



# Secrecy performance analysis of amplify-and-forward cooperative network with relay selection in the presence of multiple eavesdroppers

Mohammad Torabi<sup>1</sup> · Sahar Parkouk<sup>2</sup> · Saeed Shokrollahi<sup>2</sup>

Accepted: 23 March 2021 / Published online: 3 May 2021

© The Author(s), under exclusive licence to Springer Science+Business Media, LLC, part of Springer Nature 2021

## Abstract

The use of wireless transmission networks in various environments has become widespread. One of the main challenges in wireless networks is that the wireless transmission is highly vulnerable to eavesdropping attacks. In this paper, an amplify-and-forward cooperative relaying wireless system with relay selection is considered to improve the physical layer (PHY) security of the wireless system in the presence of multiple eavesdroppers, under two cases, namely, perfect channel state information (CSI) and outdated CSI cases. To evaluate the PHY security of the system, we derive closed-form expressions for the PHY security performance metrics, including the probability of non-zero secrecy capacity, the average secrecy capacity, and the secrecy outage probability. Then using those expressions, we obtain several numerical results under system parameters. The results show that relay selection provides significant improvement in the PHY security of the system. Moreover, it is observed that, when the CSI used to select the best relay is outdated, the PHY secrecy performance is relatively inferior compared to that of the perfect CSI case. Finally, the obtained mathematical expressions are also validated using Monte-Carlo simulation.

**Keywords** Physical layer security · Network security · Secrecy capacity · Cooperative networks

## 1 Introduction

Wireless networking has become an essential part of our daily life and is widely used in different applications. One of the major challenges of wireless networks is that the transmission between legitimate users can easily be overheard by eavesdroppers due to the broadcast nature of the wireless communication and is highly vulnerable to eavesdropping attacks. In order to increase the security of signal transmission, existing communication systems typically use encryption techniques to prevent eavesdropping attacks on transferring data between legitimate users.

However, encryption protocols face several challenges due to the rapid growth of computing systems.

Recently, physical layer (PHY) security methods have been considered as an efficient way to overcome the problems caused by eavesdropping attacks. These methods are usually considered as the alternative and complement methods to create security in wireless communications using the physical properties of the wireless channel. The basis of the physical layer security scheme is the information theoretic approach, which is based on Shannon complete security concepts [1]. The concept of physical layer security was first proposed by Wyner with examining the memoryless wiretap channels [2]. In the considered system, two legitimate users communicate with each other via a main channel, in the presence of an eavesdropper that has access to the reduced version of the channel authorized for the legitimate receivers. Then, the memoryless wiretap channel model proposed by Wyner were extended to the Gaussian wiretap channel and the secrecy capacity concept was introduced [3]. The secrecy capacity is defined as the difference between main channel capacity and wiretap

✉ Mohammad Torabi  
m\_torabi@ieee.org

<sup>1</sup> School of Electrical Engineering and Computer Science, Washington State University, Pullman, WA, USA

<sup>2</sup> Cyberspace Research Institute, Shahid Beheshti University, Tehran, Iran

channel capacity. Accordingly, secure communication is not possible unless the signal-to-noise ratio (SNR) of the main channel is higher than that of the wiretap channel. To improve the secrecy capacity of the system, it is desirable to introduce a technique which causes an increase in the capacity of the main channel, and/or a decrease in the channel capacity of wiretap channel. To this end, several theoretical and practical research works have been reported for improving the physical layer security of digital communication systems, in which some effective approaches have been proposed such as modulation, channel coding and diversity methods, cooperative relaying, space-time coding, and multiple-input multiple-output (MIMO) methods [4–16]. In several research works, the PHY security performances of a direct communication system have been evaluated, in which a source transmits information to the destination while single or multiple eavesdroppers were able to receive the information [17, 18]. On the other hand, it has been shown that cooperative networks with AF relay selection have better system performances than direct communication networks (non-cooperative communications) and the average SNR gain is increased with the number of available relays [19, 20]. Therefore, the concept of relay selection in AF relaying systems can also improve the PHY secrecy performance of the system. It was shown that the security in multicasting through generalized fading channels can be improved with the best relay selection [21].

The performances of cooperative communications with opportunistic relaying have been examined with a perfect channel state information (CSI) in [22] and [23]. However, in time-variable environments, the CSI used for the relay selection, at the moment of selection may be different from the CSI at the moment of signal transmission. Therefore, relay selection based on the outdated CSI can yield a decrease in the performance of opportunistic relay selection [10, 24–26]. For example, in [26], authors have analyzed the Shannon capacity of the opportunistic relaying technique in amplify-and-forward cooperative systems over Rayleigh fading channels under outdated channel information. They have evaluated the effects of outdated channel information on the channel capacity and the outage performance. In [9], the secrecy performance has been evaluated for a cooperative transmission in a dual-hop MIMO relay system using a combined transmit antenna selection (TAS) and maximum ratio combining (MRC) scheme, denoted TAS/MRC scheme, over the Nakagami- $m$  fading channels. The secrecy performance of the TAS/MRC scheme is then evaluated and the impacts of outdated CSI have been studied using the numerical results obtained from closed-form expressions of exact ergodic secrecy rate and exact secrecy outage probability. In [27], the impact of imperfect CSI on the PHY secrecy performance of a space

time block coded MIMO system is evaluated over Rician fading wiretap channel, showing the advantages of using MIMO system, with respect to the PHY security.

In this paper, we analyze and evaluate the PHY secrecy performance of a cooperative network with multiple AF relays, in which to improve the physical layer security, an opportunistic relay selection is employed in the presence of multiple eavesdroppers. The main contributions of this paper are summarized as follows: (1) We obtain mathematical expressions for three important PHY security performance criteria: the probability of non-zero secrecy capacity, the secrecy outage probability, and the average secrecy capacity of the system. (2) Using the obtained expressions, we evaluate the secrecy performance of signal transmissions in the AF cooperative network. (3) We evaluate and analyze the physical layer security of AF cooperative relaying systems with relay selection under outdated CSI in the presence of multiple eavesdroppers. We also examine the effects of outdated channel information for relay selection using mathematical expressions, obtained for the probability of non-zero secrecy capacity, the secrecy outage probability, and the average secrecy capacity of the system. The validity of the obtained mathematical expressions are also verified using Monte-Carlo simulation.

The rest of this paper is organized as follows: Section 2 presents the system model and the assumptions. In Sect. 3, the PHY secrecy performance analyses of the system are presented and closed-form expressions are derived for the probability of non-zero secrecy capacity, the secrecy outage probability, and the average secrecy capacity of the system, where the analysis of the system under outdated CSI is given in Sect. 4. In Sect. 5, several numerical evaluation results which are verified by computer simulations are presented and discussed. Finally, concluding remarks are given in Sect. 6.

## 2 System model

We consider a cooperative communication system over Rayleigh fading channel shown in Fig. 1. The source (S) communicates with the desired receiver (D) through  $N$  AF relays  $R_1, R_2, \dots, R_N$ , in the presence of multiple eavesdroppers  $E_1, E_2, \dots, E_K$ . The main channel consists of  $S \rightarrow D$  link and  $S \rightarrow R_n \rightarrow D$  links ( $n = 1, \dots, N$ ), and the wiretap channel consists of  $S \rightarrow E_k$  links ( $k = 1, \dots, K$ ), and  $R_n \rightarrow E_k$  links. In the first time-slot, the received signals for  $S \rightarrow D$  link in terminal D,  $S \rightarrow R_n$  link in  $R_n$  and  $S \rightarrow E_k$  link in  $E_k$  can be respectively written as:

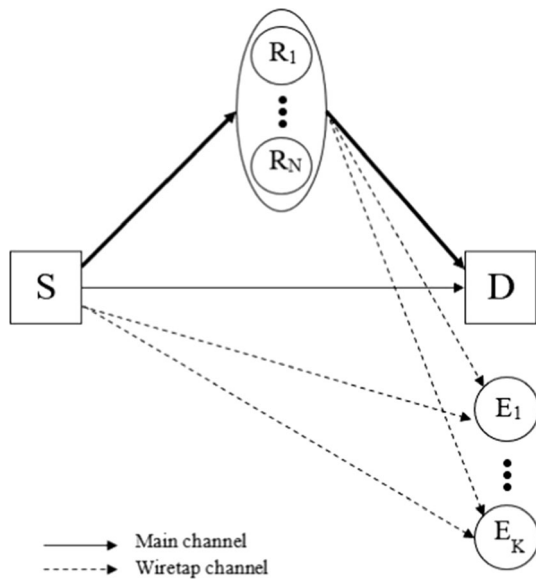


Fig. 1 System model

$$y_{SD} = \frac{1}{\sqrt{d_{SD}^\alpha}} \sqrt{P_s} h_{SD} s + n_{SD} \tag{1}$$

$$y_{SR_n} = \frac{1}{\sqrt{d_{SR_n}^\alpha}} \sqrt{P_s} h_{SR_n} s + n_{SR_n} \tag{2}$$

$$y_{SE_k} = \frac{1}{\sqrt{d_{SE_k}^\alpha}} \sqrt{P_s} h_{SE_k} s + n_{SE_k} \tag{3}$$

where  $P_s$  denotes the source transmit power,  $\alpha$  is the path loss exponent.  $d_{SD}$ ,  $d_{SR_n}$ , and  $d_{SE_k}$  are the distances of S from D, from  $n$ -th relay ( $R_n$ ) and from  $k$ -th eavesdropper ( $E_k$ ), respectively,  $h_{SD}$ ,  $h_{SR_n}$  and  $h_{SE_k}$  are the fading coefficients of  $S \rightarrow D$ ,  $S \rightarrow R_n$  and  $S \rightarrow E_k$  links, respectively, and  $s$  is the normalized information signal in S terminal with  $\mathcal{E}[|s|^2] = 1$ , where  $\mathcal{E}(\cdot)$  is the expectation operation. The parameters  $n_{SD}$ ,  $n_{SR_n}$  and  $n_{SE_k}$  are zero mean additive white Gaussian noises (AWGN) in D terminal with variance  $\sigma_{SD}^2$ , in relay  $R_n$  with variance  $\sigma_{SR_n}^2$ , and in  $E_k$  with variance  $\sigma_{SE_k}^2$ , respectively. From (1), (2) and (3), the channels' SNRs can respectively be written as

$$\gamma_{SD} = \frac{P_s |h_{SD}|^2}{d_{SD}^\alpha \sigma_{SD}^2} \tag{4}$$

$$\gamma_{SR_n} = \frac{P_s |h_{SR_n}|^2}{d_{SR_n}^\alpha \sigma_{SR_n}^2} \tag{5}$$

$$\gamma_{SE_k} = \frac{P_s |h_{SE_k}|^2}{d_{SE_k}^\alpha \sigma_{SE_k}^2} \tag{6}$$

In the second time-slot, the received signal for  $R_n \rightarrow D$  and  $R_n \rightarrow E_k$  links are given by

$$y_{R_n D} = G_n \frac{1}{\sqrt{d_{R_n D}^\alpha}} h_{R_n D} y_{SR_n} + n_{R_n D} \tag{7}$$

and

$$y_{R_n E_k} = G_n \frac{1}{\sqrt{d_{R_n E_k}^\alpha}} h_{R_n E_k} y_{SR_n} + n_{R_n E_k} \tag{8}$$

where  $G_n$  is  $n$ -th relay amplification coefficient that is equal to  $G_n = \sqrt{\frac{P_s}{d_{R_n D}^\alpha |h_{SR_n}|^2 + \sigma_{SR_n}^2}}$  and  $d_{R_n D}$  and  $d_{R_n E_k}$  are the distances of  $R_n$  from D and  $E_k$ , respectively. The parameters  $h_{R_n D}$  and  $h_{R_n E_k}$  parameters are the fading coefficients of  $R_n \rightarrow D$  and  $R_n \rightarrow E_k$ , respectively, and the parameters  $n_{R_n D}$  and  $n_{R_n E_k}$  parameters are zero mean additive white Gaussian noise (AWGN) in D terminal with variance  $\sigma_{R_n D}^2$ , in  $R_n$  with variance  $\sigma_{SR_n}^2$  and in  $E_k$  with variance  $\sigma_{R_n E_k}^2$ , respectively. The SNRs of the channels can be respectively expressed as:

$$\gamma_{R_n D} = \frac{P_s |h_{R_n D}|^2}{d_{R_n D}^\alpha \sigma_{R_n D}^2} \tag{9}$$

$$\gamma_{R_n E_k} = \frac{P_s |h_{R_n E_k}|^2}{d_{R_n E_k}^\alpha \sigma_{R_n E_k}^2} \tag{10}$$

The relay selection algorithm selects the best relay ( $b$ ) such that

$$b = \underset{n \in \mathcal{R}}{\operatorname{argmax}} \{ \gamma_{SR_n D} \} \tag{11}$$

where  $\mathcal{R} = \{1, 2, \dots, N\}$  and  $\gamma_{SR_n D}$  is the SNR of  $S \rightarrow R_n \rightarrow D$  channel. The SNR  $\gamma_{SR_n D}$  can be written as [19, 20]:

$$\gamma_{SR_n D} = \frac{\gamma_{SR_n} \gamma_{R_n D}}{1 + \gamma_{SR_n} + \gamma_{R_n D}} \tag{12}$$

For the sake of simplicity, we consider an upper bound for the equivalent SNR as the approximate SNR that is given by [19]

$$\gamma_{SR_n D} = \min(\gamma_{SR_n}, \gamma_{R_n D}) \geq \frac{\gamma_{SR_n} \gamma_{R_n D}}{1 + \gamma_{SR_n} + \gamma_{R_n D}} \tag{13}$$

This approximation has been widely used in the literature and has shown to be tight enough especially at medium to high SNR values [19, 28, 29]. Moreover, in Sect. 4, simulation results have been provided to show the validity of the use this approximation in this work.

Therefore, the SNR of the best relay link  $S \rightarrow R_b \rightarrow D$  can be expressed as:

$$\begin{aligned} \gamma_{SR_b D} &= \max_{n \in \mathcal{R}} \{ \gamma_n \} \\ &= \max_{n \in \mathcal{R}} \{ \min(\gamma_{SR_n}, \gamma_{R_n D}) \}. \end{aligned} \tag{14}$$

Since the main channel consists of  $S \rightarrow D$  and  $S \rightarrow R_n \rightarrow$

D links, then, due to the maximum ratio combining (MRC) used at terminal D, the main channel’s SNR can be written as:

$$\begin{aligned} \gamma_M &= \gamma_{SD} + \gamma_{SR_nD} \\ &= \gamma_{SD} + \max_{n \in \mathcal{R}} \{ \min(\gamma_{SR_n}, \gamma_{R_nD}) \}. \end{aligned} \tag{15}$$

Since eavesdroppers do not know the channel information of  $S \rightarrow R_n$ , then the wiretap channel consists of  $S \rightarrow E_k$  and  $R_n \rightarrow E_k$  links. Therefore, using MRC at  $k$ -th eavesdropper receiver, the SNR of  $k$ -th wiretap channel can be written as

$$\gamma_{W_k} = \gamma_{SE_k} + \gamma_{R_nE_k}. \tag{16}$$

In addition, the SNR of the wiretap channel for multiple eavesdroppers can be obtained from [18]:

$$\gamma_W = \max_{k \in \{1, \dots, K\}} \{ \gamma_{W_k} \}. \tag{17}$$

In the following, we express the probability density function (PDF) and cumulative distribution function (CDF) for the main channel’s SNR as well as for the wiretap channel’s SNR, which enable us to obtain and derive closed-form expressions for the probability of non-zero secrecy capacity, the outage probability and the average secrecy capacity of the considered system.

As shown in [19], the PDF and CDF of the main channel’s SNR are respectively given by:

$$\begin{aligned} f_{\gamma_M}(x) &= \sum_{n=1}^N \binom{N}{n} \frac{n(-1)^{n-1}}{\bar{\gamma}_C - n\bar{\gamma}_{SD}} \\ &\times \left[ \exp\left(-\frac{nx}{\bar{\gamma}_C}\right) - \exp\left(-\frac{x}{\bar{\gamma}_{SD}}\right) \right] \end{aligned} \tag{18}$$

and

$$\begin{aligned} F_{\gamma_M}(x) &= 1 + \sum_{n=1}^N \binom{N}{n} \frac{n(-1)^{n-1}}{\bar{\gamma}_C - n\bar{\gamma}_{SD}} \\ &\times \left[ \bar{\gamma}_{SD} \exp\left(-\frac{x}{\bar{\gamma}_{SD}}\right) - \frac{\bar{\gamma}_C}{n} \exp\left(-\frac{nx}{\bar{\gamma}_C}\right) \right] \end{aligned} \tag{19}$$

where  $\bar{\gamma}_{SR_n} = \bar{\gamma}_{R_nD} = \bar{\gamma}$  and  $\bar{\gamma}_C = \frac{\bar{\gamma}_{SR_n}\bar{\gamma}_{R_nD}}{\bar{\gamma}_{SR_n} + \bar{\gamma}_{R_nD}}$ .

On the other hand, similarly to the approach in [30], we can express the CDF and PDF for the  $k$ -th eavesdropper as:

$$F_{\gamma_{W_k}}(y) = 1 - \frac{\bar{\gamma}_{RE}}{\bar{\gamma}_{RE} - \bar{\gamma}_{SE}} \exp\left(-\frac{y}{\bar{\gamma}_{RE}}\right) + \frac{\bar{\gamma}_{SE}}{\bar{\gamma}_{RE} - \bar{\gamma}_{SE}} \exp\left(-\frac{y}{\bar{\gamma}_{SE}}\right) \tag{20}$$

and

$$f_{\gamma_{W_k}}(y) = \frac{1}{\bar{\gamma}_{RE} - \bar{\gamma}_{SE}} \left[ \exp\left(-\frac{y}{\bar{\gamma}_{RE}}\right) - \exp\left(-\frac{y}{\bar{\gamma}_{SE}}\right) \right] \tag{21}$$

where  $\bar{\gamma}_{SE_k} = \bar{\gamma}_{SE}$  and  $\bar{\gamma}_{R_nE_k} = \bar{\gamma}_{RE}$ .

According to (17), the wiretap channel’s SNR is given by  $\gamma_W = \max_{k \in \{1, \dots, K\}} \{ \gamma_{W_k} \}$ . Therefore, using the order statistic theory [31], the CDF of  $\gamma_W$  can be obtained from  $F_{\gamma_W}(y) = [F_{\gamma_{W_k}}(y)]^K$ , and using (20), we obtain:

$$F_{\gamma_W}(y) = \left[ 1 + \frac{\bar{\gamma}_{SE}}{\bar{\gamma}_{RE} - \bar{\gamma}_{SE}} \exp\left(-\frac{y}{\bar{\gamma}_{SE}}\right) - \frac{\bar{\gamma}_{RE}}{\bar{\gamma}_{RE} - \bar{\gamma}_{SE}} \exp\left(-\frac{y}{\bar{\gamma}_{RE}}\right) \right]^K. \tag{22}$$

Employing the binomial expansions that are  $(1+x)^K = \sum_{i=0}^K \binom{K}{i} x^i$ , and  $(1-x)^K = \sum_{i=0}^K \binom{K}{i} (-1)^i x^i$ , the expression in (23) can be written as:

$$\begin{aligned} F_{\gamma_W}(y) &= \sum_{i=0}^K \binom{K}{i} \sum_{j=0}^i \binom{i}{j} \left( \frac{\bar{\gamma}_{SE}}{\bar{\gamma}_{RE} - \bar{\gamma}_{SE}} \right)^{i-j} \\ &\times \left( \frac{\bar{\gamma}_{RE}}{\bar{\gamma}_{RE} - \bar{\gamma}_{SE}} \right)^j (-1)^j \exp\left[ -\left( \frac{i-j}{\bar{\gamma}_{SE}} + \frac{j}{\bar{\gamma}_{RE}} \right) y \right]. \end{aligned} \tag{23}$$

Using the fact that  $f_{\gamma_W}(y) = \frac{d}{dy} F_{\gamma_W}(y)$ , by obtaining the derivative of (23), the probability density function of the wiretap channel’s SNR can be expressed as

$$\begin{aligned} f_{\gamma_W}(y) &= \sum_{i=0}^K \binom{K}{i} \sum_{j=0}^i \binom{i}{j} \left( \frac{\bar{\gamma}_{SE}}{\bar{\gamma}_{RE} - \bar{\gamma}_{SE}} \right)^{i-j} \left( \frac{\bar{\gamma}_{RE}}{\bar{\gamma}_{RE} - \bar{\gamma}_{SE}} \right)^j \\ &\times (-1)^{j+1} \left( \frac{i-j}{\bar{\gamma}_{SE}} + \frac{j}{\bar{\gamma}_{RE}} \right) \exp\left[ -\left( \frac{i-j}{\bar{\gamma}_{SE}} + \frac{j}{\bar{\gamma}_{RE}} \right) y \right]. \end{aligned} \tag{24}$$

### 3 Secrecy performance analysis

In the scenarios where the eavesdropper is passive, the CSI of the eavesdroppers and the intended receiver are not available at the source terminal, hence perfect secrecy is not guaranteed. In this Section, we analyze the PHY secrecy performance of the considered system. Considering the AF relaying system shown in Fig. 1, and using the definition of the capacity of additive white Gaussian noise (AWGN) channels, with SNRs  $\gamma_M$  and  $\gamma_W$ , we can express the channel capacity of the main channel  $C_M$  and that of the wiretap channel  $C_W$  as  $C_M = \frac{1}{2} \log_2(1 + \gamma_M)$  and  $C_W = \frac{1}{2} \log_2(1 + \gamma_W)$ , respectively. Hence, the instantaneous secrecy capacity can be written as

$$C_s = \begin{cases} \frac{1}{2} [\log_2(1 + \gamma_M) - \log_2(1 + \gamma_W)] & \gamma_M > \gamma_W \\ 0 & \gamma_M \leq \gamma_W \end{cases} \tag{25}$$

where the coefficient of 1/2 is due to the fact that transmission in AF relaying system is done in two time-slots.

### 3.1 Probability of non-zero secrecy capacity (PNZSC)

According to the definition of the instantaneous secrecy capacity in (25), when  $\gamma_M > \gamma_W$ , the secrecy capacity is positive and when  $\gamma_M \leq \gamma_W$ , the secrecy capacity is zero. Thus, since  $\gamma_M$  and  $\gamma_W$  are statistically independent, the probability of non-zero secrecy capacity can be expressed as

$$\Pr(C_s > 0) = \Pr(\gamma_M > \gamma_W) = \int_{x=0}^{\infty} \int_{y=0}^x f_{\gamma_M}(x) f_{\gamma_W}(y) dy dx. \tag{26}$$

By inserting (18) and (24) into (26) and solving the integrals, we obtain the following expression

$$\Pr(C_s > 0) = \sum_{n=1}^N \binom{N}{n} \frac{n(-1)^{n-1}}{\bar{\gamma}_C - n\bar{\gamma}_{SD}} \sum_{i=0}^K \binom{K}{i} \sum_{j=0}^i \binom{i}{j} \times \left( \frac{\bar{\gamma}_{SE}}{\bar{\gamma}_{RE} - \bar{\gamma}_{SE}} \right)^{i-j} \left( \frac{\bar{\gamma}_{RE}}{\bar{\gamma}_{RE} - \bar{\gamma}_{SE}} \right)^j (-1)^j \times \left[ \left( \frac{n}{\bar{\gamma}_C} + \frac{i-j}{\bar{\gamma}_{SE}} + \frac{j}{\bar{\gamma}_{RE}} \right)^{-1} - \left( \frac{1}{\bar{\gamma}_{SD}} + \frac{i-j}{\bar{\gamma}_{SE}} + \frac{j}{\bar{\gamma}_{RE}} \right)^{-1} \right]. \tag{27}$$

### 3.2 Secrecy outage probability (SOP)

An important performance measure for evaluating the PHY secrecy is the secrecy outage probability denoted  $P_{out}(R_s)$ . The secrecy outage probability is a probability that the secrecy capacity is lower than the threshold of  $R_s$ , and can be written as [17]:

$$P_{out}(R_s) = \Pr(C_s < R_s) = \Pr(C_s < R_s | \gamma_M > \gamma_W) \Pr(\gamma_M > \gamma_W) + \Pr(C_s < R_s | \gamma_M \leq \gamma_W) \Pr(\gamma_M \leq \gamma_W). \tag{28}$$

According to the expression in (25), for  $\gamma_M \leq \gamma_W$ ,  $C_s = 0$ , and since  $R_s > 0$ , we can readily conclude that  $\Pr(C_s < R_s | \gamma_M \leq \gamma_W) = 1$ . Also, we can write  $\Pr(\gamma_M \leq \gamma_W) = 1 - \Pr(\gamma_M > \gamma_W)$ . Therefore, using (25), the secrecy outage probability in (28) can be written as:

$$P_{out}(R_s) = \Pr\left(\log_2\left(\frac{1 + \gamma_M}{1 + \gamma_W}\right) < R_s | \gamma_M > \gamma_W\right) \times \Pr(\gamma_M > \gamma_W) + \left[1 - \Pr(\gamma_M > \gamma_W)\right] \tag{29}$$

where assuming  $\mu \triangleq [2^{2R_s}(1 + \gamma_W) - 1]$ , the expression in (29) can be written as

$$P_{out}(R_s) = \Pr(\gamma_M < \mu | \gamma_M > \gamma_W) \Pr(\gamma_M > \gamma_W) + [1 - \Pr(\gamma_M > \gamma_W)] = 1 + \Pr(\gamma_W \leq \gamma_M \leq \mu) - \Pr(\gamma_M \geq \gamma_W) = 1 + \int_{y=0}^{\infty} \int_{x=y}^{\mu} f_{\gamma_M}(x) f_{\gamma_W}(y) dx dy - \int_{y=0}^{\infty} \int_{x=y}^{\infty} f_{\gamma_M}(x) f_{\gamma_W}(y) dx dy = 1 - \int_{y=0}^{\infty} \int_{x=\mu}^{\infty} f_{\gamma_M}(x) f_{\gamma_W}(y) dx dy. \tag{30}$$

Assuming  $\lambda = 2^{2R_s}$ , we solve the inner integral in (30) as follows:

$$P_{out}(R_s) = 1 - \int_{y=0}^{\infty} [1 - F_{\gamma_M}(\lambda - 1 + \lambda y)] f_{\gamma_W}(y) dy = \int_{y=0}^{\infty} F_{\gamma_M}(\lambda - 1 + \lambda y) f_{\gamma_W}(y) dy. \tag{31}$$

By inserting (19) and (24) into (31) and solving the integral, we obtain the closed-form expression of the secrecy outage probability as follows

$$P_{out}(R_s) = 1 - \sum_{n=1}^N \binom{N}{n} \frac{n(-1)^{n-1}}{\bar{\gamma}_C - n\bar{\gamma}_{SD}} \sum_{i=0}^K \binom{K}{i} \sum_{j=0}^i \binom{i}{j} \times \left( \frac{\bar{\gamma}_{SE}}{\bar{\gamma}_{RE} - \bar{\gamma}_{SE}} \right)^{i-j} \left( \frac{\bar{\gamma}_{RE}}{\bar{\gamma}_{RE} - \bar{\gamma}_{SE}} \right)^j (-1)^{j+1} \left( \frac{i-j}{\bar{\gamma}_{SE}} + \frac{j}{\bar{\gamma}_{RE}} \right) \times \left[ \frac{\bar{\gamma}_C}{n} \left( \frac{n 2^{2R_s}}{\bar{\gamma}_C} + \frac{i-j}{\bar{\gamma}_{SE}} + \frac{j}{\bar{\gamma}_{RE}} \right)^{-1} \exp\left(-\frac{n(2^{2R_s} - 1)}{\bar{\gamma}_C}\right) - \bar{\gamma}_{SD} \left( \frac{2^{2R_s}}{\bar{\gamma}_{SD}} + \frac{i-j}{\bar{\gamma}_{SE}} + \frac{j}{\bar{\gamma}_{RE}} \right)^{-1} \exp\left(-\frac{(2^{2R_s} - 1)}{\bar{\gamma}_{SD}}\right) \right]. \tag{32}$$

### 3.3 Average secrecy capacity (ASC)

The average secrecy capacity can be obtained by averaging the instantaneous secrecy capacity over the joint PDF of  $(\gamma_M, \gamma_W)$ , where assuming  $\gamma_M$  and  $\gamma_W$  are statistically independent, it can be expressed as [18]:

$$\bar{C}_s = \int_0^{+\infty} \int_0^{+\infty} C_s(x, y) f_{\gamma_M}(x) f_{\gamma_W}(y) dx dy. \tag{33}$$

By inserting (25) in above equation, we obtain

$$\bar{C}_s = \frac{1}{2} \int_{x=0}^{\infty} \int_{y=0}^x (\log_2(1+x) - \log_2(1+y)) f_{\gamma_M}(x) f_{\gamma_W}(y) dx dy = \frac{1}{2} (I_1 - I_2) \tag{34}$$

where

$$\begin{aligned}
 I_1 &= \int_{x=0}^{\infty} \int_{y=0}^x \log_2(1+x) f_{\gamma_M}(x) f_{\gamma_W}(y) dx dy \\
 &= \int_{x=0}^{\infty} \log_2(1+x) f_{\gamma_M}(x) F_{\gamma_W}(x) dx.
 \end{aligned} \tag{35}$$

By inserting (18) and (23) in above equation, and solving the integral, we get

$$\begin{aligned}
 I_1 &= \sum_{n=1}^N \binom{N}{n} \frac{n(-1)^{n-1}}{\bar{\gamma}_C - n\bar{\gamma}_{SD}} \sum_{i=0}^K \binom{K}{i} \sum_{j=0}^i \binom{i}{j} \\
 &\times \left( \frac{\bar{\gamma}_{SE}}{\bar{\gamma}_{RE} - \bar{\gamma}_{SE}} \right)^{i-j} \left( \frac{\bar{\gamma}_{RE}}{\bar{\gamma}_{RE} - \bar{\gamma}_{SE}} \right)^j (-1)^j \\
 &\times \int_{x=0}^{\infty} \log_2(1+x) \left[ \exp\left(-\left(\frac{n}{\bar{\gamma}_C} + \frac{i-j}{\bar{\gamma}_{SE}} + \frac{j}{\bar{\gamma}_{RE}}\right)x\right) \right. \\
 &\left. - \exp\left(-\left(\frac{1}{\bar{\gamma}_{SD}} + \frac{i-j}{\bar{\gamma}_{SE}} + \frac{j}{\bar{\gamma}_{RE}}\right)x\right) \right].
 \end{aligned} \tag{36}$$

Using  $\int_0^{\infty} \ln(1+x) \exp(-\mu x) dx = \frac{1}{\mu} \exp(\mu) E_1(\mu)$ , we obtain the solution of integral, which yields:

$$\begin{aligned}
 I_1 &= \frac{1}{\ln(2)} \sum_{n=1}^N \binom{N}{n} \frac{n(-1)^{n-1}}{\bar{\gamma}_C - n\bar{\gamma}_{SD}} \sum_{i=0}^K \binom{K}{i} \sum_{j=0}^i \binom{i}{j} \\
 &\times \left( \frac{\bar{\gamma}_{SE}}{\bar{\gamma}_{RE} - \bar{\gamma}_{SE}} \right)^{i-j} \left( \frac{\bar{\gamma}_{RE}}{\bar{\gamma}_{RE} - \bar{\gamma}_{SE}} \right)^j \\
 &\times \left[ \left( \frac{n}{\bar{\gamma}_C} + \frac{i-j}{\bar{\gamma}_{SE}} + \frac{j}{\bar{\gamma}_{RE}} \right)^{-1} \exp\left(\frac{n}{\bar{\gamma}_C} + \frac{i-j}{\bar{\gamma}_{SE}} + \frac{j}{\bar{\gamma}_{RE}}\right) \right. \\
 &\times E_1\left(\frac{n}{\bar{\gamma}_C} + \frac{i-j}{\bar{\gamma}_{SE}} + \frac{j}{\bar{\gamma}_{RE}}\right) - \left. \left( \frac{1}{\bar{\gamma}_{SD}} + \frac{i-j}{\bar{\gamma}_{SE}} + \frac{j}{\bar{\gamma}_{RE}} \right)^{-1} \right. \\
 &\left. \times \exp\left(\frac{1}{\bar{\gamma}_{SD}} + \frac{i-j}{\bar{\gamma}_{SE}} + \frac{j}{\bar{\gamma}_{RE}}\right) E_1\left(\frac{1}{\bar{\gamma}_{SD}} + \frac{i-j}{\bar{\gamma}_{SE}} + \frac{j}{\bar{\gamma}_{RE}}\right) \right].
 \end{aligned} \tag{37}$$

Similarly, in (34), we have

$$\begin{aligned}
 I_2 &= \int_{y=0}^{\infty} \int_{x=y}^{\infty} \log_2(1+y) f_{\gamma_M}(x) f_{\gamma_W}(y) dx dy \\
 &= \int_{y=0}^{\infty} \log_2(1+y) f_{\gamma_W}(y) [1 - F_{\gamma_M}(y)] dy.
 \end{aligned} \tag{38}$$

By inserting (19) and (24) in above equation, and solving the integral, we get

$$\begin{aligned}
 I_2 &= \frac{1}{\ln(2)} \sum_{n=1}^N \binom{N}{n} \frac{n(-1)^{n-1}}{\bar{\gamma}_C - n\bar{\gamma}_{SD}} \sum_{i=0}^K \binom{K}{i} \sum_{j=0}^i \binom{i}{j} \\
 &\times \left( \frac{\bar{\gamma}_{SE}}{\bar{\gamma}_{RE} - \bar{\gamma}_{SE}} \right)^{i-j} \left( \frac{\bar{\gamma}_{RE}}{\bar{\gamma}_{RE} - \bar{\gamma}_{SE}} \right)^j (-1)^{j+1} \left( \frac{i-j}{\bar{\gamma}_{SE}} + \frac{j}{\bar{\gamma}_{RE}} \right) \\
 &\times \int_{x'=0}^{\infty} \log_2(1+y) \left[ \frac{\bar{\gamma}_C}{n} \exp\left(-\frac{ny}{\bar{\gamma}_C}\right) - \bar{\gamma}_{SD} \exp\left(-\frac{y}{\bar{\gamma}_{SD}}\right) \right] \\
 &\times \exp\left(-\left(\frac{i-j}{\bar{\gamma}_{SE}} + \frac{j}{\bar{\gamma}_{RE}}\right)y\right) dy.
 \end{aligned} \tag{39}$$

By solving above integral, we obtain:

$$\begin{aligned}
 I_2 &= \frac{1}{\ln(2)} \sum_{n=1}^N \binom{N}{n} \frac{n(-1)^{n-1}}{\bar{\gamma}_C - n\bar{\gamma}_{SD}} \sum_{i=0}^K \binom{K}{i} \sum_{j=0}^i \binom{i}{j} \\
 &\times \left( \frac{\bar{\gamma}_{SE}}{\bar{\gamma}_{RE} - \bar{\gamma}_{SE}} \right)^{i-j} \left( \frac{\bar{\gamma}_{RE}}{\bar{\gamma}_{RE} - \bar{\gamma}_{SE}} \right)^j (-1)^{j+1} \\
 &\times \left( \frac{i-j}{\bar{\gamma}_{SE}} + \frac{j}{\bar{\gamma}_{RE}} \right) \left[ \frac{\bar{\gamma}_C}{n} \left( \frac{n}{\bar{\gamma}_C} + \frac{i-j}{\bar{\gamma}_{SE}} + \frac{j}{\bar{\gamma}_{RE}} \right)^{-1} \right. \\
 &\times \exp\left(\frac{n}{\bar{\gamma}_C} + \frac{i-j}{\bar{\gamma}_{SE}} + \frac{j}{\bar{\gamma}_{RE}}\right) \\
 &\times E_1\left(\frac{n}{\bar{\gamma}_C} + \frac{i-j}{\bar{\gamma}_{SE}} + \frac{j}{\bar{\gamma}_{RE}}\right) \\
 &\left. - \bar{\gamma}_{SD} \left( \frac{1}{\bar{\gamma}_{SD}} + \frac{i-j}{\bar{\gamma}_{SE}} + \frac{j}{\bar{\gamma}_{RE}} \right)^{-1} \right. \\
 &\times \exp\left(\frac{1}{\bar{\gamma}_{SD}} + \frac{i-j}{\bar{\gamma}_{SE}} + \frac{j}{\bar{\gamma}_{RE}}\right) \\
 &\left. \times E_1\left(\frac{1}{\bar{\gamma}_{SD}} + \frac{i-j}{\bar{\gamma}_{SE}} + \frac{j}{\bar{\gamma}_{RE}}\right) \right].
 \end{aligned} \tag{40}$$

Substituting expressions of  $I_1$  given in (37) and  $I_2$  given in (40) into (34), we obtain the following closed-form expression for the average secrecy capacity:

$$\begin{aligned}
 \bar{C}_s &= \frac{0.5}{\ln(2)} \sum_{n=1}^N \binom{N}{n} \frac{n(-1)^{n-1}}{\bar{\gamma}_C - n\bar{\gamma}_{SD}} \sum_{i=0}^K \binom{K}{i} \sum_{j=0}^i \binom{i}{j} \\
 &\times \left( \frac{\bar{\gamma}_{SE}}{\bar{\gamma}_{RE} - \bar{\gamma}_{SE}} \right)^{i-j} \left( \frac{\bar{\gamma}_{RE}}{\bar{\gamma}_{RE} - \bar{\gamma}_{SE}} \right)^j (-1)^j \\
 &\times \left\{ \left[ \left( \frac{i-j}{\bar{\gamma}_{SE}} + \frac{j}{\bar{\gamma}_{RE}} \right) \frac{\bar{\gamma}_C}{n} + 1 \right] \left( \frac{n}{\bar{\gamma}_C} + \frac{i-j}{\bar{\gamma}_{SE}} + \frac{j}{\bar{\gamma}_{RE}} \right)^{-1} \right. \\
 &\times \exp\left(\frac{n}{\bar{\gamma}_C} + \frac{i-j}{\bar{\gamma}_{SE}} + \frac{j}{\bar{\gamma}_{RE}}\right) E_1\left(\frac{n}{\bar{\gamma}_C} + \frac{i-j}{\bar{\gamma}_{SE}} + \frac{j}{\bar{\gamma}_{RE}}\right) \\
 &\left. - \left[ \left( \frac{i-j}{\bar{\gamma}_{SE}} + \frac{j}{\bar{\gamma}_{RE}} \right) \bar{\gamma}_{SD} + 1 \right] \left( \frac{1}{\bar{\gamma}_{SD}} + \frac{i-j}{\bar{\gamma}_{SE}} + \frac{j}{\bar{\gamma}_{RE}} \right)^{-1} \right. \\
 &\left. \times \exp\left(\frac{1}{\bar{\gamma}_{SD}} + \frac{i-j}{\bar{\gamma}_{SE}} + \frac{j}{\bar{\gamma}_{RE}}\right) E_1\left(\frac{1}{\bar{\gamma}_{SD}} + \frac{i-j}{\bar{\gamma}_{SE}} + \frac{j}{\bar{\gamma}_{RE}}\right) \right\}.
 \end{aligned} \tag{41}$$



### 4 Secrecy performance of the system under outdated CSI

In practice, in the AF system with relay selection, the CSI of  $S \rightarrow R_n \rightarrow D$  link, used for relay selection at the decision time  $t$ , may differ from its value at the signal transmission time  $t + \tau$ . This difference can be due to several factors such as channel variations with time, feedback delay and the channel estimation errors. In other words, the best relay selected according to the outdated CSI at time  $t$  may not be the best relay at the time of the data transmission (time  $t + \tau$ ). Therefore, it is of interest to evaluate the effects of outdated CSI on the secrecy performance of the system. In the outdated CSI scenario, in general, we have an estimate of the channel  $h$  denoted  $\hat{h}$ , defined by the following model:

$$\hat{h} = \rho h + (\sqrt{1 - \rho^2})\epsilon \tag{42}$$

where  $\hat{h}$  is the estimate of the channel  $h$ , and  $\epsilon$  is a complex Gaussian noise  $\mathcal{CN}(0, \sigma_h^2)$ . The correlation coefficient  $\rho$ ,  $0 \leq \rho \leq 1$  is a constant value which determines the average quality of the channel estimation. That model is a widely used model in the literature, which models the effects of outdated CSI and imperfect CSI [32].

In this Section, we evaluate and analyze the impacts of outdated CSI on the PHY secrecy of considered AF relaying system. To that end, we obtain closed-form expressions for the probability of non-zero secrecy capacity, the secrecy outage probability, and the average secrecy capacity average of the system under outdated CSI. Then using numerical evaluations, we study and evaluate the impacts of outdated CSI on the secrecy performance of the system. According to [20], for the AF cooperative system with relay selection under outdated CSI, the probability density function and the cumulative distribution function of the main channel’s SNR are given by:

$$f_{\gamma_M}^{\hat{h}}(x) = \sum_{n=1}^N \binom{N}{n} \frac{(-1)^{n-1}}{\bar{\gamma}_c[n(1 - \rho) + \rho]/n - \bar{\gamma}_{SD}} \times \left[ \exp\left(-\frac{nx}{\bar{\gamma}_c[n(1 - \rho) + \rho]}\right) - \exp\left(\frac{-x}{\bar{\gamma}_{SD}}\right) \right] \tag{43}$$

and

$$F_{\gamma_M}^{\hat{h}}(x) = 1 - \sum_{n=1}^N \binom{N}{n} \frac{(-1)^{n-1}}{\bar{\gamma}_c[n(1 - \rho) + \rho]/n - \bar{\gamma}_{SD}} \times \left[ \frac{\bar{\gamma}_c}{n} [n(1 - \rho) + \rho] \exp\left(\frac{-nx}{\bar{\gamma}_c[n(1 - \rho) + \rho]}\right) - \bar{\gamma}_{SD} \exp\left(\frac{-x}{\bar{\gamma}_{SD}}\right) \right] \tag{44}$$

where  $\rho$  is the correlation coefficient between the SNR of  $S \rightarrow R_n \rightarrow D$  link, at time  $t$  and the SNR of  $S \rightarrow R_n \rightarrow D$  link at time  $t + \tau$ , where  $0 \leq \rho \leq 1$  [20]. In fact, there is two

extreme cases, where  $\rho = 1$  corresponds to a perfect CSI case and  $\rho = 0$  corresponds to a completely outdated CSI case. It is also worthy to notify that for the wiretap channel’s SNR, the PDF and CDF expressions are the same as those given in expressions (23) and (24).

#### 4.1 Probability of non-zero secrecy capacity under outdated CSI

Similarly to the steps shown in Sect. 3, the expression for the probability of non-zero secrecy capacity under outdated CSI can be obtained from:

$$\Pr(C_s > 0) = \int_{x=0}^{+\infty} \int_{y=0}^x f_{\gamma_M}^{\hat{h}}(x) f_{\gamma_W}(y) dy dx \tag{45}$$

$$= \int_{x=0}^{+\infty} f_{\gamma_M}^{\hat{h}}(x) F_{\gamma_W}(x) dx.$$

By substituting (43) and (23) into (45), we obtain:

$$\Pr(C_s > 0) = \int_{x=0}^{+\infty} \left\{ \sum_{n=1}^N \binom{N}{n} \frac{(-1)^{n-1}}{\bar{\gamma}_c[n(1 - \rho) + \rho]/n - \bar{\gamma}_{SD}} \times \left[ \exp\left(-\frac{nx}{\bar{\gamma}_c[n(1 - \rho) + \rho]}\right) - \exp\left(\frac{-x}{\bar{\gamma}_{SD}}\right) \right] \right\} \times \left\{ \sum_{i=0}^K \binom{K}{i} \sum_{j=0}^i \binom{i}{j} \left(\frac{\bar{\gamma}_{SE}}{\bar{\gamma}_{RE} - \bar{\gamma}_{SE}}\right)^{i-j} \times \left(\frac{\bar{\gamma}_{RE}}{\bar{\gamma}_{RE} - \bar{\gamma}_{SE}}\right)^j (-1)^j \exp\left[-\left(\frac{i-j}{\bar{\gamma}_{SE}} + \frac{j}{\bar{\gamma}_{RE}}\right)x\right] \right\} dx. \tag{46}$$

We solve the integrals in (46), and we obtain a closed-form expression for probability of non-zero secrecy capacity, as follows:

$$\Pr(C_s > 0) = \sum_{n=1}^N \binom{N}{n} \frac{(-1)^{n-1}}{\bar{\gamma}_c[n(1 - \rho) + \rho]/n - \bar{\gamma}_{SD}} \times \sum_{i=0}^K \binom{K}{i} \sum_{j=0}^i \binom{i}{j} \left(\frac{\bar{\gamma}_{SE}}{\bar{\gamma}_{RE} - \bar{\gamma}_{SE}}\right)^{i-j} \left(\frac{-\bar{\gamma}_{RE}}{\bar{\gamma}_{RE} - \bar{\gamma}_{SE}}\right)^j (-1)^j \times \left[ \left(\frac{n}{\bar{\gamma}_c[n(1 - \rho) + \rho]} + \frac{i-j}{\bar{\gamma}_{SE}} + \frac{j}{\bar{\gamma}_{RE}}\right)^{-1} - \left(\frac{1}{\bar{\gamma}_{SD}} + \frac{i-j}{\bar{\gamma}_{SE}} + \frac{j}{\bar{\gamma}_{RE}}\right)^{-1} \right]. \tag{47}$$

#### 4.2 Secrecy Outage Probability under Outdated CSI

Similarly to the steps followed in Section 3, the expression for the secrecy outage probability of the system under outdated CSI can be obtained from:

$$P_{out}(R_s) = \int_{y=0}^{\infty} F_{\gamma_M}(\lambda - 1 + \lambda y) f_{\gamma_W}(y) dy, \tag{48}$$

where  $\lambda = 2^{2R_s}$ . Substituting (44) and (24) into (48) yields:

$$P_{out}(R_s) = \int_{y=0}^{\infty} \left\{ 1 - \sum_{n=1}^N \binom{N}{n} \frac{(-1)^{n-1}}{\bar{\gamma}_c[n(1-\rho) + \rho]/n - \bar{\gamma}_{SD}} \times \left[ \frac{\bar{\gamma}_c}{n} [n(1-\rho) + \rho] \exp\left(\frac{-n(\lambda-1 + \lambda y)}{\bar{\gamma}_c[n(1-\rho) + \rho]}\right) - \bar{\gamma}_{SD} \exp\left(\frac{-(\lambda-1 + \lambda y)}{\bar{\gamma}_{SD}}\right) \right] \right\} \times \left\{ \sum_{i=0}^K \binom{K}{i} \sum_{j=0}^i \binom{i}{j} \left(\frac{\bar{\gamma}_{SE}}{\bar{\gamma}_{RE} - \bar{\gamma}_{SE}}\right)^{i-j} \left(\frac{\bar{\gamma}_{RE}}{\bar{\gamma}_{RE} - \bar{\gamma}_{SE}}\right)^j \times (-1)^{j+1} \left(\frac{i-j}{\bar{\gamma}_{SE}} + \frac{j}{\bar{\gamma}_{RE}}\right) \exp\left[-\left(\frac{i-j}{\bar{\gamma}_{SE}} + \frac{j}{\bar{\gamma}_{RE}}\right)y\right] \right\} dy. \tag{49}$$

Solving the integrals in (49), yields the closed-form expression for the secrecy outage probability of the system under outdated CSI, which can be written as

$$P_{out}(R_s) = 1 - \sum_{n=1}^N \binom{N}{n} \frac{(-1)^{n-1}}{\bar{\gamma}_c[n(1-\rho) + \rho]/n - \bar{\gamma}_{SD}} \times \sum_{i=0}^K \sum_{j=0}^i \binom{K}{i} \binom{i}{j} \left(\frac{\bar{\gamma}_{SE}}{\bar{\gamma}_{RE} - \bar{\gamma}_{SE}}\right)^{i-j} \left(\frac{\bar{\gamma}_{RE}}{\bar{\gamma}_{RE} - \bar{\gamma}_{SE}}\right)^j \times (-1)^{j+1} \left(\frac{i-j}{\bar{\gamma}_{SE}} + \frac{j}{\bar{\gamma}_{RE}}\right) \times \left[\frac{\bar{\gamma}_c}{n} [n(1-\rho) + \rho] \times \left(\frac{n 2^{2R_s}}{\bar{\gamma}_c[n(1-\rho) + \rho] + \frac{i-j}{\bar{\gamma}_{SE}} + \frac{j}{\bar{\gamma}_{RE}}}\right)^{-1} \times \exp\left(\frac{-n(2^{2R_s} - 1)}{\bar{\gamma}_c[n(1-\rho) + \rho]}\right) - \bar{\gamma}_{SD} \left(\frac{2^{2R_s}}{\bar{\gamma}_{SD}} + \frac{i-j}{\bar{\gamma}_{SE}} + \frac{j}{\bar{\gamma}_{RE}}\right)^{-1} \exp\left(-\frac{2^{2R_s} - 1}{\bar{\gamma}_{SD}}\right) \right]. \tag{50}$$

### 4.3 Average secrecy capacity under outdated CSI

The expression for the average secrecy of the system under outdated CSI can be obtained following similar steps given in Section 3 (using (34)), which can be written as

$$\bar{C}_s = \frac{1}{2} (I_1 - I_2) = \frac{1}{2} \int_{x=0}^{\infty} \log_2(1+x) f_{\gamma_M}^{\wedge}(x) F_{\gamma_W}(x) dx - \frac{1}{2} \int_{y=0}^{\infty} \log_2(1+y) f_{\gamma_W}(y) [1 - F_{\gamma_M}^{\wedge}(y)] dy. \tag{51}$$

By inserting (43), (44), (23) and (24) into (51) and using  $\int_0^{\infty} \ln(1+x) \exp(-\mu x) dx = \frac{1}{\mu} \exp(\mu) E_1(\mu)$ , we solve the integrals and we obtain the following expression for the average secrecy capacity:

$$\bar{C}_s = \frac{0.5}{\ln(2)} \sum_{n=1}^N \binom{N}{n} \frac{(-1)^{n-1}}{\bar{\gamma}_c[n(1-\rho) + \rho]/n - \bar{\gamma}_{SD}} \sum_{i=0}^K \binom{K}{i} \times \sum_{j=0}^i \binom{i}{j} \left(\frac{\bar{\gamma}_{SE}}{\bar{\gamma}_{RE} - \bar{\gamma}_{SE}}\right)^{i-j} \left(\frac{\bar{\gamma}_{RE}}{\bar{\gamma}_{RE} - \bar{\gamma}_{SE}}\right)^j \times (-1)^j \left[ \frac{\left(\frac{i-j}{\bar{\gamma}_{SE}} + \frac{j}{\bar{\gamma}_{RE}}\right) \left(\frac{\bar{\gamma}_c[n(1-\rho) + \rho]}{n}\right) + 1}{\frac{\bar{\gamma}_c[n(1-\rho) + \rho]}{n} + \frac{i-j}{\bar{\gamma}_{SE}} + \frac{j}{\bar{\gamma}_{RE}}} \right] \times \exp\left(\frac{n}{\bar{\gamma}_c[n(1-\rho) + \rho] + \frac{i-j}{\bar{\gamma}_{SE}} + \frac{j}{\bar{\gamma}_{RE}}}\right) \times E_1\left(\frac{n}{\bar{\gamma}_c[n(1-\rho) + \rho] + \frac{i-j}{\bar{\gamma}_{SE}} + \frac{j}{\bar{\gamma}_{RE}}}\right) - \frac{\bar{\gamma}_{SD} \left(\frac{i-j}{\bar{\gamma}_{SE}} + \frac{j}{\bar{\gamma}_{RE}}\right) + 1}{\frac{1}{\bar{\gamma}_{SD}} + \frac{i-j}{\bar{\gamma}_{SE}} + \frac{j}{\bar{\gamma}_{RE}}} \exp\left(\frac{1}{\bar{\gamma}_{SD}} + \frac{i-j}{\bar{\gamma}_{SE}} + \frac{j}{\bar{\gamma}_{RE}}\right) \times E_1\left(\frac{1}{\bar{\gamma}_{SD}} + \frac{i-j}{\bar{\gamma}_{SE}} + \frac{j}{\bar{\gamma}_{RE}}\right) \Big]. \tag{52}$$

It is worthy to mention that, considering  $\rho = 1$  (which corresponds to the perfect CSI), expressions (47), (50) and (52), reduce to the expressions (27), (32) and (41), which were obtained for the perfect CSI case in Sect. 3. In other extreme case, setting  $\rho = 0$  (which corresponds to the completely outdated CSI), into expressions (47), (50) and (52) yield the corresponding expressions for the PHY secrecy of AF relaying system with one relay in the presence of multiple eavesdroppers. This implies that under completely outdated CSI, relay selection is equivalent to the random relay selection, where no diversity advantage can be achieved from using multiple relays.

## 5 Simulation and numerical results

In this section, we provide numerical and simulation results for three important PHY secrecy performance metrics for the considered AF relaying system, namely, the probability of non-zero secrecy capacity, the secrecy outage probability and the average secrecy capacity under different parameters. Numerical results are obtained from derived expressions (27), (32), (41), (47), (50) and (52), where to verify the validity of the numerical results and the analysis, we also provide Monte-Carlo simulation results. We considered the path loss for the channel to be  $\alpha = 0$  in all Figures. We also assumed that the links corresponding to the main channel have the same average SNR values, i.e.,  $\bar{\gamma}_{SD} = \bar{\gamma}_{SR_n} = \bar{\gamma}_{R_nD}$ , for  $n = 1, 2, \dots, N$ , but the SNRs associated to the eavesdroppers  $\bar{\gamma}_{SE}$  and  $\bar{\gamma}_{RE}$  may have different SNR values.



The simulation results are obtained as follows: First, using Monte Carlo simulations, we generate several realizations of the random Rayleigh distributed channel coefficients. For the outdated CSI case, we use the formula described in (42), in which we first generate several realizations of the random Rayleigh distributed channel coefficients  $h$ , and generate  $\epsilon$  that is a complex Gaussian noise  $\mathcal{CN}(0, \sigma_h^2)$ , then we obtain outdated channel coefficient  $\hat{h}$ . We then, calculate instant SNR values for each time-slot, i.e.. the values for  $\gamma_{SD}, \gamma_{SR_n}, \gamma_{R_nD}$ , the SNRs associated to the eavesdroppers  $\gamma_{SE}$ , and  $\gamma_{RE}$ . Then, we obtain the instant SNR values for  $\gamma_M$ , and  $\gamma_w$  using (15) and (17). Then, using (25), we obtain several instantaneous values for the secrecy capacity  $C_s$ . Finally, for the given system parameters, defined for each figure, and using the obtained several realizations of the secrecy capacity, the average secrecy capacity (ASC), and the probability of non-zero secrecy capacity (PNZSC), the secrecy outage probability (SOP) are calculated for a total number larger than  $10^7$  channel realizations, where  $ASC = \text{mean}(C_s)$ ,  $PNZSC = \Pr(C_s > 0)$ , and  $\mathcal{P}_{out}(R_s) = \Pr(C_s \leq R_s)$ , have been used.

Fig. 2 shows the probability of non-zero secrecy capacity versus  $\bar{\gamma}_{SD}$ , for the system assuming  $N = 5$  relays and  $K = 5$  eavesdroppers. We observe that increasing  $\bar{\gamma}_{SD}$ , yields an increase in the probability non-zero secrecy capacity. Also, we can observe that increasing  $\bar{\gamma}_{SE}$  and/or  $\bar{\gamma}_{RE}$  cause a decrease in the probability of non-zero secrecy capacity, as expected.

Fig. 3 shows the secrecy outage probability versus  $\bar{\gamma}_{SD}$  for the system with  $N = 5$  relays and  $K = 5$  eavesdroppers and  $R_s = 0.1$  bits/s/Hz. We observe that increasing  $\bar{\gamma}_{SD}$ , decreases the secrecy outage probability. We also observe that increasing  $\bar{\gamma}_{SE}$  and  $\bar{\gamma}_{RE}$  increases the secrecy outage probability of the system.

Fig. 4 shows the secrecy outage probability versus  $\bar{\gamma}_{SD}$  with  $\bar{\gamma}_{SE} = 5$  dB,  $\bar{\gamma}_{RE} = 10$  dB,  $K = 5$  eavesdroppers and

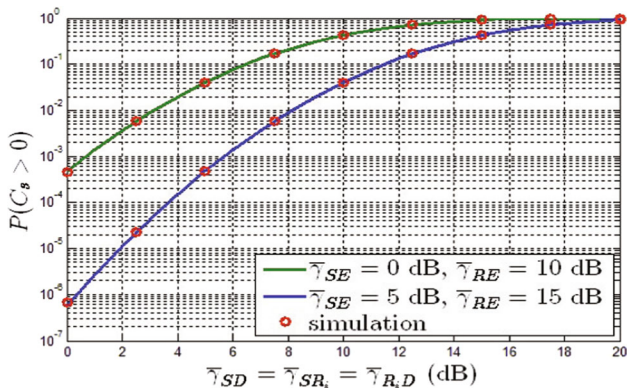


Fig. 2 Probability of non-zero secrecy capacity versus  $\bar{\gamma}_{SD}$  with  $N = K = 5$

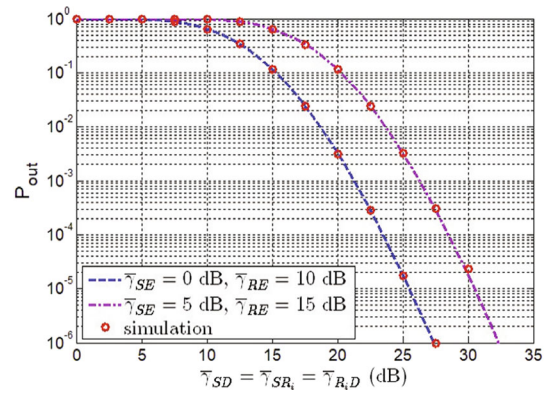


Fig. 3 Secrecy outage probability versus  $\bar{\gamma}_{SD}$  with  $N = K = 5$  and  $R_s = 0.1$  bits/s/Hz

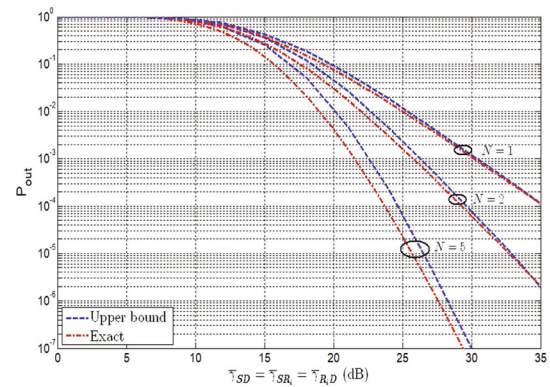
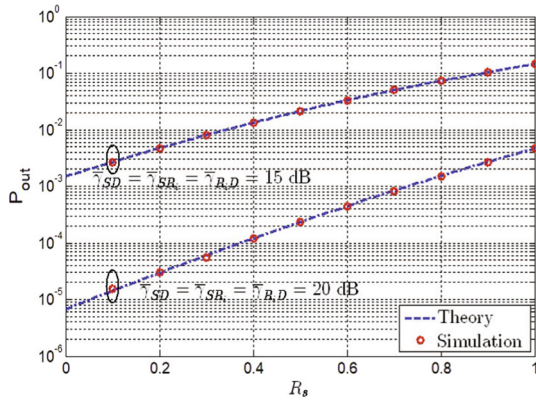


Fig. 4 Secrecy outage probability versus  $\bar{\gamma}_{SD}$  with  $\bar{\gamma}_{SE} = 5$  dB,  $\bar{\gamma}_{RE} = 10$  dB,  $K = 5$  and  $R_s = 0.1$  bits/s/Hz

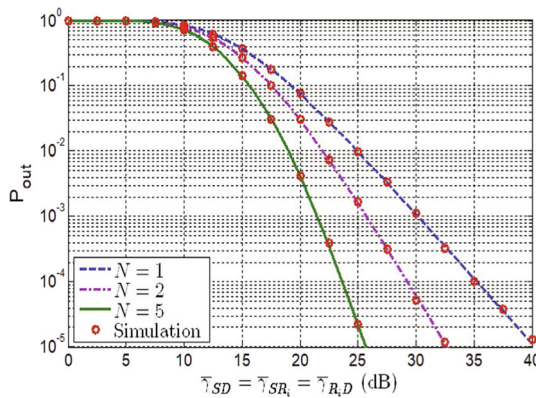
$R_s = 0.1$  bits/s/Hz, for different number of relays  $N$ . It can be observed that, increasing the number of available relays, decreases the secrecy outage probability. To show the tightness of the upper bound approximation SNR, the SOP results are obtained for both cases of the upper bound approximate SNR  $\gamma_{SR_nD} = \min(\gamma_{SR_n}, \gamma_{R_nD})$  and the exact SNR expression  $\gamma_{SR_nD} = \frac{\gamma_{SR_n}\gamma_{R_nD}}{1+\gamma_{SR_n}+\gamma_{R_nD}}$ , which is obtained via simulations. We observe that the approximate results are tight enough to the exact results, especially at the medium to high SNRs.

Fig. 5 shows the secrecy outage probability versus  $R_s$  with  $N = K = 5$ ,  $\bar{\gamma}_{SE} = 0$  dB and  $\bar{\gamma}_{RE} = 5$  dB. We observe that increasing  $R_s$ , increases the secrecy outage probability. Also we can see that increasing  $\bar{\gamma}_{SE}$  and  $\bar{\gamma}_{RE}$  increases the secrecy outage probability.

The secrecy outage probability versus  $\bar{\gamma}_{SD}$  is shown in Fig. 6, where it is assumed that  $K = 5$ ,  $R_s = 0.1$  bits/s/Hz,  $\bar{\gamma}_{SE} = 0$  dB and  $\bar{\gamma}_{RE} = 5$  dB. It can be observed that increasing the number of available relays decreases the secrecy outage probability and therefore, the physical layer security is significantly improved.

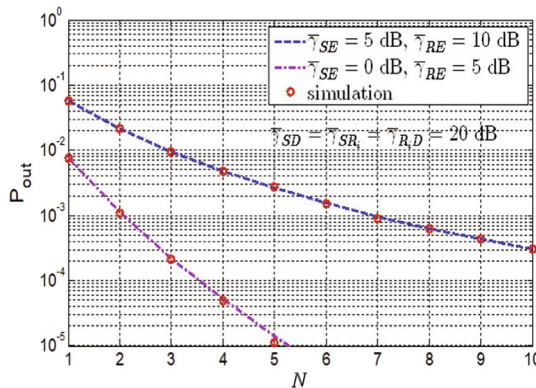


**Fig. 5** Secrecy outage probability versus  $R_s$  with  $N = K = 5$ ,  $\bar{\gamma}_{SE} = 0$  dB and  $\bar{\gamma}_{RE} = 5$  dB

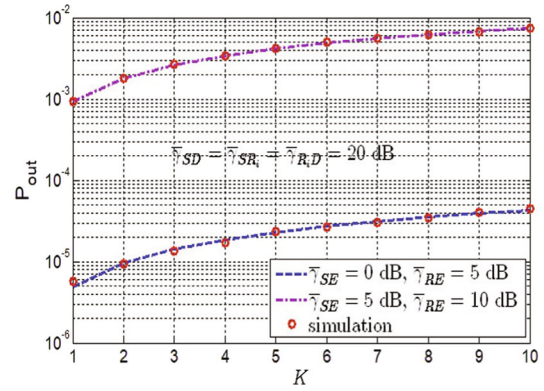


**Fig. 6** Secrecy outage probability versus  $\bar{\gamma}_{SD}$  with  $K = 5$ ,  $R_s = 0.1$  bits/s/Hz,  $\bar{\gamma}_{SE} = 0$  dB and  $\bar{\gamma}_{RE} = 5$  dB

The secrecy outage probability versus  $N$  and  $K$ , are shown in Fig. 7 and Fig. 8, respectively, where  $R_s = 0.1$  bits/s/Hz and  $\bar{\gamma}_{SD} = 20$  dB are assumed. We observe that increasing  $N$  the number of relays, decreases the secrecy outage probability. It is also observed that the secrecy outage probability increases with the number of eavesdroppers.



**Fig. 7** Secrecy outage probability versus the number of relays  $N$  with  $K = 5$ ,  $R_s = 0.1$  bits/s/Hz and  $\bar{\gamma}_{SD} = 20$  dB



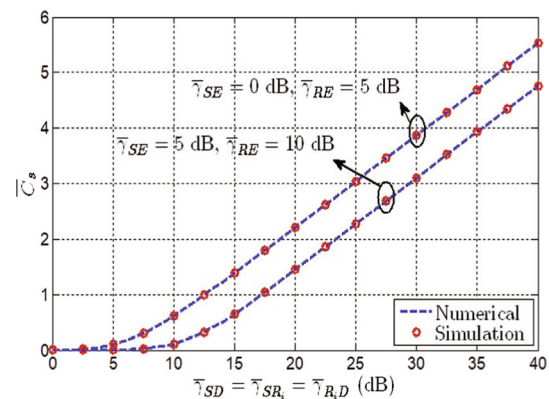
**Fig. 8** Secrecy outage probability versus the number of eavesdroppers  $K$  with  $N = 5$ ,  $R_s = 0.1$  and  $\bar{\gamma}_{SD} = 20$  dB

Fig. 9 and Fig. 10 show the average secrecy capacity. We observe that increasing  $\bar{\gamma}_{SD}$  and/or  $N$ , increases the average secrecy capacity. Also, it can be observed that increasing  $\bar{\gamma}_{SE}$  and  $\bar{\gamma}_{RE}$  decreases the average secrecy capacity.

In Fig. 2 to Fig. 10, the results are obtained assuming that the CSI used for relay selection is perfect. However, in the following, we provide the results of PHY secrecy performance under outdated CSI.

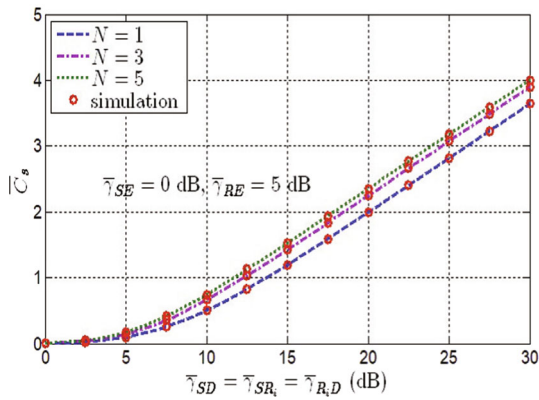
Fig. 11 shows the probability of non-zero secrecy capacity as a function of  $\bar{\gamma}_{SD}$ , with  $N = 5$  relays and  $K = 3$  eavesdroppers. We observe that increasing  $\bar{\gamma}_{SD}$ , increases the probability of non-zero secrecy capacity and also increasing  $\bar{\gamma}_{SE}$  and  $\bar{\gamma}_{RE}$ , decreases the probability of non-zero secrecy capacity. Also, we can observe that decreasing  $\rho$  which corresponds to the case where CSI becomes more outdated, cause a decrease in the probability of non-zero secrecy capacity.

Fig. 12 and Fig. 13 show the secrecy outage probability versus  $\bar{\gamma}_{SD}$  for  $K = 1$  and  $K = 3$  eavesdroppers, respectively, and  $N = 5$  relays,  $\bar{\gamma}_{SE} = 0$  dB,  $\bar{\gamma}_{RE} = 5$  dB and  $R_s = 0.1$  bits/s/Hz for different value of  $\rho$ . Increasing  $\bar{\gamma}_{SD}$ , decreases the secrecy outage probability and increasing  $K$ ,

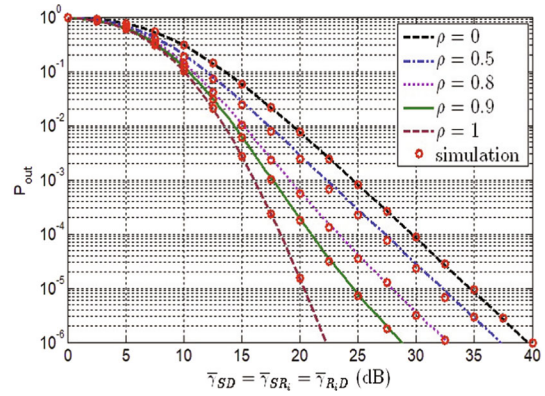


**Fig. 9** Average secrecy capacity versus  $\bar{\gamma}_{SD}$  with  $N = K = 5$

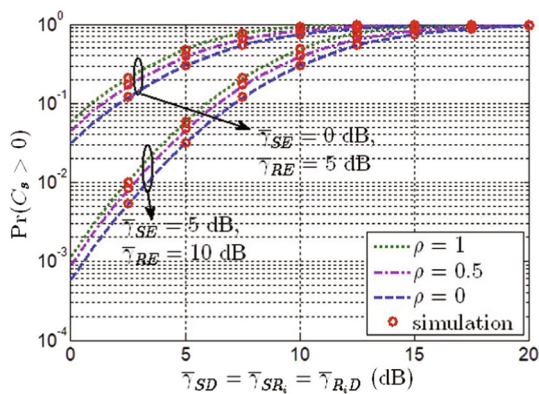




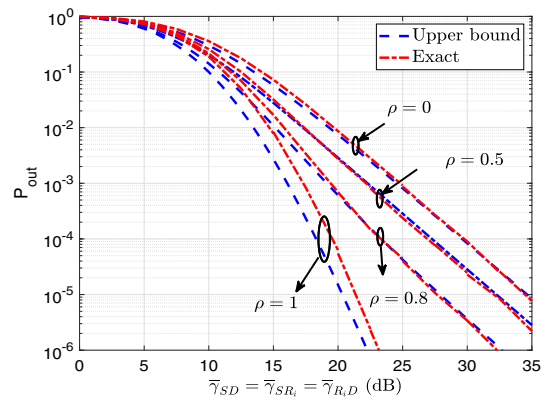
**Fig. 10** Average secrecy capacity versus  $\bar{\gamma}_{SD}$  with  $K = 5$ ,  $\bar{\gamma}_{SE} = 0$  dB and  $\bar{\gamma}_{RE} = 5$  dB



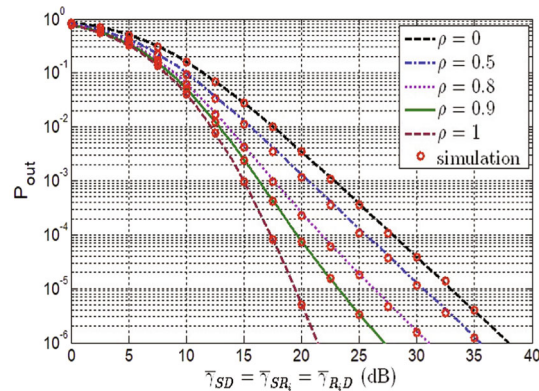
**Fig. 13** Secrecy outage probability versus  $\bar{\gamma}_{SD}$  for  $N = 5$ , and  $K = 3$ ,  $\bar{\gamma}_{SE} = 0$  dB,  $\bar{\gamma}_{RE} = 5$ , and  $R_s = 0.1$  bits/s/Hz



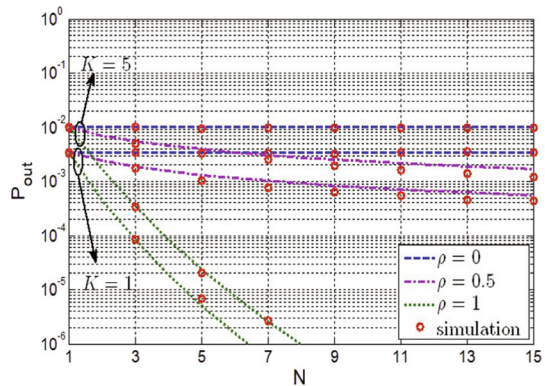
**Fig. 11** Probability of non-zero secrecy capacity versus  $\bar{\gamma}_{SD}$  for  $N = 5$  and  $K = 3$



**Fig. 14** Secrecy outage probability versus  $\bar{\gamma}_{SD}$  with  $\bar{\gamma}_{SE} = 0$  dB,  $\bar{\gamma}_{RE} = 5$  dB,  $N = 5$ ,  $K = 3$  and  $R_s = 0.1$  bits/s/Hz



**Fig. 12** Secrecy outage probability versus  $\bar{\gamma}_{SD}$  for  $N = 5$ ,  $K = 1$ ,  $\bar{\gamma}_{SE} = 0$  dB,  $\bar{\gamma}_{RE} = 5$  and  $R_s = 0.1$  bits/s/Hz



**Fig. 15** Secrecy outage probability versus  $N$  relays with  $\bar{\gamma}_{SD} = \bar{\gamma}_{SR_i} = \bar{\gamma}_{R_i,D} = 20$  dB,  $\bar{\gamma}_{SE} = 0$  dB,  $\bar{\gamma}_{RE} = 5$  and  $R_s = 0.1$  bits/s/Hz

increases the secrecy outage probability. Also, it can be observed that increasing  $\rho$  decreases the secrecy outage probability. Moreover, it can be seen that for  $\rho = 0$ , the secrecy outage probability is equal to that of the considered AF relay system with one relay, indicating that with  $\rho = 0$ , no diversity advantage can be achieved from relay selection. In the other extreme case, with  $\rho = 1$  (perfect CSI),

the diversity order is equal to  $N + 1$ , as expected. For  $0 \leq \rho < 1$  (outdated CSI), the outage probability curves have the same slope at high SNRs, implying that the diversity order in the outdated CSI is equal to 2 that is the

diversity order of the AF relaying system with a single relay and  $S \rightarrow D$  direct channel.

In order to show the tightness of the upper bound approximation SNR  $\gamma_{SR_nD} \simeq \min(\gamma_{SR_n}, \gamma_{R_nD})$  to the exact SNR expression  $\gamma_{SR_nD} = \frac{\gamma_{SR_n} \gamma_{R_nD}}{1 + \gamma_{SR_n} + \gamma_{R_nD}}$ , in Fig. 14, the simulation results for the secrecy outage probability versus  $\bar{\gamma}_{SD}$  are given assuming that  $\bar{\gamma}_{SE} = 5$  dB,  $\bar{\gamma}_{RE} = 10$  dB,  $K = 5$  eavesdroppers and  $R_s = 0.1$  bits/s/Hz, for different values of  $\rho$ . We can see that the approximate results are tight enough to the exact results, especially at the medium to high SNR values.

Fig. 15 shows the secrecy outage probability versus  $N$  with  $\bar{\gamma}_{SD} = \bar{\gamma}_{SR_n} = \bar{\gamma}_{R_nD} = 20$  dB,  $\bar{\gamma}_{SE} = 0$  dB,  $\bar{\gamma}_{RE} = 5$  dB and  $R_s = 0.1$  bits/s/Hz. It can be seen that increasing  $K$ , causes an increase in the secrecy outage probability. Also, we can observe that increasing  $\rho$ , decreases the secrecy outage probability. However, when  $\rho$  decreases to ( $\rho = 0.5$ ), the improvement in the secrecy outage probability due to the increasing of  $N$ , is small because of poor channel knowledge. Moreover, when  $\rho = 0$ , increasing  $N$ , the secrecy outage probability does not increase, since the system behaves similar to the AF relay system with one relay and  $S \rightarrow D$  direct link.

Fig. 16 shows the secrecy outage probability versus  $\rho$  with  $N = 5$ ,  $K = 3$ ,  $\bar{\gamma}_{SE} = 0$  dB,  $\bar{\gamma}_{RE} = 5$  dB and  $R_s = 0.1$  bits/s/Hz. We observe that increasing  $\rho$ , decreases the secrecy outage probability.

The average secrecy capacity versus  $\bar{\gamma}_{SD}$  is shown Fig. 17 with  $N = 5$ ,  $K = 3$ ,  $\bar{\gamma}_{SE} = 0$  dB and  $\bar{\gamma}_{RE} = 5$  dB. We observe that increasing  $\bar{\gamma}_{SD}$  and/or  $\rho$ , increases the average secrecy capacity.

Fig. 18 shows the average secrecy capacity versus  $N$  with  $K = 3$ ,  $\bar{\gamma}_{SE} = 0$  dB and  $\bar{\gamma}_{RE} = 5$  dB. We can observe that in the case of completely outdated CSI,  $\rho = 0$ , by increasing  $N$ , the average secrecy capacity does not change.

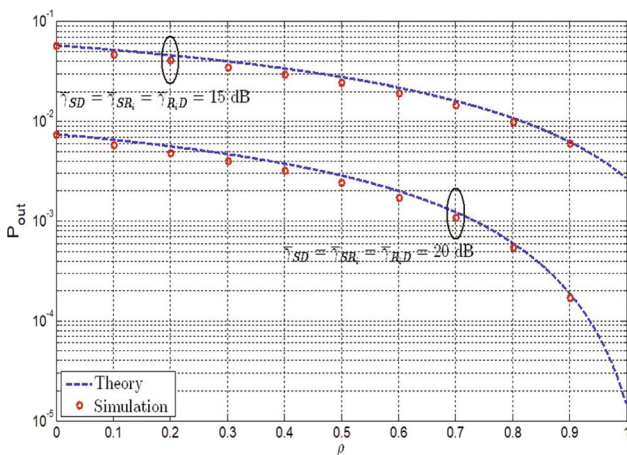


Fig. 16 Secrecy outage probability versus  $\rho$  with  $N = 5$ ,  $K = 3$ ,  $\bar{\gamma}_{SE} = 0$ dB,  $\bar{\gamma}_{RE} = 5$ dB and  $R_s = 0.1$  bits/s/Hz

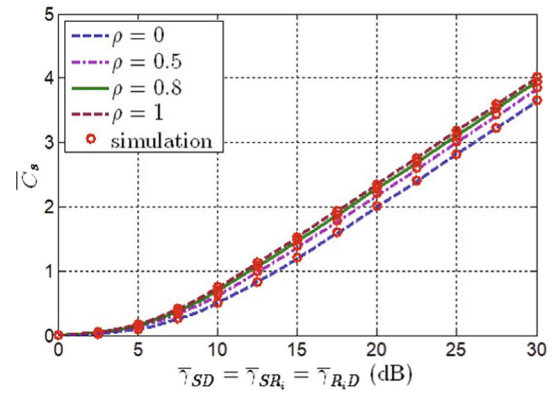


Fig. 17 Average secrecy capacity versus  $\bar{\gamma}_{SD}$  with  $N = 5$ ,  $K = 3$ ,  $\bar{\gamma}_{SE} = 0$ dB and  $\bar{\gamma}_{RE} = 5$  dB

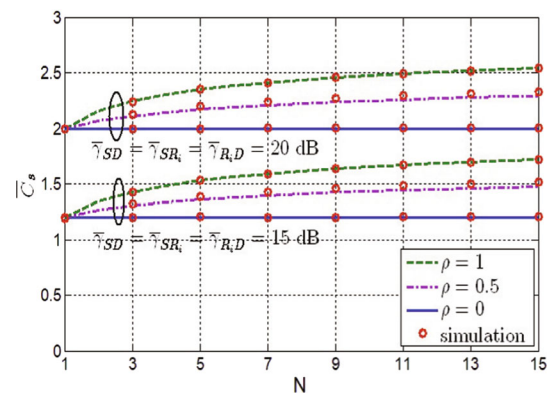


Fig. 18 Average secrecy capacity versus  $N$ , with  $K = 3$ ,  $\bar{\gamma}_{SE} = 0$  dB and  $\bar{\gamma}_{RE} = 5$  dB

This is the extreme case and implies that the relay selection based on the completely outdated CSI does not provide diversity to the system, as explained earlier.

In Fig. 2 to Fig. 18, it can be observed that the obtained numerical results obtained from theoretical mathematical formulas derived in this paper match closely with the simulation results, indicating the validity of the obtained mathematical expressions.

### 6 Conclusion

In this paper, we have analyzed and evaluated the PHY secrecy performance of an AF relaying system with relay selection under two cases, namely, perfect CSI and outdated CSI cases. We derived closed-form expressions for the probability of non-zero secrecy capacity, the average secrecy capacity and the secrecy outage probability. We provided numerical results to show the significant advantages of relay selection for improving the physical layer security. Moreover, we evaluated the effects of outdated

CSI for relay selection on the physical layer security of the AF relaying cooperative communications systems with relay selection. It is observed that when the information used to select the relay is outdated, the PHY secrecy performance can be deteriorated. We also used Monte-Carlo simulation to verify the validity of the obtained mathematical expressions.

## References

- Shannon, C. E. (1949). Communication theory of secrecy systems. *Bell system technical journal*, 28(4), 656–715.
- Wyner, A. D. (1975). The wire-tap channel. *Bell system technical journal*, 54(8), 1355–1387.
- Leung-Yan-Cheong, S., & Hellman, M. (1978). The gaussian wire-tap channel. *Information Theory, IEEE Transactions on*, 24(451–456), 08.
- Zou, Y., Zhu, J., Wang, X., & Leung, V. C. M. (2015). Improving physical-layer security in wireless communications using diversity techniques. *IEEE Network*, 29(1), 42–48.
- Zou, Y., Zhu, J., Wang, X., & Hanzo, L. (2016). A survey on wireless security: Technical challenges, recent advances, and future trends. *Proceedings of the IEEE*, 104(9), 1727–1765.
- Rawat, D. B., White, T., Parwez, M. S., Bajracharya, C., & Song, M. (2017). Evaluating secrecy outage of physical layer security in large-scale mimo wireless communications for cyber-physical systems. *IEEE Internet of Things Journal*, 4(6), 1987–1993.
- He, B., Ni, Q., Chen, J., Yang, L., & Lv, L. (2018). User-pair selection in multiuser cooperative networks with an untrusted relay. *IEEE Transactions on Vehicular Technology*, 68(1), 869–882.
- Harrison, W. K., Almeida, J., Bloch, M. R., McLaughlin, S. W., & Barros, J. (2013). Coding for secrecy: An overview of error-control coding techniques for physical-layer security. *IEEE Signal Processing Magazine*, 30(5), 41–50.
- Zhao, R., Lin, H., He, Y.-C., Chen, D.-H., Huang, Y., & Yang, L. (2017). Secrecy performance of transmit antenna selection for mimo relay systems with outdated csi. *IEEE Transactions on Communications*, 66(2), 546–559.
- Huang, Y., Al-Qahtani, F. S., Duong, T. Q., & Wang, J. (2015). Secure transmission in MIMO wiretap channels using general-order transmit antenna selection with outdated CSI. *IEEE Transactions on Communications*, 63(8), 2959–2971.
- Melki, R., Noura, H. N., Mansour, M. M., & Chehab, A. (2020). Physical layer security schemes for MIMO systems: an overview. *Wireless Networks*, 26(3), 2089–2111.
- BaghaeiPouri, A., & Torabi, M. (2019). Secrecy performance analysis of CIOD-OFDM systems over wireless fading channels. *Wireless Networks*, 1–14.
- BaghaeiPouri, A., & Torabi, M. (2019). OFDM/OQAM transmission with improved physical layer security. *Physical Communication*, 36, 100787.
- 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 & Tutorials*, 16(3), 1550–1573.
- BaghaeiPouri, A., & Torabi, M. (2020). Physical layer security in space-time block codes from coordinate interleaved orthogonal design. *IET Communications*, 14(12), 2007–2017.
- BaghaeiPouri, A., & Torabi, M. (2020). Analysis of secrecy outage performance of TAS-CIOD systems over wireless Rayleigh fading channels. *Physical Communication*, 101–129.
- Barros, J., & Rodrigues, M. R. (2006). Secrecy capacity of wireless channels. In *IEEE International Symposium on Information Theory*, (pp. 356–360), IEEE.
- Wang, P., Yu, G., & Zhang, Z. (2007). On the secrecy capacity of fading wireless channel with multiple eavesdroppers. In *IEEE International Symposium on Information Theory*, (pp. 1301–1305), IEEE.
- Torabi, M., Ajib, W., & Haccoun, D. (2009). Performance analysis of amplify-and-forward cooperative networks with relay selection over rayleigh fading channels. In *69th IEEE Vehicular Technology Conference, VTC-Spring*, (pp. 1–5), IEEE.
- Torabi, M., & Haccoun, D. (2011). Capacity of amplify-and-forward selective relaying with adaptive transmission under outdated channel information. *IEEE Transactions on Vehicular Technology*, 60(5), 2416–2422.
- Sarker, D. K., Sarkar, M. Z. I., & Anower, M. S. (2018). Secure wireless multicasting through AF-cooperative networks with best-relay selection over generalized fading channels. *Wireless Networks*, 1–14.
- 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.
- Zhao, Y., Adve, R., & Lim, T. J. (2006). Symbol error rate of selection amplify-and-forward relay systems. *IEEE Communications Letters*, 10(11), 757–759.
- Ferdinand, N. S., da Costa, D. B., & Latva-aho, M. (2013). Effects of outdated csi on the secrecy performance of miso wiretap channels with transmit antenna selection. *IEEE Communications Letters*, 17(5), 864–867.
- Fan, L., Lei, X., Yang, N., Duong, T. Q., & Karagiannidis, G. K. (2017). Secrecy cooperative networks with outdated relay selection over correlated fading channels. *IEEE Transactions on Vehicular Technology*, 66(8), 7599–7603.
- Torabi, M., & Haccoun, D. (2010). Capacity analysis of opportunistic relaying in cooperative systems with outdated channel information. *IEEE Communications Letters*, 14(12), 1137–1139.
- Kumar, R., & Chauhan, S. S. (2020). Physical layer security for space-time-block-coded MIMO system in Rician fading in the presence of imperfect feedback. *Wireless Networks*, 1–9.
- Torabi, M., Frigon, J.-F., & Haccoun, D. (2016). Impact of spatial correlation on the BER performance of cooperative wireless relay networks with OSTBC. *IET Commun.*, 10(8), 975–979.
- Anghel, P., & Kaveh, M. (2004). *Exact symbol error probability of a cooperative network in a Rayleigh-fading environment.*, 3, 1416–1421.
- Yan, Z., Ouyang, B., Zhang, X., & Liu, H. -L. (2019). Secrecy Outage Performance of Opportunistic Relay Selection with Limited CSI Feedback. *IEEE Wireless Communications Letters*.
- David, N. H. (2003). *Order statistics* (3rd ed.). New Jersey: Wiley.
- Suraweera, H. A., Smith, P. J., & Shafi, M. (2010). Capacity limits and performance analysis of cognitive radio with imperfect channel knowledge. *IEEE Transactions on Vehicular Technology*, 59(4), 1811–1822.

**Mohammad Torabi** received the Ph.D. degree in Electrical Engineering from Concordia University, Montreal, QC, Canada, in 2004. Then, he was a post-doctoral fellow at Concordia University. He was a post-doctoral fellow and was a research associate in the Department of Electrical Engineering, Polytechnique Montreal, QC, Canada. He was an Assistant Professor at the Department of Electrical Engineering, Shahid Beheshti University, Tehran, Iran. He is a Clinical Associate Professor in the School of Electrical Engineering and Computer Science, Washington State University, WA, USA. His current research interests include signal processing, communication theory, wireless communications and networking, optical communications, Internet of Things (IoT), and computer networks. He is a Senior Member of the IEEE.

**Sahar Parkouk** received the B.S. degree in electrical engineering from Hamedan University of Technology, and the M.S. degree in electrical engineering from Shahid Beheshti University. Her current

research interests are Physical Layer Security (PLS), Wireless networks, Vehicular Networks and Signal Processing.

**Saeed Shokrollahi** received his Ph.D. in software engineering from computer engineering and science department of Shahid Beheshti University. He spent his sabbatical leave at the security, privacy, and data protection laboratory (SPDP Lab), University of Milan, Crema, Italy. He is an assistant professor at Shahid Beheshti University, Tehran, Iran. His current research interests are Wireless Networks, Vehicular Networks, Internet of Things (IoT), Information Security and Access Control, Ultra-large-scale (ULS) Systems and Data Distribution Service (DDS).