

# Outage probability of selective decode and forward relaying with secrecy constraints

Xiaojun Sun, Chunming Zhao,  
National Mobile Communications Research Laboratory (NCRL),  
Southeast University, Nanjing 210096, CHINA  
Email: {sunxiaojun, cmzhao2}@seu.edu.cn

**Abstract**—We study the outage probability of opportunistic relay selection in decode-and-forward relaying with secrecy constraints. We derive the closed-form expression for the outage probability. Based on the analytical result, the asymptotic performance is then investigated. The accuracy of our performance analysis is verified by the simulation results.

## I. INTRODUCTION

Due to the broadcast nature of the transmission medium, wireless communications cause serious security issues in practice. Information-theoretic security has received much attention recently [1]-[9]. The information-theoretic security was pioneered by Wyner [1]. Later, the work in [2][3] extended Wyner's work to broadcast channels and Gaussian channels, respectively.

Recently, the information-theoretic secure communications has been generalized to wireless quasi-static fading channel [4]. The secure multiple antennas system was also studied in [5]. However, multiple antennas may not be available due to cost and size limitations. Under this scenario, cooperative network is an efficient approach to overcome this limitation. [6]-[9] discussed various relay or cooperative strategies to increase security against eavesdroppers, such as noise-forward [6], beam-forming [7], relay-jamming selection [8]. The prior work in [9] considered relay selection for secure DF cooperative communications. However, only the limiting value of the outage probability is known [9], which is meaningful only at high signal-to-noise ratios (SNRs). To the best of our knowledge, the exact expression for the outage probability is still unknown in selective decode-and-forward (DF) cooperation with secrecy constraints.

In this letter, we study the outage probability of selective DF cooperative secure communications over Rayleigh fading channels. As the main contribution, we derive the analytical expressions for the outage probability. Moreover, based on the analytical results, we also investigate the asymptotic performance in the high SNR regime. Simulation results verify the accuracy of our performance analysis.

## II. SYSTEM MODEL

The half-duplex DF relay wireless system in Fig. 1 consists of one source (S),  $N$  trusted relays (R), one destination (D) and one eavesdropper (E). Each node is equipped with single antenna.

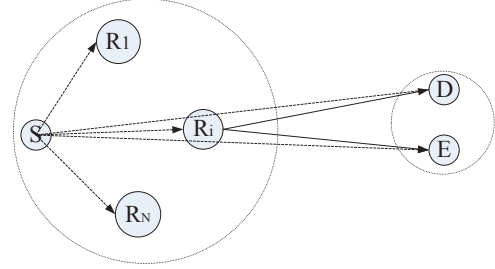


Fig. 1. Half-duplex DF relay wiretap channel model. In the first phase, S broadcasts the signal to all nodes (dotted lines). In the second phase, the best relay node retransmits the signal to D and E (solid lines).

The communication occurs in two hops. During the first hop, S broadcasts the information to all nodes. For simplicity but without loss of generality, we focus on the high SNR region where all the relay nodes successfully decode the source transmission [7]-[9]. During the second hop, relay selection based on instantaneous secrecy rate is performed. Let  $\gamma_{sd}$ ,  $\gamma_{se}$ ,  $\gamma_{rd}^n$  and  $\gamma_{re}^n$  denote the instantaneous SNR of the link  $S \rightarrow D$ ,  $S \rightarrow E$ ,  $R_i \rightarrow D$  and  $R_i \rightarrow E$ , respectively. All channels are subject to Rayleigh fading. Thus, the PDFs of the SNRs,  $f(\gamma_{sd})$ ,  $f(\gamma_{se})$ ,  $f(\gamma_{rd}^n)$  and  $f(\gamma_{re}^n)$ , are exponentially distributed with parameter  $\lambda_{sd}$ ,  $\lambda_{se}$ ,  $\lambda_m$  and  $\lambda_e$ , respectively.

In the second hops, only the relay node with the largest instantaneous secrecy rate is selected to forward the message to D. Thus, D and E can combine the two received signals using maximal ratio combining, respectively. Following the definition in [4], we write the instantaneous secrecy rate about  $n$ th-relay link as

$$\begin{aligned} R_s^n &= \max[\ln(1 + \gamma_{m,n}) - \ln(1 + \gamma_{e,n}), 0] \\ &= \max[\ln(Z_n), 0], \end{aligned} \quad (1)$$

where  $\gamma_{m,n} = \gamma_{rd}^n + \gamma_{sd}$  denotes the instantaneous SNR of the main channel,  $\gamma_{e,n} = \gamma_{re}^n + \gamma_{se}$  denotes the instantaneous SNR of the eavesdropping channel, and  $Z_n = 1 + \gamma_{m,n}/1 + \gamma_{e,n}$ . The output of the relay selection can be expressed as

$$Z_{\max} = \max\{Z_1, \dots, Z_N\} \quad (2)$$

with cumulative density function (CDF) as

$$F_{\max}(z) = \prod_{n=1}^N F_n(z), \quad (3)$$

$$\begin{aligned}
P_{out}(R) &= 1 - \frac{\lambda_{sd}}{e^R \lambda_{se} + \lambda_{sd}} \exp\left(-\frac{e^R - 1}{\lambda_{sd}}\right) + \left(\frac{e^R \lambda_e}{e^R \lambda_e + \lambda_m}\right)^N \frac{\left(\frac{1}{\lambda_{sd}} + \frac{N}{e^R \lambda_e}\right)^{-1}}{e^R \lambda_{se} + \lambda_{sd}} \exp\left(-\left(e^R - 1\right)\left(\frac{1}{\lambda_{sd}} + \frac{N}{e^R \lambda_e} - \frac{N}{\lambda_m}\right)\right) \\
&+ \sum_{n=1}^N C_n^N \left(\frac{-\lambda_m}{e^R \lambda_e + \lambda_m}\right)^n \exp\left(-\frac{n(e^R - 1)}{\lambda_m}\right) \frac{1}{e^R \lambda_{se} + \lambda_{sd}} \left[\frac{e^R \lambda_{se} \lambda_m}{n e^R \lambda_{se} + \lambda_m} + f\right],
\end{aligned} \tag{8}$$

where  $F_n(z)$  is the CDF of  $Z_n$ . After relay selection, the instantaneous secrecy rate can be given by

$$\begin{aligned}
R_s &= \max[\max(\ln(Z_n)), 0] = \max[\ln(\max(Z_n)), 0] \\
&= \max[\ln(Z_{\max}), 0].
\end{aligned} \tag{4}$$

This work characterizes the relay selection with secrecy constraints in terms of outage probability as follows.

### III. OUTAGE PROBABILITY OF RELAY SELECTION WITH SECRECY CONSTRAINTS

Outage probability is an important performance measure, widely used to characterize wireless communications. It is defined the probability that the instantaneous secrecy capacity falls below a target rate  $R$  as

$$P_{out}(R) = P_r(R_s \leq R) = F_{max}(e^R). \tag{5}$$

#### A. Relay selection without direct links

In this subsection, we follow the system model in [9], where S has no direct links with D and E.

In this case, the instantaneous SNR of the main channel and the eavesdropping channel is  $\gamma_{m,n} = \gamma_{rd}^n$  and  $\gamma_{e,n} = \gamma_{re}^n$ , respectively. Therefore, the CDF of  $Z_n$ ,  $F_n(z)$ , can be expressed as

$$\begin{aligned}
F_n(z) &= \int_0^\infty f(\gamma_{re}^n) d\gamma_{re}^n \int_0^{z\gamma_{re}^n + z - 1} f(\gamma_{rd}^n) d\gamma_{rd}^n \\
&= 1 - \exp\left(-\frac{z-1}{\lambda_m}\right) \frac{\lambda_m}{z\lambda_e + \lambda_m}.
\end{aligned} \tag{6}$$

Substituting (6) in (3),  $F_{\max}(z)$  can be solved. Thus, in the case of independent identically distributed (IID), using the binomial expansion, the outage probability for a target rate  $R$  is given by

$$P_{out}(R) = \sum_{n=0}^N C_n^N \left(\frac{-\lambda_m}{e^R \lambda_e + \lambda_m}\right)^n \exp\left(-\frac{n(e^R - 1)}{\lambda_m}\right), \tag{7}$$

where  $C_n^N = N!/n!(N-n)!$ .

#### B. Relay selection with direct links

We extend the system model in [9] by considering the direct links between S and D/E in this subsection.

In this scenario, the outage probability for a target rate  $R$  (8) is shown at the top of this page, where

$$f = \begin{cases} \frac{\lambda_{sd} \lambda_m \left[ \exp\left(\left(e^R - 1\right)\left(\frac{n}{\lambda_m} - \frac{1}{\lambda_{sd}}\right)\right) - 1 \right]}{n \lambda_{sd} - \lambda_m}, & n \lambda_{sd} \neq \lambda_m \\ e^R - 1, & n \lambda_{sd} = \lambda_m \end{cases} \tag{9}$$

*Proof:* The CDF of  $Z_n$ ,  $F_n(z)$ , can be expressed as

$$F_n(z) = P_r\left(\frac{1 + \gamma_{rd}^n + \gamma_{sd}}{1 + \gamma_{re}^n + \gamma_{se}} < z\right) = P_r(\gamma_{rd}^n < z\gamma_{re}^n + u), \tag{10}$$

where  $u = z\gamma_{se} - \gamma_{sd} + z - 1$ . The conditional CDF  $F_n(z|u)$  is calculated as follows.

In the case of  $u \geq 0$ , the conditional CDF  $F_n(z|u)$  is given by

$$\begin{aligned}
F_n(z|u) &= \int_0^\infty f(\gamma_{re}^n) d\gamma_{re}^n \int_0^{z\gamma_{re}^n + u} f(\gamma_{rd}^n) d\gamma_{rd}^n \\
&= 1 - \exp\left(-\frac{u}{\lambda_m}\right) \frac{\lambda_m}{z\lambda_e + \lambda_m}
\end{aligned} \tag{11}$$

On the other hand, in the case of  $u < 0$ , the conditional CDF  $F_n(z|u)$  can be expressed as

$$\begin{aligned}
F_n(z|u) &= \int_{-u/z}^\infty f(\gamma_{re}^n) d\gamma_{re}^n \int_0^{z\gamma_{re}^n + u} f(\gamma_{rd}^n) d\gamma_{rd}^n \\
&= \exp\left(\frac{u}{z\lambda_e}\right) \frac{z\lambda_e}{z\lambda_e + \lambda_m}.
\end{aligned} \tag{12}$$

Therefore, using the binomial expansion, we can express the conditional CDF  $F_{\max}(z|u)$  (maximum among  $N$  IID random variable) as

$$F_{\max}(z|u) = \begin{cases} \sum_{n=0}^N C_n^N \left(\frac{-\lambda_m}{z\lambda_e + \lambda_m}\right)^n \exp\left(-\frac{nu}{\lambda_m}\right), & u \geq 0 \\ \left(\frac{z\lambda_e}{z\lambda_e + \lambda_m}\right)^N \exp\left(\frac{Nu}{z\lambda_e}\right), & u < 0 \end{cases} \tag{13}$$

Through introducing  $v = z\gamma_{se} - \gamma_{sd}$ , we can obtain  $F_{\max}(z)$  in the following. The PDF  $f(v)$  of  $v$  is given by [10]

$$f(v) = \begin{cases} \frac{1}{z\lambda_{se} + \lambda_{sd}} \exp\left(-\frac{v}{z\lambda_{se}}\right), & v \geq 0 \\ \frac{1}{z\lambda_{se} + \lambda_{sd}} \exp\left(\frac{v}{\lambda_{sd}}\right), & v < 0 \end{cases} \tag{14}$$

Using (14),  $u = v + z - 1$  and after simplifications, we can express  $P_{out}(R)$  as (8). ■

#### C. Asymptotic outage probability

It is also important to examine the asymptotic behavior of the outage probability at the high SNRs, where  $\lambda_m \rightarrow \infty$  and  $\lambda_e \rightarrow \infty$  with a constant  $\kappa = \lambda_m/\lambda_e$ .

Without direct links, the asymptotic outage probability [9]

$$P_{out}^a(R) = \left(\frac{e^R}{e^R + \kappa}\right)^N. \tag{15}$$

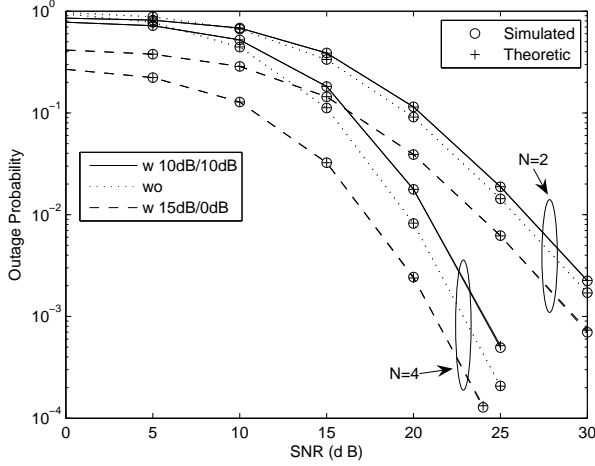


Fig. 2. Outage probability of  $R = 0.3$  V.S.  $\lambda_m$ . 'wo' denotes that S has no direct links with D/E. 'w xdB/ydB' denotes  $\lambda_{sd} = xdB$  and  $\lambda_{se} = ydB$ .

When S has direct links with D and E, we calculate the asymptotic outage probability as follows. From (8), for fixed SNRs  $\lambda_{sd}$  and  $\lambda_{se}$ , we have

$$P_{out}^a(R) = 1 - \frac{\lambda_{sd}}{e^R \lambda_{se} + \lambda_{sd}} \exp\left(-\frac{e^R - 1}{\lambda_{sd}}\right) + \left(\frac{e^R}{e^R + \kappa}\right)^N \frac{e^R \lambda_{sd}}{(e^R \lambda_{se} + \lambda_{sd})(e^R + \kappa_d)} + \sum_{n=1}^N \frac{C_n^N}{e^R \lambda_{se} + \lambda_{sd}} \left(\frac{-\kappa}{e^R + \kappa}\right)^n \left[ \frac{e^R \lambda_{se}}{ne^R \kappa_e + 1} + f_a \right] \quad (16)$$

where  $\kappa_d = \lambda_{sd}/\lambda_e$ ,  $\kappa_e = \lambda_{se}/\lambda_m$  and  $\kappa_m = \lambda_{sd}/\lambda_m$ . If  $n\kappa_m = 1$ ,  $f_a = e^R - 1$ ; else,  $f_a = \left(\exp\left(\frac{(e^R - 1)(n\kappa_m - 1)}{\lambda_{sd}}\right) - 1\right) \frac{\lambda_{sd}}{n\kappa_m - 1}$ . In the case of  $\lambda_{sd} \rightarrow \infty$  and  $\lambda_{se} \rightarrow \infty$  with a constant  $\kappa_s = \lambda_{sd}/\lambda_{se}$ , (16) is re-expressed as

$$P_{out}^a(R) = \frac{e^R}{e^R + \kappa_s} + \left(\frac{e^R}{e^R + \kappa}\right)^N \frac{e^R \kappa_s}{(e^R + \kappa_s)(e^R + N\kappa_d)} + \sum_{n=1}^N \frac{e^R C_n^N}{(e^R + \kappa_s)(ne^R \kappa_e + 1)} \left(\frac{-\kappa}{e^R + \kappa}\right)^n \quad (17)$$

If  $\kappa_d \rightarrow 0$ ,  $\kappa_e \rightarrow 0$  and  $\kappa_m \rightarrow 0$ , (16) and (17) can be re-expressed as (15). In this case, the effect of direct links is negligible.

#### IV. SIMULATION RESULTS

Figure 2 shows the outage probability of  $R = 0.3$  for  $\lambda_e = 15dB$  under different  $\lambda_m$  and relay nodes  $N$ . It can be observed that the experimental curves match exactly with the theoretical results. These curves show that the outage probability decreases with the increase of the number of relay nodes.

The asymptotic behavior of outage probability of  $R = 0.3$  as functions of  $\lambda_m$  under different relay nodes  $N$  is illustrated in Fig. 2. Here, SNR  $\lambda_e$  is equal to SNR  $\lambda_m$ . As can be seen from

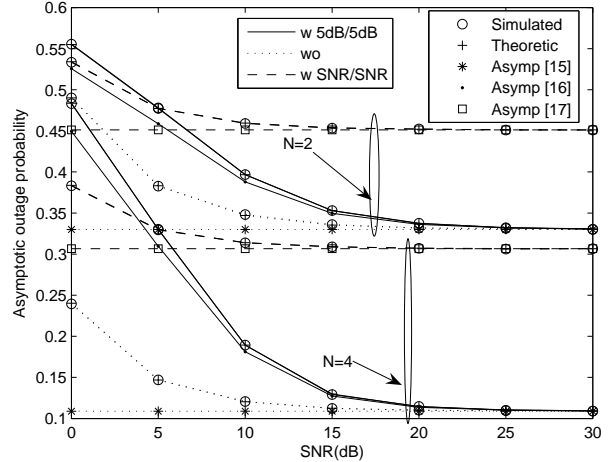


Fig. 3. Asymptotic outage probability of  $R = 0.3$  V.S.  $\lambda_m$ . 'wo' denotes that S has no direct links with D/E. 'w xdB/ydB' denotes  $\lambda_{sd} = xdB$  and  $\lambda_{se} = ydB$ . 'w SNR/SNR' denotes  $\lambda_{sd} = \lambda_{se} = \lambda_m$ .

Fig. 2, these plotted curves follow the above behavior. When  $\kappa_d, \kappa_e, \kappa_m \rightarrow 0$  with the increasing SNR  $\lambda_m$ , for example, SNRs  $\lambda_{sd}$  and  $\lambda_{se}$  are fixed to be 5dB, (16) converges to (15) as shown in Fig. 2. Furthermore, the asymptotic analysis efficiently converges to the true outage probability in the high SNR regime. We also observe that the effect of direct links is negligible in the high SNR regime when the ratios of SNRs,  $\kappa_d$ ,  $\kappa_e$  and  $\kappa_m$ , are very small.

#### V. CONCLUSION

We have derived closed-form expression for the outage probability of secure DF cooperative communications. It was shown that the relay selection can reduce the outage probability. The experimental curves are in excellent agreement with the theoretical results obtained in this work. The future work will consider the relay-jamming selection.

#### REFERENCES

- [1] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol.54, no.5, pp.1355-1367, Oct. 1975.
- [2] I. Csiszár and J. Körner, "Broadcast channels with confidential messages," *IEEE Trans. Info. Theory.*, vol.24, no.3, pp. 339-348, May 1978.
- [3] S. K. Leung-Yan-Cheong and M. E. Hellman, "The Gaussian wire-tap channel," *IEEE Trans. Inf. Theory.*, vol.24, no.4, pp. 451-456, Jul 1978.
- [4] M. Bloch, J. Barros, M. R. D. Rodrigues, and S. W. McLaughlin, "Wireless Information-Theoretic Security," *IEEE Trans. Info.Theory.*, vol.54, no.6, pp. 2515-2534, May 2008.
- [5] F. He, H. Man, and W. Wang, "Maximal ratio diversity combining enhanced security," *IEEE Commun. Lett.*, Vol.15, no.5, pp. 509 - 511, May 2011.
- [6] L. Lai and H. El Gamal, "The relay-eavesdropper channel: cooperation for secrecy," *IEEE Trans. Inf. Theory.*, vol.54, no.9, pp. 4005-4019, Sept 2008.
- [7] L. Dong, Z. Han, A. Petropulu, and H. V. Poor, "Improving wireless physical layer security via cooperating relays," *IEEE Trans. Signal.Process.*, vol.58, no.3, pp. 1875-1888, Mar 2010.
- [8] I. Krikidis, J. S. Thompson, and S. McLaughlin, "Relay Selection for Secure Cooperative Networks with Jamming," *IEEE Trans. Wireless.Comm.*, vol.8, no.10, pp. 5003-5011, Oct. 2009.
- [9] I. Krikidis, "Opportunistic relay selection for cooperative networks with secrecy constraints," *IET Commun.*, vol.4, no.15, pp. 1787-1791, 2010.
- [10] M. K. Simon, *Probability distributions involving Gaussian random variables*, Springer Press, 2006.