-\Omega_{i,j}x\right). \tag{25}$$

Where $\Omega_{i,j} = \left(\lambda_{i,j}\frac{P}{N_0}\right)^{-1}$. By using (23) the CDF of $Z_{3,2}$ will take the form

$$F_{Z_{3,2}}(x) = \prod_{j=1}^{M}\left(1 - \exp\left(-\Omega_{i,j}x\right)\right) = 1 + \sum_{j=1}^{M}(-1)^j \sum_{l_1<l_2<\cdots l_M} \exp\left(-\sum_{k=1}^{j}\Omega_{i,l_k}x\right). \tag{26}$$

By applying following relation

$$\begin{aligned} &\prod_{j=1}^{M}\left(1-\theta_j\right) = 1 + \sum_{j=1}^{M}(-1)^j \sum_{l_1<l_2<\ldots l_M} \prod_{k=1}^{j}\theta_{l_k} \\ &where \sum_{l_1<l_2<\cdots l_M} \equiv \sum_{l_1=1}^{M-j+1}\sum_{l_2=l_1+1}^{M-j+2}\cdots\sum_{l_j=l_{j-1}+1}^{M}. \end{aligned} \tag{27}$$

Then, the PDF of can be expressed as

$$f_{Z_{3,2}}(x) = \sum_{j=1}^{M}(-1)^{j-1} \sum_{l_1<l_2<\cdots l_M} \exp\left(-\sum_{k=1}^{j}\left(\Omega_{i,l_k} - \ln\left(\Omega_{i,l_k}\right)\right)x\right). \tag{28}$$

Theorem 2 *The relay selection rule according to (16) is determined statistically by selecting i that maximizes The CDF of the achievable secrecy rate* $\left(i.e.C_{sJ,2}\right)$ *of the second communication phase can be derived as,*

$$i_{per-hop(2)} = \arg\max_i \left(C_{sJ,2}\right) \Rightarrow \arg \Pr(\max_i \left(\frac{\frac{Z_{1,2}}{Z_{4,2}}+1}{\frac{Z_{3,2}}{Z_{4,2}}+1}\right) \leq \gamma) \Rightarrow \arg\left(\prod_{i=1}^{N} F_{\sigma_i}(\gamma)\right),$$

where

$$F_{\sigma_i}(\sigma) = \begin{cases} \sum_{\substack{j=1 \\ j\neq r}}^{M} (-1)^{j-1} \sum_{l_1<l_2\cdots l_M} \frac{\frac{\zeta_{i,j}}{\sigma}\frac{\Omega_{i,p}}{\sigma-1}}{\frac{\zeta_{i,j}}{\sigma}-\frac{\Omega_{i,p}}{\sigma-1}}\left(\frac{1}{\frac{\Omega_{i,p}}{\sigma-1}+\Omega_{i,d}} - \frac{1}{\frac{\zeta_{i,j}}{\sigma}+\Omega_{i,d}}\right) + (-1)^r\left(\frac{\lambda_i}{\lambda_i+\Omega_{i,d}}\right)^2 & for\ \frac{\Omega_{i,p}}{\sigma-1} = \frac{\zeta_{i,r}}{\sigma}\Big|_{r\in\{1,2,\ldots M\}} \\ 1-\sum_{j=1}^{M}(-1)^{j-1}\sum_{l_1<l_2\cdots l_M}\frac{\frac{\zeta_{i,j}}{\sigma}\frac{\Omega_{i,p}}{\sigma-1}}{\frac{\zeta_{i,j}}{\sigma}-\frac{\Omega_{i,p}}{\sigma-1}}\left(\frac{1}{\frac{\Omega_{i,p}}{\sigma-1}+\Omega_{i,d}} - \frac{1}{\frac{\zeta_{i,j}}{\sigma}+\Omega_{i,d}}\right) & otherwise \end{cases} \quad (29)$$

where $\Omega_{\mathrm{i,p}} = \left(\lambda_{\mathrm{i,p}}\right)^{-1}, \Omega_{\mathrm{i,d}} = \left(\lambda_{\mathrm{i,d}}\frac{\mathrm{P_{R_p}}}{\mathrm{N_0}}\right)^{-1}$ *and* γ *is the threshold SINR.*

Proof For the second communication phase, one can innovate in (15) that the relay selection relies again only on i which is independent of $Z_{2,2}$.

Firstly, the CDF of the R.V. $\sigma_i = \frac{1+Z_{1,2}/Z_{4,2}}{1+Z_{3,2}/Z_{4,2}} \rightarrow F_{\sigma_i}(\sigma) = Pr\left(\sigma_i \leq \sigma\right)$ can be derived as follows

$$F_{\sigma_i}(\sigma) = \Pr\left(Z_{1,2} \leq \left(\sigma Z_{3,2} + (\sigma-1)Z_{4,2}\right)\right) \quad (30)$$

Let the CDF of $Z_{1,2}$ takes the forms

$$F_{Z_1}(x) = 1 - \exp\left(-\Omega_{i,d}x\right). \quad (31)$$

By using (28) and after some algebraic manipulations, the PDF $\sigma Z_{3,2}$ of can be expressed as

$$f_{\sigma Z_{3,2}}(x) = \sum_{j=1}^{M}(-1)^{j-1}\sum_{l_1<l_2\prec\cdots l_M}\exp\left(-\sum_{k=1}^{j}\left(\frac{\Omega_{i,l_k}}{\sigma} - \ln\left(\frac{\Omega_{i,l_k}}{\sigma}\right)\right)x\right) \quad (32)$$

For simplicity, a decomposed form can be denoted as

$$f_{\sigma Z_{3,2}}(x) = \sum_{j=1}^{M}(-1)^{j-1}\sum_{l_1<l_2\prec\cdots l_M}\frac{\zeta_{i,j}}{\sigma}\exp\left(-\frac{\zeta_{i,j}}{\sigma}x\right)$$
$$where\ \zeta_{i,j} = \sum_{k=1}^{j}\Omega_{i,l_k}. \quad (33)$$

The PDF of the R.V. $(\sigma-1)Z_{4,2}$ is given by

$$f_{(\sigma-1)Z_{4,2}}(x) = \frac{\Omega_{i,p}}{\sigma-1}\exp\left(-\frac{\Omega_{i,p}}{\sigma-1}x\right). \tag{34}$$

Then, the PDF of $Y_i = \sigma Z_{3,2} + (\sigma-1)Z_{4,2}$ can be computed as

$$f_{Y_i}(x) = \begin{cases} \sum_{j=1}^{M}(-1)^{j-1}\sum_{l_1<l_2>-l_M}\frac{\frac{\zeta_{i,j}}{\sigma}\frac{\Omega_{i,p}}{\sigma-1}}{\frac{\zeta_{i,j}}{\sigma}-\frac{\Omega_{i,p}}{\sigma-1}}\left(\exp\left(-\frac{\Omega_{i,p}}{\sigma-1}x\right)-\exp\left(-\frac{\zeta_{i,j}}{\sigma}x\right)\right) & for\ \frac{\Omega_{i,p}}{\sigma-1}\neq\frac{\zeta_{i,j}}{\sigma}\forall j\in\{1,2,\dots M\} \\ \lambda_i^2 x\exp\left(-\lambda_i x\right) & for\ \lambda_i=\frac{\Omega_{i,p}}{\sigma-1}=\frac{\zeta_{i,j}}{\sigma}\Big|_{j=1,2,\dots M} \end{cases}. \tag{35}$$

By applying the integral

$$f_{Y_i}(x) = \int_0^x f_{\sigma Z_3}(\tau) f_{(\sigma-1)Z_4}(x-\tau)d\tau, \tag{36}$$

Hence, $F_{\sigma_i}(\sigma)$ can be given by

$$F_{\sigma_i}(\sigma) = \begin{cases} 1-\sum_{j=1}^{M}(-1)^{j-1}\sum_{l_1<l_2\dots l_M}\frac{\frac{\zeta_{i,j}}{\sigma}\frac{\Omega_{i,p}}{\sigma-1}}{\frac{\zeta_{i,j}}{\sigma}-\frac{\Omega_{i,p}}{\sigma-1}}\left(\frac{1}{\frac{\Omega_{i,p}}{\sigma-1}+\Omega_{i,d}}-\frac{1}{\frac{\zeta_{i,j}}{\sigma}+\Omega_{i,d}}\right) & for\ \frac{\Omega_{i,p}}{\sigma-1}\neq\frac{\zeta_{i,j}}{\sigma}\forall j\in\{1,2,\dots M\} \\ 1-\left(\frac{\lambda_i}{\lambda_i+\Omega_{i,d}}\right)^2 & for\ \lambda_i=\frac{\Omega_{i,p}}{\sigma-1}=\frac{\zeta_{i,j}}{\sigma}\Big|_{j=1,2,\dots M} \end{cases}. \tag{37}$$

Where the following integral is solved for $x = 1$ as

$$F_{\sigma_i}(x,\sigma) = \int_0^\infty f_{Y_i}(z_i)F_{Z_1}(xz_i)dz_i. \tag{38}$$

Consequently, (29) immediately follows after some algebraic manipulations by using a similar form as (23). □

Case 2: Co-operative eavesdroppers:
In this case, the group SINR is given by,

$$\gamma_{i,J} = \sum_{j=1}^{M}\gamma_{i,j} \Rightarrow |h_{i,J}|^2 = \sum_{j=1}^{M}\left|h_{i,j}\right|^2, \tag{39}$$

where the eavesdroppers cooperate the MRC reception. Thus, the CDF of the R.V. $Z_{3,2}$ can be computed as follows

$$F_{|h_{i,J}|^2}(x) = \Pr\left(\sum_{j=1}^{M}\left|h_{i,j}\right|^2 \le x\right) = \underset{\sum_{j=1}^{M-1}|h_{i,j}|^2}{E}\left[\underset{\sum_{j=1}^{M-2}|h_{i,j}|^2}{E}\left(\cdots\left(\underset{|h_{i,j}|^2}{E}\left(F_{|h_{i,j}|^2}\left(x-\sum_{j=1}^{M-1}\left|h_{i,j}\right|^2\right)\right)\right)\right)\right], \tag{40}$$

where the subscripts $\sum_{j=1}^{\epsilon} \left|h_{i,j}\right|^2$ of E represent the computation of the mean under the PDF of the R.V. $\sum_{j=1}^{\epsilon} \left|h_{i,j}\right|^2, \in$ *is an integer*.

Applying recursive calculus, the CDF of $Z_{3,2}$ will take the form,

$$F_{Z_{3,2}}(x) = \frac{1}{(M-1)!} \int_0^{\Omega_{iJ}x} t^{M-1} \exp(-t) dt, \tag{41}$$

where $\Omega_{\mathrm{iJ}} = \mathrm{aver}_j \Omega_{i,j}$, the PDF (Chi square distribution) of the R.V. $Z_{3,2}$ is determined directly by differentiating (41) by x as follows,

$$f_{Z_{3,2}}(x) = \frac{\left(\Omega_{iJ}\right)^M}{(M-1)!} x^{M-1} \exp\left(-\Omega_{iJ}x\right). \tag{42}$$

Theorem 3 *The relay selection rule according to* (16) *and* (42) *is determined statistically by selecting i that maximizes the CDF of the achievable secrecy rate* $\left(i.e. C_{sJ,2}\right)$ *whose CDF can be derived as,*

$$F_{\sigma_i}(\sigma) = \begin{cases} \dfrac{\left(\frac{\Omega_{iJ}}{\sigma}\right)^M \Omega_{i,d}}{\left(\frac{\Omega_{iJ}}{\sigma} - \frac{\Omega_{i,p}}{\sigma-1}\right)^M \left(\frac{\Omega_{i,p}}{\sigma-1} + \Omega_{i,d}\right)} - \dfrac{\left(\frac{\Omega_{iJ}}{\sigma}\right)^M \frac{\Omega_{i,p}}{\sigma-1}}{\left(\frac{\Omega_{iJ}}{\sigma} - \frac{\Omega_{i,p}}{\sigma-1}\right)^M} \\ \left(\left(\sum_{\delta=0}^{M-1} \left(\dfrac{1}{\left(\frac{\Omega_{iJ}}{\sigma}\right)^{\delta+1}} - \dfrac{1}{\left(\frac{\Omega_{iJ}}{\sigma} + \Omega_{i,d}\right)^{\delta+1}}\right) \left(\frac{\Omega_{iJ}}{\sigma} - \frac{\Omega_{i,p}}{\sigma-1}\right)^{\delta}\right)\right) & for\ \frac{\Omega_{i,p}}{\sigma-1} \neq \frac{\Omega_{iJ}}{\sigma} \\ 1 - \left(\frac{\lambda_i}{\lambda_i + \Omega_{i,d}}\right)^{M+1} & for \frac{\Omega_{i,p}}{\sigma-1} = \frac{\Omega_{iJ}}{\sigma} = \lambda_i \end{cases}. \tag{43}$$

Proof Applying similar steps as Theorem 2, it is necessary to compute the PDF of $Y_i = \sigma Z_{3,2} + (\sigma - 1) Z_{4,2}$, in this case, which is given by

$$f_{Y_i}(x) = \begin{cases} \dfrac{\left(\frac{\Omega_{iJ}}{\sigma}\right)^M \frac{\Omega_{i,p}}{\sigma-1}}{\left(\frac{\Omega_{iJ}}{\sigma} - \frac{\Omega_{i,p}}{\sigma-1}\right)^M} \left(\exp\left(-\frac{\Omega_{i,p}}{\sigma-1}x\right) - \left(\exp\left(-\frac{\Omega_{iJ}}{\sigma}x\right) \sum_{\delta=0}^{M-1} \frac{x^{\delta}}{\delta!} \left(\frac{\Omega_{iJ}}{\sigma} - \frac{\Omega_{i,p}}{\sigma-1}\right)^{\delta}\right)\right) & for\ \frac{\Omega_{i,p}}{\sigma-1} \neq \frac{\Omega_{iJ}}{\sigma} \\ \lambda_i^{M+1} \frac{x^M}{M!} \exp\left(-\lambda_i x\right) & for\ \frac{\Omega_{i,p}}{\sigma-1} = \frac{\Omega_{i,J}}{\sigma} = \lambda_i \end{cases}, \tag{44}$$

where the integral (36) is utilized. Consequently, $F_{\sigma_i}(\sigma)$ is given by,

$$F_{\sigma_i}(\sigma)=\begin{cases}\dfrac{\left(\frac{\Omega_{iJ}}{\sigma}\right)^{M}\frac{\Omega_{i,p}}{\sigma-1}}{\left(\frac{\Omega_{iJ}}{\sigma}-\frac{\Omega_{i,p}}{\sigma-1}\right)^{M}}\left(\left(\dfrac{1}{\frac{\Omega_{i,p}}{\sigma-1}}-\dfrac{1}{\left(\frac{\Omega_{i,p}}{\sigma-1}+\Omega_{i,d}\right)}\right)\right. & for\ \frac{\Omega_{i,p}}{\sigma-1}\neq\frac{\Omega_{iJ}}{\sigma}\\ \left.-\left(\sum_{\delta=0}^{M-1}\left(\dfrac{1}{\left(\frac{\Omega_{iJ}}{\sigma}\right)^{\delta+1}}-\dfrac{1}{\left(\frac{\Omega_{iJ}}{\sigma}+\Omega_{i,d}\right)^{\delta+1}}\right)\left(\frac{\Omega_{iJ}}{\sigma}-\frac{\Omega_{i,p}}{\sigma-1}\right)^{\delta}\right)\right)\\ 1-\left(\frac{\lambda_i}{\lambda_i+\Omega_{i,d}}\right)^{M+1} & for\ \frac{\Omega_{i,p}}{\sigma-1}=\frac{\Omega_{iJ}}{\sigma}=\lambda_i\end{cases}, \tag{45}$$

where the integral (38) is solved for $x = 1$ (see [[33], Eq. (3.351.1)]). Then, (43) follows after some algebraic manipulations by using a similar form as (23).□

3.2 The Optimal Relay Selection Schemes

In the previous analysis, we state the statistical conditions of relay selection schemes for the two per-hop communication, individually. However, the relay selected to achieve maximum secrecy rate at one hop, can severely interrupt the reception security at the other.

To investigate the corresponding diversity analysis and propose a relay selection scheme to maintain secure and reliable communication, it suffices to check in and deal with the relay index dependent coefficients of dual hop communication phases.

Thus, in order to guarantee that neither of the separate secrecy rates falls down to a low level (i.e., which implies a security degradation), a low complexity overall relay selection scheme is adopted to select a relay, i.e., or more, out of N relays in the co-operative system that maximizes the minimum of the dual secrecy rates as follows.

3.2.1 Optimal Relay Selection in Global CSI Availability

Let $C_{sJ,\omega}, \omega \in \{1, 2\}$ denote the achievable secrecy rates at the first and the second communication phases, respectively. The optimal relay R_i^* can be formulated by maximizing the relation

$$i^* = \arg\max_i C_{sJ,1,2}. \tag{46}$$

Where $C_{sJ,1,2} = min\left(C_{sJ,1}, C_{sJ,2}\right)$. Therefore, the CDF of $C_{sJ,1,2}$ leads directly to

$$F_{C_{sJ,1,2}}(\gamma) = \Pr\left(\min\left(C_{sJ,1}, C_{sJ,2}\right) \le \tau\right) = F_{C_{sJ,1}}(\tau) + F_{C_{sJ,2}}(\tau) - F_{C_{sJ,1}}(\tau)F_{C_{sJ,2}}(\tau). \tag{47}$$

Where $\gamma = 2^{\tau} - 1$ is the threshold capacity, $F_{C_{sJ,1}}(\tau) and F_{C_{sJ,2}}(\tau)$ are the CDFs of $C_{sJ,1} and C_{sJ,2}$. The CDF of $C_{sJ,1}$ is sufficiently given by (17) and the CDF of $C_{sJ,2}$ can be given by $F_{\sigma_i}(\gamma)$ in (29) and (43), respectively.

The assumption of spatial independence can be exclusively deduced from the uncorrelated ordering concept where the CDF of the selected *i*th relay for each path satisfies

$$F_{C_{sJ,1,2}(i)}(\gamma) = N \int_0^{\tau} \Pr\left(i = k \middle| C_k = x\right) f_{C_k}(x) dx. \tag{48}$$

Where $C_{sJ,1,2}(i)$ denote the achievable secrecy R.V.s of the ith relay index. For simplicity, it is assumed that for each communication phase, the order statistics of the best relay selection in (48) is independent of τ, the threshold capacity as

$$\Pr\left(i = k \middle| C_k = \tau\right) = \Pr\left(i = k\right) = \frac{1}{N}. \tag{49}$$

Thus, to evaluate (48), we have exclusively to determine $C_{sJ,1,2}(i)$ and the diversity order statistics of the best relay selection for the system relies only on the joint order statistics of the two combined communication phases, as it will be investigated.

Let us consider that the cooperative relay system will select the same relay to interconnect the secondary source, S, to the destination, D, for a certain, $r \triangleq numberofselectedrelays$, an optimal relay selection expression can be derived from the equivalent permanent order statistics (see [34]) represented by

$$\begin{aligned} F_{C_{r:N}}(\gamma) &= \Pr\left(C_{r:N} \le \tau\right) \\ &= \sum_{l=r}^{N} \Pr\left(exactly(l)outof(N) \,:\, \max F_{C_{i_l}}(x) \le \tau\right) \\ &= \sum_{l=r}^{N} \frac{1}{l!(N-l)!} \sum_{\mathfrak{J}} F_{C_{i_1}}(\tau) \cdots F_{C_{i_l}}(\tau) \left(1 - F_{C_{i_{l+1}}}(\tau)\right) \cdots \left(1 - F_{C_{i_N}}(\tau)\right). \end{aligned} \tag{50}$$

Where $\sum_{\mathfrak{J}} \triangleq$ represents the sum over all $N!$ permutations $\left(i_1, i_2, i_3, \ldots i_N\right)$ *of* $(1, 2, 3, \ldots N)$. Let $\gamma_{i\omega}, \omega \in \{1, 2\}$, represent the SINR within the first and the second phases, respectively, where $\gamma_{i1} = \frac{1+\gamma_M}{1+\gamma_{E_J}}$, $M \in \{(s,i)\}$, $E_J \in \{(s,J)\}$, $\gamma_{i2} = \frac{1+\gamma_M}{1+\gamma_{E_J}}$, $M \in \{(i,d)\}$, $E_J \in \{(i,J)\}$ and $\gamma_i = \min\left(\gamma_{i1}, \gamma_{i2}\right)$, then, $C_{sJ,1,2}(i)$ can be replaced by γ_i, by substituting $F_{C_{i_l}}(\tau) = F_{\gamma_i|i=i_l}(\gamma)$ *in* (47), $i_1 < i_2 \ldots i_N$, the CDF of the achievable rate of the ith selected relay that has the order l can be formulated.

Finally, the optimal relay, i.e., $R^*_{i|i=i^*}$, $r = 1$, is selected based on a robust form of (50) as

$$F_{C_{1:N}}(\gamma) = \Pr\left(\max_{i_l}\left(\gamma_{i_l}\right) \le \gamma, l_1 \prec l_2 \prec \ldots l_N\right) = \sum_{l=1}^{N} \sum_{\mathfrak{J}_L} \left(\prod_{s=1}^{l} F_{\gamma_{i_s}}(\gamma)\right)\left(\prod_{s=l+1}^{N} 1 - F_{\gamma_{i_s}}(\gamma)\right). \tag{51}$$

where $\sum_{\mathfrak{J}_l} \triangleq$ *represents the sum over all permutations* $\left(i_1, i_2, i_3, \ldots i_N\right)$ *of* $(1, 2, 3, \ldots N)$. *that includes* $\binom{N}{l}$ *terms instade of* $N!$*terms in* (50), $i_1 < i_2 \ldots i_N$.

3.2.2 Optimal Relay Selection in Statistical CSI Availability

In this subsection, we rely on the statistical data of the global CSI of all links where it is confirmed that the small and large scale computations of the channels' characteristics do not vary drastically over a long period of time. Thus, it is sufficient to compute and test a

specific performance metric such as the secrecy outage probability to decide which relay will be selected.

The secrecy outage probability is defined as the probability that the achievable secrecy rate (e.g., correspondingly SINR) falls below a desired secrecy rate (e.g., correspondingly a desired level).

Let the desired threshold levels γ_{out1} and γ_{out2} for the first and the second phases, respectively. The secrecy outage probability may be computed equivalently as

$$P_{out_i} = 1 - \underbrace{\Pr\left(\gamma_{i1} \succ \gamma_{out1}, \gamma_{i2} \succ \gamma_{out2}\right)}_{\alpha} = 1 - \Pr\left(\gamma_{i1} \succ \gamma_{out1}\right) \times \Pr\left(\gamma_{i2} \succ \gamma_{out2}\right)$$
$$= 1 - \left(1 - \Pr\left(\gamma_{i1} \leq \gamma_{out1}\right)\right)\left(1 - \Pr\left(\gamma_{i2} \leq \gamma_{out2}\right)\right) = 1 - \left(\left(1 - F_{\gamma_{i1}}\left(\gamma_{out1}\right)\right)\left(1 - F_{\gamma_{i2}}\left(\gamma_{out2}\right)\right)\right), \tag{52}$$

where α indicates the joint probability and the last two terms follow from the fact that they are two disjoint events.

Hence, the optimal relay selection can be formulated by selecting R_i^* that minimizing the statistical secrecy outage probability by satisfying

$$i^* = \arg\min_i P_{out_i}(\gamma). \tag{53}$$

In the next section, we are going to derive expressions for the secrecy outage probability and some other performance metrics such as non-zero achievable secrecy rate and asymptotic secrecy outage probability.

3.3 Performance Metrics

In the concerned system, one feasible method to ensure a confidential data security and reliability against eavesdropping is to transmit the data with a rate that is less than its dedicated channel capacity (i.e., from the source to destination) while maintain the difference between the transmitted and the confidential data rates larger than the channel capacity dedicated for the eavesdropping system. This guarantees that any transmitted data rate will become beyond the reliable illegal interception.

3.3.1 The Exact Secrecy Outage Probability

A special case of (52) when the communication channel requires one desired or predefined SINR level, γ. In such a case, $P_{out_i}(\gamma)$ of the ith relay is given by

$$P_{out_i}(\gamma) = 1 - \Pr\left(\min\left(\gamma_{i1}, \gamma_{i2}\right) \succ \gamma\right) = F_{\gamma_{i1}}(\gamma) + F_{\gamma_{i2}}(\gamma) - F_{\gamma_{i1}}(\gamma) F_{\gamma_{i2}}(\gamma). \tag{54}$$

Unlike the relay selection scheme, closed form expressions for $P_{out_i}(\gamma)$ can be derived in terms of γ_{i1} and γ_{i2} as shown in the following theorems.

Let $\gamma_{i\omega} = \dfrac{1+\frac{Z_{1,\omega}}{Z_{2,\omega}}\Big/Z_{4,\omega}}{1+Z_{3,\omega}/Z_{4,\omega}}$, $\omega \in \{1, 2\}$, be the SINRs of the first and the second communication phases, then, we have the following cases.

Case 1: Maximum of the eavesdroppers:

Theorem 4 *The CDF of* the SINR $\gamma_{i\omega}$, $\omega \in \{1,2\}$, according *to* (28) *can be derived statistically as*

$$F_{\gamma_{i\omega}}(\gamma) = \begin{cases} \sum_{\substack{j=1 \\ j\neq r}}^{M} (-1)^{j-1} \sum_{l_1 \prec l_2 \ldots l_M} \aleph_j(\gamma) + (-1)^{r-1} \ell_r(\gamma) \; for \; \frac{\Omega_{Z_{4,\omega}}}{\gamma - 1} = \frac{\zeta_{\omega,r}}{\gamma}\Big|_{r\in\{1,2,\ldots M\}} \\ \sum_{j=1}^{M} (-1)^{j-1} \sum_{l_1 \prec l_2 \ldots l_M} \aleph_j(\gamma) \qquad\qquad otherwise \end{cases}$$

where

$$\begin{cases} \aleph_j(\sigma) = \exp\left(\Omega_{Z_{2,\omega}}\right)\left(1 + \frac{\frac{\alpha_j}{\sigma}\frac{\Omega_{Z_{4,\omega}}}{\sigma-1}}{\frac{\zeta_{\omega,j}}{\sigma} - \frac{\Omega_{Z_{4,\omega}}}{\sigma-1}}\left(\exp\left(\frac{\alpha_j}{\sigma}\right)Ei\left(-\frac{\alpha_j}{\sigma}\right)\right) - \frac{\frac{\zeta_{\omega,j}}{\sigma}\frac{\beta}{\sigma-1}}{\frac{\zeta_{\omega,j}}{\sigma} - \frac{\Omega_{Z_{4,\omega}}}{\sigma-1}}\left(\exp\left(\frac{\beta}{\sigma-1}\right)Ei\left(-\frac{\beta}{\sigma-1}\right)\right)\right) \\ \ell_j(\sigma) = 1 - \frac{\Omega_{Z_{2,\omega}}}{\Omega_{Z_{1,\omega}}}\lambda_i - \left(\frac{\Omega_{Z_{2,\omega}}}{\Omega_{Z_{1,\omega}}}\lambda_i\right)^2 \exp\left(\frac{\Omega_{Z_{2,\omega}}}{\Omega_{Z_{1,\omega}}}\lambda_i\right)Ei\left(-\frac{\Omega_{Z_{2,\omega}}}{\Omega_{Z_{1,\omega}}}\lambda_i\right), \lambda_i = \frac{\zeta_{\omega,j}}{\sigma} = \frac{\Omega_{Z_{4,\omega}}}{\sigma-1} \end{cases} \tag{55}$$

where $\zeta_{1,j} \in \{\zeta_{s,j}\}, \zeta_{2,j} \in \{\zeta_{i,j}\}$, $\alpha_j = \frac{\Omega_{Z_{2,\omega}}\zeta_{\omega,j}}{\Omega_{Z_{1,\omega}}}$, $\forall j = 1, \ldots M$, $\beta = \frac{\Omega_{Z_{2,\omega}}\Omega_{Z_{4,\omega}}}{\Omega_{Z_{1,\omega}}}$, $\left|\arg\left(\frac{\Omega_{Z_{2,\omega}}}{\Omega_{Z_{1,\omega}}}\right)\right| \leq \pi$ *and* γ *is the SINR threshold.*

Proof Applying similar steps as Theorem 2, the CDF of the R.V. $\gamma_{i\omega}$ can be derived as follows

$$F_{\gamma_{i\omega}}(\sigma) = \Pr\left(\frac{Z_{1,\omega}}{Z_{2,\omega}} \leq \left(\sigma Z_{3,\omega} + (\sigma - 1)Z_{4,\omega}\right)\right), \max.of(eaves.). \tag{56}$$

First, we have to compute the CDF of $Z_{i\omega} = \frac{Z_{1,\omega}}{Z_{2,\omega}}$, which can be computed in a similar form as (21) using (22) as

$$F_{Z_{i\omega}}(x) = \frac{\Omega_{Z_{1,\omega}} x \exp\left(\Omega_{Z_{2,\omega}}\right)}{\Omega_{Z_{1,\omega}} x + \Omega_{Z_{2,\omega}}}. \tag{57}$$

Then, it is necessary to compute the PDF of $Y_{i\omega} = \sigma Z_{3,\omega} + (\sigma - 1)Z_{4,\omega}$ in that case, in a similar way to (36)

$$f_{Y_{i\omega}}(x) = \begin{cases} \sum_{j=1}^{M} (-1)^{j-1} \sum_{l_1 \prec l_2 \ldots l_M} \frac{\frac{\zeta_{\omega,j}}{\sigma}\frac{\Omega_{Z_{4,\omega}}}{\sigma-1}}{\frac{\zeta_{\omega,j}}{\sigma} - \frac{\Omega_{Z_{4,\omega}}}{\sigma-1}}\left(\exp\left(-\frac{\Omega_{Z_{4,\omega}}}{\sigma-1}x\right) - \exp\left(-\frac{\zeta_{\omega,j}}{\sigma}x\right)\right) \; for \; \frac{\Omega_{Z_{4,\omega}}}{\sigma-1} \neq \frac{\zeta_{\omega,j}}{\sigma} \forall j \in \{1,2,\ldots M\} \\ \lambda_i^2 x \exp\left(-\lambda_i x\right) \qquad\qquad for \; \lambda_i = \frac{\Omega_{Z_{4,\omega}}}{\sigma-1} = \frac{\zeta_{\omega,j}}{\sigma}\Big|_{j=1,2,\ldots M} \end{cases} \tag{58}$$

Utilizing a similar integral as (38) (see [33, Eq. (3.353.5)]) and some algebraic manipulations the CDF of the R.V. $\gamma_{i\omega}$ can be derived in part as

$$F_{\gamma_{i\omega}}(\sigma)=\begin{cases}\sum_{j=1}^{M}(-1)^{j-1}\sum_{l_1<l_2\ldots l_M}\exp\left(\Omega_{Z_{2,\omega}}\right)\left(1+\frac{\frac{\alpha_j}{\sigma}\frac{\Omega_{Z_{4,\omega}}}{\sigma-1}}{\frac{\zeta_{\omega,j}}{\sigma}-\frac{\Omega_{Z_{4,\omega}}}{\sigma-1}}\left(\exp\left(\frac{\alpha_j}{\sigma}\right)Ei\left(-\frac{\alpha_j}{\sigma}\right)\right)\right. & \\ \left.-\frac{\frac{\zeta_{\omega,j}}{\sigma}\frac{\beta}{\sigma-1}}{\frac{\zeta_{\omega,j}}{\sigma}-\frac{\Omega_{Z_{4,\omega}}}{\sigma-1}}\left(\exp\left(\frac{\beta}{\sigma-1}\right)Ei\left(-\frac{\beta}{\sigma-1}\right)\right)\right) & for\frac{\Omega_{Z_{4,\omega}}}{\sigma-1}\neq\frac{\zeta_{\omega,j}}{\sigma}\forall j\in\{1,2,\ldots M\}\\ 1-\frac{\Omega_{Z_{2,\omega}}}{\Omega_{Z_{1,\omega}}}\lambda_i-\left(\frac{\Omega_{Z_{2,\omega}}}{\Omega_{Z_{1,\omega}}}\lambda_i\right)^2\exp\left(\frac{\Omega_{Z_{2,\omega}}}{\Omega_{Z_{1,\omega}}}\lambda_i\right)Ei\left(-\frac{\Omega_{Z_{2,\omega}}}{\Omega_{Z_{1,\omega}}}\lambda_i\right) & for\lambda_i=\frac{\Omega_{Z_{4,\omega}}}{\sigma-1}=\frac{\zeta_{\omega,j}}{\sigma}\Big|_{j=1,2,\ldots M}\end{cases} \tag{59}$$

and (55) follows after rearranging the terms.□

Case 2: Co-operative eavesdroppers:

Theorem 5 *The CDF of the SINR* $\gamma_{i\omega}$ (42), $\omega\in\{1,2\}$, *can be derived statistically as*

$$F_{\gamma_{i\omega}}(\sigma)=\begin{cases}\frac{\left(\frac{\Omega_{Z_{3,\omega}}}{\sigma}\right)^M\exp\left(\Omega_{Z_{2,\omega}}\right)}{\left(\frac{\Omega_{Z_{3,\omega}}}{\sigma}-\frac{\Omega_{Z_{4,\omega}}}{\sigma-1}\right)^M}\left(1+\frac{\beta}{\sigma-1}\exp\left(\frac{\beta}{\sigma-1}\right)Ei\left(-\frac{\beta}{\sigma-1}\right)-\frac{\beta}{\sigma-1}\sum_{w=0}^{M}\frac{(-1)^w}{w!}(\alpha-\beta)\right. & \\ \left.\left(\exp\left(\frac{\alpha}{\sigma}\right)Ei\left(-\frac{\alpha}{\sigma}\right)+\sum_{\delta=0}^{w}(-1)^{\delta}\delta!\left(\frac{\alpha}{\sigma}\right)^{-(\delta+1)}\right)\right) & for\ \frac{\Omega_{Z_{4,\omega}}}{\sigma-1}\neq\frac{\Omega_{Z_{3,\omega}}}{\sigma}\\ \frac{(-1)^M}{M!}\left(\Omega_{\alpha\beta}\right)^{M+1}\exp\left(\Omega_{Z_2}\right)\left(\exp\left(\Omega_{\alpha\beta}\right)Ei\left(-\Omega_{\alpha\beta}\right)+\sum_{w=0}^{M}(-1)^w w!\left(\Omega_{\alpha\beta}\right)^{-(w+1)}\right) & for\ \frac{\Omega_{Z_{4,\omega}}}{\sigma-1}=\frac{\Omega_{Z_{3,\omega}}}{\sigma}=\lambda_i\end{cases} \tag{60}$$

Where $\Omega_{Z_{3,1}}\in\left\{\Omega_{sJ}\triangleq \text{aver}_j\left(\Omega_{s,j}\right)\right\}$, $\Omega_{Z_{3,2}}\in\left\{\Omega_{iJ}\triangleq \text{aver}_j\left(\Omega_{i,j}\right)\right\}$, $\forall j=1,\ldots M$, $\alpha=\frac{\Omega_{Z_{2,\omega}}\Omega_{Z_{3,\omega}}}{\Omega_{Z_{1,\omega}}}$, $\beta=\frac{\Omega_{Z_{2,\omega}}\Omega_{Z_{4,\omega}}}{\Omega_{Z_{1,\omega}}}$, $\Omega_{\alpha\beta}=\lambda_i\frac{\Omega_{Z_{2,\omega}}}{\Omega_{Z_{1,\omega}}}$, $\left|\arg\left(\frac{\Omega_{Z_{2,\omega}}}{\Omega_{Z_{1,\omega}}}\right)\right|\leq\pi$ and σ *is the SINR threshold.*

Proof Applying similar steps as Theorem 3, the CDF of the R.V. $\gamma_{i\omega}$ can be derived as follows

$$F_{\gamma_{i\omega}}(\sigma)=\Pr\left(\frac{Z_{1,\omega}}{Z_{2,\omega}}\leq\left(\sigma Z_{3,\omega}+(\sigma-1)Z_{4,\omega}\right)\right),\ Cooperative(eaves.). \tag{61}$$

The CDF of $Z_{i\omega}=\frac{Z_{1,\omega}}{Z_{2,\omega}}$ is given by (57). Then, the PDF of $Y_{i\omega}=\sigma Z_{3,\omega}+(\sigma-1)Z_{4,\omega}$ in that case, which is directly given as (36) by

$$f_{Y_{i\omega}}(x) = \begin{cases} \frac{\left(\frac{\Omega_{Z_{3,\omega}}}{\sigma}\right)^M \frac{\Omega_{Z_{4,\omega}}}{\sigma-1}}{\left(\frac{\Omega_{Z_{3,\omega}}}{\sigma} - \frac{\Omega_{Z_{4,\omega}}}{\sigma-1}\right)^M} \left(\exp\left(-\frac{\Omega_{Z_{4,\omega}}}{\sigma-1}x\right)\right. & for\ \frac{\Omega_{Z_{4,\omega}}}{\sigma-1} \neq \frac{\Omega_{Z_{3,\omega}}}{\sigma} \\ \left. -\left(\exp\left(-\frac{\Omega_{Z_{3,\omega}}}{\sigma}x\right)\sum_{\delta=0}^{M-1}\frac{x^\delta}{\delta!}\left(\frac{\Omega_{Z_{3,\omega}}}{\sigma} - \frac{\Omega_{Z_{4,\omega}}}{\sigma-1}\right)^\delta\right)\right) & \\ \lambda_i^{M+1}\frac{x^M}{M!}\exp\left(-\lambda_i x\right) & for\ \frac{\Omega_{Z_{4,\omega}}}{\sigma-1} = \frac{\Omega_{Z_{3,\omega}}}{\sigma} = \lambda_i \end{cases}. \tag{62}$$

Utilizing a similar integral as (38) (see [33, Eq. (3.353.5)]) and some algebraic manipulations the CDF of the R.V. $\gamma_{i\omega}$ or (60) follow after rearranging the terms.□

Hence, the secrecy outage probability can be expressed by substituting in (54) and its related form of the optimal relay selection which can be likely written without order statistics as

$$P_{out_{optimal}} = \prod_{i=1}^{N} P_{out_i}. \tag{63}$$

3.3.2 The Non-zero Achievable Secrecy Rate

By employing the fact that $\forall \epsilon \in \Re, \left(\log_2 \epsilon\right) > 0 \overset{yields}{\rightarrow} \epsilon > 1$, it is obtained from (56) and (61) by substituting for $\sigma = 1$ as in the following forms.

Let $P_{secrecy}$ be the optimal achievable non-zero secrecy probability which occurs when there exists a non-zero secrecy capacity for the secondary communication network, namely

$$P_{secrecy} = \Pr\left(C_{i^*} \succ 0\right) = \Pr\left(\gamma_{i^*} \succ 1\right) = \prod_{i=1}^{N}\left(1 - P_{out_i}(1)\right). \tag{64}$$

Where i^* represents the optimal relay, by considering the cases of eavesdropping $P_{out_i}(1)$ can be determined as follows:

Case 1: Maximum of the eavesdroppers:

Plugging (33) and (57) into (56), solving for $\sigma = 1$ and using a similar integral as (36), $F_{\gamma_{i\omega}}(1)$ is given by,

$$F_{\gamma_{i\omega}}(1) = \Pr\left(\frac{Z_{1,\omega}}{Z_{2,\omega}} \leq Z_{3,\omega}\right), \max.of(eaves.) = 1 + \sum_{j=1}^{M}(-1)^{j-1}\sum_{l_1<l_2\prec\ldots l_M}\alpha_j \exp\left(\alpha_j\right)Ei\left(-\alpha_j\right). \tag{65}$$

Where $\alpha_j = \frac{\Omega_{Z_{2,\omega}}\zeta_{\omega,j}}{\Omega_{Z_{1,\omega}}}, \forall j = 1, \ldots M$ *and* $\left|arg\left(\frac{\Omega_{Z_{2,\omega}}}{\Omega_{Z_{1,\omega}}}\right)\right| \leq \pi$, by substituting in (54) for $\omega = 1$ or 2, $P_{out_i}(1)$ follows directly.

Case 2: Co-operative eavesdroppers:

Plugging (42) and (57) into (61), solving for $\sigma = 1$ and using a similar integral as (36), $F_{\gamma_{i\omega}}(1)$ is given by

$$F_{\gamma_{i\omega}}(1) = \Pr\left(\frac{Z_{1,\omega}}{Z_{2,\omega}} \leq Z_{3,\omega}\right), Cooperative(eaves.)$$
$$= \frac{(-1)^{M-1}\alpha^M}{(M-1)!}\exp\left(\Omega_{Z_{2,\omega}}\right)\left(\exp(\alpha)Ei(-\alpha) + \sum_{\delta=1}^{M}\frac{(-1)^{\delta}(\delta-1)!}{\alpha^{\delta}}\right). \quad (66)$$

Where $\left|arg\left(\frac{\Omega_{Z_{2,\omega}}}{\Omega_{Z_{1,\omega}}}\right)\right| \leq \pi$, by substituting in (54) for $\omega = 1$ or 2, $P_{out_i}(1)$ follows directly.

3.3.3 Inner and Outer System Bounds for the Secrecy Outage Probability

As a reference relay selection scheme, system bounds can be considered by assuming that the cooperative system can possess the buffering capability [37] at the relay nodes. Therefore, the cooperative system has the option to store data for the next phase and select the two relays of the strongest secrecy rates for the two phases yielding the lowest secrecy outage probability. Thus, we can define an inner (lower) bound for the secrecy outage probability when the minimum secrecy outage probability of a dual-hop communication itself for a certain selected relay is indeed the minimum outage amongst the entire relays, namely

$$P_{out}^{\min} = \Pr\left(\max_i\left(\max\left(\gamma_{i1},\gamma_{i2}\right) \leq \gamma\right)\right) = F_{\gamma_{i^*}}(\gamma) = \prod_{i=1}^{N}\left(F_{\gamma_{i1}}(\gamma)F_{\gamma_{i2}}(\gamma)\right). \quad (67)$$

In contrary, the system outer (upper) bound is defined by

$$P_{out}^{\max} = \Pr\left(\max_i\left(P_{out_i}\right) \leq \gamma\right) = 1 - \prod_{i=1}^{N}\left(1 - P_{out_i}\right). \quad (68)$$

In this case, the maximum secrecy outage probability of a dual-hop communication itself for a certain selected relay is indeed the maximum outage amongst the entire relays.

3.4 The Asymptotic Outage Probability

Exact expressions are too complicated to interpret conceptually the impact of interference and eavesdropping for high SINR regime which represents the main agent that identifies and controls the network behavior. In the following, the effect of increasing the SINR statistically on all network parameters will be studied.

If the transmit SINR is abruptly increased toward the received nodes to enhance the system performance within the secondary network, the CDF of $Z_{1,\omega}$ can be approximated to its first order term, simply

$$F_{Z_{1,\omega}}(x) = \Omega_{Z_{1,\omega}}x. \quad (69)$$

Upon this fact, let the other R.V. s be dependently unchanged, then, by applying similar statistical analysis the system asymptotic optimal secrecy outage probability can be expressed in a generalized form as

$$P_{out_{i^*}}^{\infty} = \left(\kappa \times SINR_{system}\right)^{-\eta}. \quad (70)$$

Where the impact of diversity order (gain) η will be emphasized here,[5] (e.g., it can be enhanced by using relays with distinguishable parameters). The diversity gain can be defined as the negative exponent of the average symbol error probability SEP in a log–log scale when SINR goes to infinity [35, 36] and related to the secrecy outage probability by (70), κ is the coding gain parameter, i^* is the optimal relay and $SINR_{system}$ is the overall system SINR.

To investigate the impact of the diversity order, system high SINR and coding gain, $P^{\infty}_{out_{i^*}}$ should be computed and coincided with (70), then, by extracting comparative relations for κ, $SINR_{system}$ and η, one can study a unified framework for the effect of those system communication metrics and build up relay selection strategies.

Accordingly, we have to compute $P^{\infty}_{out_i}$ of relay R_i in terms of the CDF of the corresponding SINR as in (54).

Theorem 6 *By considering (70) the CDF of $\gamma_{i\omega}$ may be generally derived as*

$$F_{\gamma_{i\omega}}(\gamma) = \varphi_{i\omega}\gamma. \tag{71}$$

Where $\phi_{i\omega}$ is expressed as follows:
Case of max. of eavesdroppers

$$\varphi_{i\omega} = \begin{cases} \sum\limits_{\substack{j=1 \\ j\neq r}}^{M} (-1)^{j-1} \sum\limits_{l_1<l_2\ldots l_M} \Xi_j + (-1)^{r-1}\Theta_r \; for \frac{\Omega_{Z_{4,\omega}}}{\sigma-1} = \frac{\zeta_{\omega,r}}{\sigma}\Big|_{r\in\{1,2,\ldots M\}} \\ \sum\limits_{j=1}^{M} (-1)^{j-1} \sum\limits_{l_1<l_2\ldots l_M} \Xi_j \qquad\qquad otherwise \end{cases}$$

where

$$\begin{cases} \Xi_j(\sigma) = \frac{\Omega_{Z_{1,\omega}}}{\Omega_{Z_{2,\omega}}} \exp\left(\Omega_{Z_{2,\omega}}\right) \sum\limits_{j=1}^{M} (-1)^{j-1} \sum\limits_{l_1<l_2\ldots l_M} \frac{\frac{\zeta_{\omega,j}}{\sigma}+\frac{\Omega_{Z_{4,\omega}}}{\sigma-1}}{\frac{\zeta_{\omega,j}}{\sigma}\frac{\Omega_{Z_{4,\omega}}}{\sigma-1}} \; for \frac{\Omega_{Z_{4,\omega}}}{\sigma-1} \neq \frac{\zeta_{\omega,j}}{\sigma} \forall j \in \{1,2,\ldots M\} \\ \Theta_j(\sigma) = \frac{2\Omega_{Z_{1,\omega}}}{\lambda_i\Omega_{Z_{2,\omega}}} \exp\left(\Omega_{Z_{2,\omega}}\right) \qquad for \lambda_i = \frac{\Omega_{Z_{4,\omega}}}{\sigma-1} = \frac{\zeta_{\omega,j}}{\sigma}\Big|_{j=1,2,\ldots M} \end{cases}. \tag{72}$$

Case of cooperative eavesdroppers

$$\phi_{i\omega} = \begin{cases} \frac{\left(\frac{\Omega_{Z_{3,\omega}}}{\sigma}\right)^{M}\frac{\Omega_{Z_{4,\omega}}}{\sigma-1}}{\left(\frac{\Omega_{Z_{3,\omega}}}{\sigma}-\frac{\Omega_{Z_{4,\omega}}}{\sigma-1}\right)^{M}}\left(\frac{1}{\left(\frac{\Omega_{Z_{4,\omega}}}{\sigma-1}\right)^{2}} - \left(\sum\limits_{\delta=0}^{M-1} \frac{(\delta+1)}{\left(\frac{\Omega_{Z_{3,\omega}}}{\sigma}\right)^{\delta+2}}\left(\frac{\Omega_{Z_{3,\omega}}}{\sigma}-\frac{\Omega_{Z_{4,\omega}}}{\sigma-1}\right)^{\delta}\right)\right) & for \frac{\Omega_{Z_{4,\omega}}}{\sigma-1} \neq \frac{\Omega_{Z_{3,\omega}}}{\sigma} \\ \frac{(M+1)\Omega_{Z_{1,\omega}}}{\lambda_i\Omega_{Z_{2,\omega}}} \exp\left(\Omega_{Z_{2,\omega}}\right) & for \frac{\Omega_{Z_{4,\omega}}}{\sigma-1} = \frac{\Omega_{Z_{3,\omega}}}{\sigma} = \lambda_i \end{cases} \tag{73}$$

Proof From (70), the CDF of $Z_{i\omega} = \frac{Z_{1,\omega}}{Z_{2,\omega}}$ is given easily by

$$F_{Z_{iw}}(x) = \frac{\Omega_{Z_{1,\omega}} \exp\left(\Omega_{Z_{2,\omega}}\right)}{\Omega_{Z_{2,\omega}}} x. \tag{74}$$

[5] The diversity gain can be improved to approach $N, N \triangleq numberofrelays$, in this simple model by utilizing optimal relay selection and/or optimal combining.

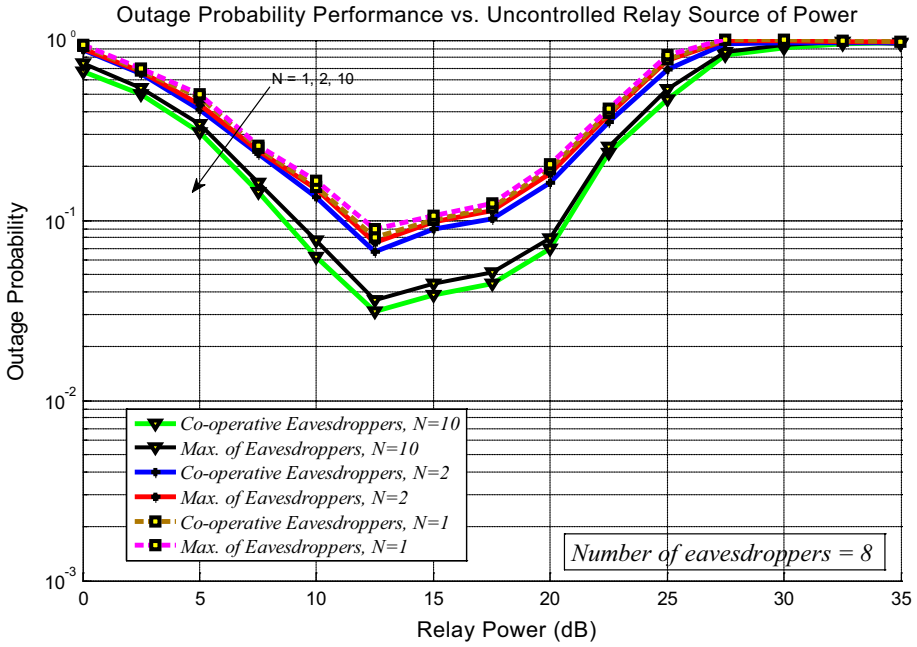

Fig. 2 Outage probability versus relay transmit power for target secrecy rate of 0.8, with N = 1, 2, 10

The CDF of the R.V. $\gamma_{i\omega}$ which is given by (56) and (61) of the considerable cases can be derived here after computing the PDF of $Y_{i\omega}$ in these cases, which are directly given by (58) and (62), respectively.

Applying similar steps as *the above theorems*, after utilizing a similar integral as (38) (see [33, Eq. (3.351.1–3)]), some algebraic manipulations and rearranging the terms, the CDF of the R.V. $\gamma_{i\omega}$ (71) follows. □

Therefore, $P^{\infty}_{out_i}\, ofrelay R_i$ can be expressed by substituting in (54) which leads to

$$P^{\infty}_{out_i} = \phi_{i1}\gamma + \phi_{i2}\gamma - \phi_{i1}\phi_{i2}\gamma^2, \tag{75}$$

By inserting (75) into a similar form of (51), it can be found that it perfectly matches (70) to the extent of

$$P^{\infty}_{out_{r^*:N}}(\gamma) = \sum_{l=r}^{N} \sum_{\Im_L} \left(\prod_{s=1}^{l} P_{out_{i_s}}(\gamma) \right) \left(\prod_{s=l+1}^{N} 1 - P_{out_{i_s}}(\gamma) \right) \overset{(a)}{=} (C\gamma)^{N-r+1} + \mathrm{O}(\gamma). \tag{76}$$

Where $P^{\infty}_{out_{r^*:N}}$ represents the asymptotic secrecy outage probability of optimal rth out of N relays, C is an arbitrary constant, $C \triangleq f\left(\phi_{i1}, \phi_{i2}\right)$, $\mathrm{O}(\gamma)$ are the higher order terms of γ and (a): follows after algebraic manipulations, equating powers and inserting

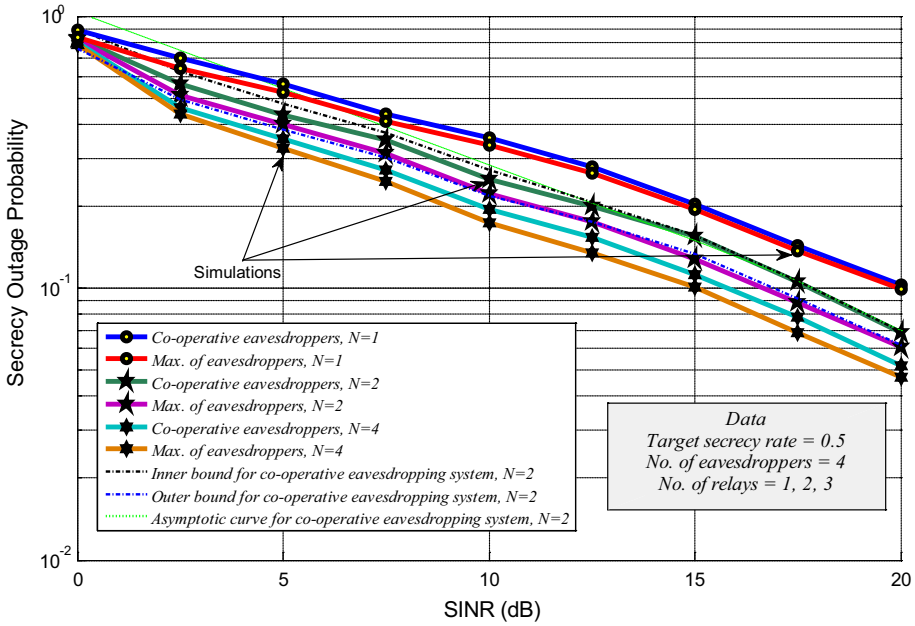

Fig. 3 Secrecy Outage probability versus SINR for relaxed target secrecy rate of 0.5

$$\prod_{s=l+1}^{M}\left(1-P_{outi_s}\right)=1+\sum_{s=l+1}^{M}(-1)^s\sum_{l_1<l_2<\ldots l_M}\prod_{k=1}^{s}P_{outi_{l_k}}$$
$$\text{where}\sum_{l_1<l_2<\ldots l_M}\equiv\sum_{l_1=1}^{M-j+1}\sum_{l_2=l_1+1}^{M-j+2}\cdots\sum_{l_j=l_{j-1}+1}^{M}. \tag{77}$$

The diversity order of the system can be extracted by equating lowest order exponent of SINR to (70), this shows that the achievable diversity can be of the order of $N - r + 1$.

4 Simulation Results

In this section, the analytical derivations are verified to be in consistent with simulation results as well as the impact of the system parameters on the security performance will be studied. This is confirmed by performing Monte Carlo simulations with 10^6 experimental trials.

From the previous analysis, one can find that the impact of relay interference is more severe with respect to the primary network than the source and destination and consequently, it dominates. However, we are interested in the impact of diversity gain that can be enhanced to approach $N, N \triangleq$ *number of relays*, in optimal relay selection. In general, the simulation is carried assuming equal values of fading coefficients ($\Omega_{q,r} = \Omega = 0.3$ dB, $q, r \in \{s, i, p, j, d\}$).

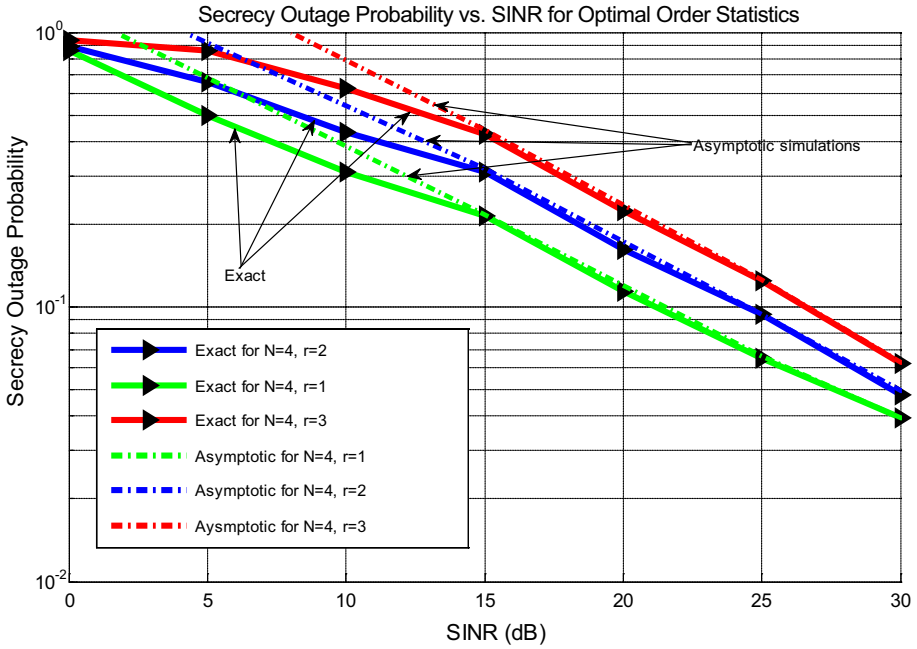

Fig. 4 Secrecy Outage Probability versus average SINR

Figure 2 illustrates the exact curves between the outage probability and a relay transmit power while fixing the source power, i.e., relay transmitters are the dominant interfere sources of power, with different number of co-operative relays. This figure indicates a local minimum value of outage which represents the optimal value of the relay power for security interference trade off. This value can be verified by plugging the inequality of arithmetic and geometric means together, i.e., $\prod_{i=1}^{N} P_{out_i} \leq \left(\frac{1}{N}\sum_{i=1}^{N} P_{out_i}\right)^{N}$, into (63) and solving for the equality. This figure also compares our exposed eavesdropping models. It is obvious that the co-operative eavesdropping scheme exhibits worse performance than the maximum of eavesdroppers scheme due to its robust overhearing procedure. Increasing the number of relays adds a quite degree of freedom that improves the system performance.

For low transmitted power the outage probability begins to deteriorate until it reaches its minimum value, then, it again begins to increase by increasing the transmitted power due to primary network constraints.

In Fig. 3 a statistical CSI knowledge about the primary network i.e., $\Omega_{p,i}, \Omega_{i,p}, \Omega_{s,p}$ and $\Omega_{p,d}$ is considered where constraint sources of power are maintained. The performance of the secrecy outage probability against the increasing in SINR is highlighted, i.e., when $\Omega_{s,i} = \Omega_{i,d}$. Moreover, the impact of increasing the number of relays, the inner and outer bounds are included in this figure. It is cleared that case of the maximum of eavesdroppers scheme outperforms the case of co-operative eavesdropping scheme. It is notable that the outage probability drops down when the SINR increases. The asymptotic responses and bounds approximate the exact ones to the extent that asymptotic, outer bound and exact curves are tightly compromised at high SINR. Finally, parallel slops for

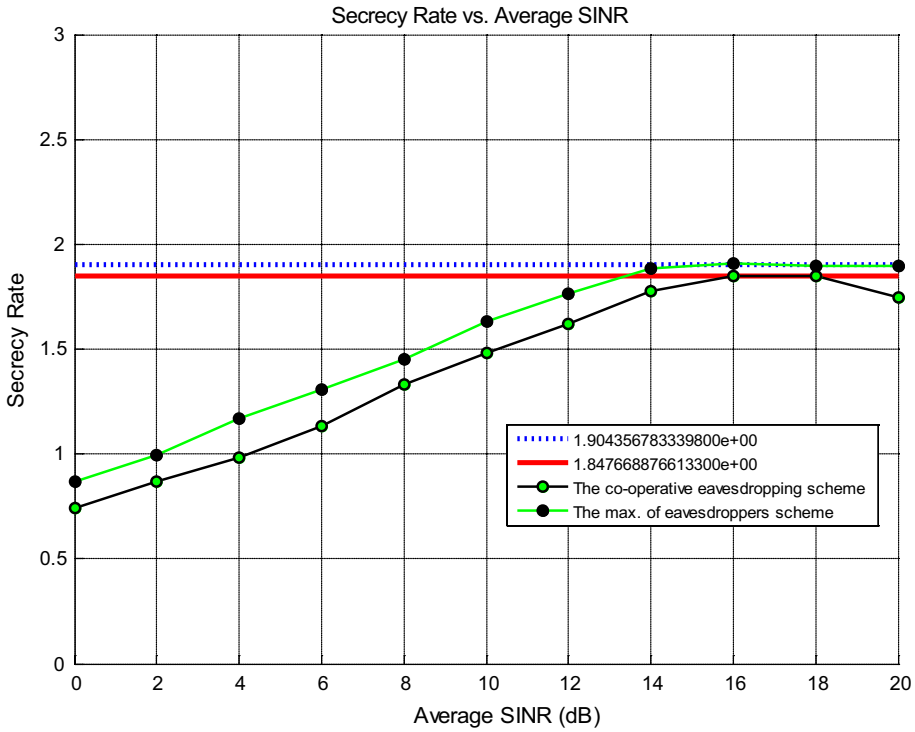

Fig. 5 Achievable capacity versus average SINR

different values of $N, N \triangleq$ *number of relays*, reflect the equality of the diversity gain.[6] There exists a successful agreement between the theoretical and simulation results which justifies our derivations.

In Fig. 4, it is anticipated that the secrecy outage probability increases when moving towards the decreased order statistics of the optimal relay selection, i.e., towards the optimal rth order relay selection, given the number of active relays in the co-operative relay system. It is also worthwhile to see that the asymptotic curve exhibits wider divergence from the exact curve at low SINR, when higher order statistics relay is selected. This verifies the impact of diversity order on the system performance. However, at high SINR the asymptotic curve perfectly fits the exact one. Moreover, it is evident that the asymptotic curve is plotted using (76) by substituting $C \triangleq f\left(\gamma_{i1}, \gamma_{i2}\right) = \gamma_{i1} + \gamma_{i2}$ and neglecting the higher order terms.

An illustration for the maximum achievable secrecy rate versus the average SINR ($\Omega_{s,i} = \Omega_{i,d} = \Omega$) is shown in Fig. 5. Using the proposed optimal selection and constraint

[6] It is noted that we simply plot one case for inner bound, outer bound and asymptotic curves so that the graphics do not interfere so as to be more visible.

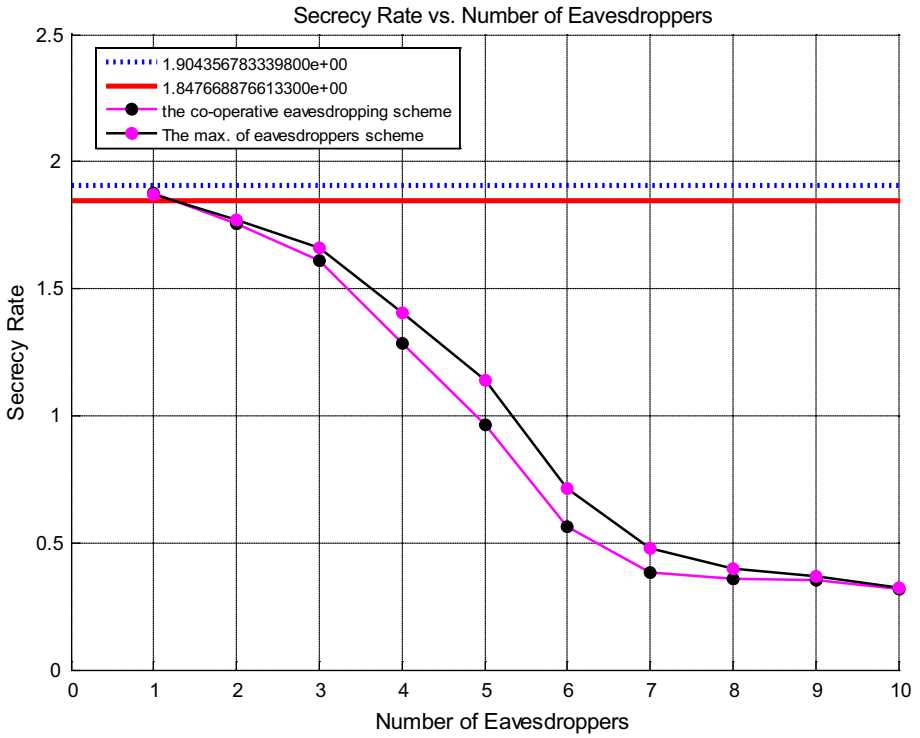

Fig. 6 The impact of the number of eavesdroppers on the secrecy rate

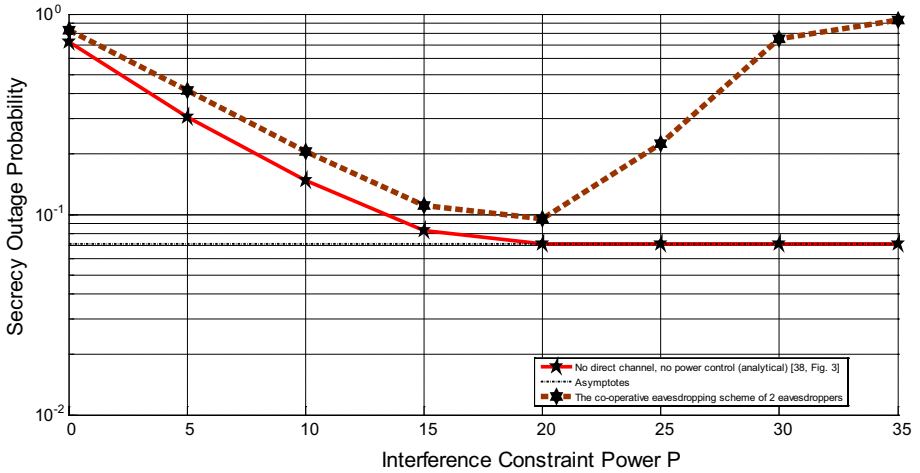

Fig. 7 The impact of increasing the constraint power P on the secrecy outage probability

power sources, one can observe that there is a limited maximum capacity values "upper floor" [25] after which the secrecy rate will collapse unless the constraints are preserved. This means that at high SINR the secrecy rate is approximately fixed.

As depicted in Fig. 6, the secrecy rate decreases when the overhearing nodes "M" increase. With a target rate of the secondary network of 0.5 bits/s/Hz, P_{Tx} power of 6 dB and S power of 2 dB, it can be shown that, increasing the number of eavesdroppers causes significant degradation in the secrecy rate. For $M \gg 1$, the performance curve over the co-operative eavesdropping scheme or the maximum of eavesdroppers scheme is asymptotically the same.

For a selected optimal relay i^*, our results are compared with [38, Fig. 3] where we use the same system parameters, i.e., the channel coefficients are modeled as $\Omega_{q,r} = \left(\frac{1}{d_{q,r}}\right)^{\delta}$, $=3$, where is the path loss exponent and $d_{q,r}$ is the distance between the node and the node . Thus, the following parameters are assumed: $d_{s,i^*} = d_{i^*,d} = 1$, $d_{s,J} = d_{s,p} = d_{i^*,p} = 6$, $d_{i^*,J} = 4$, $P = \vartheta P_p$; where $0 \leq \vartheta < 1$ is an arbitrary constant, $N_0 = 1$ and a target secrecy rate of 0.5 bits/s/Hz. The secrecy outage probability is plotted against the secondary constraint power $\frac{P}{|h_{s,p}|^2}$ as shown in Fig. 7, where for the comparison we consider MRC at the eavesdropping system (e.g., as in [38] and our cooperative eavesdropper scheme with two eavesdroppers). Different from the results in [38], it is observed that the relaxation of the constraint power by increasing the P_{Tx} transmit power can cause severe interference at the secondary networks. In [38], the secrecy outage first decreases with increase in the constraint power and later exhibits a floor because of increasing in parallel the ability of overhearing by the eavesdropping system. However, in our case, the interference of the primary network increases significantly the secrecy outage probability.

5 Conclusions

In this paper, relay selection schemes have been proposed and investigated to maintain secure communications in relay assisted underlay cognitive radio networks in the presence of multiple eavesdroppers. To evaluate the system performance, some important metrics have been computed such as secrecy outage probability and achievable secrecy rate to give an account on security and reliability trade-off parameters. Analytical expressions have been derived upon the exposed model to verify the impact of mutual interferences, sources of power and target rates of both the primary and the secondary networks in order to optimize the communication quality. Some system bounds have also been derived where the impact of their tightness at high SINR was demonstrated. Co-operative diversity adds another degree of freedom especially when the instantaneous CSI of the eavesdroppers is known. It is worth mentioning that the dual-hop secrecy optimization has replaced the per-hop one in order to jointly enhance the secrecy performance via exploiting the diversity gain. Simulation results were in accordance with the analytical ones. In the future work, we will examine the situation when the eavesdropping system realizes the same benefit of diversity order.

References

1. Haykin, S. (2005). Cognitive radio: Brain-empowered wireless communications. *IEEE Journal on Selected Areas in Communications, 23,* 201–220.

2. Liu, K. J. R., Sadek, A. K., Su, W., & Kwasinski, A. (2008). *Cooperative communications and networking*. Cambridge: Cambridge University Press.
3. Amarasuriya, G., Ardakani, M., & Tellambura, C. (2010). Output-Threshold multiple relay selection scheme for cooperative wireless networks. *IEEE Transactions on Vehicular Technology, 59*(6), 3091–3097.
4. Ikki, S. S., & Ahmed, M. H. (2009). On the performance of amplify-and forward cooperative diversity with the *n*th best-relay selection scheme. In *Proceedings of 2009 IEEE international conference on communications (ICC'09)* (pp. 1–6).
5. Duy, T. T., An, B., & Kong, H.-Y. (2010). A novel cooperative-aided transmission in multi-hop wireless networks. *IEICE Transactions on Communications, E93.B*(3), 716–720.
6. Laneman, J. N., Tse, D. N. C., & Wornell, G. W. (2004). Cooperative diversity in wireless networks: Efficient protocols and outage behavior. *IEEE Transactions on Information Theory, 50*(12), 3062–3080.
7. Bletsas, A., Khisti, A., Reed, D. P., & Lippman, A. (2006). A simple cooperative diversity method based on network path selection. *IEEE Journal on Selected Areas in Communications, 24*(3), 659–672.
8. Cuba, F. G., Cacheda, R. A., & Castaño, F. J. G. (2012). A survey on cooperative diversity for wireless networks. *IEEE Communications Surveys & Tutorials, 14*(3), 822–835.
9. Hasna, M. O., & Alouini, M. S. (2003). End-to-end performance of transmission systems with relays over Rayleigh-fading channels. *IEEE Transactions on Wireless Communications, 2*(6), 1126–1131.
10. Ikki, S., & Ahmed, M. H. (2009), Performance analysis of decode-and-forward incremental relaying cooperative diversity networks over Rayleigh fading channels. In *Proceedings of IEEE VTC spring, Barcelona*, April 2009 (pp. 1–6).
11. Ikki, S., Uysal, M., & Ahmed, M. H. (2009). Performance analysis of incremental-best-relay amplify-and-forward technique. In *Proceedings of IEEE GLOBECOM, Honolulu, Hawaii, November 30–December 4* (pp. 1–6).
12. Krikidis, I., Thompson, J., McLaughlin, S., & Goertz, N. (2008). Amplify-and forward with partial relay selection. *IEEE Communications Letters, 12*(4), 235–237.
13. Suraweera, H. A., Michalopoulos, D. S., & Karagiannidis, G. K. (2009). Semi blind amplify-and-forward with partial relay selection. *Electronics Letters, 45*(6), 317–319.
14. Duy, T. T., & Kong, H.-Y. (2013). Performance analysis of incremental amplify-and-forward relaying protocols with nth best partial relay selection under interference constraint. *Wireless Personal Communications, 71*(4), 2741–2757.
15. Gopala, P. K., Lai, L., & Gamal, H. E. (2008). On the secrecy capacity of fading channels. *IEEE Transactions on Information Theory, 54*(10), 4687–4698.
16. Dong, L., Han, Z., Petropulu, A. P., & Poor, H. V. (2010). Improving wireless physical layer security via cooperating relays. *IEEE Transactions on Signal Processing, 58*(3), 1875–1888.
17. Mo, J., Tao, M., & Liu, Y. (2012). Relay placement for physical layer security: A secure connection perspective. *IEEE Communications Letters, 16*(6), 878–881.
18. Zou, Y., Wang, X., & Shen, W. (2013). Optimal relay selection for physical layer security in cooperative wireless networks. *IEEE Journal on Selected Areas in Communications, 31*(10), 2099–2111.
19. Sakran, H., Shokair, M., Nasr, O., El-Rabaie, S., & El-Azm, A. A. (2012). Proposed relay selection scheme for physical layer security in cognitive radio networks. *IET Communications, 6*(16), 2676–2687.
20. Mukherjee, A., Fakoorian, S. A. A., Huang, J., & Swindlehurst, A. L. (2014). Principles of physical layer security in multiuser wireless networks: A survey. *IEEE Communications Surveys and Tutorials, 16*(3), 1550–1573.
21. Srinivasa, S., & Jafar, S. A. (2007). Cognitive radios for dynamic spectrum access-the throughput potential of cognitive radio: A theoretical perspective. *IEEE Communications Magazine, 45*(5), 73–79.
22. Akyildiz, I. F., et al. (2008). A survey on spectrum management in cognitive radio networks. *IEEE Communications Magazine, 46*(4), 40–48.
23. Goldsmith, A., Jafar, S. A., Maric, I., & Srinivasa, S. (2009). Breaking spectrum gridlock with cognitive radios: An information theoretic perspective. *Proceedings of the IEEE, 97*(5), 894–914.
24. Tourki, K., Qaraqe, K. A., & Alouini, M. S. (2013). Outage analysis for underlay cognitive networks using incremental regenerative relaying. *IEEE Transactions on Vehicular Technology, 62*(2), 721–734.
25. Bao, V. N. Q., Trung, N. L., & Debbah, M. (2013). Relay selection schemes for dual-hop networks under security constraints with multiple eavesdroppers. *IEEE Transactions on Wireless Communications, 12*(12), 6067–6085.
26. Zou, Y., Champagne, B., Zhu, W. P., & Hanzo, L. (2015). Relay-selection improves the security-reliability trade-off in cognitive radio systems. *IEEE Transactions on Communications, 63*(1), 215–228.
27. Jindal, A., Kundu, C., & Bose, R. (2014). Secrecy outage of dual-hop AF relay system with relay selection without eavesdropper's CSI. *IEEE Communications Letters, 18*(10), 1759–1762.

28. Kundu, C., Ghose, S., & Bose, R. (2015). Secrecy outage of dual-hop regenerative multi-relay system with relay selection. *IEEE Transactions on Wireless Communications, 14*(8), 4614–4625.
29. Salhab, A., & Zummo, S. (2014). Cognitive DF generalized order relay selection networks with imperfect channel estimation and interference from primary user. In *2014 IEEE global communications conference*.
30. Ghose, S., Kundu, C., & Bose, R. (2016). Secrecy performance of dual-hop decode-and-forward relay system with diversity combining at the eavesdropper. *IET Communications, 10*(8), 904–914.
31. Dan Ngoc, P. T., Duy, T. T., Bao, V. N. Q., & Nhat, N. L. (2016). Security-reliability analysis for underlay cognitive radio networks with relay selection methods under impact of hardware noises. In *2016 International conference on advanced technologies for communications (ATC), Hanoi* (pp. 174–179).
32. Bloch, M., Barros, J., Rodrigues, M. R. D., & McLaughlin, S. W. (2008). Wireless information-theoretic security. *IEEE Transactions on Information Theory, 54*(6), 2515–2534.
33. Gradshteyn, I. S., & Ryzhik, I. M. (2007). *Table of integrals, series and products* (7th ed.). San Diego, CA: Academic.
34. Vaughan, R. J., & Venables, W. N. (1972). Permanent expressions for order statistics densities. *Journal of the Royal Statistical Society Series B, 34*(2), 308–310.
35. Simon, M. K., & Alouini, M.-S. (2005). *Digital communication over fading channels* (2nd ed.). New York: Wiley.
36. Ding, H., Ge, J., da Costa, D. B., & Jiang, Z. (2011). Asymptotic analysis of cooperative diversity systems with relay selection in a spectrum-sharing scenario. *IEEE Transactions on Vehicular Technology, 60,* 457–472.
37. Ikhlef, A., Michalopoulos, D. S., & Schober, R. (2011). Buffers improve the performance of relay selection. In *Proceedings of 2011 IEEE global communications conference* (pp. 1–6).
38. Chakraborty, P., & Prakriya, S. (2017). Secrecy outage performance of a cooperative cognitive relay network. *IEEE Communications Letters, 21*(2), 326–329.

Waleed Saad has received his BSc (Hons), M.Sc. and Ph.D. degrees from the Faculty of Electronic Engineering Menoufia University, Menouf, Egypt, in 2004, 2008 and 2013, respectively. He joined the teaching staff of the Department of Electronics and Electrical Communications of the same faculty since 2014. In 2005 and 2008, he worked as a demonstrator and assistant lecturer in the same faculty, respectively. He is a co-author of many papers in national and international conference proceedings and journals. He received the best paper award in NRSC 2016. His research areas of interest include mobile communication systems, computer networks, cognitive radio networks, D2D communication, OFDM systems, interference cancellation, resource allocations, PAPR reduction, physical and MAC layers design, and implementation of digital communication systems using FPGA.

Mona Shokair received the B.E. and M.E. degrees in electronics engineering from El-Menoufia University, El-Menoufia, Egypt, in 1993 and 1997, respectively. She received Ph.D. from Kyushu University, Japan, 2005. She was lecturer in El-Menoufia University from 2005 to 2010. She was Associated Professor in El-Menoufia University from 2011 to 2015. Since 2016, she received a Professor degree. Now, she is a head of Electrical and Electronic Communication Department of El-Menoufia University. She received VTS chapter IEEE award from Japan in 2003. Also, she received with co-authors the best paper in NRSC in Egypt 2016 and 2017, respectively. She published more than 140 papers until Jan. 2018. Now her current research is in OFDM system, WIMAX system, cognitive radios, D2D Communication and Wireless Sensor Network.

Shady M. Ibraheem received the B.S. degree in electronics and communications engineering from Tanta University, Egypt, 2003. Since then, he has worked as a maintenance engineer in Telecom Egypt for 15 years. Currently, he is looking forward to the M.S. degree at Menoufia University. His main research interests include channel coding and cognitive radio networks.