

Closed-Form Expressions for Relay Selection with Secrecy Constraints

Xiaojun Sun, Chunming Zhao, Ming Jiang

Abstract—An opportunistic relay selection based on instantaneous knowledge of channels is considered to increase security against eavesdroppers. The closed-form expressions are derived for the average secrecy rates and the outage probability when the cooperative networks use Decode-and-Forward (DF) or Amplify-and-Forward (AF) strategy. These techniques are demonstrated analytically and with simulation results.

Index Terms—relay selection, Decode-and-Forward, Amplify-and-Forward, secure communications.

I. INTRODUCTION

Due to the broadcast nature of transmission medium, wireless communications are susceptible to eavesdropping. Traditional security mechanisms mainly rely on cryptographic protocols at higher layers. In contrast with this paradigm, the physical layer security strategies exploit the randomness of wireless channels, and significantly strengthen the security of wireless communications [1]-[14]. Potential benefits of deriving secure information from physical layer have been reported in [1].

There has been a growing interest in physical layer security. Wyner introduced wiretap channel model to evaluate secure transmissions at the physical layer [2]. Csiszar generalized it to broadcast channels [3]. Leung-Yan-Cheong defined the secrecy capacity as the difference between the main Gaussian channel capacity and the wiretap Gaussian channel capacity [4]. Wei Kang studied secure communications over a two-user semi-deterministic broadcast channels [5]. Barros generalized the Gaussian wiretap channel model to wireless quasi-static fading channel [6]-[7]. The secure MIMO systems were studied in [8]-[9]. Motivated by emerging wireless application, relay or cooperative strategies are exploited to increase security against eavesdroppers [10]-[13]. Lai has shown that secure communications can take place via untrusted relay nodes jamming eavesdroppers [10]. Recently, physical layer secure protocols based on Decode-and-Forward (DF) or Amplify-and-Forward (AF) strategy have been proposed in [11]-[14] and trusted relay nodes are employed. To maximize the secrecy capacity, some power allocation schemes have been presented for DF or AF strategy in [11] and [12], respectively.

This paper investigates relay selection with secrecy constraints in dual-hop cooperative networks, which use DF or AF strategy. We select the relay node with the maximal instantaneous secrecy rate to retransmit the received messages. We assume that the global channel state information (CSI) is available [6]-[14] and the number of relays with successful decoding is *a priori* [11][13]. Under this assumption, the closed-form expressions are derived for the average secrecy

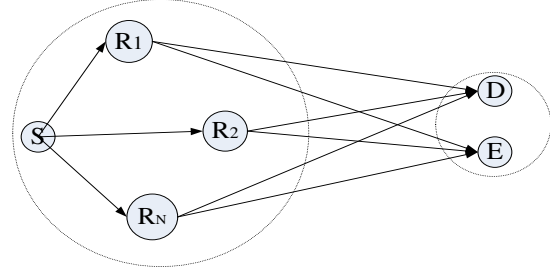


Fig. 1. Dual-hop relay wiretap channel model. Define S-R-D link as the main channel and S-R-E link as the wiretap channel. Eve and destination are located within one cluster while source is at a faraway location outside the cluster.

rates and the outage probability. A similar work, which also considered relay selection for secure cooperative communications, was presented in [14], but it focused on jamming and outage probability.

II. DUAL-HOP RELAY WIRETAP MODEL

Fig. 1 shows the half-duplex relay system consisting of one source (S), N relays (R), one destination (D) and one Eve (E). We assume that the direct links ($S \rightarrow D$, $S \rightarrow E$) are not available [11]-[12][14]. Therefore, S transmits confidential information to D using a trusted R. A third party (Eve) is capable of eavesdropping on relay's transmissions. Suppose that R can access to CSI on wiretap channel and feed back the CSI to S. This assumption corresponds to the scenario where Eve is another user interacting with the Time Division Multiple Access (TDMA) network, thus sending signals that allow R to estimate the CSI [6][7].

The communication occurs in two hops. In the first hop, S broadcasts the information to relays. During the second hop, D and Eve observe the output of the main channel and the wiretap channel from R, respectively. Denoting $h_{SR,n}$, $h_{RD,n}$ and $h_{RE,n}$ ($n = 1, \dots, N$) as the independent channel gains for S to n th R link ($S \rightarrow R_n$), the n th R to D link ($R_n \rightarrow D$) and to Eve link ($R_n \rightarrow E$), respectively. These channel coefficients are modeled as zero-mean complex Gaussian random variables. Furthermore, additive white Gaussian noise (AWGN) is assumed with zero mean and unit variance. Define the instantaneous signal-to-noise ratio (SNR) for $S \rightarrow R_n$, $R_n \rightarrow D$ and $R_n \rightarrow E$ as $\gamma_{SR,n} = |h_{SR,n}|^2$, $\gamma_{RD,n} = \gamma_n |h_{RD,n}|^2$ and $\gamma_{RE,n} = \gamma_n |h_{RE,n}|^2$, where γ_n is the average SNR. Then $\gamma_{SR,n}$, $\gamma_{RD,n}$ and $\gamma_{RE,n}$ are exponentially distributed random variables with rate parameter 1, $\lambda_{m,n}$ and $\lambda_{e,n}$, respectively.

In the second hops, only the R with the largest instantaneous secrecy rate is selected, which assists S to deliver messages to D via a DF or AF strategy. The instantaneous secrecy rate about n th-relay link is defined as [6]

$$R_s(Z_n) = \begin{cases} \ln Z_n, & \text{if } Z_n > 1 \\ 0, & \text{if } Z_n \leq 1 \end{cases} \quad (1)$$

where $Z_n = (1 + \gamma_{m,n}) / (1 + \gamma_{e,n})$ is the equivalent SNR, $\gamma_{m,n}$ is the SNR of main channels and $\gamma_{e,n}$ denotes the SNR of wiretap channels.

III. RELAY SELECTION WITH SECRECY CONSTRAINTS

This section characterizes the relay selection with secrecy limitations in terms of average secrecy rate and outage probability as follows. The equivalent instantaneous SNR at 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

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

where $F_n(z)$ is the CDF of Z_n . Then, the average secrecy rate can be calculated by using (1) and (3)

$$R_s = \int_0^\infty P_r(\ln Z_{\max} > x) dx = \int_0^\infty 1 - F_{\max}(e^x) dx \quad (4)$$

and the outage probability at a target secrecy rate R can be written as

$$P_{out}(R) = P_r(\ln Z_{\max} \leq R) = F_{\max}(e^R) \quad (5)$$

A. Relay Selection Based on DF:S-DF

The exact expressions for average secrecy rate are calculated in this subsection. When DF strategy is used, the instantaneous SNR is $\gamma_{m,n} = \gamma_{RD,n}$ and $\gamma_{e,n} = \gamma_{RE,n}$. The CDF of Z_n is given by

$$F_n(z) = 1 - \frac{\lambda_{e,n} \exp(-\lambda_{m,n}(z-1))}{\lambda_{m,n}(z-1) + \lambda_{m,n} + \lambda_{e,n}} \quad (6)$$

Proof: We rewrite Z_n as $Z_n = (1 + \gamma_{RD,n}) / (1 + \gamma_{RE,n}) = (1 + x) / (1 + y)$. Since x and y are independently exponentially distributed random variables, the CDF of Z_n can be derived as

$$\begin{aligned} F_n(z) &= P_r(Z_n \leq z) \\ &= \int_0^\infty f(y) dy \int_0^{yz+z-1} f(x) dx \\ &= 1 - \lambda_{e,n} e^{-\lambda_{m,n}(z-1)} \int_0^\infty e^{-y(\lambda_{m,n}z + \lambda_{e,n})} dy \end{aligned} \quad (7)$$

which yields (6) after some simple manipulations. ■

Using (3), (6) and after applying some algebraic manipulations, we can express $1 - F_{\max}(e^x)$ as $\sum_i \varsigma_i \frac{\exp(-\beta_i(e^x-1))}{e^x + \alpha_i}$

when channels are independent but not identically distributed (INID). The integration in (4) can be rewritten as

$$\begin{aligned} R_{sdf} &= \sum_i \varsigma_i \int_0^\infty \frac{\exp(-\beta_i(e^x-1))}{e^x + \alpha_i} dx \xrightarrow{u=e^x-1} \\ &= \sum_i \varsigma_i \int_0^\infty \frac{\exp(-\beta_i u)}{(u+1+\alpha_i)(u+1)} du \\ &= \sum_i \frac{\varsigma_i}{\alpha_i} [F_e(\beta_i) - F_e(\beta_i + \alpha_i \beta_i)] \end{aligned} \quad (8)$$

where ς_i , β_i and α_i are the coefficients of the identical equation. $F_e(x) = \exp(x) E_1(x)$ and $E_1(x)$ is the exponential-integral function [15]. A similar result can be obtained when the channels are independent identically distributed (IID) by using [15, Eq.(3.353-2)].

B. Relay Selection Based on AF:S-AF

Selection AF with the average power scaling (APS) constraint [16] for secure communications is studied in the following. The analytical result for AF-APS relay is difficult unless we assume that the SNR of the $S \rightarrow R_n$ links is larger than the SNR of the $R_n \rightarrow D/E$ links [16]. And then, the instantaneous approximate SNR is $\gamma_{m,n} = \gamma_{SR,n} \gamma_{RD,n}$ and $\gamma_{e,n} = \gamma_{SR,n} \gamma_{RE,n}$. Let μ denote $\gamma_{SR,n}$ and use (6) and [15, Eq.(3.324-1)], we can write the approximate CDF of Z_n as

$$F_n(z) = 1 - \frac{2\lambda_{e,n} \sqrt{\lambda_{m,n}(z-1)}}{\lambda_{m,n}z + \lambda_{e,n}} K_1 \left(2\sqrt{\lambda_{m,n}(z-1)} \right) \quad (9)$$

where $K_1(\cdot)$ is the 1th-order modified Bessel function of the seconde kind [15].

Applying (6) and these approximate expressions to (4), we have a closed-form approximation (10) by using (8) and [15, Eq.(6.565-7)]

$$\begin{aligned} R_{saf} &= \sum_i \frac{\varsigma_i}{\alpha_i} \int_0^\infty [F_e(\beta_i/\mu) - F_e(\beta_i(1+\alpha_i)/\mu)] e^{-\mu} d\mu \\ &= \sum_i \frac{4\varsigma_i}{\alpha_i} [\xi_{1,i} S_{-2,1}(\xi_{1,i}) - \xi_{2,i} S_{-2,1}(\xi_{2,i})] \end{aligned} \quad (10)$$

where $\xi_{1,i} = 2\sqrt{\beta_i}$, $\xi_{2,i} = 2\sqrt{\beta_i(1+\alpha_i)}$ and $S_{a,b}(\cdot)$ is the Lommel functions [15]. Simulation results show that (10) provides an upper bound for the average secrecy rate.

C. Optimal Power Allocation for DF:OPA-DF

For comparison purpose, we just introduced the power allocation scheme for DF-based protocol [11]. Let us define the $N \times 1$ vectors $\mathbf{w} = [w_1, \dots, w_N]^H$, $\mathbf{h}_m = [h_{RD,1}, \dots, h_{RD,N}]^H$ and $\mathbf{h}_e = [h_{RE,1}, \dots, h_{RE,N}]^H$, the $N \times N$ matrices $\mathbf{R}_m = \mathbf{h}_m \mathbf{h}_m^H$ and $\mathbf{R}_e = \mathbf{h}_e \mathbf{h}_e^H$. For a fix transmit power γ_0 , the problem of maximizing the secrecy rate $\ln[(1 + \mathbf{w}^H \mathbf{R}_m \mathbf{w}) / (1 + \mathbf{w}^H \mathbf{R}_e \mathbf{w})]$ is formulated as

$$\begin{aligned} &\max (1 + \mathbf{w}^H \mathbf{R}_m \mathbf{w}) / (1 + \mathbf{w}^H \mathbf{R}_e \mathbf{w}) \\ &\text{s.t. } \mathbf{w}^H \mathbf{w} = \gamma_0 \end{aligned} \quad (11)$$

The solution reported in [8][9], is the scaled eigenvector corresponding to the largest eigenvalue of the symmetric matrix $(\mathbf{I}_N + \gamma_0 \mathbf{R}_m) (\mathbf{I}_N + \gamma_0 \mathbf{R}_e)^{-1}$.

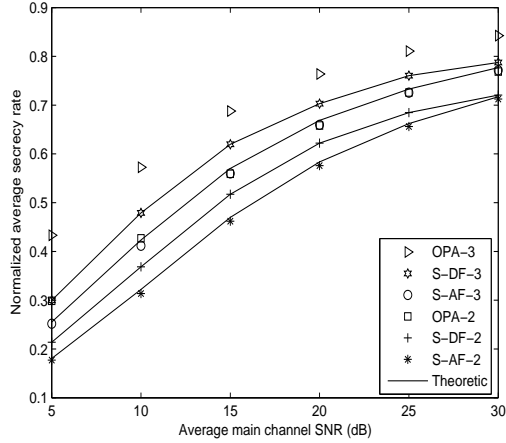


Fig. 2. The average secrecy rate assuming IID Rayleigh fading. Normalization is performed with respect to the capacity of an AWGN channel with the same SNR of main channel.

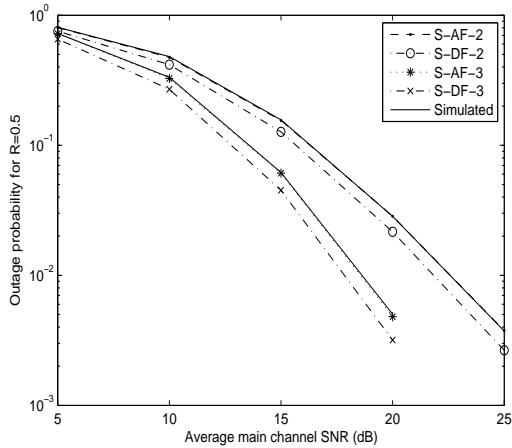


Fig. 3. Outage probability for a target secrecy rate 0.5 assuming IID Rayleigh fading.

IV. SIMULATION RESULTS

We illustrate the performance of S-DF, S-AF and OPA-DF in this section. In our test, we assume that all channels are IID Rayleigh fading and the average wiretap channel SNR is $\gamma_e = 10$ dB. Similar conclusions can also be derived when channels are INID and γ_e is other values. We do not plot these curves due to space limit.

Fig. 2 shows the average secrecy rate of S-DF, S-AF and OPA-DF. The average secrecy rate of S-DF is larger than that of S-AF. For comparison purpose, we also plot the curves of OPA-DF. It can be seen that OPA-DF outperforms S-DF. Compared to selection model, OPA may have higher implementation complexity, such as, synchronization of multiple access. The outage probabilities of S-DF and S-AF for a target secrecy rate 0.5 are depicted in Fig. 3. As expected, S-DF is also better than S-AF. Taking into account the same number of relay nodes, we find that the performance of selection AF-APS, which has the lowest complexity, is the worst. Fig. 2-3 also show that S-AF may outperform S-DF when the number of AF relay nodes is larger than that of DF relay nodes.

We can see from Fig. 2-3 that the theoretical results of S-

DF are almost the same as the experimental curves. Simulation results show that the analytical results of S-AF match exactly with the simulated curves when the SNR of $S \rightarrow R_n$ link is about 16dB higher than that of $R_n \rightarrow D/E$ links.

V. CONCLUSION

This paper presents the exact mathematical expressions for the average secrecy rate (ASR) and the outage probability (OP) of selection DF with secrecy limitations. As a result of computer simulation, the theoretical results are almost the same as the experimental curves. The closed-form approximations for the ASR and OP of selection AF have been derived and match exactly with the simulated curves when the SNR of $S \rightarrow R_n$ link is about 16dB higher than that of $R_n \rightarrow D/E$ links.

REFERENCES

- [1] U. Maurer, "Secret key agreement by public discussion from common information," *IEEE Trans. Info.Theory.*, vol.39, pp. 733-742, May. 1993.
- [2] A. D.Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol.54, no.5, pp.1355-1367, Oct. 1975.
- [3] I. Csiszár and J. Körner, "Broadcast channels with confidential messages," *IEEE Trans. Info. Theory.*, vol.24, no.3, pp. 339-348, May 1978.
- [4] 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.
- [5] Wei kang and Nan Liu, "The Secrecy Capacity of the Semi-deterministic Broadcast Channel," in *Proc. IEEE ISIT*, Seoul, Korea, Jun. 2009, pp. 2767-2771.
- [6] J. Barros and M. R. D. Rodrigues, "Secrecy capacity of wireless channels," in *Proc. IEEE ISIT*, Seattle, WA, Jul. 2006, pp. 356-360.
- [7] Matthieu Bloch, João Barros, Miguel R. D. Rodrigues and Steven W. McLaughlin, "Wireless Information-Theoretic Security," *IEEE Trans. Info.Theory.*, vol.54, no.6, pp. 2515-2534, May 2008.
- [8] Z. Li, W. Trappe and R. Yates, "Secrecet communication via multiantenna transmission," in *Proc. 41st Conference on Information Sciences and Systems.*, Mar 2007.
- [9] S. Shafiee and S. Ulukus, "Achievable rates in Gaussian MISO channels with secrecy constraints," in *Proc. IEEE ISIT*, Jun 2007, pp. 2466 - 2470.
- [10] 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.
- [11] L. Dong, Z. Han, A. Petropulu and H. V. Poor, "Secure wireless communications via cooperation," in *Proc. 46th Annual Allerton Conf. Commun., Control, and Computing.*, Sept 2008, pp.1132 - 1138.
- [12] L. Dong, Z. Han, A. Petropulu and H. V. Poor, "Amplify-and-forward based cooperation for secure wireless communications," in *Proc. IEEE ICASSP*, Apr 2009, pp.2613 - 2616.
- [13] Pengyu Zhang, Jian Yuan, Jianshu Chen, Jian Wang and Jin Yang, "Analyzing Amplify-and-Forward and Decode-and-Forward Cooperative Strategies in Wyner's Channel Model," in *Proc. IEEE WCNC.*, Apr 2009, pp:1 - 5.
- [14] 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.
- [15] I. S. Gradshteyn and I. M. Ryzhik, *Table of Integrals, Series, and Products, 6th ed.*, Singapore: Elsevier, 2004.
- [16] Himal A. Suraweera, and Jean Armstrong, "Performance of OFDM-Based Dual-Hop Amplify-and-Forward Relaying," *IEEE Commun. Lett.*, vol. 11, pp. 726-728, Set 2006.