Computers, Materials & Continua CMC, vol.62, no.3, pp.1387-1395, 2020

Secrecy Outage Probability Analysis Based on Cognitive Decode-and-Forward Relaying

Ruoyu Su[1, 4], Xiaojun Sun[1, 3], Fei Ding[1, 2, *], Dengyin Zhang[1, 2], Hongbo Zhu[1, 2], and M. I. M. Wahab[5]

Abstract: Wireless communications have to face to several different security issues in practice due to the nature of broadcast. The information theory is well known to provide efficient approaches to address security issues in wireless communications, which attracts much attention in both industry and academia in recent years. In this paper, inspired by information theory, we study the outage probability of the opportunistic relay selection based on cognitive decode-and-forward relaying with the secrecy consideration. Specifically, the closed-form expression of the outage probability is proposed. Moreover, the asymptotic performance evaluation on the basis of the analytical results is investigated. The simulation results show that the relay selection can reduce the outage probability in accordance with our theoretical analysis.

Keywords: Secure communication, average secrecy rate, relay selection, probability density function.

1 Introduction

Wireless communications cause serious practical security issues because of the broadcast nature of the transmission medium. Information-theoretic security has recently attracted much research interests in recent years [Sun, Wang, Xu et al. (2012)]. The pioneering work was proposed by Wyner [Wyner (1975)] and was effectively extended by other scholars in [Jiang (2019); Leung and Hellman (1978); Csiszar and Korner (1978); Sun, Xu, Jiang et al. (2013); Alotaibi and Hamdi (2014); Ghosh and Roy (2015)], which considered the properties of Gaussian channels in the broadcast fashion.

The security of multiple-antenna systems was also investigated in Shrestha et al. [Shrestha and Kwak (2014)]. Information-theoretic security in wireless communications has been used to improve security in the wireless quasi-static fading channels [Chrysikos,

1 Jiangsu Key Laboratory of Wireless Communications, Nanjing University of Posts and Tele-Communications, Nanjing, 210003, China.

2 Key Laboratory of Broadband Wireless Communication and Sensor Network Technology, Ministry of Education, Nanjing University of Posts and Telecommunications, Nanjing, 210003, China.

3 School of Information Science and Engineering, Southeast University, Nanjing, 210018, China.

4 Department of Electrical and Computer Engineering, Faculty of Engineering and Applied Science, Memorial University of Newfoundland, St. John's, A1B 3X5, Canada.

5 Department of Mechanical and Industrial Engineering, Ryerson University, Toronto M5B 2K3, Canada.

* Corresponding Author: Fei Ding. Email: dingfei@njupt.edu.cn.

Birkos, Dagiuklas et al. (2016)]. However, multiple antennas may not be always available in practice because of their high cost and large size. In this scenario, cooperative communications were proposed to efficiently overcome this limitation. Some research results are presented to investigate various relay or cooperative strategies, which aim to increase security against eavesdroppers. These strategies include noise forwarding [Dong, Han, Petropulu et al. (2010); Pham and Kong (2014); Ibrahim, Hassan and El-Dolil (2015); Namdar and Basgumus (2017)]. It is worth noting that a previous study [Krididis (2010)] considered relay selection in secure decode-and-forward (DF) cooperative communications. The value of outage probability is derived in Krididis [Krididis (2010)], which is meaningful at high signal-to-noise ratios (SNRs). As to the simulation results of the study, a closed-form expression of the outage probability remains unclear in selective DF cooperative communications with secrecy constraints in different values of SNRs.

In this paper, we investigate the outage probability of selective DF cooperative secure communications over Rayleigh fading channels. The system model is proposed in Section 2. As the main contribution of the study, analytical expressions for the outage probability are derived in Section 3 The asymptotic performances in the high SNR regime are also investigated based on the analytical results in Section 3. The accuracy of our performance analysis is verified by simulation in Section 4. The paper is concluded in Section 5.

2 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 a single antenna.

The communication link between the S and the destination nodes occurs in two hops. In the first hop, S broadcasts the signal to all nodes. For simplicity but without loss of generality, we focus on the high SNR region where all relay nodes successfully decode the source transmission [Krikidis (2010); Dong, Han and Petropulu (2010); Pham and Kong (2014); Khalil, Berber and Sowerby (2016); Namdar and Basgumus (2017)]. In the second hop, relay selection based on instantaneous average secrecy rate is performed. Let γ_{sd}, γ_{se}, γ_{rd}^{n} and γ_{re}^{n} denote the instantaneous SNR of the link $S \to D$, $S \to E$, $R_i \to D$ and $R_i \to E$, respectively. The multiple-access channel is defined with Rayleigh fading. Thus, the probability density functions (PDFs) of the SNRs, $f(\gamma_{sd})$, $f(\gamma_{se})$, $f(\gamma_{rd}^{n})$ and $f(\gamma_{re}^{n})$, and the corresponding exponential distributions are identified by λ_{sd}, λ_{se}, λ_{m} and λ_{e}, respectively.

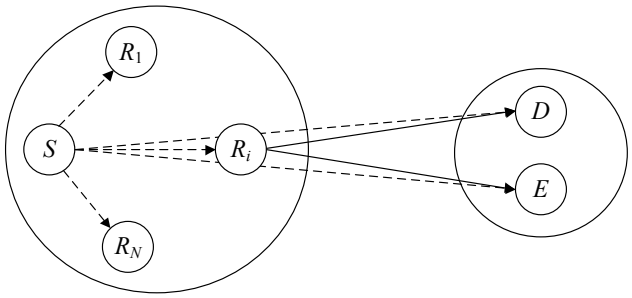

Figure 1: A typical Half-duplex DF relay wiretap channel model. In the first phase, *S* broadcasts the signal to all the destination nodes (dotted lines). In the second phase, the best relay node re-forwards the signal to *D* and *E* (solid lines)

In the second hop, only the relay node with the highest instantaneous average secrecy rate is selected to forward the message to *D*. Thus, *D* and *E* can combine the two received signals by maximum-ratio combining. In accordance with the definition in [Bloch (2008)], the instantaneous average secrecy rate [Wyner (1975)] about the *n*th relay link is given by

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

where $\gamma_{m,n} = \gamma_{rd}^n + \gamma_{sd}$ denotes the instantaneous SNR of the mail channel, $\gamma_{e,n} = \gamma_{re}^n + \gamma_{se}$ represents 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

$$Z_{\max} = \max\{Z_1, \cdots, Z_N\} \tag{2}$$

with the cumulative density function (CDF) as

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

where $Fn(z)$ is the CDF of Z_n. After the relay selection is executed, the instantaneous average secrecy rate is expressed as

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

This study characterizes the relay selection with secrecy constraints in terms of outage probability.

3 Outage probability of relay selection with secrecy constraints

In a wireless communication network, the secrecy outage probability is an important performance measure. Outage probability is defined as the probability that the instantaneous secrecy capacity falls below a target rate *R,* expressed as

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

3.1 Relay selection without direct links

In this subsection, we follow the system model in Krikidis [Krikidis (2010)], where *S* has no direct links with *D* and *E*.

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

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

Substituting Eq. (6) in Eq. (3), $F_{\max}(z)$ can be determined. Thus, for independent identically distributed (I.I.D.), by using the binomial expansion, and the secrecy 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 $C_n^N = N!/n!/(N-n)!$.

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

3.2 Relay selection with direct links

We extend the system model in Krikidis [Krikidis (2010)] by considering the direct links between *S* and *D*/*E* in this subsection.

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

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

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

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

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

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

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

Otherwise, if $u<0$, the conditional CDF $F_n(z\,|\,u)$ can be expressed as

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

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

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

By introducing $v=z\lambda_{se}-\lambda_{sd}$, we obtain $F_{\max}(z)$. The PDF $f(v)$ of v is given by

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

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

3.3 Asymptotic outage probability

The asymptotic outage probability at high SNRs can better characterize the performance of the algorithm, where $\lambda_m \to \infty$ and $\lambda_e \to \infty$ with a constant $k = \lambda_m / \lambda_e$.

Without direct links, the asymptotic outage probability [Krikidis (2010)] is expressed as

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

When *S* has direct links with *D* and *E*, we calculate the asymptotic outage probability. In accordance with Eq. (8), for fixed SNRs λ_{sd} and λ_{se}, we have

$$\begin{aligned} P_{out}^{a}(R) = 1 &- \frac{\lambda_{sd}}{e^R \lambda_{se} + \lambda_{sd}} \exp\left(-\frac{e^R - 1}{\lambda_{sd}} \right) \\ &+ \left(\frac{e^R}{e^R + k} \right)^N \frac{e^R \lambda_{sd}}{\left(e^R \lambda_{se} + \lambda_{sd} \right)\left(e^R + k_d \right)} \\ &+ \sum_{n=1}^{N} \frac{C_n^N}{e^R \lambda_{se} + \lambda_{sd}} \left(\frac{-k}{e^R + k} \right)^n \left[\frac{e^R \lambda_{se}}{n e^R k_e + 1} + f_a \right], \end{aligned} \tag{16}$$

where $k_d = \lambda_{sd} / \lambda_e$, $k_e = \lambda_{se} / \lambda_m$ and $k_m = \lambda_{sd} / \lambda_m$. If $nk_m - 1$, then $f_a = e^R - 1$; else, $f_a = \left(\exp\left(\frac{\left(e^R - 1 \right)\left(nk_m - 1 \right)}{\lambda_{sd}} \right) - 1 \right) \frac{\lambda_{sd}}{nk_m - 1}$. In the case of $\lambda_{sd} \to \infty$ and $\lambda_{se} \to \infty$ with a constant $k_s = \lambda_{sd} / \lambda_{se}$, Eq. (16) is rewritten as

$$\begin{aligned} P_{out}^{a}(R) = &\frac{e^R}{e^R + k_s} + \left(\frac{e^R}{e^R + k} \right)^N \frac{e^R k_s}{\left(e^R + k_s \right)\left(e^R + N k_d \right)} \\ &+ \sum_{n=1}^{N} \frac{e^R C_n^N}{\left(e^R + k_s \right)\left(n e^R k_e + 1 \right)} \left(\frac{-k}{e^R + k} \right)^n . \end{aligned} \tag{17}$$

If $k_d \to 0$, $k_e \to 0$ and $k_m \to 0$, Eq. (16) and Eq. (17) can be rewritten as Eq. (15). In this case, the effect of direct links is negligible.

4 Simulation results

Fig. 2 shows the outage probability of $R = 0.3$ for $\lambda_e = 15\,dB$ under different λ_m and relay nodes *N*. As observed, the experimental curves exactly match the theoretical results.

These curves show that secrecy outage probability decreases with the increasing number of relay nodes.

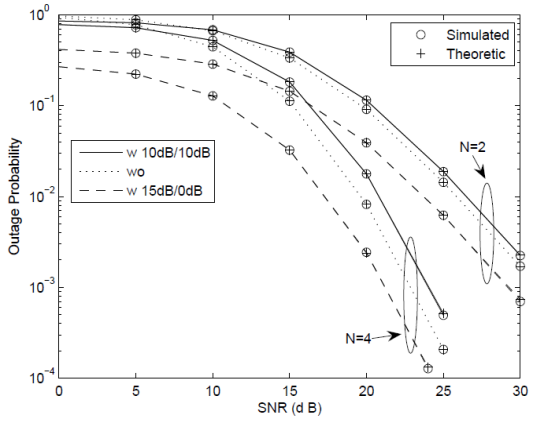

Figure 2: Outage probability of $R = 0.3$ *vs.* λ_m. "wo" indicates that S has no direct links with *D*/*E*. "w x dB/y dB" denotes $\lambda_{sd} = x\,dB$ and $\lambda_{se} = y\,dB$

The asymptotic behavior of outage probability of $R = 0.3$ as functions of λ_m under different relay nodes *N* is illustrated in Fig. 3. SNR λ_e is equal to SNR λ_m. As presented in Fig. 3, these plotted curves follow the previously described behavior. When $k_d, k_e, k_m \to 0$ with increasing SNR λ_m, SNRs λ_{sd} and λ_{se} are fixed as $5dB$; Eq. (16) converges to Eq. (15), as shown in Fig. 3. Moreover, asymptotic outage analysis efficiently converges to the true outage probability in the high SNR regime. The effect of direct links is negligible in the high SNR regime when SNRs k_d, k_e, k_m are considerably small.

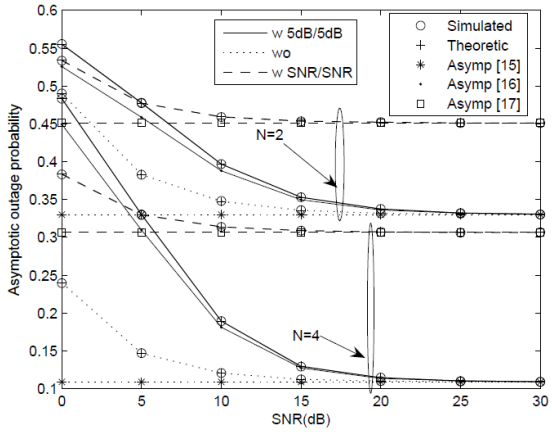

Figure 3: Asymptotic outage probability of $R = 0.3$ and λ_m. "wo" indicates that *S* has no direct links with *D*/*E*. "w x dB/y dB" denotes $\lambda_{sd} = x\,dB$ and $\lambda_{se} = y\,dB$. "w SNR/SNR" indicates $\lambda_{sd} = \lambda_{se} = \lambda_m$

5 Conclusions

In this paper, we derived closed-form expressions of the outage probability in secure DF cooperative communications. The relay selection is proved to reduce the outage probability. Specifically, the closed-form expression of the outage probability is proposed. Moreover, the asymptotic performance evaluation on the basis of the analytical results is investigated. The simulation results show that the relay selection can reduce the outage probability in accordance with our theoretical analysis. The simulation results verify the theoretical results in this study. We will consider the relay-jamming selection as the future work.

Acknowledgement: This work is partially supported by National Major Project of China (No. 2010ZX03006-006), National Natural Science Foundation of China (No. 61571241), the Ministry of Education-China Mobile Research Foundation, China (No. MCM20170205), the Communication Soft Science Research Project of Ministry of Industry and Information Technology, China (No. 2017-R-34), the Scientific Research Foundation of the Higher Education Institutions of Jiangsu Province, China (No. 15KJA510002 and 17KJB510043), the Research Foundation for Advanced Talents, Nanjing University of Posts and Telecommunications (No. NY217146), Open Foundation of the Remote Measuring and Control Key Lab of Jiangsu Province, China (No. 2242015k30005).

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

Alotaibi, E. R.; Hamdi, K. A. (2014): Relay selection for multi-destination in cooperative networks with secrecy constraints. *Proceeding of the IEEE Vehicular Technology Conference (VTC Fall)*, pp. 1-5.

Bloch, M. (2008): *Physical-Layer Security (Ph.D. Thesis)*. Georgia Institute of Technology, USA.

Chrysikos, T.; Birkos, K.; Dagiuklas, T.; Kotsopoulos, S. (2016): Wireless information-theoretic security: theoretical analysis & experimental measurements with multiple eavesdroppers in an outdoor obstacle-dense MANET. *Physical Communication*, vol. 25 no. 2, pp. 577-587.

Csiszar, I.; Korner, J. (1978): Broadcast channels with confidential messages. *IEEE Transactions on Information Theory*, vol. 24, no. 3, pp. 339-348.

Dong, L.; Han, Z.; Petropulu, A.; Poor, H. V. (2010): Improving wireless physical layer security via cooperating relays. *IEEE Transactions on Signal Processing*, vol. 58, no. 3, pp. 1875-1888.

Ghosh, J.; Roy, S. D. (2015): Qualitative analysis for coverage probability and energy efficiency in cognitive-femtocell networks under macrocell infrastructure. *Electronics Letters*, vol. 51, no. 17, pp. 1378-1379.

Han, S; Xu, S.; Meng, W.; Li, C. (2018): Dense-device-enabled cooperative networks for efficient and secure transmission. *IEEE Network*, vol. 32, no. 2, pp. 100-106.

Ibrahim, D. H.; Hassan, E. S.; El-Dolil, S. A. (2015): Relay and jammer selection schemes for improving physical layer security in two-way cooperative networks. *Computers & Security*, vol. 50, pp. 47-59.

Jiang, X.; Liu, M.; Yang, C.; Liu, Y.; Wang, R. (2019): A blockchain-based authentication protocol for WLAN mesh security access. *Computers, Materials & Continua*, vol. 58, no. 1, pp. 45-59.

Khalil, M. I.; Berber, S. M.; Sowerby, K. W. (2016): Bit error rate performance analysis in amplify-and-forward relay networks. *Wireless Networks*, vol. 23, no.3, pp. 947-957.

Krikidis, I. (2010): Opportunistic relay selection for cooperative networks with secrecy constraints. *IET Communications*, vol. 4, no. 15, pp. 1787-1791.

Leung, S. K.; Hellman, M. (1978): The Gaussian wire-tap channel. *IEEE Transactions on Information Theory*, vol. 24, no. 4, pp. 451-456.

Namdar, M.; Basgumus, A. (2017): Outage performance analysis of underlay cognitive radio networks with decode-and-forward relaying. *Cognitive Radio*, IntechOpen. https://www.intechopen.com/books/cognitive-radio/outage-performance-analysis-of-underlay-cognitive-radio-networks-with-decode-and-forward-relaying.

Sun, X. J.; Wang, J. H.; Xu, W.; Zhao, C. M. (2012): Performance of secure communications over correlated fading channels. *IEEE Signal Processing Letters*, vol. 19, no. 8, pp. 479-482.

Sun, X. J.; Xu, W.; Jiang, M.; Zhao, C. M. (2013): Opportunistic selection for decode-and-forward cooperative networks with secure probabilistic constraints. *Wireless Personal Communications*, vol. 70, no. 4, pp. 1633-1652.

Shrestha, A. P.; Kwak, K. S. (2014): Performance of opportunistic scheduling for physical layer security with transmit antenna selection. *EURASIP Journal on Wireless Communications & Networking*, vol. 2014, no. 1, pp. 1-9.

Pham, N. S.; Kong, H. Y. (2014): Spectrum sharing with secure transmission. *EURASIP Journal on Wireless Communications & Networking*, vol. 2014, no. 1, pp. 1-15.

Wyner, A. D. (1975): The wire-tap channel. *Bell System Technical Journal*, vol. 54, no. 5, pp. 1355-1367.