Journal of Korea Multimedia Society Vol. 19, No. 3, March 2016(pp. 620-625)
http://dx.doi.org/10.9717/kmms.2016.19.3.620

# Secrecy Outage Probability of AF Relay Transmission with MRC/TAS in Presence of Eavesdropper

Kyu-Sung Hwang†

## ABSTRACT

In this paper, we offer the secrecy outage probability of the amplify-and-forward (AF) transmission, which consists of one source, one destination, one relay, and one passive eavesdropper. Particularly, we consider that the relay is equipped with multiple antennas while other terminals is utilized with single antenna and apply diversity techniques (for both the reception and the transmission) at the relay to achieve gains in a secrecy outage performance. Additionally, we analyze the exact secrecy outage probability of the proposed systems in a one-integral form. Finally, some numerical examples are given to verify our provided analytical results for different system conditions.

**Key words:** *Secrecy Outage Probability, Amplify-and-Forward, Maximal Ratio Combining, Transmit Antenna Selection

## 1. INTRODUCTION

Due to the broadcast nature of wireless communications, the security issues have been received a lot of attention as a variety of wireless communications increases, where wireless medium allow to be susceptible of eavesdropping without evidences. While the traditional security based on cryptography is performed in the upper layers (e.g., network layer), the information-theoretic approach [1] is utilized to strengthen the security of wireless communications in the physical layer. There are some pioneering works [1-3] on physical layer security based on a wiretap channel consisting a source (Alice), a destination (Bob), and an eavesdropper (Eve) where the perfect secrecy can be achieved without the help of cryptography when the difference between the capacities of main and eavesdropper channels keeps positive.

Relay transmission has been considered as an efficient technique to attain broader coverage and to overcome channel impairments [4-5]. In order to achieve more system capacity, the multiple-input multiple-output (MIMO) relay systems have been investigated in the literlature [6]. Moreover, some multi-antenna techniques (e.g. maximal ratio combining (MRC), antennas selection, beamforming, etc) have been considered as a promising one because they can enhance the overall system performance [7], [8]. In [7], authors examined the impact of the multi-antenna relay on the end-to-end error performance with the threshold-based MRC and the threshold-based selection combining (SC) at the relay. Authors in [8] considered the optimal signal-to-noise ratio (SNR)-based transmit antenna selection at the source and relay for the amplify-and-forward (AF) protocol. Additionally, Wang et. al in [6] applied the protocol

※ Corresponding Author : Kyu-Sung Hwang, Address: (38428) Gamasil-gil 50, Gyeongsan, Gyeobgbuk, Korea, TEL : +82-53-600-5624, FAX : +82-53-600-5559, E-mail : kshwang@kiu.ac.kr

Receipt date : Sep. 22, 2015, Revision date : Nov. 6, 2015
Approval date : Nov. 11, 2015

† Dept. of Electronic Eng., Kyungil University

※ This research was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Science, ICT, and Future Planning under Grant 2015R1C1A1A 0203651

that the MRC and the maximal ratio transmission (MRT) are utilized at the relay as well as considered the partial relay selection.

Recently, the information-theoretic security with relay transmission in the presence of eavesdroppers has been investigated in the previous works [9], [10]. Specifically, authors in [9] introduced the relay-eavesdropper channel and offered an outer-bound on the rate-equivocation region over several cooperation strategies. Dong et al. in [10] investigated the optimal relay weights to maximize the achievable secrecy rate for the multiple relays employing several relay protocols. However, to the best of our knowledge, the impact of MIMO relay or multi-antenna relay while existing an eavesdropper has been not studied sufficiently. This interest is steadily growing because the performance of a secure transmission in the presence of an eavesdropper is very different from one of a conventional transmission.

In this paper, we analyze the secrecy outage probability (SOP) of the AF transmission in the presence of a passive eavesdropper. In detail, we apply reception/transmission diversity techniques at the multi-antenna relay and provide the exact SOP of the proposed AF-based secure transmission in a one-integral form. Finally, we verify our analytical results with some selected computer-based simulation results.

Notation: Throughout this paper, $\overline{F}_X(\cdot)$ and $f_X(\cdot)$ denote a complementary cumulative distribution function (CCDF) and a probability density function (PDF) of a random variable $X$,

respectively. $x \sim CN(\mu,\sigma^2)$ denotes a circular symmetric complex Gaussian random variable $x$ with mean $\mu$ and variance $\sigma^2$. $\mathrm{E}[\cdot]$ is an expectation operator.

## 2. SYSTEM DESCRIPTION

### 2.1 System Model

As shown in Fig. 1, we consider an AF relaying protocol consisting of a source, a destination, a relay, and an eavesdropper denoted by $S$, $D$, $R$, and $E$, respectively, which operates a half-duplex transmission. In addition, the relay is equipped with $L$ antennas whereas other terminals has one antenna, and there is no direct transmission between the source and the destination as well as between the source and the eavesdropper. We denote $h_{S,R_i}$, $h_{R_i,D}$, and $h_{R_i,E}$ as channel coefficients for the $S$-$R$, $R$-$D$, and $R$-$E$ links with the $l$-th antenna of the relay, respectively. Specifically, we assume that the independent identically distributed (i.i.d.) channel condition per link where $h_{S,R_l} \sim CN(0,\Omega_{S,R})$, $h_{R_l,D} \sim CN(0,\Omega_{R,D})$, and $h_{R_l,E} \sim CN(0,\Omega_{R,E})$. In the first time slot of a half-duplex mode, the received signals at the relay are given by

$$\mathbf{y}_R = \mathbf{h}_{S,R}\, x_S + \mathbf{n}_R, \tag{1}$$

where $x_S$ is the transmitted signal with $\mathrm{E}\left[|x_S|^2\right] = \varepsilon_S \mathbf{h}_{S,R}$ is an $N \times 1$ complex channel co-

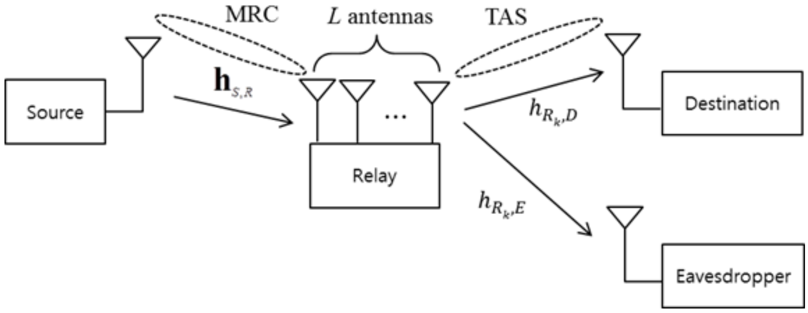

Fig. 1. Proposed AF relay system model in the presence of an eavesdropper.

efficient vector for the $S$-$R$ link as $\mathbf{h}_{S,R} = \left[h_{S,R_1} h_{S,R_2} \cdots h_{S,R_L}\right]^T$, $\mathbf{n}_{R_l}$ is a noise vector at the relay as $\mathbf{n}_R = \left[n_{R_1} n_{R_2} \cdots n_{R_L}\right]^T$, and $n_{R_l}$ is the additive white Gaussian noise (AWGN) as $n_{R_l} \sim CN(0, N_0)$. Additionally, in the second time slot, the relay amplifies its received signal and forwards it to the destination. In the wiretapper channel between the relay and the eavesdropper, the eavesdropper plays a passive role where no channel state information (CSI) feedback is available. This implies that the eavesdropper just overhears the information conveyed from the relay to the destination [11].

In this work, we consider the MRC/transmit antenna selection (TAS) transmission at the relay where the MRC for received signals from the source and the TAS for forwarding them to the destination are applied. The relay has a scalar symbol $\mathbf{h}_{S,R}^H \mathbf{y}_R$ based on the MRC, and then retransmits it to the destination with an amplifying gain via the best transmit antenna. In the second time slot, the received signal at the destination can be represented by

$$y_D = \beta_R h_{R_k,D} \left( \boldsymbol{h}_{S,R}^H \boldsymbol{h}_{S,R} x_S + \boldsymbol{h}_{S,R}^H \boldsymbol{n}_R \right) + n_D, \tag{2}$$

where $\beta_R$ is an amplifying gain at the relay as $\beta_R = 1/\sqrt{\mathrm{E}\left[ \| \mathbf{y}_\mathrm{R} \|^2 \right]}$, $h_{R_k,D}$ is a complex channel coefficient for the $R$-$D$ link with the selected best transmit antenna $k$, $k = \mathrm{argmax}_i \left\{ \left| h_{R_i,D} \right|^2 \right\}$ for $i = 1, \cdots, L$, and $n_D$ is the AWGN at the destination. On the other hand, the received signal at the eavesdropper can be given by

$$y_E = \beta_R h_{R_k,E} \left( \boldsymbol{h}_{S,R}^H \boldsymbol{h}_{S,R} x_S + \boldsymbol{h}_{S,R}^H \boldsymbol{n}_R \right) + n_E, \tag{3}$$

where $h_{R_k,E}$ is a complex channel coefficient vector for the $R$-$E$ link and $n_E$ is the AWGN at the eavesdropper. According to (2), the instantaneous output SNR at the destination can be given by

$$\gamma_{SD} = \frac{\gamma_{S,R}\gamma_{R,D}}{\gamma_{S,R} + \gamma_{R,D} + 1}, \tag{4}$$

where $\gamma_{S,R} = \frac{\varepsilon_S}{N_0} \| \mathbf{h}_{S,R} \|^2$ and $\gamma_{R,D} = \frac{\varepsilon_R}{N_0} \left| h_{R_k,D} \right|^2$. Additionally, the instantaneous output SNR at the eavesdropper can be written as

$$\gamma_{SE} = \frac{\gamma_{S,R}\gamma_{R,E}}{\gamma_{S,R} + \gamma_{R,E} + 1}, \tag{5}$$

where $\gamma_{R,E} = \frac{\varepsilon_R}{N_0} \left| h_{R_k,E} \right|^2$.

### 2.2 Achievable Secrecy Rate

In this work, we assume that all the channels are quasistatic fading channels which implies the fading coefficients are invariant during the transmission of an entire codeword. In addition, the codeword is enough long to achieve for secrecy-capacity codes in every transmission. Under the these assumptions, the achievable secrecy capacity $C_S$ can be calculated by a difference between the main channel capacity (for the destination) and the wiretap channel capacity (for the eavesdropper) as [3]

$$C_S = \left[ C_M - C_W \right]^+, \tag{6}$$

where $\left[ A_S \right]^+$ denotes $\max(A, 0)$, $C_M = \frac{1}{2}\log_2(1 + \gamma_{SD})$ and $C_W = \frac{1}{2}\log_2(1 + \gamma_{SE})$. From (2)-(3), the achievable secrecy capacities of the proposed scheme can be represented as

$$C_S = \left[ \frac{1}{2} \log_2 \left( \frac{1 + \dfrac{\gamma_{S,R}\gamma_{R,D}}{\gamma_{S,R} + \gamma_{R,D} + 1}}{1 + \dfrac{\gamma_{S,R}\gamma_{R,E}}{\gamma_{S,R} + \gamma_{R,E} + 1}} \right) \right]^+. \tag{7}$$

From the preliminary studies of MRC and TAS [12] over the i.i.d. Rayleigh fading channels, the PDFs of $\gamma_{S,R}$ and $\gamma_{R,D}$ are given by

$$f_{\gamma_{S,R}}(x) = \frac{1}{(L-1)!} \frac{x^{L-1}}{\bar{\gamma}_{S,R}^L} \exp\left( -\frac{x}{\bar{\gamma}_{S,R}} \right) \tag{8}$$

and

$$f_{\gamma_{R,D}}(x) = L \sum_{i=1}^{L} \binom{L-1}{i-1} \frac{(-1)^{i-1}}{\bar{\gamma}_{R,D}} \exp\left( -\frac{ix}{\bar{\gamma}_{R,D}} \right). \tag{9}$$

respectively, where $\bar{\gamma}_{S,R} = \frac{\varepsilon_S}{N_0}\Omega_{S,R}$ and $\bar{\gamma}_{R,D} = \frac{\varepsilon_R}{N_0}\Omega_{R,D}$. Additionally, when considering a passive eavesdropper, the PDF of $\gamma_{R,E}$ can be given by $f_{\gamma_{R,E}}(x) = \frac{1}{\bar{\gamma}_{R,E}}\exp\left(-\frac{x}{\bar{\gamma}_{R,E}}\right)$ where $\bar{\gamma}_{R,E} = \frac{\varepsilon_R}{N_0}\Omega_{R,E}$.

## 3. SECRECY OUTAGE PROBABILITY OF THE PROPOSED AF RELAY TRANSMISSION

In this section, the SOP analysis of the AF transmission with a multi-antenna relay while existing an eavesdropper is presented. More specifically, we obtain the exact SOP of the proposed system in a one-integral form where the SOP is defined as the probability that the achievable secrecy capacity $C_S$ is below the target secrecy capacity $C_T$ as [3]

$$P_{out}(C_T) = \Pr\left[C_S < C_T\right]. \tag{10}$$

Using (6), the SOP of the proposed system in (10) can be rewritten as

$$P_{out}(C_T) = \Pr\left[\frac{\frac{(1+\gamma_{S,R})(1+\gamma_{R,D})}{\gamma_{S,R}+\gamma_{R,D}+1}}{\frac{(1+\gamma_{S,R})(1+\gamma_{R,E})}{\gamma_{S,R}+\gamma_{R,E}+1}} < T\right], \tag{11}$$

where $T = 2^{2C_T}$. Letting $z = \gamma_{R,E}$, then the SOP in (11) can be evaluated as

$$P_{out}(C_T) = \int_0^{\infty}\Upsilon(z) f_{\gamma_{R,E}}(z)\,dz, \tag{12}$$

where

$$\Upsilon(z) = \Pr\left[\frac{\frac{(1+\gamma_{S,R})(1+\gamma_{R,D})}{\gamma_{S,R}+\gamma_{R,D}+1}}{\frac{(1+\gamma_{S,R})(1+z)}{\gamma_{S,R}+z+1}} < T\right]. \tag{13}$$

With some manipulations, the probability $\Upsilon(z)$ in (13) can be rewritten as

$$\Upsilon(z) = \Pr\left[(\gamma_{S,R}-(T-1)(z+1))\gamma_{R,D} < T(z+1)(\gamma_{S,R}+1) - (\gamma_{S,R}+z+1)\right]. \tag{14}$$

The parameter $T$ always is more than 1 since the target secrecy capacity $C_T$ is positive real number. Therefore, it is easily known that the term $T(z+1)(\gamma_{S,R}+1) - (\gamma_{S,R}+z+1)$ in (14) is also always positive. Finally, the probability $\Upsilon(z)$ can be divided into two probabilities as

$$\Upsilon(z) = \Pr\left[\gamma_{S,R} \le (T-1)(z+1)\right] + \Pr\left[\gamma_{R,D} < A(\gamma_{S,R}, T, z),\ \gamma_{S,R} > (T-1)(z+1)\right], \tag{15}$$

where

$$A(\gamma_{S,R}, T, z) = \frac{T(z+1)(\gamma_{S,R}+1) - (\gamma_{S,R}+z+1)}{\gamma_{S,R} - (T-1)(z+1)}. \tag{16}$$

Since $\gamma_{S,R}$ and $\gamma_{R,D}$ are independent random variables, the probability $\Upsilon(z)$ can be calculated as

$$\begin{aligned}\Upsilon(z) &= \int_0^{(T-1)(z+1)} f_{\gamma_{S,R}}(x)\,dx + \int_{(T-1)(z+1)'}^{\infty} \int_0^{A(x,T,z)} f_{\gamma_{S,R}}(x) f_{\gamma_{R,D}}(y)\,dy\,dx \\ &= 1 - \int_{(T-1)(z+1)}^{\infty} \bar{F}_{\gamma_{R,D}}(A(x,T,z)) f_{\gamma_{S,R}}(x)\,dx.\end{aligned} \tag{17}$$

Using the probability theories of the i.i.d. Rayleigh fading conditions in (8)-(9) and the multi-binomial theorem, one can obtain the final results of the probability $\Upsilon(z)$ for the proposed scheme as

$$\begin{aligned}\Upsilon(z) = 1 - \sum_{i=1}^{L}\sum_{j=0}^{L-1}\binom{L}{i}\binom{L-1}{j}\frac{2(-1)^i}{(L-1)!\bar{\gamma}_{S,R}^{-L}}\exp\left(-\frac{(T-1)(z+1)}{\bar{\gamma}_{S,R}} - \frac{iT(z+1)}{\bar{\gamma}_{R,D}}\right) \\ \times((T-1)(z+1))^{L-j-1}\left(\frac{iT(T-1)(z+1)^2\bar{\gamma}_{S,R}}{\bar{\gamma}_{R,D}}\right)^{\frac{j+1}{2}} K_{j+1}\left(2\sqrt{\frac{iT(T-1)(z+1)^2}{\bar{\gamma}_{S,R}\bar{\gamma}_{R,D}}}\right),\end{aligned} \tag{18}$$

where $K_v$ is the modified Bessel function of the second kind with order $v$. Finally, Substituting the probability of $\Upsilon(z)$ in (18) into (12), we can calculate the exact SOP of the propose system in a one-integral form.

## 4. NUMERICAL EXAMPLES AND DISCUSSION

In this section, we evaluate the SOP of the multi-antenna relay-based AF transmission in a presence of an eavesdropper over i.i.d. Rayleigh fading channels by Monte-Carlo simulations and compare them with our analysis in (12) and (18).

Fig. 2 shows the secrecy outage probability of the proposed scheme with the different number of antennas at the relay where the average SNR is set to $\bar{\gamma} = \bar{\gamma}_{S,R} = \bar{\gamma}_{R,D}$, $\bar{\gamma}_{R,E} = 5$ dB, and the target secrecy data rate $R = 2$ bps/Hz. As shown in Fig. 2, the secrecy outage probability decreases as the average SNR increases and as the number of available antennas increases. For example, when considering the secrecy outage probability $10^{-1}$, the convention system with $L = 1$ requires the about 25 SNR [dB] while the proposed system with $L = 4$ requires only the about 15 SNR [dB]. In order to show an efficiency of our proposed scheme, we compare the previous multi-antenna relaying scheme, *Strategy 2,* in [13] with ours. In addition, our analytical results by using (12) and (18) are in a good agreement with our simulation results.

## 5. CONCLUSION

In this paper, we analyzed the secrecy outage probability of multi-antenna AF relay transmission in a presence of eavesdropper. In order to improve system performances, we applied MRC/TAS diversity techniques at the relay side. For the performance analysis, we offered the exact secrecy outage probability in one-integral form. From the selected numerical examples, we verified that our analytical results are well-matched with simulation results.

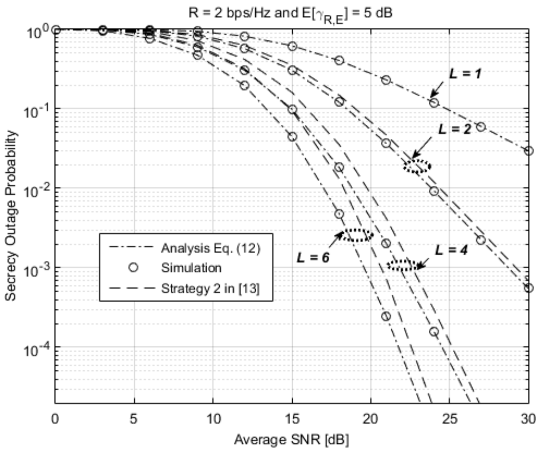

Fig. 2. Secrecy outage probability of the proposed system with L=1,2,4,6, $\bar{\gamma} = \bar{\gamma}_{S,R} = \bar{\gamma}_{R,D}$, $\bar{\gamma}_{R,E} = 5$ dB, and R = 2 bps/Hz.

## REFERENCE

[1] A.D. Wyner, "The Wire-tap Channel," *The Bell Systems Technical Journal*, Vol. 54, No. 8, pp. 1355-1367, 1975.

[2] S.K.L.Y. Cheong and M.E. Hellman, "The Gaussian Wire-tap Channel," *IEEE Transactions on Information Theory*, Vol. 24, No. 4, pp. 451-456, 1978.

[3] M. Bloch, J. Barros, M.R.D. Rodrigues, and S. W. McLaughlin, "Wireless Information-theoretic Security," *IEEE Transactions on Information Theory*, Vol. 54, No. 6, pp. 2515- 2534, 2008.

[4] A. Sendonaris, E. Erkip, and B. Aazhang, "User Cooperation Diversity Part I: System Description," *IEEE Transactions on Communications*, Vol. 51, No. 11, pp. 1927-1938, 2003

[5] H. Kim and S.G. Kwon, "System Performance with Synchronization Errors in Distributed Beamforming Systems," *Journal of Korea Multimedia Society*, Vol. 18, No. 4, pp. 452-459, 2015.

[6] B. Wang, Z. Zhang, and A.H. Madsen, "On the Capacity of MIMO Relay Channels," *IEEE Transactions on Information Theory*, Vol. 51, No. 1, pp. 29-43, 2005.

[7] A. Adinoyi and H. Yanikomeroglu, "Cooperative Relaying in Multiantenna Fixed Relay Networks," *IEEE Transactions on Wireless Communications*, Vol. 6, No. 2, pp. 533-544, 2007.

[8] S.W. Peters and J.R.W. Heath, "Nonregenerative MIMO Relaying with Optimal Transmit Antenna Selection," *IEEE Signal Pro-*

*cessing Letters*, Vol. 15, pp. 421-424, 2008.

[9] L. Lai and H.E. Gamal, "The Relay-eavesdropper Channel: Cooperation for Secrecy," *IEEE Transactions on Information Theory*, Vol. 54, No. 9, pp. 4005-4019, 2008.

[10] L. Dong, Z. Han, A.P. Petropulu, and H.V. Poor, "Improving Wireless Physical Layer Security via Cooperating Relays," *IEEE Transactions on Signal Processing*, Vol. 58, No. 3, pp. 1875-1888, 2010.

[11] N. Yang, P.L. Yeoh, M. Elkashlan, R. Schober, and I.B. Collings, "Transmit Antenna Selection for Security Enhancement in MIMO Wiretap Channels," *IEEE Transactions on Communications*, Vol. 61, No. 1, pp. 144-154, 2013.

[12] M.K. Simon and M.S. Alouini, *Digital Communication over Fading Channels*, 2nd ed., John Wiley & Sons, Inc., New York, 2004.

[13] K. Hwang and M. Ju, "Secrecy Outage Probability of Amplify-and-Forward Transmission with Multi-antenna Relay in Presence of Eavesdropper," *Proceeding of IEEE International Conference on Communications*, pp. 5408-5412, 2014.

Kyu-Sung Hwang

He received the B.Eng. degree in Electrical Engineering in 2004 and the Ph.D. degree in Electrical and Computer Engineering in 2010, both from Korea University, Seoul, Korea. In Jan. 2010, he joined the Korea Electronics Technology Institute (KETI), Seoul, Korea, as a senior researcher. He has been with Kyungil University as an Assistant Professor, Gyeongbuk, Korea since Sept. 2011, where his current research interests include energy harvesting network and system optimization.