Performance Analysis of Decode-and-Forward System

ZHANG Wei[1,a], RUI Xian-yi[1,b]

[1]Institute of Electronic and Information Engineering, Soochow University, Suzhou 215006, China

[a] email:zhangwei20112015@163.com, [b] email: xyrui@suda.edu.cn

Keywords: Physical layer security; decode-and-forward; relay selection; secrecy outage probability

Abstract: For cooperative system, in which eavesdropper can be anywhere, so it may overhear information through both source and relay' transmission . In this letter, we evaluate the secrecy performance of decode-and- forward (DF) system with both the optimal relay selection (ORS) and the conventional relay selection (CRS) schemes, and the closed expression on the secrecy outage probability(SOP) of two schemes are derived; The derivations are confirmed through Monte Carlo simulations.

1. Introduction

The traditional technology of secure communication through high-level encryption[1] to ensure the secure transmission of information, but the use of secret key is too complex. Based on the theory of communication, [2] put forward the concept of physical layer security (PLS). [3] Introduces PLS into the Gauss channel. [4-5] studied the secrecy capacity and the secrecy rate of Multiple-Input Multiple-Output and Multiple-Input Single-Output systems. [6] put forward the transmit antenna selection scheme, and analyzed the security performance of system when the receiver uses selection combining and maximum ratio combining schemes respectively; it also derived the closed expression of SOP and approximation of SOP. The virtual array formed by relay nodes at different locations in the space can also improve the security performance of the system[7]. [8-9] studied how to maximize the security energy efficiency of system with eavesdropper through power control and relay selection. [10] studied the SOP and intercept probability of optimal relay selection under amplified-and-forward and decode-and-forward system respectively. Based on the above, this paper studies the relationship between the secrecy outage probability and relay selection of communication system.

2. System Model

It is assumed that there is a pair of legitimate source-destination nodes, multiple relay nodes, and an eavesdropper in the network which use DF protocol. The network model is as follow

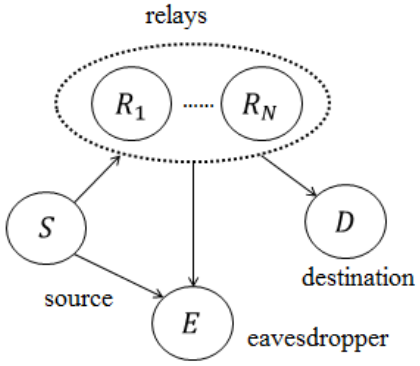

Figure 1 Cooperation communication network model

  DOI: 10.35532/JCES.V1.024

There is a source node S, a destination node D, N alternate relays nodes $R_1, R_2, \ldots R_N$, and an eavesdropper E in the network. Each node has only a single antenna, and operated in the half duplex mode which means the node cannot transmit and receive information simultaneously. Due to obstacles and other factors, a direct link between the source and the destination is assumed to be unavailable, and thus communication can only be established via relays [11]. Meanwhile eavesdropper can overhear the legitimate information from source and relay respectively, thus we get channels of $S \to R_i, S \to E, R_i \to D$ and $R_i \to E$ of system. We denote ρ_j, h_j as average channel gain and channel coefficient respectively, where $j \in \{SR, SE, RD, RE\}$.These channel gains are subjected to i.n.i.d Rayleigh fading. The noise associated with each channel is modeled as mutually independent additive white Gaussian noise (AWGN) with zero mean and variance N_0.The probability density function(PDF) and cumulative distribution function(CDF) of each channel gain are given as follows

$$f_{Y_j}(y) = \lambda_j \exp(-\lambda_j y) \tag{1}$$

$$F_{Y_j}(y) = 1 - \exp(-\lambda_j y) \tag{2}$$

Where $\lambda_j = 1/\rho_j$.

Firstly, the source node transmits the signal x with power P_s, and received signal in relay node and eavesdropper are given as follows respectively

$$y_{SR_i} = \sqrt{P_s} h_{SR_i} x + n_{SR} \tag{3}$$

$$y_{SE} = \sqrt{P_s} h_{SE} x + n_{SE} \tag{4}$$

Where n_{SR} and n_{SE} represent AWGN of corresponding channel respectively. Thus, the channel capacity from S to R_i is given by

$$C_{SR_i} = \frac{1}{2}\log_2(1 + \alpha Y_{SR_i}) \tag{5}$$

Where $\alpha = P_s / N_0$. And the channel capacity from S to E is given by

$$C_{SE} = \frac{1}{2}\log_2(1 + \alpha Y_{SE}) \tag{6}$$

Secondly, relay node forwards it's received signal to destination, and eavesdropper can also overhear the signal. The channel capacity from R_i to D and R_i to E are given as follows respectively

$$C_{R_iD} = \frac{1}{2}\log_2(1 + \beta Y_{R_iD}) \tag{7}$$

$$C_{R_iE} = \frac{1}{2}\log_2(1 + \beta Y_{R_iE}) \tag{8}$$

Where $\beta = P_r / N_0$, P_r represents the transmission power of relay.

The instantaneous signal to noise ratio of eavesdropper through maximum ratio combining can be given by $\gamma_E^b = \alpha Y_{SE} + \beta Y_{R_iE}$.Thus; the instantaneous secrecy capacity of system can be expressed as

$$C_S = \frac{1}{2}\log_2(1 + \beta Y_{R_iD}) - \frac{1}{2}\log_2(1 + \alpha Y_{SE} + \beta Y_{R_iE}) \tag{9}$$

3 Relay Selections and Secrecy Outage Probability

3.1 ORS scheme

When CSI of all channels are available, from (9) the ORS scheme is naturally proposed to select the relay that maximizes the system secrecy capacity. The optimal relay is

$$r = \arg\max_i [\frac{1}{2}\log_2(1+\beta Y_{R_iD}) - \frac{1}{2}\log_2(1+\alpha Y_{SE}+\beta Y_{R_iE})]^+$$

$$= \arg\max_i (\frac{1+\beta Y_{R_iD}}{1+\alpha Y_{SE}+\beta Y_{R_iE}}) \tag{10}$$

The secrecy capacity of ORS can be expressed as

$$C_S^{ORS} = \frac{1}{2}\log_2(\gamma_{eq}) \tag{11}$$

Where $\gamma_{eq} = \max_i(\gamma_{eq}^i) = \max_i(\frac{1+\beta Y_{R_iD}}{1+\alpha Y_{SE}+\beta Y_{R_iE}})$. The CDF of γ_{eq}^i under Y_{SE} can be expressed as

$$F_{\gamma_{eq}^i|Y_{SE}}(\gamma) = \int_0^\infty F_{RD}(\frac{\alpha\gamma}{\beta}Y_{SE} + \gamma y + \frac{\gamma-1}{\beta}) f_{Y_{RE}}(y)dy$$

$$= 1 - \frac{\lambda_{RE}}{\lambda_{RD}\gamma + \lambda_{RE}} \exp(-\lambda_{RD}(\frac{\alpha\gamma}{\beta}Y_{SE} + \frac{\gamma-1}{\beta})) \tag{12}$$

The CDF of γ_{eq} under Y_{SE} can be expressed as

$$F_{\gamma_{eq}|Y_{SE}}(\gamma) = \prod_i F_{\gamma_{eq}^i|Y_{SE}}(\gamma)$$

$$= \sum_{l=0}^{N} \frac{N!(-1)^l}{l!(N-l)!} (\frac{\lambda_{RE}}{\lambda_{RD}\gamma + \lambda_{RE}})^l \exp(-\lambda_{RD} l(\frac{\alpha\gamma}{\beta}Y_{SE} + \frac{\gamma-1}{\beta})) \tag{13}$$

Thus, the CDF of γ_{eq} can be expressed as

$$F_{\gamma_{eq}}(\gamma) = \int_0^\infty F_{\gamma_{eq}|Y_{SE}}(\gamma) f_{Y_{SE}}(y)dy$$

$$= \sum_{l=0}^{N} \frac{N!(-1)^l \beta\lambda_{SE}}{l!(N-l)!(\lambda_{RD} l\alpha\gamma + \beta\lambda_{SE})} (\frac{\lambda_{RE}}{\lambda_{RD}\gamma + \lambda_{RE}})^l \exp(-\lambda_{RD} l\frac{\gamma-1}{\beta}) \tag{14}$$

Secrecy outage probability is defined as the probability that the instantaneous secrecy rate of the system is less than a predefined rate R_s (in bps/Hz) [13]. Mathematically, SOP can be expressed as

$$P_{out} = \Pr(C_S \le R_S) \tag{15}$$

From (14) and (15), we derived the SOP of ORS

$$P_{out}^{ORS} = \sum_{l=0}^{N} \frac{N!}{l!(N-l)!} \times \frac{(-1)^l \lambda_{SE}}{\lambda_{RD} l\frac{\alpha}{\beta}\theta + \lambda_{SE}} (\frac{\lambda_{RE}}{\lambda_{RD}\theta + \lambda_{RE}})^l \exp(-\lambda_{RD} l\frac{\theta-1}{\beta}) \tag{16}$$

Where $\theta = 2^{2R_S}$.

3.2 CRS scheme

In ORS scheme, all CSI are available. However, only the CSI from R to D is available in CRS scheme [14]. The selected relay is

$$r = \arg\max_i (\beta Y_{R_i D}) \tag{17}$$

The secrecy capacity of CRS can be expressed as

$$C_S^{CRS} = \frac{1}{2}[\log_2(1+\gamma_D^{CRS}) - \log_2(1+\gamma_E^{CRS})]^+ \tag{18}$$

where $\gamma_D^{CRS} = \max_i (\beta Y_{R_i D})$, $\gamma_E^{CRS} = \alpha Y_{SE} + \beta Y_{R_i E}$. After a series of derivation, the CDF of γ_D^{CRS} can be expressed as

$$F_{\gamma_D^{CRS}}(\gamma) = \prod_i F_{Y_{R_i D}}(\frac{\gamma}{\beta}) = (1-\exp(-\lambda_{RD}\frac{\gamma}{\beta}))^N \tag{19}$$

And the PDF of γ_E^{CRS} can be expressed as

$$f_{\gamma_E^{CRS}}(y) = \frac{\lambda_{SE}\lambda_{RE}}{\alpha\lambda_{RE} - \beta\lambda_{SE}}(\exp(-\frac{\lambda_{SE}}{\alpha}y) - \exp((-\frac{\lambda_{RE}}{\beta}y)) \tag{20}$$

From (15),(19) and (20), we derived the SOP of CRS

$$P_{out}^{CRS} = \sum_{n=0}^{N} \frac{N!}{l!(N-l)!} \times \frac{(-1)^n \lambda_{SE}\lambda_{RE}}{\alpha\lambda_{RE} - \beta\lambda_{SE}} \times \exp(-n\lambda_{RD} l \frac{\theta-1}{\beta})(\frac{\alpha\beta}{n\alpha\lambda_{RD}\theta + \beta\lambda_{SE}} - \frac{\beta}{n\lambda_{RD}\theta + \lambda_{SE}}) \tag{21}$$

4 Simulations and Analysis

In this section, we provide simulation results to validate our analysis. The parameters are set as follows: $\rho_{SE} = 1$dB, $N_0 = 1$W, $R_S = 0.1$bps/Hz, and simulation precision is 10^5. In the following figures, the solid line represents the analytical results, and "*" represents the Monte Carlo simulation results. The analytical results are compared with the simulated results and a good agreement is obtained from the figures.

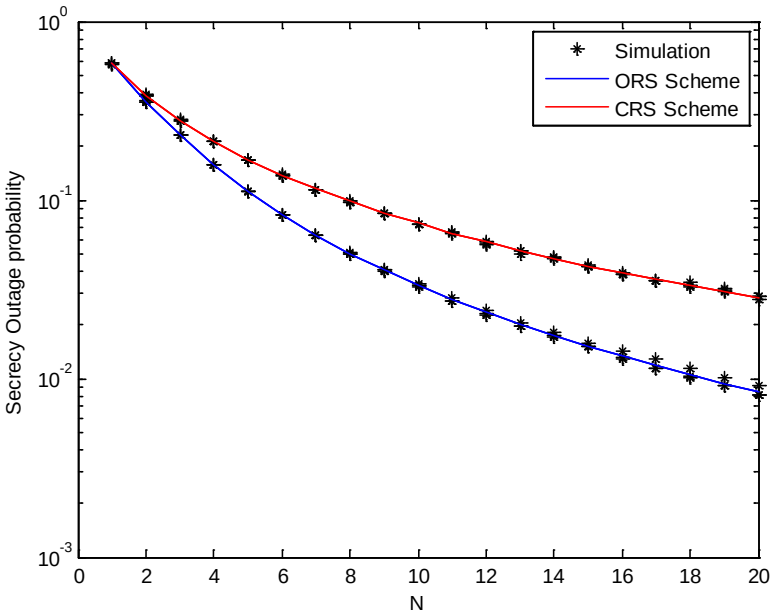

Figure 2 Secrecy outage probability versus N

In Figure 2, we assume $\rho_{SR} = \rho_{RD}$=5dB , ρ_{RE}=2dB , P_S=P_R =1dBW . We can observe two schemes have same SOP when $N = 1$. This is because there is no selection with only a relay node. It can be seen that the SOP of two schemes both decreases when N increases, so the secrecy performance of system can be improved by increasing relays. We can also observe that the secrecy performance of ORS scheme is better than CRS scheme when $N > 1$.

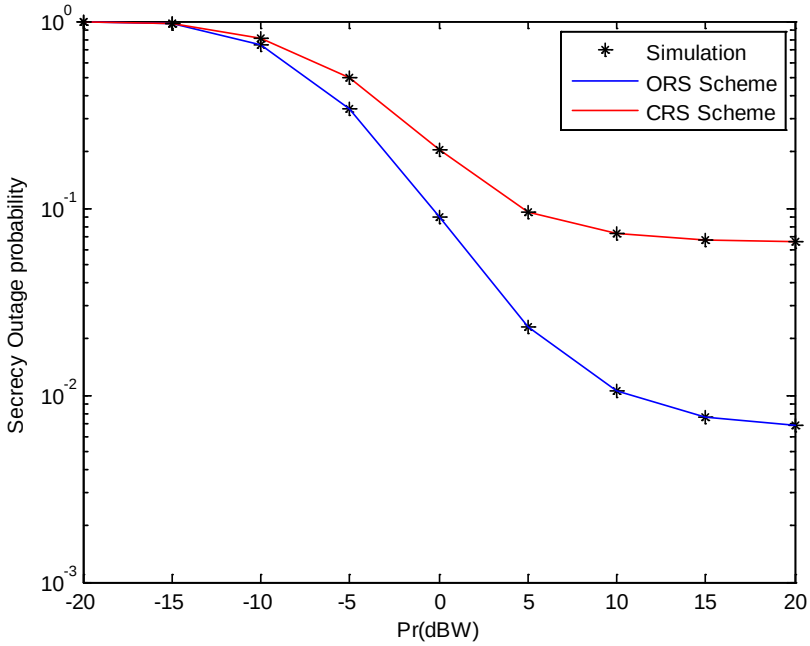

Figure 3 Secrecy outage probability versus Pr

In Figure 3, the parameters are set as follows: N=5 , $\rho_{SR} = \rho_{RD}$=5dB , ρ_{RE}=2dB , Ps = 1dBW. We can observe that the SOP of two schemes both decreases when Pr increases in somewhere and the SOP converges to a positive constant in the high Pr region. It means the secrecy capacity and the SOP of system are obviously bounded [14] .

5 Conclusion

In this letter, we derived the closed expressions of ORS and CRS schemes in multi relays cooperative communication system in which eavesdropper can overhear both source and relay. The simulations verified the analytical results. We can improve the secrecy performance of system by increasing relays and the transmission power within a certain range.

Acknowledgements

This work is supported by Natural Science Found of China (No.61201213).

References

[1] Delfs H, Knebl H. Introduction to Cryptography: Principles and Applications [M].2nd ed.Berlin , Germany : Spinger , 2007.

[2] Wyner A D.The Wire-tap Channel [J].Bell System Technical Journal , 1975 , 54(8) : 1355-1387.

[3] Leung Yan Cheong S K , Hellman M E. The Gaussian Wiretap Channel [J]. IEEE Transactions on Information Theory , 1978 , 24 (4) : 451-456 .

[4] Oggier F，Hassibi B． The Secrecy Capacity of the MIMO Wiretap Channel［J］. IEEE Transactions on Information Theory，2011，57(8):4961-4972.

[5] Pei M，Swindlehurst A L，Ma D，et al． On Ergodic Secrecy Rate for MISO Wiretap Broadcast Channels with

Opportunistic Scheduling ［J］. IEEE Communications Letters，2014，18(1):50-53.

[6] Yang N, Yeoh P L, Elkashlan M, et al. Transmit antenna selection for security enhancement in MIMO wiretap channels. IEEE Trans Commun, 2013, 61: 144–154

[7] Zou Y L, Zhu J, Wang X B, et al. Improving physical-layer security in wireless communications using diversity techniques. IEEE Netw, 2015, 29: 42–48

[8] WANG D，BAI B，CHEN W，et al.Achieving high energyefficiency and physical-layer security in AF relaying[J].IEEE Transactions on Wireless Communications ， 2016 ， 15(1) ： 740-752.

[9] WANG D， BAI B， CHEN W， et al.Energy efficient secure communication over decode-and-forward relay channels[J]. IEEE Transactions on Communications ， 2015 ， 63(3) ： 892-905.

[10] Zou Y L, Wang X B, Shen W M. Optimal relay selection for physical-layer security in cooperative wireless networks. IEEE J Sel Areas Commun, 2013, 31: 2099–2111

[11]Zhang X, Zhang Y, Yan Z, et al. Performance analysis of cognitive relay networks over Nakagami-m fading channels. IEEE J Sel Areas Commun, 2015, 33: 865–877

[12]Bloch M, Barros J, Rodrigues M R, et al. Wireless information-theoretic security. IEEE Trans Inf Theory, 2008, 54:2515–2534

[13]Zhang X, Zhang Y, Yan Z, et al. Performance analysis of cognitive relay networks over Nakagami-m fading channels. IEEE J Sel Areas Commun, 2015, 33: 865–877

[14]Lei H J, Ansari I S, Pan G F, et al. Secrecy capacity analysis over α-μ fading channels. IEEE Commun Lett, 2017,21: 1445–1448