Wireless Pers Commun (2017) 96:2271–2288
DOI 10.1007/s11277-017-4297-x

Exact Outage Probability Analysis of a Dual-Hop Cognitive Relaying Network Under the Overhearing of an Active Eavesdropper

Sang Quang Nguyen[1,2] · Hyung Yun Kong[2]

Published online: 20 May 2017

Abstract In this paper, we study the secure communication of dual-hop cognitive relaying networks. An eavesdropper can combine two received signals from two hops by using the maximum ratio combining technique. The data transmission from the secondary source to the secondary destination is assisted by the best decode-and-forward relay, which is selected from four relay selection schemes. The first scheme, MaSR, is based on the maximum channel gain from the source to the relays. In the second scheme, MaRD, the best relay is selected on the basis of the maximum channel gain from the relays to the destination. In the third scheme, MiRE, the gain to the eavesdroppers is instead minimized. Finally, optimal relay selection is considered as the fourth scheme. For these four schemes, we study the system security performance by deriving the exact analytical secrecy outage probability. These analytical expressions are then verified by comparing them with the results of Monte Carlo simulations. Herein, we evaluate and discuss the outage performance of the schemes while varying important system parameters: the number and locations of the relay nodes, primary user node, and eavesdropper; the transmit power threshold; and the target secure rate.

Keywords Cognitive relay network · Physical layer security · Relay selection · Decode-and-forward · Active eavesdropper · Outage probability

1 Introduction

Privacy and security issues caused by the broadcast nature of wireless media have attracted considerable attention. Conventionally, confidential messages are protected by using a key, as was introduced by Shannon [1], or by using cryptographic methods [2]. More recently,

✉ Sang Quang Nguyen
sangnqdv05@gmail.com

Hyung Yun Kong
hkong@mail.ulsan.ac.kr

1 Duy Tan University, Da Nang City, Vietnam

2 University of Ulsan, Ulsan, Republic of Korea

physical layer security (PLS) was proposed by Whyner with the basic idea that secure communication is guaranteed if the eavesdropper channel is a degraded version of the main channel [3]. PLS has been considered in Gaussian wiretap channels [4] and has also been extended to broadcast channels [5], fading channels [6], and in the presence of an eavesdropper in the communication between two legitimate users [7, 8].

To combat multipath fading in wireless communication, cooperative communication is an effective solution that increases the diversity capacity [9, 10]. Decode-and-forward (DF) and amplify-and-forward (AF) are the two main strategies applied at relay nodes in cooperative networks. In DF mode, the relay node detects information from the received signal and then re-encodes and forwards it in the following hop. In AF mode, the relay only amplifies the received signal and forwards it; this is simpler than DF but has the drawback that it contains additional noise.

To deal with attack from an eavesdropper, numerous studies have focused on PLS in cooperative communication (e.g., [11–15] and the references therein). In [11], three relay strategies [AF, DF, and cooperative jamming (CJ)] were employed to improve the security of wireless communications. In [12], the exact and asymptotic ergodic secrecy rate was studied in cooperative single-carrier systems under the affecting by multiple eavesdroppers. The authors in [13] investigate two best relay and user pair selection strategies to enhance the physical layer security of a multiuser cooperative relaying network in term of the secrecy outage probability (SOP). In [14], the authors design relay beamforming weights to enhance the secrecy rate under total and individual power constraint for relaying network. In [15], the authors proposed two user and relay pair selection criterions for multi-user multi-relay networks under considering the communication between multi-user and the base station is assisted by direct links and by multi-relay.

Cognitive radio has considered as an efficient technique to improve the spectrum efficiency in wireless communication systems [16]. It allows secondary users to access the spectrum bands of primary users without interfering with primary users communications by intelligently sensing to the environment. In the underlay mode of cognitive radio, secondary users transmit simultaneously with primary users over the same spectrum without degrading the quality of the primary transmission by keeping the interference to the primary users under a predefined threshold [17]. In [18], the authors investigate the performance of cognitive multi-hop DF and AF relay networks over independent but not necessarily identically distributed (i.n.i.d) Rayleigh fading channels. In [19], the optimal power allocation and relay selection strategies are proposed to enhance the transmission quality between source and destination in both dual-hop and multi-hop scenarios. Some relay-selection schemes [20] as well as assistance from a cooperative friendly jammer [21] have been shown to enhance the secrecy outage performance in cooperative cognitive radio networks.

To the best of our knowledge, there have been no studies investigating the effect of an active eavesdropper in cognitive radio networks under wiretapping by eavesdroppers. Therefore, we were motivated to analyze the exact secrecy outage probability of secure communication conducted via underlay cognitive relaying networks. In this model, we consider the communication between a secondary source and a secondary destination by means of assistance from multiple intermediate secondary relays (taking place in the presence of multiple primary users and eavesdroppers). To allow for performance evaluation and comparison, exact expressions are derived for the secrecy outage probability of four partial relay selection schemes. Four relay selection schemes are presented in order to select the one with the best relay to decode the information from the received signal and forward it to the destination: 1) a scheme for maximizing the channel gain from the source to the relays (MaSR), 2) a scheme for minimizing the channel gain from the relays to the primary users (MiRP), 3) a scheme for minimizing the channel gain from the relays to the eavesdroppers (MiRE), and 4) the optimal relay selection (ORS). Monte Carlo simulations are used to verify our theoretical analysis.

The rest of the paper is organized as follows. Section 2 presents the system model. Section 3 presents the secrecy outage probability analyses for the four schemes that were studied. Section 4 presents the numerical results from the simulations and theoretical analyses. Finally, Section 5 presents our conclusions.

Notation The functions $f_X(.)$ and $F_X(.)$ present the probability density function (PDF) and cumulative distribution function (CDF) of RV X. $[x]^+$ returns x if $x \geq 0$ and 0 if $x < 0$. $\mathcal{E}\{.\}$ denotes mathematical expectation. Pr[.] returns the probability. $C_b^a = \frac{b!}{a!(b-a)!}$. The function $\Gamma(x, y)$ is an incomplete Gamma function [22, Eq. (8.350.2)]. The function ${}_2F_1(.)$ represents Gausss hypergeometric function [22].

2 System Model and the Principle Operation of Three Protocols

As shown in Fig. 1, we consider a dual-hop spectrum sharing network under physical layer security. This consists of a secondary source (S), a secondary destination (D), N secondary relays (R_n, $n \in \{1, 2, \ldots, N\}$, where R_n indicates the nth relay node among N relays located in a cluster), a primary receiver (P), and an eavesdropper (E). In the network, all nodes are equipped with a single antenna operating in a half-duplex mode [15]. We assume that the primary transmitter is far enough away from the secondary receiver such that interference to the secondary receivers (i.e., R_n, D, and E) can be ignored. We denote (h_{1n}, d_{1n}), (h_{2n}, d_{2n}), (h_3, d_3), (h_{4n}, d_{4n}), (h_5, d_5), and (h_{6n}, d_{6n}) as the Rayleigh fading channel coefficients and distances of the links $S - R_n$, $R_n - D$, $S - E$, $R_n - E$, $S - PR$, and $R_n - PR$, respectively. Thus, the corresponding channels $g_\Omega = |h_\Omega|^2$, with $\Omega \in \{1n, 2n, 3, 4n, 5, 6n\}$, are exponentially distributed independent random variables (RVs) with parameters $\lambda_\Omega = (d_\Omega)^\beta$, where β denotes the path loss exponent (typically between 2 and 6). The corresponding cumulative distribution functions (CDFs) and probability density functions (PDFs) of the RVs g_Ω are expressed as $F_{g_\Omega}(x) = \lambda_\Omega e^{-\lambda_\Omega x}$ and $f_{g_\Omega}(x) = 1 - e^{-\lambda_\Omega x}$, respectively. The distances between two relay nodes in a cluster are insignificant compared to the distances between a relay node in a cluster and a node outside. Thus, we denote $d_{\Phi n} = d_\Phi$ and $\lambda_{\Phi n} = \lambda_\Phi$ with $\Phi \in \{1, 2, 4, 6\}$. Let us assume that there is no direct link from to (due to deep shadowing). Additionally, the global channel state information (CSI) is assumed to be available [11].

In this underlay network, the secondary transmitters S and R_n are adapted from their transmit powers as P_S and P_R, respectively, such that the interference caused at the PR does not exceed the maximum allowable interference power limit I.

$$P_S = \frac{I}{|h_5|^2} = \frac{I}{g_5}\ , \qquad P_{R_n} = \frac{I}{|h_{6n}|^2} = \frac{I}{g_{6n}} \tag{1}$$

There are two phases of total communication. In the first phase, S broadcasts its signal $x(t)$, with $\mathcal{E}\left\{|x(t)|^2\right\} = 1$, by the transmit power P_S to all relays under the overhearing of an eavesdropper. The best relay (R_b), which was selected from available relay nodes [from the four relay selection schemes presented in Eqs. (14), (19), (23), and (28)], decodes the

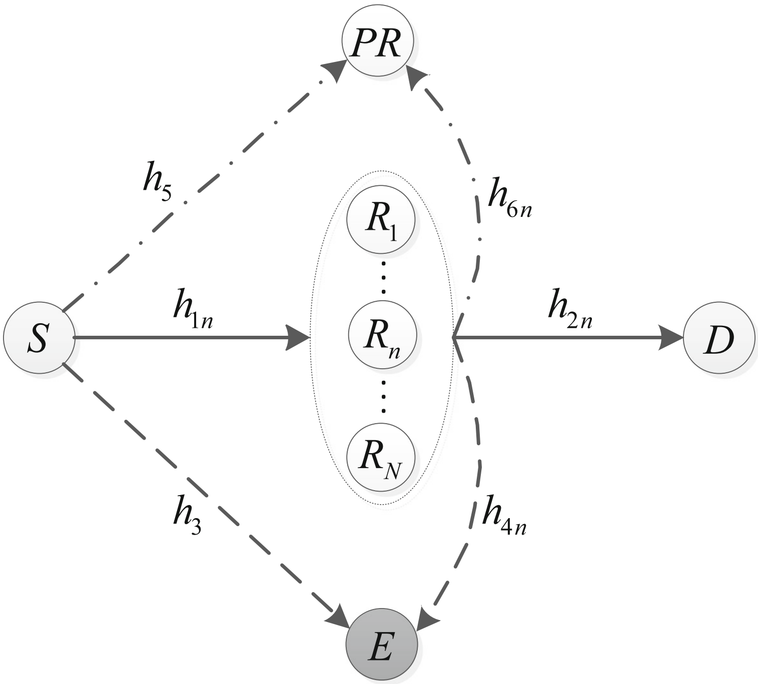

Fig. 1 System model

information from the received signal. Based on this, the received instantaneous signal-to-noise ratios (SNRs) at R_b and E are given by:

$$\gamma_{SR_b} = \frac{P_S}{N_0}|h_{1b}|^2 = \gamma\frac{g_{1b}}{g_5}\ , \qquad \gamma_{SE} = \frac{P_S}{N_0}|h_3|^2 = \gamma\frac{g_3}{g_5} \tag{2}$$

where, N_0 is the noise variance at all receivers, and we denote $\gamma \triangleq \frac{I}{N_0}$.

The secrecy capacity for the first hop is defined as follows:

$$\psi_{1b} = \left[\psi_{SR_b} - \psi_{SE}\right]^+ = \left[\frac{1}{2}\log_2\left(\frac{1+\gamma_{SR_b}}{1+\gamma_{SE}}\right)\right]^+ \tag{3}$$

where $\psi_{SR_b} = \frac{1}{2}\log_2\left(1+\gamma_{SR_b}\right)$ and $\psi_{SE} = \frac{1}{2}\log_2(1+\gamma_{SE})$ denote the capacity of the links $S-R_b$ and $S-E$, respectively.

In the second phase, after successful decoding, R_b re-encodes and forwards the signal to D with the transmit power P_{Rb} under the eavesdropping of E. The received instantaneous SNRs at D and E in this phase are expressed as:

$$\gamma_{R_bD} = \frac{P_{R_b}}{N_0}|h_{2b}|^2 = \gamma\frac{g_{2b}}{g_{6b}}\ , \qquad \gamma_{R_bE} = \frac{P_{R_b}}{N_0}|h_{4b}|^2 = \gamma\frac{g_{4b}}{g_{6b}} \tag{4}$$

The capacity of the link R_b-D is given as $\psi_{R_bD} = \frac{1}{2}\log_2\left(1+\gamma_{R_bD}\right)$. Since eavesdropper E receives two independent copies of the source signal, the worst case is considered, i.e., E adopts the MRC scheme: $\gamma_E = \gamma_{SE} + \gamma_{R_bE}$. Additionally, the capacity at $\psi_E =$

$\frac{1}{2}\log_2(1+\gamma_E)$ is expressed as . Therefore, the secrecy capacity for this second hop can be obtained as:

$$\psi_{2b} = \left[\psi_{R_bD} - \psi_E\right]^+ = \left[\frac{1}{2}\log_2\left(\frac{1+\gamma_{R_bD}}{1+\gamma_{SE}+\gamma_{R_bE}}\right)\right]^+ \tag{5}$$

3 Secrecy Outage Probability Analyses

In this section, we analyze the secrecy outage probability of four relay selection schemes. The best relay is selected to have the maximum channel gain to S (MaSR) and to D (MaRD), the minimum channel gain to E (MiRE), or the optimal relay selection criteria (ORS). The exact SOP expressions are derived without using the assumption of a high SNR (as was done in previous works). The SOP is defined as the probability that the secrecy capacity $\psi_s = \min(\psi_{1b}, \psi_{2b})$ will be less than the desired threshold secrecy rate ψ_{th}. By denoting $X_3 \triangleq g_3$ and $X_5 \triangleq g_5$, the SOP can be given by:

$$P_{out} = \int_0^\infty f_{X_5}(x_5)\int_0^\infty F_{\psi_s}(\psi_t) f_{X_3}(x_3)dx_3dx_5 \tag{6}$$

The term $F_{\psi_s}(\psi_t)$ is computed by:

$$\begin{aligned}
F_{\psi_s}(\psi_t) =& \Pr\left\{\min\left[\frac{1}{2}\log_2\left(\frac{1+\gamma\frac{g_{1b}}{X_5}}{1+\gamma\frac{X_3}{X_5}}\right), \frac{1}{2}\log_2\left(\frac{1+\gamma\frac{g_{2b}}{g_{6b}}}{1+\gamma\frac{X_3}{X_5}+\gamma\frac{g_{4b}}{g_{6b}}}\right)\right] < \psi_{th}\right\} \\
=& 1-\Pr\left[\frac{1}{2}\log_2\left(\frac{1+\gamma\frac{g_{1b}}{X_5}}{1+\gamma\frac{X_3}{X_5}}\right) \geq \psi_{th}, \frac{1}{2}\log_2\left(\frac{1+\gamma\frac{g_{2b}}{g_{6b}}}{1+\gamma\frac{X_3}{X_5}+\gamma\frac{g_{4b}}{g_{6b}}}\right) \geq \psi_{th}\right] \\
=& 1-\Pr\left[g_{1b} \geq \frac{\theta-1}{\gamma}X_5+\theta X_3, g_{2b} \geq \left(\frac{\theta-1}{\gamma}+\theta\frac{X_3}{X_5}\right)g_{6b}+\theta g_{4b}\right] \\
=& 1-\int_{\frac{\theta-1}{\gamma}X_5+\theta X_3}^\infty f_{g_{1b}}(x_1)\int_0^\infty f_{g_{6b}}(x_6)\int_0^\infty f_{g_{4b}}(x_4)\int_{\left(\frac{\theta-1}{\gamma}+\theta\frac{X_3}{X_5}\right)x_6+\theta x_4}^\infty f_{g_{2b}}(x_2)dx_2dx_4dx_6dx_1
\end{aligned} \tag{7}$$

where $\theta \triangleq 2^{2\psi_{th}}$. The next five subsections present the SOP derivations for the case of single-relay and four-relay selection schemes.

3.1 Single Relay

We first consider the system model with one relay, i.e., $N=1$. Thus, there is no relay selection scheme. The PDFs of RVs g_{1b}, g_{2b}, g_{4b}, and g_{6b} are expressed by $f_{g_{1b}}(x_1) = \lambda_1 e^{-\lambda_1 x_1}$, $f_{g_{2b}}(x_2) = \lambda_2 e^{-\lambda_2 x_2}$, $f_{g_{4b}}(x_4) = \lambda_4 e^{-\lambda_4 x_4}$, and $f_{g_{6b}}(x_6) = \lambda_6 e^{-\lambda_6 x_6}$, respectively. Substituting these PDFs into (7), we obtain:

$$\begin{aligned} F_{\psi_s}(\psi_t) =& 1 - \int_{\frac{\theta-1}{\gamma}X_5+\theta X_3}^{\infty} f_{g_{1b}}(x_1) \int_0^{\infty} f_{g_{6b}}(x_6) e^{-\lambda_2\left(\frac{\theta-1}{\gamma}+\theta\frac{X_3}{X_5}\right)x_6} \\ & \int_0^{\infty} f_{g_{4b}}(x_4) e^{-\lambda_2\theta x_4} dx_4 dx_6 dx_1 \\ =& 1 - \frac{\lambda_4}{\lambda_4+\lambda_2\theta} \frac{\lambda_6}{\lambda_6+\lambda_2\frac{\theta-1}{\gamma}+\lambda_2\theta\frac{X_3}{X_5}} \int_{\frac{\theta-1}{\gamma}X_5+\theta X_3}^{\infty} f_{g_{1b}}(x_1)dx_1 \\ =& 1 - \frac{\lambda_4\lambda_6}{\lambda_4+\lambda_2\theta}\left(\lambda_6+\lambda_2\frac{\theta-1}{\gamma}+\lambda_2\theta\frac{X_3}{X_5}\right)^{-1} e^{-\lambda_1\frac{\theta-1}{\gamma}X_5} e^{-\lambda_1\theta X_3} \end{aligned} \tag{8}$$

Then, the SOP for this case is expressed by:

$$\begin{aligned} P_{out}^{1\,\mathrm{relay}} =& \int_0^{\infty} f_{X_5}(x_5) \int_0^{\infty} \left[1 - \frac{\lambda_4\lambda_6}{\lambda_4+\lambda_2\theta}\left(\lambda_6+\lambda_2\frac{\theta-1}{\gamma}+\lambda_2\theta\frac{x_3}{x_5}\right)^{-1} e^{-\lambda_1\frac{\theta-1}{\gamma}x_5} e^{-\lambda_1\theta x_3}\right] f_{X_3}(x_3)dx_3dx_5 \\ =& 1 - \frac{\lambda_4\lambda_6\lambda_3\lambda_5}{\lambda_4+\lambda_2\theta}\int_0^{\infty} e^{-\left(\lambda_5+\lambda_1\frac{\theta-1}{\gamma}\right)x_5} \underbrace{\int_0^{\infty}\left(\lambda_6+\lambda_2\frac{\theta-1}{\gamma}+\lambda_2\theta\frac{x_3}{x_5}\right)^{-1} e^{-(\lambda_3+\lambda_1\theta)x_3}dx_3}_{I_1} dx_5 \end{aligned} \tag{9}$$

Lemma 1 *The following expression is valid for the integral* I_1.

$$I_1 = \int_0^{\infty}\left(\lambda_6+\lambda_2\frac{\theta-1}{\gamma}+\lambda_2\theta\frac{x_3}{x_5}\right)^{-1} e^{-(\lambda_3+\lambda_1\theta)x_3}dx_3 = \frac{x_5}{\lambda_2\theta}e^{\omega_1 x_5}\Gamma(0,\omega_1 x_5) \tag{10}$$

where

$$\omega_1 \triangleq \left(\lambda_6+\lambda_2\frac{\theta-1}{\gamma}\right)\left(\frac{\lambda_3+\lambda_1\theta}{\lambda_2\theta}\right)$$

Proof Given in "Appendix 1". □

Using Eq. (6.455.1) of [22]: $\int_0^{\infty} x^{\mu-1}e^{-\beta x}\Gamma(v,\alpha x)dx = \frac{\alpha^v\Gamma(\mu+v)}{\mu(\alpha+\beta)^{\mu+v}}\,{}_2F_1\left(1,\mu+v;\mu+1;\frac{\beta}{\alpha+\beta}\right)$ with $\mu=2$, $\beta=\lambda_5+\lambda_1\frac{\theta-1}{\gamma}-\omega_1$, $v=0$, and $\alpha=\omega_1$, we obtain:

$$\begin{aligned} &\int_0^{\infty} x_5 e^{-\left[\lambda_5+\lambda_1\frac{\theta-1}{\gamma}-\omega_1\right]x_5}\Gamma(0,\omega_1x_5)dx_5 \\ &= \frac{1}{2\left(\lambda_5+\lambda_1\frac{\theta-1}{\gamma}\right)^2}\,{}_2F_1\left(1,2;3;\frac{\lambda_5+\lambda_1\frac{\theta-1}{\gamma}-\omega_1}{\lambda_5+\lambda_1\frac{\theta-1}{\gamma}}\right) \end{aligned} \tag{11}$$

Combining (10) and (11), we have:

$$\begin{aligned} &\int_0^{\infty} e^{-\left(\lambda_5+\lambda_1\frac{\theta-1}{\gamma}\right)x_5}\int_0^{\infty}\left(\lambda_6+\lambda_2\frac{\theta-1}{\gamma}+\lambda_2\theta\frac{x_3}{x_5}\right)^{-1} e^{-(\lambda_3+\lambda_1\theta)x_3}dx_3dx_5 \\ &= \frac{1}{\lambda_2\theta}\frac{1}{2\left(\lambda_5+\lambda_1\frac{\theta-1}{\gamma}\right)^2}\,{}_2F_1\left(1,2;3;1-\frac{\left(\lambda_6+\lambda_2\frac{\theta-1}{\gamma}\right)\left(\frac{\lambda_3+\lambda_1\theta}{\lambda_2\theta}\right)}{\lambda_5+\lambda_1\frac{\theta-1}{\gamma}}\right) \end{aligned} \tag{12}$$

Substituting (12) into (9), the exact expression for the SOP with a single relay is given by:

$$P_{out}^{1\,\text{relay}} = 1 - \frac{\lambda_4\lambda_6\lambda_3\lambda_5}{2\lambda_2\theta(\lambda_4+\lambda_2\theta)\left(\lambda_5+\lambda_1\frac{\theta-1}{\gamma}\right)^2}\,{}_2F_1\left(1,2;3;1-\frac{\left(\lambda_6+\lambda_2\frac{\theta-1}{\gamma}\right)\left(\frac{\lambda_3+\lambda_1\theta}{\lambda_2\theta}\right)}{\lambda_5+\lambda_1\frac{\theta-1}{\gamma}}\right) \tag{13}$$

3.2 The MaSR Scheme

This subsection considered the MaSR relay selection scheme is applied. This is formulated by:

$$R_b = \arg\max_{n=1,2,\ldots,N} g_{1n} \tag{14}$$

The CDF of RV g_{1b} is different compared to what was shown in Sect. 3.1; the new value is given by:

$$\begin{aligned} F_{g_{1b}}(x_1) &= \Pr[g_{1b}<x_1] = \Pr\left[\max_{n=1,2,\ldots,N} g_{1n}<x_1\right] \\ &= \prod_{n=1}^{N}\Pr[g_{1n}<x_1] = \left(1-e^{-\lambda_1x_1}\right)^N \end{aligned} \tag{15}$$

Taking the derivative of $F_{g_{1b}}$ with respect to x_1, we obtain the PDF of RV g_{1b}:

$$f_{g_{1b}}(x_1) = N\lambda_1e^{-\lambda_1x_1}\left(1-e^{-\lambda_1x_1}\right)^{N-1} = N\lambda_1\sum_{n=0}^{N-1}C_{N-1}^n(-1)^ne^{-\lambda_1(n+1)x_1} \tag{16}$$

Substituting the PDFs $f_{g_{1b}}(x_1)$, $f_{g_{2b}}(x_2)$, $f_{g_{4b}}(x_4)$, and $f_{g_{6b}}(x_6)$ into (7), we obtain the term $F_{\psi_s}(\psi_t)$ for this protocol after some mathematical manipulations as

$$\begin{aligned} F_{\psi_s}(\psi_t) =& 1-\frac{\lambda_4}{\lambda_4+\lambda_2\theta}\frac{\lambda_6}{\lambda_6+\lambda_2\frac{\theta-1}{\gamma}+\lambda_2\theta\frac{X_3}{X_5}}\int_{\frac{\theta-1}{\gamma}X_5+\theta X_3}^{\infty}N\lambda_1\sum_{n=0}^{N-1}C_{N-1}^n(-1)^ne^{-\lambda_1(n+1)x_1}dx_1 \\ =& 1-\frac{N\lambda_4\lambda_6}{\lambda_4+\lambda_2\theta}\left(\lambda_6+\lambda_2\frac{\theta-1}{\gamma}+\lambda_2\theta\frac{X_3}{X_5}\right)^{-1}\sum_{n=0}^{N-1}\frac{C_{N-1}^n(-1)^n}{n+1}e^{-\lambda_1(n+1)\frac{\theta-1}{\gamma}X_5}e^{-\lambda_1(n+1)\theta X_3} \end{aligned} \tag{17}$$

Substituting (17) into (6), we can obtain the SOP for this protocol:

$$\begin{aligned} P_{out}^{\text{MaSR}} \overset{(18.1)}{=}& \int_0^\infty f_{X_5}(x_5)\int_0^\infty\left[\begin{array}{c}1-\frac{N\lambda_4\lambda_6}{\lambda_4+\lambda_2\theta}\left(\lambda_6+\lambda_2\frac{\theta-1}{\gamma}+\lambda_2\theta\frac{x_3}{x_5}\right)^{-1} \\ \sum_{n=0}^{N-1}\frac{C_{N-1}^n(-1)^n}{n+1}e^{-\lambda_1(n+1)\frac{\theta-1}{\gamma}x_5}e^{-\lambda_1(n+1)\theta x_3}\end{array}\right]f_{X_3}(x_3)dx_3dx_5 \\ \overset{(18.2)}{=}& 1-\frac{N\lambda_4\lambda_6\lambda_3\lambda_5}{\lambda_4+\lambda_2\theta}\sum_{n=0}^{N-1}\frac{C_{N-1}^n(-1)^n}{n+1} \\ & \int_0^\infty e^{-\left(\lambda_5+\lambda_1(n+1)\frac{\theta-1}{\gamma}\right)x_5}\int_0^\infty\left(\lambda_6+\lambda_2\frac{\theta-1}{\gamma}+\lambda_2\theta\frac{x_3}{x_5}\right)^{-1}e^{-[\lambda_3+\lambda_1(n+1)\theta]x_3}dx_3dx_5 \\ \overset{(18.3)}{=}& 1-\frac{N\lambda_4\lambda_6\lambda_3\lambda_5}{2\lambda_2\theta(\lambda_4+\lambda_2\theta)} \\ & \sum_{n=0}^{N-1}\frac{C_{N-1}^n(-1)^n}{n+1}\frac{1}{\left(\lambda_5+\lambda_1(n+1)\frac{\theta-1}{\gamma}\right)^2}\,{}_2F_1\left(1,2;3;1-\frac{\left(\lambda_6+\lambda_2\frac{\theta-1}{\gamma}\right)\left(\frac{\lambda_1(n+1)\theta+\lambda_3}{\lambda_2\theta}\right)}{\lambda_5+\lambda_1(n+1)\frac{\theta-1}{\gamma}}\right) \end{aligned} \tag{18}$$

where (18.3) is obtained from (18.2) by using the result of Eq. (12):

$$\int_0^\infty e^{-\left(\lambda_5+\lambda_1(n+1)\frac{\theta-1}{\gamma}\right)x_5}\int_0^\infty\left(\lambda_6+\lambda_2\frac{\theta-1}{\gamma}+\lambda_2\theta\frac{x_3}{x_5}\right)^{-1}e^{-[\lambda_3+\lambda_1(n+1)\theta]x_3}dx_3dx_5$$
$$=\frac{1}{\lambda_2\theta}\frac{1}{2\left(\lambda_5+\lambda_1(n+1)\frac{\theta-1}{\gamma}\right)^2}\,{}_2F_1\left(1,2;3;1-\frac{\left(\lambda_6+\lambda_2\frac{\theta-1}{\gamma}\right)\left(\frac{\lambda_1(n+1)\theta+\lambda_3}{\lambda_2\theta}\right)}{\lambda_5+\lambda_1(n+1)\frac{\theta-1}{\gamma}}\right)$$

3.3 The MaRD Scheme

The best relay R_b is selected based on the MaRD relay selection scheme as follows:

$$R_b=\arg\max_{n=1,2,\ldots,N} g_{2n} \tag{19}$$

Then, the PDF of RV g_{2b} is changed and given by:

$$f_{g_{2b}}(x_2)=N\lambda_2e^{-\lambda_2x_2}\left(1-e^{-\lambda_2x_2}\right)^{N-1}=N\lambda_2\sum_{n=0}^{N-1}C_{N-1}^n(-1)^ne^{-\lambda_2(n+1)x_2} \tag{20}$$

Similarly, we also $F_{\psi_s}(\psi_t)$ from (7) for this protocol as

$$\begin{aligned}F_{\psi_s}(\psi_t)=&1-\int_{\frac{\theta-1}{\gamma}X_5+\theta X_3}^\infty f_{g_{1b}}(x_1)\int_0^\infty f_{g_{6b}}(x_6)\int_0^\infty f_{g_{4b}}(x_4)\\&\int_{\left(\frac{\theta-1}{\gamma}+\theta\frac{X_3}{X_5}\right)x_6+\theta x_4}^\infty f_{g_{2b}}(x_2)dx_2dx_4dx_6dx_1\\=&1-\int_{\frac{\theta-1}{\gamma}X_5+\theta X_3}^\infty f_{g_{1b}}(x_1)\\&\int_0^\infty N\sum_{n=0}^{N-1}\frac{C_{N-1}^n(-1)^n}{n+1}\frac{\lambda_4}{\lambda_4+\lambda_2(n+1)\theta}e^{-\lambda_2(n+1)\left(\frac{\theta-1}{\gamma}+\theta\frac{X_3}{X_5}\right)x_6}f_{g_{6b}}(x_6)dx_6dx_1\\=&1-N\lambda_4\lambda_6\sum_{n=0}^{N-1}\frac{C_{N-1}^n(-1)^n}{n+1}\frac{1}{[\lambda_4+\lambda_2(n+1)\theta]}\\&\left(\lambda_6+\lambda_2(n+1)\frac{\theta-1}{\gamma}+\lambda_2(n+1)\theta\frac{X_3}{X_5}\right)^{-1}e^{-\lambda_1\frac{\theta-1}{\gamma}X_5}e^{-\lambda_1\theta X_3}\end{aligned} \tag{21}$$

The SOP for this protocol can be obtained by substituting (21) into (6) as

$$
\begin{aligned}
P_{out}^{\text{MARD}} &\overset{(22.1)}{=} \int_0^\infty f_{X_5}(x_5) \\
&\int_0^\infty \left[\begin{array}{c} 1 - N\lambda_4\lambda_6 \sum_{n=0}^{N-1} \frac{C_{N-1}^n(-1)^n}{n+1} \frac{1}{[\lambda_4 + \lambda_2(n+1)\theta]} \\ \left(\lambda_6 + \lambda_2(n+1)\frac{\theta-1}{\gamma} + \lambda_2(n+1)\theta\frac{X_3}{X_5}\right)^{-1} e^{-\lambda_1\frac{\theta-1}{\gamma}x_5} e^{-\lambda_1\theta x_3} \end{array} \right] f_{X_3}(x_3)dx_3dx_5 \\
&\overset{(22.2)}{=} 1 - N\lambda_4\lambda_6\lambda_3\lambda_5 \sum_{n=0}^{N-1} \frac{C_{N-1}^n(-1)^n}{n+1} \frac{1}{\lambda_4 + \lambda_2(n+1)\theta} \\
&\int_0^\infty e^{-\left(\lambda_5+\lambda_1\frac{\theta-1}{\gamma}\right)x_5} \int_0^\infty \left(\lambda_6 + \lambda_2(n+1)\frac{\theta-1}{\gamma} + \lambda_2(n+1)\theta\frac{x_3}{x_5}\right)^{-1} e^{-(\lambda_3+\lambda_1\theta)x_3} dx_3dx_5 \\
&\overset{(22.3)}{=} 1 - \frac{N\lambda_4\lambda_6\lambda_3\lambda_5}{2\left(\lambda_5 + \lambda_1\frac{\theta-1}{\gamma}\right)^2} \sum_{n=0}^{N-1} \frac{C_{N-1}^n(-1)^n}{n+1} \\
&\frac{1}{[\lambda_4 + \lambda_2(n+1)\theta][\lambda_2(n+1)\theta]} \, {}_2F_1\left(1,2;3;1 - \frac{\left(\lambda_6 + \lambda_2(n+1)\frac{\theta-1}{\gamma}\right)\left(\frac{\lambda_3+\lambda_1\theta}{\lambda_2(n+1)\theta}\right)}{\lambda_5 + \lambda_1\frac{\theta-1}{\gamma}}\right)
\end{aligned} \tag{22}
$$

where (22.3) is obtained from (22.2) by using the result of Eq. (12):

$$
\begin{aligned}
&\int_0^\infty e^{-\left(\lambda_5+\lambda_1\frac{\theta-1}{\gamma}\right)x_5} \int_0^\infty \left(\lambda_6 + \lambda_2(n+1)\frac{\theta-1}{\gamma} + \lambda_2(n+1)\theta\frac{x_3}{x_5}\right)^{-1} e^{-(\lambda_3+\lambda_1\theta)x_3} dx_3dx_5 \\
&= \frac{1}{\lambda_2(n+1)\theta} \frac{1}{2\left(\lambda_5 + \lambda_1\frac{\theta-1}{\gamma}\right)^2} \, {}_2F_1\left(1,2;3;1 - \frac{\left(\lambda_6 + \lambda_2(n+1)\frac{\theta-1}{\gamma}\right)\left(\frac{\lambda_3+\lambda_1\theta}{\lambda_2(n+1)\theta}\right)}{\lambda_5 + \lambda_1\frac{\theta-1}{\gamma}}\right)
\end{aligned}
$$

3.4 The MiRE Scheme

The MiRE relay selection scheme is expressed by (23), and the CDF of RV g_{4b} is changed compared to the case of Sect. 3.1 and given by (24) as follows

$$R_b = \arg \min_{n=1,2,\ldots,N} g_{4n} \tag{23}$$

$$
\begin{aligned}
F_{g_{4b}}(x_4) &= \Pr\left[\min_{n=1,2,\ldots,N} g_{4n} < x_4\right] \\
&= 1 - \prod_{n=1}^{N} \Pr[g_{4n} \geq x_4] = 1 - e^{-\lambda_4 N x_4}
\end{aligned} \tag{24}
$$

The PDF of RV g_{4b} is obtained by taking the derivative of $F_{g_{4b}}(x_4)$:

$$f_{g_{4b}}(x_4) = \frac{d\{F_{g_{4b}}(x_4)\}}{dx_4} = N\lambda_4 e^{-\lambda_4 N x_4} \tag{25}$$

We also obtain $F_{\psi_s}(\psi_t)$ from (7) as

$$F_{\psi_s}(\psi_t) =1 - \int_{\frac{\theta-1}{\gamma}X_5+\theta X_3}^{\infty} f_{g_{1b}}(x_1) \int_0^{\infty} f_{g_{6b}}(x_6) e^{-\lambda_2\left(\frac{\theta-1}{\gamma}+\theta\frac{X_3}{X_5}\right)x_6} \int_0^{\infty} \lambda_4 N e^{-(N\lambda_4+\lambda_2\theta)x_4} dx_4 dx_6 dx_1 \\ =1 - \frac{N\lambda_4\lambda_6}{N\lambda_4+\lambda_2\theta}\left(\lambda_6+\lambda_2\frac{\theta-1}{\gamma}+\lambda_2\theta\frac{X_3}{X_5}\right)^{-1} e^{-\lambda_1\frac{\theta-1}{\gamma}X_5} e^{-\lambda_1\theta X_3} \tag{26}$$

Then, substituting (25) into (6), we can obtain the SOP for this protocol:

$$P_{out}^{\text{MIRE}} \overset{(26.1)}{=} \int_0^{\infty} f_{X_5}(x_5) \int_0^{\infty}\left[1-\frac{N\lambda_4\lambda_6}{N\lambda_4+\lambda_2\theta}\left(\lambda_6+\lambda_2\frac{\theta-1}{\gamma}+\lambda_2\theta\frac{X_3}{X_5}\right)^{-1} e^{-\lambda_1\frac{\theta-1}{\gamma}x_5} e^{-\lambda_1\theta x_3}\right] f_{X_3}(x_3)dx_3 dx \\ \overset{(26.2)}{=} 1-\frac{N\lambda_4\lambda_6\lambda_3\lambda_5}{\lambda_4 N+\lambda_2\theta}\int_0^{\infty} f_{X_5}(x_5) e^{-\left(\lambda_5+\lambda_1\frac{\theta-1}{\gamma}\right)x_5} \int_0^{\infty}\left(\lambda_6+\lambda_2\frac{\theta-1}{\gamma}+\lambda_2\theta\frac{X_3}{X_5}\right)^{-1} e^{-(\lambda_3+\lambda_1\theta)x_3} dx_3 dx_5 \\ \overset{(26.3)}{=} 1-\frac{N\lambda_4\lambda_6\lambda_3}{2\lambda_2\theta(\lambda_4 N+\lambda_2\theta)\left(\lambda_5+\lambda_1\frac{\theta-1}{\gamma}\right)^2}\, {}_2F_1\left(1,2;3;1-\frac{\left(\lambda_6+\lambda_2\frac{\theta-1}{\gamma}\right)\left(\frac{\lambda_3+\lambda_1\theta}{\lambda_2\theta}\right)}{\lambda_5+\lambda_1\frac{\theta-1}{\gamma}}\right) \tag{27}$$

where (26.3) is obtained by using the result in (12):

$$\int_0^{\infty} f_{X_5}(x_5) e^{-\lambda_1\frac{\theta-1}{\gamma}x_5} \int_0^{\infty}\left(\lambda_6+\lambda_2\frac{\theta-1}{\gamma}+\lambda_2\theta\frac{X_3}{X_5}\right)^{-1} e^{-(\lambda_3+\lambda_1\theta)x_3} dx_3 dx_5 \\ =\frac{1}{\lambda_2\theta}\frac{1}{2\left(\lambda_5+\lambda_1\frac{\theta-1}{\gamma}\right)^2}\, {}_2F_1\left(1,2;3;1-\frac{\left(\lambda_6+\lambda_2\frac{\theta-1}{\gamma}\right)\left(\frac{\lambda_3+\lambda_1\theta}{\lambda_2\theta}\right)}{\lambda_5+\lambda_1\frac{\theta-1}{\gamma}}\right).$$

3.5 The Optimal Relay Selection Scheme

The best relay is selected optimally by using the following strategy:

$$R_b = arg \max_{n=1,2,\ldots,N} \min(\psi_{1n}, \psi_{2n}) \tag{28}$$

Then, th

$$\begin{aligned}
P_{out}^{\text{ORS}} &= \Pr[\min(\psi_{1b}\psi_{2b}) < \psi_t] \\
&= \Pr\left[\underset{n=1,2,\ldots,N}{max}\{\min(\psi_{1n},\psi_{2n})\} < \psi_t\right] \\
&= \Pr\left\{\max_{n=1,2,\ldots,N}\min\left[\underbrace{\frac{1}{2}\log_2\left(\frac{1+\gamma\frac{g_{1n}}{g_5}}{1+\gamma\frac{g_3}{g_5}}\right)}_{\psi_{1n}},\underbrace{\frac{1}{2}\log_2\left(\frac{1+\gamma\frac{g_{2n}}{g_{6n}}}{1+\gamma\frac{g_3}{g_5}+\gamma\frac{g_{4n}}{g_{6n}}}\right)}_{\psi_{2n}}\right] < \psi_t\right\} \\
&= \Pr\left\{\max_{n=1,2,\ldots,N}\min\left[\underbrace{\frac{1}{2}\log_2\left(\frac{1+\gamma\frac{g_{1n}}{X_5}}{1+\gamma\frac{X_3}{X_5}}\right)}_{\psi_{1n}},\underbrace{\frac{1}{2}\log_2\left(\frac{1+\gamma\frac{g_{2n}}{g_{6n}}}{1+\gamma\frac{X_3}{X_5}+\gamma\frac{g_{4n}}{g_{6n}}}\right)}_{\psi_{2n}}\right] < \psi_t\right\} \\
&= \Pr\left\{\max_{n=1,2,\ldots,N}\underbrace{\min\left[\frac{1+\gamma\frac{g_{1n}}{X_5}}{1+\gamma\frac{X_3}{X_5}},\frac{1+\gamma\frac{g_{2n}}{g_{6n}}}{1+\gamma\frac{X_3}{X_5}+\gamma\frac{g_{4n}}{g_{6n}}}\right]}_{\psi_n} < \theta\right\} \\
&= \int_0^\infty f_{X_5}(x_5)\int_0^\infty \prod_{n=1}^{N} F_{\psi_n}(\theta) f_{X_3}(x_3)dx_3dx_5
\end{aligned} \tag{29}$$

e secrecy outage probability for this protocol can be expressed by:Using the result in (8), the CDF of , where the term ψ_n is defined by $\psi_n = \min\left[\frac{1+\gamma\frac{g_{1n}}{X_5}}{1+\gamma\frac{X_3}{X_5}},\frac{1+\gamma\frac{g_{2n}}{g_{6n}}}{1+\gamma\frac{X_3}{X_5}+\gamma\frac{g_{4n}}{g_{6n}}}\right]$, is obtained by

$$F_{\psi_n}(\theta) = 1 - \frac{\lambda_4\lambda_6}{\lambda_4+\lambda_2\theta}\left(\lambda_6+\lambda_2\frac{\theta-1}{\gamma}+\lambda_2\theta\frac{X_3}{X_5}\right)^{-1} e^{-\lambda_1\frac{\theta-1}{\gamma}X_5}e^{-\lambda_1\theta X_3} \tag{30}$$

The term ψ_n with $n \in \{1,2,\ldots,N\}$ are independent of each other, thus we have

$$\begin{aligned}
\prod_{n=1}^{N} F_{\psi_n}(\theta) &= \left[F_{\psi_n}(\theta)\right]^N \\
&= \left[1-\frac{\lambda_4\lambda_6}{\lambda_4+\lambda_2\theta}\left(\lambda_6+\lambda_2\frac{\theta-1}{\gamma}+\lambda_2\theta\frac{X_3}{X_5}\right)^{-1} e^{-\lambda_1\frac{\theta-1}{\gamma}X_5}e^{-\lambda_1\theta X_3}\right]^N \\
&= \sum_{n=0}^{N} C_N^n(-1)^n\left(\frac{\lambda_4\lambda_6}{\lambda_4+\lambda_2\theta}\right)^n\left(\lambda_6+\lambda_2\frac{\theta-1}{\gamma}+\lambda_2\theta\frac{X_3}{X_5}\right)^{-n} e^{-\lambda_1\frac{\theta-1}{\gamma}X_5 n}e^{-\lambda_1\theta X_3 n}
\end{aligned} \tag{31}$$

Then, by substituting (31) into (29), we obtain:

$$\begin{aligned} P_{out}^{\mathrm{ORS}} &= \int_0^\infty f_{X_5}(x_5) \int_0^\infty \prod_{n=1}^{N} F_{\psi_n}(\theta) f_{X_3}(x_3) dx_3 dx_5 \\ &= \lambda_3\lambda_5 \sum_{n=0}^{N} C_N^n (-1)^n \left(\frac{\lambda_4\lambda_6}{\lambda_4+\lambda_2\theta}\right)^n \int_0^\infty e^{-\left(\lambda_5+\lambda_1\frac{\theta-1}{\gamma}n\right)x_5} \\ &\quad \int_0^\infty \left(\lambda_6+\lambda_2\frac{\theta-1}{\gamma}+\lambda_2\theta\frac{x_3}{x_5}\right)^{-n} e^{-(\lambda_3+\lambda_1\theta n)x_3} dx_3 dx_5 \end{aligned} \tag{32}$$

By setting $u = \lambda_2\theta\frac{x_3}{x_5}$, we obtain (33.1). Using equation 3.382.4 of [22], we obtain (33.2) as follows:

$$\begin{aligned} &\int_0^\infty \left(\lambda_6+\lambda_2\frac{\theta-1}{\gamma}+\lambda_2\theta\frac{x_3}{x_5}\right)^{-n} e^{-(\lambda_3+\lambda_1\theta n)x_3} dx_3 \\ &\overset{(33.1)}{=} \frac{x_5}{\lambda_2\theta}\int_0^\infty \left(\lambda_6+\lambda_2\frac{\theta-1}{\gamma}+u\right)^{-n} e^{-\left(\frac{\lambda_3+\lambda_1\theta n}{\lambda_2\theta}\right)x_5 u} du \\ &\overset{(33.2)}{=} \frac{x_5}{\lambda_2\theta}\left[\left(\frac{\lambda_3+\lambda_1\theta n}{\lambda_2\theta}\right)x_5\right]^{n-1} e^{\left(\lambda_6+\lambda_2\frac{\theta-1}{\gamma}\right)\left(\frac{\lambda_3+\lambda_1\theta n}{\lambda_2\theta}\right)x_5} \\ &\quad \Gamma\left[1-n, \left(\lambda_6+\lambda_2\frac{\theta-1}{\gamma}\right)\left(\frac{\lambda_3+\lambda_1\theta n}{\lambda_2\theta}\right)x_5\right] \end{aligned} \tag{33}$$

Using equation 6.455.1 of [22], we obtain:

$$\begin{aligned} &\int_0^\infty e^{-\left[\lambda_5+\lambda_1\frac{\theta-1}{\gamma}n-\left(\lambda_6+\lambda_2\frac{\theta-1}{\gamma}\right)\left(\frac{\lambda_3+\lambda_1\theta n}{\lambda_2\theta}\right)\right]x_5}(x_5)^n\Gamma\left[1-n,\left(\lambda_6+\lambda_2\frac{\theta-1}{\gamma}\right)\left(\frac{\lambda_3+\lambda_1\theta n}{\lambda_2\theta}\right)x_5\right]dx_5 \\ &= \frac{\left(\left(\lambda_6+\lambda_2\frac{\theta-1}{\gamma}\right)^{1-n}\left(\frac{\lambda_3+\lambda_1\theta n}{\lambda_2\theta}\right)^{1-n}\right)}{(n+1)\left(\lambda_5+\lambda_1\frac{\theta-1}{\gamma}n\right)^2}\, {}_2F_1\left(1,2;n+2;1-\frac{\left(\lambda_6+\lambda_2\frac{\theta-1}{\gamma}\right)\left(\frac{\lambda_3+\lambda_1\theta n}{\lambda_2\theta}\right)}{\lambda_5+\lambda_1\frac{\theta-1}{\gamma}n}\right) \end{aligned} \tag{34}$$

Finally, by substituting (33) and (34) into (32), we obtain:

$$\begin{aligned} P_{out}^{\mathrm{ORS}} &= \int_0^\infty f_{X_5}(x_5)\int_0^\infty \prod_{n=1}^{N} F_{\psi_n}(\psi_t) f_{X_3}(x_3) dx_3 dx_5 \\ &= \lambda_3\lambda_5\sum_{n=0}^{N} C_N^n(-1)^n\left(\frac{\lambda_4\lambda_6}{\lambda_4+\lambda_2\theta}\right)^n\left(\frac{\lambda_3+\lambda_1\theta n}{\lambda_2\theta}\right)^{n-1}\frac{1}{\lambda_2\theta} \\ &\quad \int_0^\infty e^{-\left[\lambda_5+\lambda_1\frac{\theta-1}{\gamma}n-\left(\lambda_6+\lambda_2\frac{\theta-1}{\gamma}\right)\left(\frac{\lambda_3+\lambda_1\theta n}{\lambda_2\theta}\right)\right]x_5}(x_5)^n\Gamma\left[1-n,\left(\lambda_6+\lambda_2\frac{\theta-1}{\gamma}\right)\left(\frac{\lambda_3+\lambda_1\theta n}{\lambda_2\theta}\right)x_5\right]dx_5 \\ &= \frac{\lambda_3\lambda_5}{\lambda_2\theta}\sum_{n=0}^{N} C_N^n(-1)^n\left(\frac{\lambda_4\lambda_6}{\lambda_4+\lambda_2\theta}\right)^n\frac{\left(\lambda_6+\lambda_2\frac{\theta-1}{\gamma}\right)^{1-n}}{(n+1)\left(\lambda_5+\lambda_1\frac{\theta-1}{\gamma}n\right)^2} \\ &\quad {}_2F_1\left(1,2;n+2;1-\frac{\left(\lambda_6+\lambda_2\frac{\theta-1}{\gamma}\right)\left(\frac{\lambda_3+\lambda_1\theta n}{\lambda_2\theta}\right)}{\lambda_5+\lambda_1\frac{\theta-1}{\gamma}n}\right) \end{aligned} \tag{35}$$

4 Numerical Results

This section presents the numerical results used to verify the analytical results of the four relay selection schemes that we considered for use in the underlay cognitive cooperative network under physical layer security; these were the results derived in the previous section.

The analyses considered a network in a two-dimensional plane with the following coordinates for the source S, the destination D, the relay cluster, the primary user PR, and the eavesdropper E: $(0,0)$, $(1,0)$, $(x_R,0)$, $(0.5,y_P)$, and $(0.5,y_E)$, respectively. Hence, we have distances $d_{SD}=1$, $d_{SR}=|x_R|$, $d_{SP}=\sqrt{0.5^2+(y_P)^2}$, $d_{RD}=\sqrt{(1-x_R)^2}$, and $d_{RE}=\sqrt{(x_R-0.5)^2+(y_E)^2}$. In all simulation scenarios, we assumed the path loss to be $\beta=3$.

First, in Fig. 2, we compare and discuss the exact and approximate secrecy outage probability expressions for each scheme with Monte Carlo simulations. The simulated and theoretical results matched perfectly, demonstrating the accuracy of our analysis. When $N=1$, no relay selection process is used; thus, the four protocols all achieved the same performance. Their performances were improved when the number of relays was increased, i.e., the performances when $N=3$ were higher than those when $N=1$, and the performances were further improved when $N=5$. When $N=3$ and $N=5$, the four

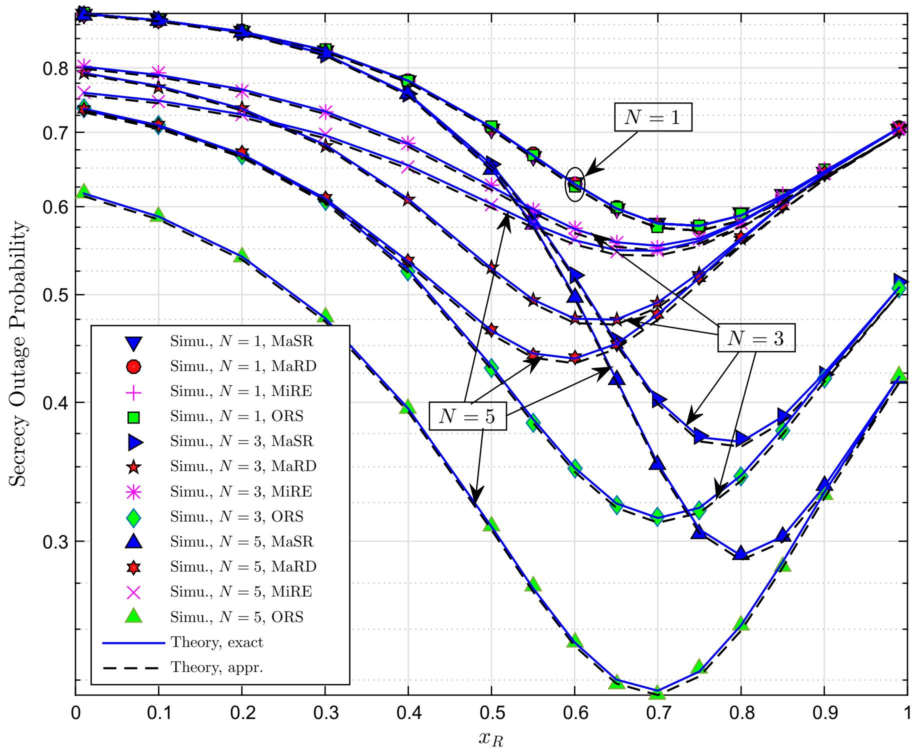

Fig. 2 Secrecy outage probability versus x_R for the four protocols studied. $N=1$, 3, and 5 with $\gamma=20$ dB, $y_P=0.5$, $y_E=-0.8$, and $\psi_t=0.5$ bits/s/Hz

protocols yield their best performance at the optimal value of x_R for each protocol, i.e., the MaSR, MaRD, MiRE, and ORS protocols achieved the highest performance compared to themselves when $x_R \approx 0.8$, $x_R \approx 0.6$, $x_R \approx 0.65$, and $x_R \approx 0.7$, respectively. In addition, the performance of MaRD is higher than that of MiRE for all values of x_R, and their performances are equal when $0.9 < x_R < 1$. The performance of MaSR is the worst, compared to the other three protocols, when $0 < x_R < 0.55$. This is the case because the MaSR relay selection scheme is not effective when the relays are located close to the source. However, its performance is increased and superior to those of the MaRD and MiRE protocols when the relays move closer to the destination, i.e., $x_R > 0.55$. As expected, ORS achieved the highest secrecy outage performance for all values of x_R. Interestingly, MaRS can perform similarly to the ORS protocol when the relays are very close to the destination ($0.9 < x_R < 1$).

Figure 3 illustrates the secrecy outage probability for the four relay selection schemes as a function of $\gamma = \frac{I}{N_0}$ for two secrecy target values, $\psi_t = 0.1$ and $\psi_t = 0.5$. The outage performances of all four schemes were degraded with increasing ψ_t (e.g., from $\psi_t = 0.1$ to $\psi_t = 0.5$) due to the increasing quality requirement of the system. Their performances were all improved when γ increased because more transmitted power is allowed at the source S and the best relay R_b; this helps the decoding process at the receiver nodes. This trend is stable in the approximation form when γ is sufficiently high ($\gamma > 15$ dB) due to the

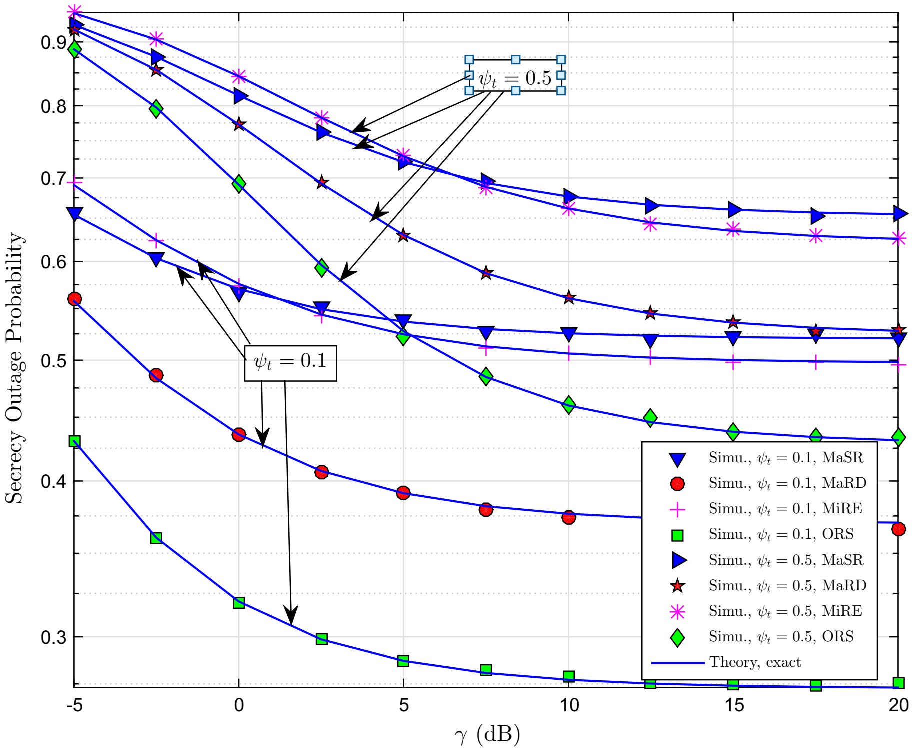

Fig. 3 Secrecy outage probability versus γ (in dB) for the four protocols studied. ψ_t of 0.1 and 0.5 bits/s/Hz, $N = 3$, $x_R = 0.5$, $y_P = 0.5$, and $y_E = -0.8$

effect of the eavesdropper. The MaSR protocol has the worst performance (compared to the other three protocols) except when γ is low, i.e., $\gamma < 7$ dB with $\psi_t = 0.5$ and $\gamma < 1$ dB with $\psi_t = 0.1$, when its performance is superior to that of MiRE.

Figures 4 and 5 show the effects of the primary user and eavesdropper positions, i.e., $y_P \in (0.1, 1)$ and $y_E \in (-1, -0.1)$, respectively. The secrecy outage performances of all four protocols are increased when the primary user and eavesdropper are located far away from the source and the relays; this is due to the decreasing impact of the primary user and eavesdropper on the two-hop transmission. The outage performances are also improved when the number of relays is increased because relay selection schemes are used. As expected, the ORS protocol achieved the highest performance. In this network, the MRC technique is used at the eavesdropper; thus, the impact of the eavesdropper on the second hop is greater than that of the first hop. Consequently, the MaRD relay selection scheme, which increases the secrecy capacity of the second hop, is more suitable than the MaSR and MiRE relay selection schemes. Therefore, as can be seen in Figs. 3 and 5, the performance of the MaRD protocol is better than those of the MaSR and MiRE protocols.

In this network, the MRC technique is used at the eavesdropper; thus, the impact of the eavesdropper on the second hop $(R - D)$ is greater than that of the first hop $(S - R)$. Consequently, the MaRD relay selection scheme, which increases the secrecy capacity of the second hop, is more suitable than the MaSR and MiRE relay selection schemes.

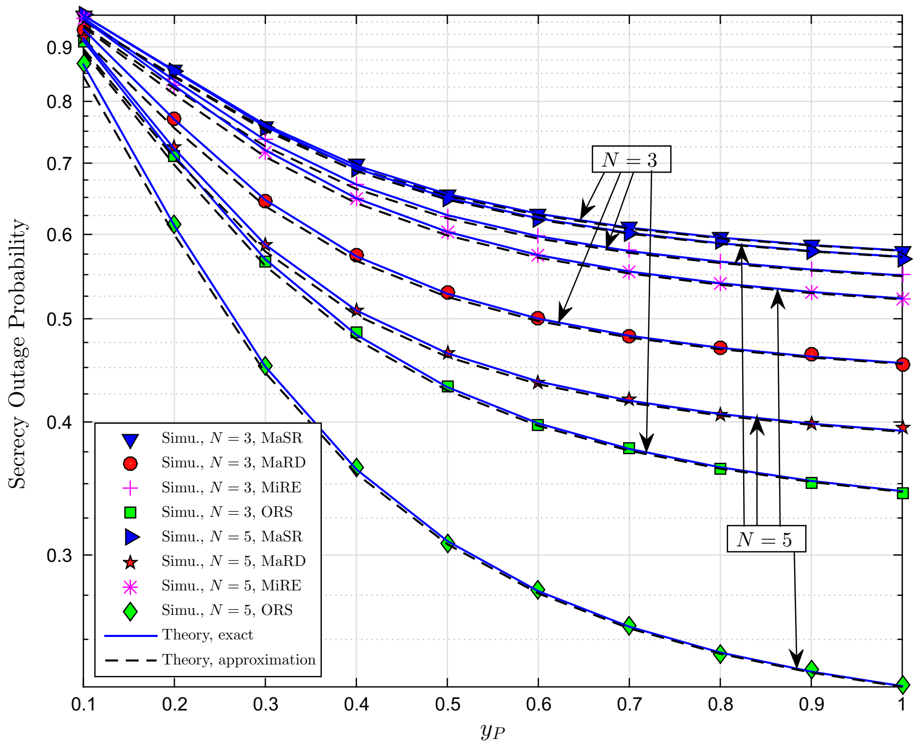

Fig. 4 Secrecy outage probability versus y_P (in dB) for the four protocols studied. N = 3 and 5, $\gamma = 20$, $x_R = 0.5$, $y_E = -0.8$, and $\psi_t = 0.5$ bits/s/Hz

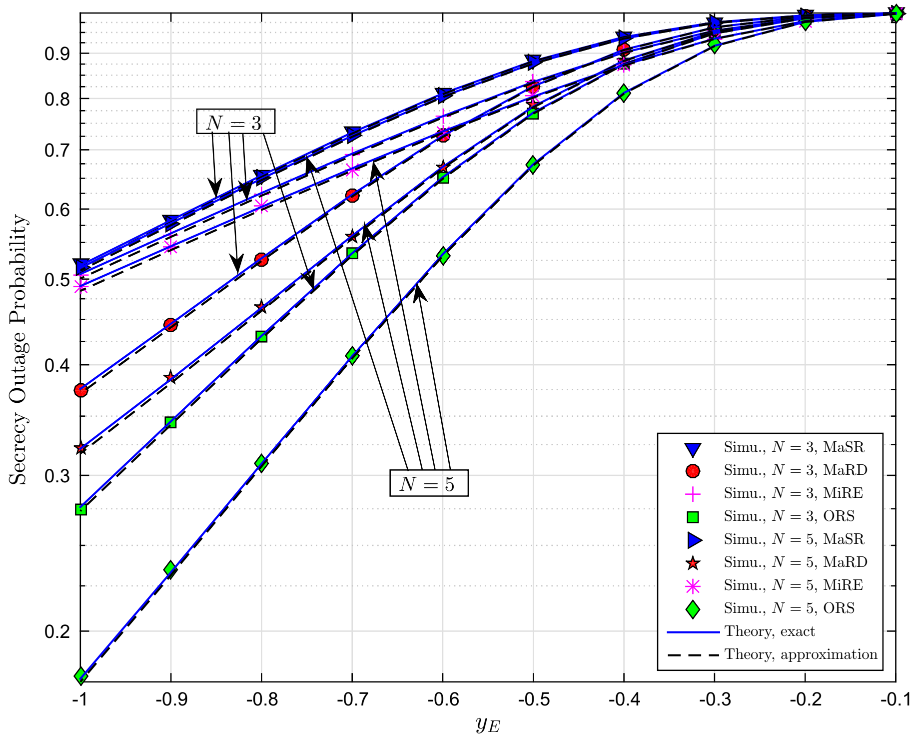

Fig. 5 Secrecy outage probability versus y_E (in dB) for the four protocols studied. $N = 3$ and 5, $\gamma = 20$, $x_R = 0.5$, $y_P = 0.5$, and $\psi_t = 0.5$ bits/s/Hz

Therefore, as can be seen in Figs. 3 and 5, the performance of the MaRD protocol is better than those of the MaSR and MiRE protocols.

5 Conclusions

We have proposed and analyzed an underlay cognitive cooperative energy network under physical layer security. For comparison purposes, we presented four relay selection schemes for this model: MaSR, MaRD, MiRE, and ORS. Monte Carlo simulations were used to verify the theoretical expressions. The exact secrecy outage probability expressions agreed very well with the simulated curves for all scenarios. By analyzing the simulation and theoretical results, it was discovered that 1) when the number of relay nodes is increased, the power threshold is increased, or the target rate is decreased, the outage performances of all protocols are improved; 2) the outage performance of the system is enhanced when the relays are located close to the destination or the primary user and eavesdropper are located far from the source; 3) when the best relay is at the optimal location, the secrecy outage probability of all four schemes are at their lowest; 4) the MaSR scheme yields the worst performance in some cases; and 5) the ORS scheme achieves the best performance in all scenarios.

Appendix 1: Proof of Lemma 1

By setting $u = \lambda_2 \theta \frac{x_3}{x_5}$, the integral I_1 can be rewritten by:

$$I_1 = \frac{x_5}{\lambda_2 \theta} \int_0^{\infty} \left(\lambda_6 + \lambda_2 \frac{\theta - 1}{\gamma} + u \right)^{-1} e^{-(\lambda_3 + \lambda_1 \theta) \frac{x_5}{\lambda_2 \theta} u} du \tag{36}$$

Using equation 3.382.4 in [22] ($\int_0^{\infty} (x + \beta)^{\nu} e^{-\mu x} dx = \mu^{-\nu-1} e^{\beta\mu} \Gamma(\nu + 1, \beta\mu)$), we obtain:

$$\begin{aligned} I_1 &= \frac{x_5}{\lambda_2 \theta} \int_0^{\infty} \left(\lambda_6 + \lambda_2 \frac{\theta - 1}{\gamma} + u \right)^{-1} e^{-(\lambda_3 + \lambda_1 \theta) \frac{x_5}{\lambda_2 \theta} u} du \\ &= \frac{x_5}{\lambda_2 \theta} e^{\left(\lambda_6 + \lambda_2 \frac{\theta-1}{\gamma}\right)\left(\frac{\lambda_3 + \lambda_1 \theta}{\lambda_2 \theta}\right) x_5} \Gamma\left[0, \left(\lambda_6 + \lambda_2 \frac{\theta - 1}{\gamma}\right)\left(\frac{\lambda_3 + \lambda_1 \theta}{\lambda_2 \theta}\right) x_5\right] \end{aligned} \tag{37}$$

This finishes the proof.

References

1. Shannon, C. E. (1949). Communication theory of secrecy systems. *Bell System Technical Journal*, *28*(4), 646–715.
2. Silva, E. D., Santos, A. L. D., Albini, L. C. P., & Lima, M. N. (2008). Identity-based key management in mobile ad hoc networks: Schemes and applications. *IEEE Wireless Communications*, *15*(5), 46–52.
3. Wyner, A. D. (1975). The wire-tap channel. *The Bell System Technical Journal*, *54*(8), 1355–1387.
4. Leung-Yan-Cheong, S., & Hellman, M. (1978). The Gaussian wire-tap channel. *IEEE Transaction on Information Theory*, *24*(4), 451–456.
5. Csiszar, I., & Korner, J. (1978). Broadcast channels with confidential messages. *IEEE Transactions on Information Theory*, *24*(3), 339–348.
6. Liang, Y., Poor, H. V., & Shamai, S. (2008). Secure Communication Over Fading Channels. *IEEE Transactions on Information Theory*, *54*(6), 2470–2492.
7. Barros, J., & Rodrigues, M. (2006). Secrecy capacity of wireless channels. In *Proceedings of IEEE ISIT* (pp. 356–360).
8. 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.
9. Nosratinia, A., Hunter, T. E., & Hedayat, A. (2004). Cooperative communication in wireless networks. *IEEE Communications Magazine*, *42*(10), 74–80.
10. Laneman, J. N., Tse, D. N. C., & Wornell, G. W. (2004). Cooperative diversity in wireless networks: Efficient protocols and outage behavior. *IEEE Transaction on Information Theory*, *50*(12), 3062–3080.
11. 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.
12. Wang, L., Kim, K. J., Duong, T. Q., Elkashlan, M., & Poor, H. V. (2014). On the security of cooperative single carrier systems. In *Proceedings of IEEE GLOBECOM* (pp. 1956–1601).
13. Fan, L., Lei, X., Duong, T. Q., Elkashlan, M., & Karagiannidis, G. K. (2014). Secure multiuser communications in multiple amplify-and-forward relay networks. *IEEE Transactions on Communications*, *62*(9), 3299–3310.
14. Lee, J.-H. (2015). Cooperative relaying protocol for improving physical layer security in wireless decode-and-forward relaying networks. *Wireless Personal Communications*, *83*(4), 3033–3044.
15. Fan, L., Yang, N., Duong, T. Q., Elkashlan, M., & Karagiannidis, G. K. (2016). Exploiting direct links for physical layer security in multi-user multi-relay networks. *IEEE Transactions on Wireless Communications, 15*(6), 3856–3867.
16. Akyildiz, L. F., Lee, W. Y., Vuran, M. C., & Mohanty, S. (2008). A survey on spectrum management in cognitive radio networks. *IEEE Communications Magazine*, *46*(4), 40–48.
17. Duong, T. Q., Costa, D. B., Tsiftsis, T. A., Zhong, C., & Nallanathan, A. (2012). Outage and diversity of cognitive relaying systems under spectrum sharing environments in Nakagami-m fading. *IEEE Communications Letters*, *16*(12), 2075–2078.
18. Najafi, M., Ardebilipour, M., Nasab, E. S., & Vahidian, S. (2015). Multi-hop cooperative communication technique for cognitive DF and AF relay networks. *Wireless Personal Communications*, *83*(4), 3209–3221.

19. Zhang, Q., Feng, Z., Yang, T., & Li, W. (2015). Optimal power allocation and relay selection in multi-hop cognitive relay networks. *Wireless Personal Communications*, *86*(3), 1673–1692.
20. Duong, T. Q., Duy, T. T., Elkashlan, M., Tran, N. H., & Dobre, O. A. (2014). Secured cooperative cognitive radio networks with relay selection. In *Proceedings of IEEE GLOBECOM* (pp. 3074–3079).
21. Liu, Y., Wang, L., Duy, T. T., Elkashlan, M., & Duong, T. Q. (2015). Relay selection for security enhancement in cognitive relay networks. *IEEE Wireless Communications Letters*, *4*(1), 46–49.
22. Gradshteyn, I. S., & Ryzhik, I. M. (2007). *Table of integrals, series, and products* (7th ed.). Waltham: Academic.

Sang Quang Nguyen He received the BE degree (2010) and M.E. degree (2013) in Ho Chi Minh City University of Transport and Ho Chi Minh City University of Technology, Vietnam, respectively. In 2017, he received the Ph.D. degree in Electrical Engineering from University of Ulsan, South Korea. He is currently with Institute of Research and Development, Duy Tan University, Vietnam. His major research interests are cooperative communications, cognitive radio, physical layer security, energy harvesting, combining techniques.

Hyung Yun Kong He received the M.E. and Ph.D. degrees in electrical engineering from Polytechnic University, Brooklyn, New York, USA, in 1991 and 1996, respectively. He also received a BE in electrical engineering from New York Institute of Technology, New York, in 1989. From 1996 to 1998, he was with LG electronics Co., Ltd., as a member of the multimedia research lab developing PCS mobile phone systems. In 1997, he was promoted to the LG chairman's office planning future satellite communication systems. From 1998 until now, he is a Professor in School of Electrical Engineering at the University of Ulsan, Korea. His research area includes channel coding, detection and estimation, cooperative communications, cognitive radio and wireless sensor networks. He is a member of IEEK, KICS, KIPS, IEEE, and IEICE.