Improved Relay Selection for Decode-and-Forward Cooperative Wireless Networks under Secrecy Rate Maximization

Seifeddine BOUALLEGUE[1], Mazen O. HASNA[1], Ridha HAMILA[1], and Kaouthar SETHOM[2]

[1]Electrical Engineering Department, Qatar University , $\{bouallegue, hasna, hamila\}@qu.edu.qa$
[2]INNOV'COM LAB, SUPCOM, University of Carthage , *k_sethombr@yahoo.fr*

***Abstract*—Privacy and security have an increasingly important role in wireless networks. A secure communication enables a legitimate destination to successfully retrieve information sent by a source, while it disables the eavesdropper (illegitimate destination) to interpret the intercepted information. Physical (PHY) layer security approaches for wireless communications can prevent eavesdropping without encryption. It exploits the physical characteristics of the wireless channel in order to transmit messages securely. They are typically feasible when the source-destination channel is better than the source-eavesdropper channel. Cooperative schemes are a means to improve the performance of secure wireless communications. We propose an improved relay selection scheme, based on source-eavesdropper channel SNR restriction, that will guarantee the best secrecy rate at the destination under QoS condition. Performance has been studied in terms of secrecy rate, outage probability and average error probability. Simulations shows that the proposed scheme outperforms in terms of the secrecy rate at the destination when compared to techniques in the literature.**

***Index Terms*—Physical-Layer, security, channel capacity, secrecy rate, outage probability**

I. Introduction

Secure tranmissions is one of the biggest concerns in wireless communications since their broadcast nature allows illegitimate users to receive a copy of the transmitted signal. Shannon's pioneering work [1] inspired some approaches based on cryptocgraphy that tries to make it more difficults for illegitimate users to decode the received signal. But cryptography started to show its limitations in the last decade due to the fact that it is mostly based on calculation power which is growing exponentially. In fact, a code that was seen unbreakable in the 70's and took years to find the key, can be now ealisy broken and its key found in minutes or even seconds. Physical layer security approaches overtake the computational power limitation since they are based on whether a positive data rate can be supported, and this is not depending on the type of the decoding method the eavesdropper uses.

These approaches have been studied in [2],[3] and [4] based on previous studies and works of [5]. In fact, secrecy rate for the Gaussian channel has been defined in [5] as the difference between the capacity at the legitimate receiver (destination) and that at the illegitimate receiver (eavesdropper). It is also shown that this rate can be positive if the channel to the illegitimate receiver is noisier than the channel to the legitimate receiver.

Relaying techniques are used to improve the performance of relay-based wireless networks. Cognitive networks received close attention in [6]. Performance Selective OFDMA has been studied in [7]. Switch and Examine Combining (SEC) performance was studied as a diversity scheme in [8]. In this paper, we introduce a cooperative scheme to select the relay that will maximize the secrecy rate at the destination and will benefit from increasing the number of relays under QoS constraint at the destination. In fact, the proposed scheme, named Restricted Best Second Hop (RBSH), chooses the best relay over two steps. In the first step, a subgroup of relays verifying a quality condition on the link between them and the eavesdropper is first chosen. In the second step, the relay among the selected subgroup that has the best link to the destination is chosen as the best one. We compared the RBSH scheme performance with two other schemes in terms of average capacity, secrecy rate, outage probability and average BER.

We will detail all the steps of our work in the rest of this paper which is organized as follows. Section II details the system model and its analytical expressions. Secrecy rate, outage probability and average error probability expressions are derived in section III. Section VI presents the simulation setup and the numerical results. Finally, conclusions are drawn in section V.

II. System Model

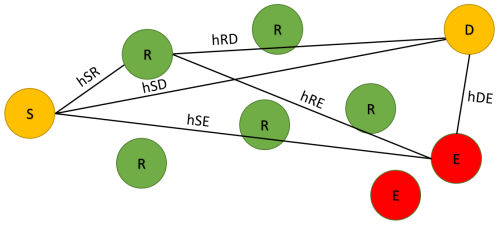

Fig. 1: System Model.

We consider a distributed wireless cooperative network configuration as depicted in 1, with one source, one destination, one eavesdropper and M relays. h_{SD}, h_{SR}, h_{SE}, h_{RE}, h_{RD} represent respectively the channel gains between the source and the destination, the source and the best relay, the source and the eavesdropper, the best relay and the eavesdropper and the best relay and the destination.

All these channels are assumed to be independent and identically distributed (i.i.d.) complex Gaussian with unit variance. The goal of this paper is to design a proper cooperative transmission strategy at the source, destination and relays to improve the secrecy rate. It is assumed that the global channel state information (CSI) is available at a fusion center for designing the transmission scheme. Global CSI knowledge, including that of the eavesdropper CSI, is possible in cases in which the eavesdropper is a known but unauthorized user. Perfect Decode-and-Forward relaying strategy is considered.

We will present in details our proposed schemes: the Restricted Best Second Hop (RBSH) and the Worst Relay-Eavesdropper Link (WREL). We compared these schemes to two reference schemes in [9] and [10] which we will name, further in this paper, Best Second Hop (BSH) and Best Destination-Eavesdropper Ratio (BDER).

The BSH scheme does not take into consideration the quality of the link between the best relay and the eavesdropper. As it is considered that the relays perfectly decode the message sent by the source and use the same codeword to send it to the destination, the first link will not be considered in the choice of the best relay. So the best relay is the one that has the best link with the destination in terms of SNR, it verifies this equation: $\gamma_{R^*D} = max(\gamma_{R^iD})$ where γ_{R^*D} and γ_{R^iD} are respectively the instantaneous SNRs of the links between the best and the i^{th} relay and the destination. We have also derived the analytical results of the reference method in order to study its performance.

The second reference scheme BDER, as opposite to BSH, takes into consideration the the quality of the link between the best relay and the eavesdropper. In fact, the best relay: $i^* = \arg\max_{i=1,\dots,N_R}\{\frac{\gamma_{R^iD}}{\gamma_{R^iE}}\}$. This method will be used as a comparative scheme in the simulation part.

1) Restricted best second hop (RBSH): The best relay selection algorithm consists of the following steps:

1) Choose a subgroup E of relays that comply with the condition: $\gamma_{R^iE} < \gamma_{th}$, where γ_{R^iE} is the instantaneous SNR of the link between the i^{th} relay and the eavesdropper and γ_{th} is an SNR threshold on below of which, the eavesdropper is considered not listening to the message sent from the i^{th} relay to the destination. $E = \{R_i|\gamma_{R^iE} < \gamma_{th}\}$.
2) Choose the relay among E that has the best channel to the destination (γ_{R^iD}). $\gamma_{R^*D} = max(\gamma_{R^iD}|\gamma_{R^iE} \in E)$.
3) If $E = \{\emptyset\}$ then direct transmission link is used.

This methods, takes into consideration the link betewen the best relay and the eavesdropper.

2) Worst relay-eavesdropper link (WREL): This scheme does not take in consideration the link between the relay and the destination. In fact, the best relay is the one that has the weakest link to the eavesdropper. It verifies this equation: $\gamma_{R^*E} = min(\gamma_{R^iE})$.

A. Probability Density Function

1) Restricted best second hop: The probability that the eavesdropper is not listening to the message sent from the relay to the destination is expressed by the following equation:

$$P_{NI} = P(\gamma_{R^iE} \leq \gamma_{th}) = \int_0^{\gamma_{th}} \frac{1}{\bar{\gamma}_{RE}} exp\left(-\frac{\gamma_{R^iE}}{\bar{\gamma}_{RE}}\right) \mathrm{d}\gamma_{R^iE} = 1 - exp\left(-\frac{\gamma_{th}}{\bar{\gamma}_{R^iE}}\right). \tag{1}$$

The next step is to choose from E the relay which maximizes the SNR of the second hop γ_{R^iD}. Let γ_{R^*D} denotes the instantaneous SNR between the best relay R^* and the destination. In order to average over all relay selection possibilities, a binomial distribution should be used for the interference constraint which is given by

$$\sum_{k=1}^{N_R} \binom{N_R}{k} \; P_{NI}^k \; P_I^{N_R-k} \tag{2}$$

where N_R is the number of relays, $\binom{N_R}{k} = \frac{N_R!}{k!\ (N_R-k)!}$, and $P_I(= 1 - P_{NI})$ is the probability that the eavesdropper is listening to the message sent from the selected relay. By using the order statistics [11] and the binomial expansion form, the PDF of γ_{R^*D} under the above mentioned constraint is given by

$$\sum_{k=1}^{N_R} \binom{N_R}{k} P_{NI}^k P_I^{N_R-k} k \; \frac{exp^{\left(\frac{-\gamma_{R^*D}}{\bar{\gamma}_{R^*D}}\right)}}{\bar{\gamma}_{R^*D}} \left(1 - exp^{\left(\frac{-\gamma_{R^*D}}{\bar{\gamma}_{R^*D}}\right)}\right)^{k-1} = \sum_{k=1}^{N_R} \binom{N_R}{k} P_{NI}^k P_I^{N_R-k} \sum_{i=1}^{k} \binom{k}{i} \frac{i\ (-1)^{i-1}}{\bar{\gamma}_{R^*D}}\ exp^{\left(-\frac{\gamma_{R^*D}}{\bar{\gamma}_{R^*D}}\right)} \tag{3}$$

where, $\gamma_{R^*D} = \frac{E_s\ |h_{R^*D}|^2}{N_0}$ is the instantaneous SNR of the link between the best relay R^* and the destination with average SNR $= \bar{\gamma}_{R^*D}$ and E_s is the transmission energy. The PDF of γ_{SD} which follows the exponential distribution is expressed by the following expression:

$$p(\gamma_{SD}) = \frac{1}{\bar{\gamma}_{SD}} exp\left(-\frac{\gamma_{SD}}{\bar{\gamma}_{SD}}\right) \tag{4}$$

where, $\gamma_{SD} = \frac{E_s\ |h_{SD}|^2}{N_0}$ is the instantaneous SNR of the link between the source and the destination with average SNR $= \bar{\gamma}_{SD}$. At the destination MRC is adopted and the combined SNR can be written as $\gamma_{eq}^D = \gamma_{R^*D} + \gamma_{SD}$. Due to the independence of γ_{R^*D} and γ_{SD}, we can obtain the PDF of γ_{eq}^D through the convolution of the PDFs γ_{R^*D} and γ_{SD} as follows

$$p(\gamma_{eq}^D) = \int_0^{\gamma_{eq}^D} p_{\gamma_{R^*D}}(\tau)\ p_{\gamma_{SD}}(\gamma_{eq}^D - \tau)\ d\tau. \tag{5}$$

Using (3), (4), and (5), the PDF of the MRC scheme satisfying the above mentioned constraint is obtained as

$$p(\gamma_{eq}^D) = \sum_{k=1}^{N_R} \binom{N_R}{k}\ P_{NI}^k\ P_I^{N_R-k}\ \sum_{i=1}^{k} \binom{k}{i}\ \frac{i\ (-1)^{i-1}}{\bar{\gamma}_{SD}\bar{\gamma}_{R^*D}} exp\left(-\frac{\gamma_{eq}^D}{\bar{\gamma}_{SD}}\right) \int_0^{\gamma_{eq}^D} exp\left(\frac{\tau}{\bar{\gamma}_{SD}} - \frac{i\tau}{\bar{\gamma}_{R^*D}}\right) d\tau. \tag{6}$$

Equation (6) is simplified by evaluating its integral, and the following expression is obtained

$$p(\gamma_{eq}^D) = \sum_{k=1}^{N_R} \binom{N_R}{k}\ P_{NI}^k\ P_I^{N_R-k}\ \sum_{i=1}^{k} \binom{k}{i}\ \frac{i\ (-1)^{i-1}}{i\ \bar{\gamma}_{SD} - \bar{\gamma}_{R^*D}} \left[exp\left(-\frac{\gamma_{eq}^D}{\bar{\gamma}_{SD}}\right) - exp\left(-\frac{i\gamma_{eq}^D}{\bar{\gamma}_{R^*D}}\right)\right]. \tag{7}$$

If the constraint is not satisfied, only the direct link is used in the transmission and the total PDF of γ_{eq}^D at the destination becomes

$$p_T(\gamma_{eq}^D) = \sum_{k=1}^{N_R} \binom{N_R}{k}\ P_{NI}^k\ P_I^{N_R-k}\ \sum_{i=1}^{k} \binom{k}{i}\ \frac{i\ (-1)^{i-1}}{i\ \bar{\gamma}_{SD} - \bar{\gamma}_{R^*D}} \left[exp\left(-\frac{\gamma_{eq}^D}{\bar{\gamma}_{SD}}\right) - exp\left(-\frac{i\gamma_{eq}^D}{\bar{\gamma}_{R^*D}}\right)\right] + P_I^{N_R} p(\gamma_{SD}) \tag{8}$$

The PDF of γ_{SE} between the source and the eavesdropper which follows the exponential distribution is expressed by the following expression:

$$p(\gamma_{SE}) = \frac{1}{\bar{\gamma}_{SE}} exp\left(-\frac{\gamma_{SE}}{\bar{\gamma}_{SE}}\right) \tag{9}$$

where, $\gamma_{SE} = \frac{E_s\ |h_{SE}|^2}{N_0}$ is the instantaneous SNR of the link between the source and the eavesdropper with average SNR $= \bar{\gamma}_{SE}$. The PDF of γ_{R^*E} is equal to 0 since we consider that the eavesdropper is not getting any information from the best relay. Thus the total PDF at the eavesdropper is as follows

$$p(\gamma_{eq}^E) = p(\gamma_{SE}) \tag{10}$$

2) Best second hop method: For this method, there is no constraint on the best relay-eavesdropper link. Thus the choice of the best relay does not rely on the mentioned link. The relay that have the strongest link with the destination is chosen. The PDFs of γ_{SD} and γ_{SE} are the same as calculated for the previous method. The PDF of γ_{R^*D} for this method is as follows:

$$p(\gamma_{R^*D}) = \sum_{i=1}^{N_R} \binom{N_R}{i}\ \frac{i\ (-1)^{i-1}}{\bar{\gamma}_{R^*D}}\ exp^{\left(-\frac{\gamma_{R^*D}}{\bar{\gamma}_{R^*D}}\right)} \tag{11}$$

where, $\gamma_{R^*D} = \frac{E_s\ |h_{R^*D}|^2}{N_0}$ is the instantaneous SNR of the link between the best relay and the destination with average SNR $= \bar{\gamma}_{R^*D}$. The difference now resides in the PDF of γ_{R^*E} since there is no constraint on the best relay-eavesdropper link, it is written as follows:

$$p(\gamma_{R^*E}) = \frac{1}{\bar{\gamma}_{R^*E}} exp\left(-\frac{\gamma_{R^*E}}{\bar{\gamma}_{R^*E}}\right) \tag{12}$$

Using the equation (11) and the PDF of γ_{SD}, the total PDF at the destination can be written as follows (assuming MRC reception):

$$p_T(\gamma_{eq}^D) = \sum_{i=1}^{N_R} \binom{N_R}{i}\ \frac{i\ (-1)^{i-1}}{i\ \bar{\gamma}_{SD} - \bar{\gamma}_{R^*D}} \left[exp\left(-\frac{\gamma_{eq}^D}{\bar{\gamma}_{SD}}\right) - exp\left(-\frac{i\gamma_{eq}^D}{\bar{\gamma}_{R^*D}}\right)\right] \tag{13}$$

with $\gamma_{eq}^D = \gamma_{R^*D} + \gamma_{SD}$. The total PDF at the eavesdropper is expressed by:

$$p(\gamma_{eq}^E) = \frac{1}{\bar{\gamma}_{SE} - \bar{\gamma}_{R^*E}} \left[exp\left(-\frac{\gamma_{eq}^E}{\bar{\gamma}_{SE}}\right) - exp\left(-\frac{\gamma_{eq}^E}{\bar{\gamma}_{R^*E}}\right)\right] \tag{14}$$

3) Worst relay-eavesdropper link: In this method, relays are chosen according to the link with the eavesdropper. This leads to a total PDF at the destination as follows:

$$p_T(\gamma_{eq}^D) = \frac{1}{\bar{\gamma}_{SD} - \bar{\gamma}_{R^*D}} \left[exp\left(-\frac{\gamma_{eq}^D}{\bar{\gamma}_{SD}}\right) - exp\left(-\frac{\gamma_{eq}^D}{\bar{\gamma}_{R^*D}}\right)\right] \tag{15}$$

While the total PDF at the eavesdropper is characterized by choosing the minimal γ_{R^*E} which can be expressed by:

$$p_T(\gamma_{eq}^E) = \frac{1}{\bar{\gamma}_{SE} - \frac{\bar{\gamma}_{R^*E}}{N_R}} \left[exp\left(-\frac{\gamma_{eq}^D}{\bar{\gamma}_{SD}}\right) - exp\left(-\frac{N_R\gamma_{eq}^D}{\bar{\gamma}_{R^*D}}\right)\right] \tag{16}$$

III. Performance Study

In this section we will study the performance of the proposed schemes in terms of average capacity, secrecy rate, outage probability and average BER.

A. Average Capacity and Secrecy Rate

We could obtain a generic channel capacity equation that is valid for the above mentioned methods and both Destination and Eavesdropper:

$$C = \int_0^{+\infty} \frac{1}{2}\log_2(1+\gamma_{eq}^*) f_T(\gamma_{eq}^*|\gamma_{eq}^* = \gamma^* + \gamma_{DT})\,\mathrm{d}\gamma_{eq}^* + \int_0^{+\infty} \log_2(1+\gamma_{eq}^*) f_T(\gamma_{eq}^*|\gamma_{eq}^* = \gamma_{DT})\,\mathrm{d}\gamma_{eq}^* \quad (17)$$

with, γ_{DT} is the SNR of the direct transmission, γ^* is the SNR of the relay {Destination,Eavesdropper} link, f_T means total PDF at the {Destination,Eavesdropper}.

The secrecy rate is given by the difference between the capacity at the destination and the capacity at the eavesdropper. In the following, we will derive this equation for all the methods we cited.

1) Restricted best second hop: The capacity at the destination is expressed by the following:

$$C_D = \sum_{n=1}^{NR} \binom{N_R}{n} \frac{((-1)^{(n-1)})}{2n(\bar{\gamma}_{SD} - \bar{\gamma}_{R^*D})\log(2)} (n\bar{\gamma}_{SD} \exp\left(\frac{1}{\bar{\gamma}_{SD}}\right) \exp_i\left(\frac{1}{\bar{\gamma}_{SD}}\right) - \bar{\gamma}_{R^*D} \exp\left(\frac{n}{\bar{\gamma}_{R^*D}}\right) \exp_i\left(\frac{n}{\bar{\gamma}_{R^*D}}\right)) + \left(\frac{\exp\frac{1}{\bar{\gamma}_{SD}}}{\log(2)}(P_l^{NR}) \exp_i \frac{1}{\bar{\gamma}_{SD}}\right) \quad (18)$$

where N_R is the number of relays, $\bar{\gamma}_{SD}$ is the average SNR between the source and the destination, $\bar{\gamma}_{R^*D}$ is the average SNR between the best relay and the destination, P_l^{NR} is the probability that the condition $\gamma_{R^iE} < \gamma_{th}$ is not verified and $\exp_i$ is the exponential integral.

The capacity at the eavesdropper is equal to [12]:

$$C_E = \exp\left(\frac{1}{\bar{\gamma}_{SE}}\right) \frac{\exp_i\left(\frac{1}{\bar{\gamma}_{SE}}\right)}{log(2)} \quad (19)$$

2) Best second hop: The capacity at the destination is expressed as follows:

$$C_D = \sum_{n=1}^{NR} \binom{N_R}{n} \frac{((-1)^{(n-1)})}{2n(\bar{\gamma}_{SD} - \bar{\gamma}_{R^*D})\log(2)} (n\bar{\gamma}_{SD} \exp\left(\frac{1}{\bar{\gamma}_{SD}}\right) \exp_i\left(\frac{1}{\bar{\gamma}_{SD}}\right) - \bar{\gamma}_{R^*D} \exp\left(\frac{n}{\bar{\gamma}_{R^*D}}\right) \exp_i\left(\frac{n}{\bar{\gamma}_{R^*D}}\right)) \quad (20)$$

In addition, the capacity at the eavesdropper is given by [12]:

$$C_E = \frac{1}{2(\bar{\gamma}_{SE} - \bar{\gamma}_{R^*E})\log(2)} (\bar{\gamma}_{SE} \exp\left(\frac{1}{\bar{\gamma}_{SE}}\right) \exp_i\left(\frac{1}{\bar{\gamma}_{SE}}\right) - \bar{\gamma}_{R^*E} \exp\left(\frac{1}{\bar{\gamma}_{R^*E}}\right) \exp_i\left(\frac{1}{\bar{\gamma}_{R^*E}}\right)) \quad (21)$$

3) Worst relay-eavesdropper link: The capacity at the destination using this method is equal to:

$$C_D = \frac{1}{2(\bar{\gamma}_{SD} - \bar{\gamma}_{R^*D})\log(2)} (\bar{\gamma}_{SD} \exp\left(\frac{1}{\bar{\gamma}_{SD}}\right) \exp_i\left(\frac{1}{\bar{\gamma}_{SD}}\right) - \bar{\gamma}_{R^*D} \exp\left(\frac{1}{\bar{\gamma}_{R^*D}}\right) \exp_i\left(\frac{1}{\bar{\gamma}_{R^*D}}\right)) \quad (22)$$

The capacity at the eavesdropper using the smallest γ_{RE} method is expressed as follows:

$$C_E = \frac{1}{2(\bar{\gamma}_{SE} - \frac{\bar{\gamma}_{R^*E}}{NR})\log(2)} (\bar{\gamma}_{SE} \exp\left(\frac{1}{\bar{\gamma}_{SE}}\right) \exp_i\left(\frac{1}{\bar{\gamma}_{SE}}\right) - \frac{\bar{\gamma}_{R^*E}}{NR} \exp\left(\frac{NR}{\bar{\gamma}_{R^*E}}\right) \exp_i\left(\frac{NR}{\bar{\gamma}_{R^*E}}\right)) \quad (23)$$

B. Outage Probability

In this section we will show the outage probability that we derived using [12] for the three methods.

1) Restricted best second hop: From (8), the outage probability P_{out} is expressed as:

$$P_{out} = \sum_{k=1}^{N_R} \binom{N_R}{k} P_{NI}^k P_I^{N_R-k} \sum_{i=1}^{k} \binom{k}{i} \left((-1)^{i-1} + \frac{(-1)^{i-1}}{i\bar{\gamma}_{SD} - \bar{\gamma}_{R^*D}} \left[\bar{\gamma}_{R^*D} exp\left(\frac{-i\gamma_{th}}{\bar{\gamma}_{R^*D}}\right) - i\ \bar{\gamma}_{SD}\ exp\left(\frac{-\gamma_{th}}{\bar{\gamma}_{SD}}\right)\right]\right) + P_I^{N_R} \left[1 - exp\left(\frac{-\gamma_{th}}{\bar{\gamma}_{SD}}\right)\right] \quad (24)$$

2) Best second hop: From (13), the outage probability P_{out} is expressed as:

$$P_{out} = \sum_{i=1}^{N_R} \binom{N_R}{i} \left((-1)^{i-1} + \frac{(-1)^{i-1}}{i\bar{\gamma}_{SD} - \bar{\gamma}_{R^*D}} \left[\bar{\gamma}_{R^*D}\ exp\left(\frac{-i\gamma_{th}}{\bar{\gamma}_{R^*D}}\right) - i\ \bar{\gamma}_{SD}\ exp\left(\frac{-\gamma_{th}}{\bar{\gamma}_{SD}}\right)\right]\right) \quad (25)$$

3) Worst relay-eavesdropper link: From (15), the outage probability P_{out} is expressed as:

$$P_{out} = 1 + \frac{1}{\bar{\gamma}_{SD} - \bar{\gamma}_{R^*D}} \left[\bar{\gamma}_{R^*D} \; exp\left(\frac{-\gamma_{th}}{\bar{\gamma}_{R^*D}} \right) - \bar{\gamma}_{SD} \; exp\left(\frac{-\gamma_{th}}{\bar{\gamma}_{SD}} \right) \right] \quad (26)$$

C. Average Error Probability

Based on the derived total PDF and the BER expression we can write the following:

$$BER = \sum_{k=1}^{N_R} \binom{N_R}{k} \; P_{NI}^{k} \; P_I^{N_R - k} \; \sum_{i=1}^{k} \binom{k}{i} \; \frac{i \; (-1)^{i-1}}{i \; \bar{\gamma}_{SD} - \bar{\gamma}_{R^*D}} \int_0^{+\infty} Q(\sqrt{2 \; \alpha}) \left[exp\left(-\frac{\alpha}{\bar{\gamma}_{SD}} \right) - exp\left(-\frac{i\alpha}{\bar{\gamma}_{R^*D}} \right) \right] \; d\alpha + P_I^{N_R} \int_0^{+\infty} Q(\sqrt{2 \; \alpha}) f(\gamma_{SD}) d\gamma_S D. \quad (27)$$

We derive the BER expressions for the three methods by evaluating the integrals in (27) and adapting it to each method.

1) Restricted best second hop: From (8), the average BER is expressed as:

$$P_e = \left(\sum_{k=1}^{N_R} \binom{N_R}{k} \; P_{NI}^{k} \; P_I^{N_R - k} \sum_{i=1}^{k} \binom{k}{i} \; \frac{(-1)^{i-1}}{2(i \; \bar{\gamma}_{SD} - \bar{\gamma}_{R^*D})} \left(i \; \bar{\gamma}_{SD} \; Binc_{z_{SD}} \left[1, \frac{1}{2} \right] - \bar{\gamma}_{R^*D} \; Binc_{z_{RD}} \left[1, \frac{1}{2} \right] \right) \right) + P_I^{N_R} \frac{1}{2} \left(1 - \sqrt{\frac{\bar{\gamma}_{SD}}{1 + \bar{\gamma}_{SD}}} \right) \quad (28)$$

where, $Binc_x[.,.]$ is the incomplete beta function, $z_{SD} = \frac{1}{\bar{\gamma}_{SD}+1}$, and $z_{RD} = \frac{i}{\bar{\gamma}_{R^*D}+i}$ [12].

2) Best second hop: The average BER of this method is expressed by the following equation. Note that we remove the part of the direct link since it is never used outside of the MRC:

$$P_e = \sum_{i=1}^{NR} \binom{NR}{i} \; \frac{(-1)^{i-1}}{2(i \; \bar{\gamma}_{SD} - \bar{\gamma}_{R^*D})} \left(i \; \bar{\gamma}_{SD} \; Binc_{z_{SD}} \left[1, \frac{1}{2} \right] - \bar{\gamma}_{R^*D} Binc_{z_{RD}} \left[1, \frac{1}{2} \right] \right) \quad (29)$$

3) Worst relay-eavesdropper link: From (15), the average BER is expressed as:

$$P_e = \frac{1}{2(\; \bar{\gamma}_{SD} - \bar{\gamma}_{R^*D})} \left(\bar{\gamma}_{SD} \; Binc_{z_{SD}} \left[1, \frac{1}{2} \right] - \bar{\gamma}_{R^*D} \; Binc_{z_{RD}} \left[1, \frac{1}{2} \right] \right) \quad (30)$$

IV. Numerical Results

In this section, we investigate the performance of the proposed design algorithms numerically.

A. Simulation Setup

In the simulation setup, we assume that the average SNR of the direct link is proportional to the average SNR of the second hop as: $\bar{\gamma}_{SD} = 0.21 \; \bar{\gamma}_{R^*D}$, average SNR between the relays and destination is the same as that between relays and eavesdropper, and unit transmission power at the source and the relays. BPSK modulation technique is used, and the number of relays and the value of interference threshold are varying as shown in the simulation figures.

B. Simulation results interpretation

Fig. 2 shows the secrecy rates achieved by the three studied methods while changing the number of relays. It is noticeable that RBSH scheme is realizing better secrecy rate than the other two methods.

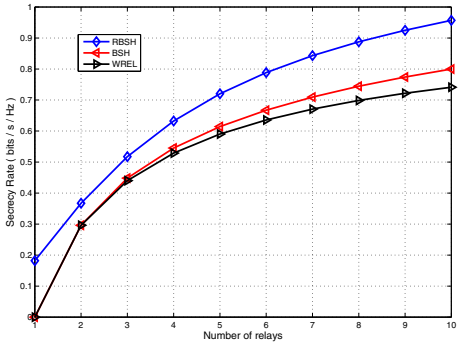

Fig. 2: Secrecy Rate vs Number of Relays. $\gamma_{th} = 10dB$

Fig. 3 reveals that the BSH method offers a lower outage probability than the other three methods. We notice that the outage probability of WREL is constant, this is due to the fact that it does not depend on the number of relays. We remark the same behavior for the average error probability of the methods shown in the figure 6. The BDER method offers a higher outage probability than the RBSH. This confirm the fact that having the maximum Destination-Eavesdropper SNR ratio does not guarantee the best QoS at the destination.

Fig. 4 shows the secrecy rates achieved by the three methods while changing $\bar{\gamma}_{R^*D}$. It shows that when the average SNR is below $\gamma_{th} = 10dB$, RBSH scheme offers better results since there are relays that satisfies the condition $E = \{R_i | \gamma_{R^i E} < \gamma_{th}\}$. But when the average SNR is higher than $\gamma_{th} = 10dB$, RBSH scheme does not offer better results because none of the relays satisfies the secrecy condition. The same behavior is also shown in the Fig. 5.

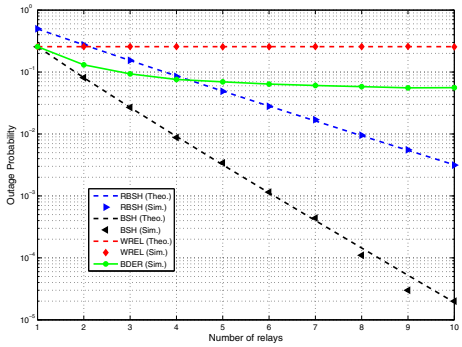

Fig. 3: Outage Probability vs Number of Relays

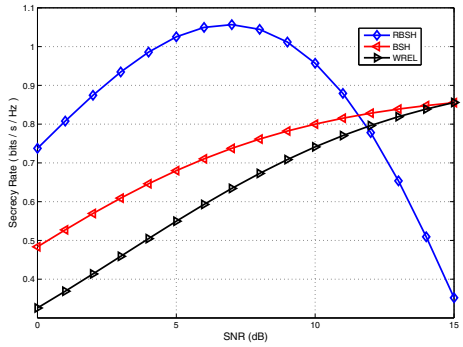

Fig. 4: Secrecy Rate vs SNR, $\gamma_{th} = 10dB$.

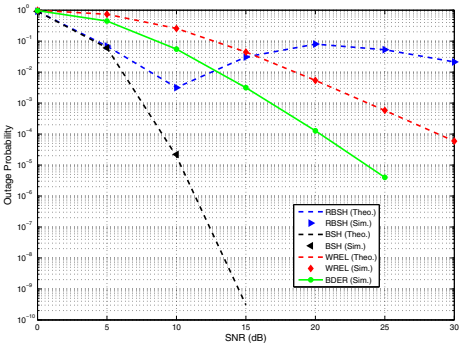

Fig. 5: Outage Probability vs SNR, $\gamma_{th} = 10dB$.

V. Conclusion

In this paper, we have introduced an efficient cooperative communications scheme which maximizes the secrecy rate. We proposed a better relay selection method that maximizes the secrecy rate and benefits from increasing the number of relays under QoS constraint at the destination. The proposed transmission scheme was studied for both DF relaying strategy. Performance has been studied in terms of secrecy rate, outage probability and average error probability expressions have been derived. Simulations results are used to confirm

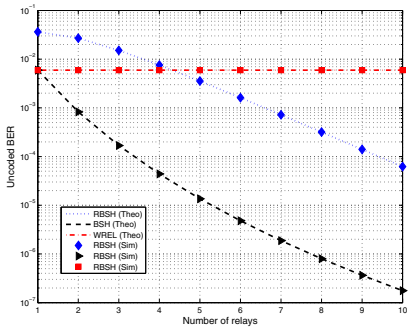

Fig. 6: Average Error Probability vs Number of relays, $\gamma_{th} = 10dB$.

the mathematical derivations and an agreement results are observed. The results confirm the better secrecy rate of the introduced transmission scheme compared to well established techniques introduced in the literature.

Acknowledgement

This work was supported by Ooredoo under the project QUEX-Qtel-09/10-10.

References

[1] C. E. Shannon, "Communication theory of secrecy systems," *Bell Syst. Tech. J.*, vol. 28, pp. 656–715, 1949.

[2] Y. Liang, H. V. Poor, and S. Shamai (Shitz), "Secure communication over fading channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2470–2492, 2008.

[3] Y. Liang, H. V. Poor, and S. Shamai (Shitz), "Physical layer security in broadcast networks," *Security Comm. Networks*, vol. 2, no. 3, pp. 227–238, 2009.

[4] R. Liu, T. Liu, H. V. Poor, and S. Shamai (Shitz), "Mimo gaussian broadcast channels with confidential messages," *IEEE Int. Symp. Inf. Theory (ISIT)*, vol. 56, no. 9, pp. 4215–4227, September 2010.

[5] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, 1975.

[6] H. Shamkhia, M. Hasna, and R. Hamila, "Performance analysis of relay selection schemes in underlay cognitive networks with decode and forward relaying," *IEEE International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC'12), Sydney Australia*, pp. 1552 – 1558, September 2012.

[7] A. Gouissem, M. Hasna, R. Hamila, H. Besbes, and F. Abdelkefi, "Optimized selective ofdma in multihop network," *IEEE International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC'12), Sydney Australia*, pp. 1348 – 1353, September 2012.

[8] H. Chamkhia, M.O. Hasna, and R. Hamila, "Performances analysis of sec based transmit diversity systems with mrc receivers," *Computing, Communications and Applications Conference (ComComAp), Hong Kong*, pp. 71 – 75, February 2012.

[9] Yupeng Liu, Athina P. Petropulu, and H. Vincent Poor, "Joint decode-and-forward and jamming for wireless physical layer security with destination assistance," *Signals, Systems and Computers (ASILOMAR), Pacific Grove, CA*, pp. 109–113, March 2011.

[10] I. Krikidis, "Opportunistic relay selection for cooperative networks with secrecy constraints," *Communications, IET*, vol. 4, no. 15, pp. 1787–1791, 2010.

[11] H. C. Yang and M. S. Alouini, *Order Statistics in Wireless Communications Diversity, Adaptation, and Scheduling in MIMO and OFDM Systems*, Cambridge University Press, 2011.

[12] Omri A. and Hasna M.O., "Enhancing wireless networks performance through cooperative communications with interference management," *ICT Convergence (ICTC)*, pp. 524 – 529, October 2012.