Amirkabir University of Technology
(Tehran Polytechnic)

Amirkabir International Jounrnal of Science & Research
Electrical & Electronics Engineering
(AIJ-EEE)
Vol. 48, No. 2, Fall 2016, pp. 93-99

Performance Study of Untrusted Relay Network Utilizing Cooperative Jammer

A. Kuhestani[1], A. Mohammadi[2,*], M. J. Emadi[3]

1- Ph.D. Student, Electrical Engineering Department, Amirkabir University of Technology
2- Professor, Electrical Engineering Department, Amirkabir University of Technology
3- Assistant Professor, Electrical Engineering Department, Amirkabir University of Technology

(Received 30 September 2015, Accepted 23 January 2016)

ABSTRACT

In this paper, the problem of secure transmission in two-hop amplify-and-forward (AF) systems with an untrusted relay is investigated. To prevent the untrusted relay from intercepting the source message and to achieve positive secrecy rate, the destination-based cooperative jamming (DBCJ) technique is used. In this method, the destination sends an intended jamming signal to the relay. This jamming signal helps protect the source message from being captured reliably at the untrusted relay, while the destination cancels itself the intended jamming signal. The optimal power allocation (OPA) technique is considered for the presented system. It is observed that the objective function is a quasi-concave function at high signal-to-noise-ratio (SNR) regimes. Based on this OPA technique, we study the ergodic secrecy rate (ESR) and the secrecy outage probability (SOP) of the system when the source and relay are equipped with a single antenna while the destination is equipped with large-scale antenna arrays (LSA). Using the achieved closed-form expressions, one can evaluate the performance of the secure system easily and fast and also, they provide significant insights into the system design. Finally, simulation results indicate the accuracy of the derived expressions.

KEYWORDS:

Physical Layer Security, Untrusted Relay, Optimal Power Allocation, Uplink Transmission

Please cite this article using:
Kuhestani, A., Mohammadi, A., and Emadi, M. J., 2016. "Performance Study of Untrusted Relay Network Utilizing Cooperative Jammer". *Amirkabir International Journal of Electrical and Electronics Engineering*, 48(2), pp. 93–99.
DOI: 10.22060/eej.2016.820
URL: http://eej.aut.ac.ir/article_820.html
*Corresponding Author, Email: abm125@aut.ac.ir

1- Introduction

Cooperative relaying is an effective method for power reduction, coverage extension and throughput enhancement in wireless communications [1]. Recently, with the advance of wireless information-theoretic security at the physical layer, a new dimension for designing relaying strategies has emerged. In specific, from a perspective of physical layer security (PLS) which eliminates the requirement of complex higher-layer secrecy techniques, such as encryption and cryptographic key management [2], a relay can be friendly and may help keep the message from being eavesdropped by malicious users [2]. This perfect secure transmission is done by degrading the received signal-to-noise ratio (SNR) at the eavesdropper nodes [3].

While most of the recent works assume that the relay nodes are trustworthy and the eavesdropper is an external node, in this paper, we consider an amplify-and-forward (AF) cooperative network with an untrusted relay. This system model may correspond to several scenarios in practice. For instance, in a public network, an untrusted relay may be used without the same security clearance [4]. In these networks, the relays required for connectivity may be untrusted. Also, in a government intelligence network or the network of a financial institution, the relay may have a lower security permission than the source and the destination. In both of these examples, although the relay is a cooperating node, the transmitted information must be kept secret from it. The first proposed strategy to achieve a positive secrecy rate was the destination-based cooperative jamming (DBCJ) [5,6], in which CJ is performed at the destination for the source-destination communication at the first phase and then the destination perfectly cancels the jamming signal via self-interference cancelation at the second phase. Recently, some literature have been investigated the performance of the DBCJ technique for the untrusted relay networks [4-9]. In [4,7], the authors investigated a relay network where the source can potentially utilize an untrusted non-regenerative relay to augment its direct transmission of a confidential message to the destination. A lower bound for the ergodic secrecy rate (ESR) of an untrusted relay network without optimal power allocation (OPA) and under the assumption of single-antenna nodes was evaluated in [8]. Furthermore, an upper bound with OPA is presented in [9]. In this paper, different from aforementioned works, we study the performance of the DBCJ of the two-hop AF untrusted relay network under OPA strategy and when the source and relay nodes are equipped with a single antenna while the base station (destination) is equipped with multiple antennas. The ESR is evaluated as the metric of secrecy at high signal-to-noise ratio (SNR) regime and we shall find a closed-form solution for it. Motivated by the recent works on large-scale antenna systems [10], we also derive closed-form expressions for the ESR and secrecy outage probability (SOP).

The remainder of this paper is organized as follows. Section II describes our system model, whereas, in section III, the optimal power allocation problem is presented. In sections IV and V, the ESR and SOP of the optimized network are evaluated, respectively. In section VI, we provide numerical results and show that the OPA scheme provides the better ESR and SOP than EPA scheme. Finally, section V presents our concluding remarks.

2- System model

We consider a two-hop CJ wireless network which consists of one source, one destination, and one untrusted AF relay. The destination is equipped with N_d antennas, while the other nodes are equipped with a single antenna. Each node operates in a half-duplex mode. There is not a direct link between the source and relay, and thus the relay performs as an intermediate node to establish the communication link between the source and destination. A time-division-multiple-access based protocol is assumed. The message transmission is divided into two phases, i.e., the broadcast phase and the relaying phase. Against the conventional relaying protocol [1] is inefficient in the perspective of secure communication, therefore we used the proposed protocol, in the proposed protocol, during the first phase, while the source transmits the information signal, and the destination transmits the jamming signal. During the second phase, the relay sends the scaled version of the received signals to the destination. The maximum-ratio transmission (MRT) beamformer and maximum-ratio combining (MRC) are applied at the destination to maximize the received SNR at the relay and at the destination, respectively.

The complex Gaussian channel vector from the source to the relay and the relay to the destination are denoted by $h_{sr} \sim CN(0,\mu_{sr})$ and $h_{rd} \sim CN(0,\mu_{rd}\mathbf{I}_{N_d})$, respectively. All the channel coefficients remain constant within one frame and vary independently from one frame to another. We also assume that the

nodes are perfectly synchronized and the channels satisfy the reciprocity theorem. The additive white noise n_m ($m\in\{r,d\}$) at each receiver is represented by a zero-mean complex Gaussian variable with variance N_0. The total transmit power of each phase is limited by P. Furthermore, $\gamma_{sr}=\rho|h_{sr}|^2$ and $\gamma_{rd}=\rho||h_{rd}||^2$, where $\rho=P/N_0$ is the transmit SNR of the system. Moreover, the average SNRs per branch are $\bar{\gamma}_{sr}=\rho\mu_{sr}$ and $\bar{\gamma}_{rd}=\rho\mu_{rd}$.

In the first phase or broadcast phase, the source transmits its message with power λP, and simultaneously, the destination emits artificial noise with power $(1-\lambda)P$, where $\lambda\in(0,1)$ is the power allocation factor. Thus, the signal-to-interference and-noise-ratio (SINR) at the relay is expressed as [9]

$$\gamma_R=\frac{\lambda\gamma_{sr}}{(1-\lambda)\gamma_{rd}+1} \tag{1}$$

In the second phase or relaying phase, the relay sends the scaled version of the received signals from both the source and destination, so that the power constraint P is maintained. Finally, since the destination knows its own signal or the jamming signal, it subtracts that signal and then decodes the source information from the reminder signal. Therefore, the SINR at the destination can be calculated as:

$$\gamma_D=\frac{\lambda\gamma_{sr}\gamma_{rd}}{\lambda\gamma_{sr}+(2-\lambda)\gamma_{rd}+1} \tag{2}$$

3- Optimal power allocation problem

The instantaneous secrecy rate is evaluated by [2]

$$C_s=\frac{1}{2}[\log_2\left(\frac{1+\gamma_D}{1+\gamma_R}\right)]^+ \tag{3}$$

where $[x]^+=\max\{0,x\}$. For the conventional scheme which is a standard AF relaying protocol [1], $C_s=0$. This fact is found by considering the inequality $xy/(x+y)\le\min\{x,y\}\le x$ [11]. However, for the proposed system, the result is different. If we consider $\lambda=0$ in (1) and (2), one can obtain $C_s=0$. Since in this paper, we want to allocate the power optimally to the source and destination, therefore $C_s\ge0$. Thus, the instantaneous secrecy rate (3) is changed to

$$C_s=\frac{1}{2}\log_2\left(\frac{1+\gamma_D}{1+\gamma_R}\right) \tag{4}$$

In order to maximize the instantaneous secrecy rate, we should find the OPA factor which is denoted by λ^*. With regard to (4), λ^* is the solution of the following constrained optimization problem

$$\lambda^*=\arg\max\phi(\lambda),\quad \text{s.t. } 0<\lambda<1 \tag{5}$$

where $\phi(\lambda)=(1+\gamma_D)/(1+\gamma_R)$. In this study, we first perform the analysis at high-SNR regime and then, for large N_d. The high-SNR analysis is beneficial in the analytical approach. Because we will observe that the function $\phi(\lambda)$ is a quasiconcave function, and its optimal solution in the feasible set ($0<\lambda<1$) is simple and easy to handle for further analysis. For large N_d, we can say that while a secure transmission is maintained, the received SNR at the destination is increased and therefore, the instantaneous secrecy rate is increased. Moreover, the recent researches show that exploiting large scale-antenna arrays at the base stations present advantageous and therefore in the next generation, the base stations are equipped with large scale antenna arrays [10].

$$\gamma_R\approx\frac{\lambda\gamma_{sr}}{(1-\lambda)\gamma_{rd}}=\frac{\lambda v}{(1-\lambda)}\gamma_D\approx\frac{\lambda\gamma_{sr}}{\lambda v+2-\lambda} \tag{6}$$

where $v=\gamma_{sr}/\gamma_{rd}$.

Theorem 1: At the high-SNR regime, the function $\phi(\lambda)$ is a quasiconcave function of λ in the feasible set and its maximum can be expressed in general form as

$$\lambda^*=\frac{1}{\sqrt{\frac{v^2+v}{2}}+1} \tag{7}$$

and in special case of $v\ll1$, it is $\lambda^*=1-(v/2)^{1/2}$.

Proof: See paper [9].

4- Ergodic secrecy rate

In this section, we investigate the ESR of the proposed secure transmission scheme when OPA technique is applied. The ESR is defined as [2]

$$\bar{C}_s=E\{C_s(\gamma_{sr},\gamma_{rd}\} \tag{8}$$

To evaluate the average of C_s, we first get the conditional probability of a random variable and then we take an average over that random variable [12], thus the ESR can be reformulated as

$$\begin{aligned}\bar{C}_s&=E_{\gamma_{rd}}\{E_{\gamma_{sr}}\{C_s(\gamma_{sr},\gamma_{rd})|\gamma_{rd}\}\}\\&=E_{\gamma_{rd}}\{\int_0^\infty(C_s|\gamma_{rd})f_{\gamma_{sr}}(x)dx\}\\&=\int_0^\infty\int_0^\infty C_s y f_{\gamma_{sr}}(vy)f_{\gamma_{rd}}(y)dvdy\end{aligned} \tag{9}$$

where $E_x\{y\}$ is the expectation of y with respect to x. Moreover, $f_{\gamma_{sr}}(x)$ and $f_{\gamma_{rd}}(x)$ are the probability density functions (PDF) of γ_{sr} and γ_{rd}, respectively. Here, γ_{sr} and γ_{rd} are exponential and chi-square random variables respectively, with the following PDFs

$$f_{\gamma_{sr}}(x)=\frac{1}{\bar{\gamma}_{sr}}e^{-x/\bar{\gamma}_{sr}},\quad f_{\gamma_{rd}}(x)=\frac{x^{N_d-1}e^{-x/\bar{\gamma}_{rd}}}{\Gamma(N_d)\bar{\gamma}_{rd}^{N_d}} \tag{10}$$

In the following, we investigate the ESR of the proposed system at the high-SNR regime and for LSA and VLSA.

4- 1- High SNR analysis

It is straightforward to evaluate the ESR at high-SNR. To this end, by inserting (7) into (6) and using (10) and MAPLE software, we obtain a compact expression for the ESR as

$$C_s=\frac{1}{2\ln 2}\{\ln\bar{\gamma}_{\rm sr}-C-N_{\rm d}\times\frac{\mu_{\rm rd}}{\mu_{\rm sr}}\times \int_0^{\infty}\ln(1+3x+2\sqrt{2(x+x^2)})\left(\frac{\mu_{\rm rd}}{\mu_{\rm sr}}x+1\right)^{-(N_{\rm d}+1)}{\rm dx}\} \tag{11}$$

where $C\approx0.577$ is the Euler's constant (Eq. (8.365) in [14]). In the above numerical expression, by increasing N_d, the function in the integral is considerably around zero. As we know, for x→0, ln(1+x)≈ln(x), therefore $\ln\{1+3x+2[2(x+x^2)]^{1/2}\}\approx2(2x)^{1/2}$. By using Eq. (ET I 310(21)) in [14], the expression (11) is changed to the the following closed-form solution

$$\bar{C}_s=\frac{1}{2\ln 2}\{\ln\bar{\gamma}_{\rm sr}-C-N_{\rm d}\sqrt{\frac{\mu_{\rm sr}}{\mu_{\rm rd}}}B\left(\frac{3}{2},N_{\rm d}-\frac{1}{2}\right)\} \tag{12}$$

where $B(x,y)$ is the Beta function (part 8.38 in [14]).

4- 2- Large-scale antenna arrays

In this case, $v=|h_{\rm sr}|^2/\|h_{\rm rd}\|^2<<1$, and thus according to theorem 1, $\lambda^*=1-(v/2)^{1/2}$. Therefore, one can obtain

$$\gamma_R=\sqrt{2v}-v\approx\sqrt{2v}$$

$$\gamma_{\rm D}=\frac{\left(1-\sqrt{\frac{v}{2}}\right)v\gamma_{\rm rd}}{v-v\sqrt{\frac{v}{2}}+\sqrt{\frac{v}{2}}+1}\approx\gamma_{\rm sr} \tag{13}$$

Using (13) and following the same approach in the ESR of part 1, the ESR can be written as

$$\begin{aligned}\bar{C}_s&=\frac{1}{2}\{\log_2(1+\gamma_{\rm sr})-\log_2(1+\sqrt{2v})\}\\&=\frac{1}{2\ln 2}(\int_0^{\infty}\ln(1+x)f_{\gamma_{\rm sr}}(x)dx\\&-\int_0^{\infty}\int_0^{\infty}y\ln(1+\sqrt{2v})f_{\gamma_{\rm sr}}(vy)f_{\gamma_{\rm rd}}(y)dvdy)\\&=\frac{1}{2\ln 2}\{e^{\frac{1}{\bar{\gamma}_{\rm sr}}}E_1\left(\frac{1}{\bar{\gamma}_{\rm sr}}\right)-N_{\rm d}\bar{\gamma}_{\rm rd}\bar{\gamma}_{\rm sr}^{N_{\rm d}}\times\end{aligned} \tag{14}$$

$$\int_0^{\infty}\ln(1+\sqrt{2v})\left(\frac{1}{\bar{\gamma}_{\rm sr}+v\bar{\lambda}_{\rm rd}}\right)^{N_d+1}dv\}$$

where $E_1(x)$ is the exponential integral function [14]. Since $\bar{\gamma}_{\rm rd}$ and N_d are large numbers, thus the dominant values of the function in the above integral are around zero. Therefore $\ln(1+(2v)^{1/2})\approx(2v)^{1/2}$.

Using Eq. (EH I 205) in [14] the ESR can be approximated as the following compact form

$$\begin{aligned}\bar{C}_s&=\frac{1}{2\ln 2}\{e^{\frac{1}{\bar{\gamma}_{\rm sr}}}E1\left(\frac{1}{\bar{\gamma}_{\rm sr}}\right)-\sqrt{2}N_d\left(\frac{\mu_{\rm sr}}{\mu_{\rm rd}}\right)^2\\&\times B\left(N_{\rm d}-\frac{1}{2},\frac{3}{2}\right)\times2F_1(N_{\rm d}+1,N_{\rm d}-\frac{1}{2};N_{\rm d}+1,1-\frac{\mu_{\rm sr}}{\mu_{\rm rd}}\}\end{aligned} \tag{15}$$

where $2F_1$ (a,b;c,d) denotes the incomplete Beta function (part 8.39 in [14]).

4- 3- Very large-scale antenna arrays

For very large antenna arrays, $v\to0$, the ESR is reduced to a simple closed-form expression as

$$\bar{C}_s=\frac{e^{\frac{1}{\bar{\gamma}_{\rm sr}}}}{2\ln 2}E_1\left(\frac{1}{\bar{\gamma}_{\rm sr}}\right) \tag{16}$$

5- Secrecy outage probability

Inserting (13) the SOP definition, the SOP is given by

$$\begin{aligned}P_{out}&=P_r\{\frac{1}{2}\log_2\left(\frac{1+\gamma_{\rm sr}}{1+\sqrt{2v}}\right)<R\}\\&=P_r\{\gamma_{sr}<2\gamma_{\rm sr}(2^{-2R}\gamma_{\rm sr}+2^{-2R}-1)^{-2}\}\\&=E_{\gamma_{\rm sr}}\{F_{\gamma_{\rm rd}}(\zeta\,|\,\gamma_{\rm sr}=x)\}=1-E_{\gamma_{\rm sr}}\{e^{-\frac{\zeta}{\bar{\gamma}_{\rm rd}}}\sum_{k=0}^{N_{\rm d}-1}\frac{1}{k!}(\frac{\zeta}{\bar{\gamma}_{\rm rd}})^k\}\\&=1-\sum_{k=0}^{N_d-1}\int_0^{\infty}\frac{1}{k!\bar{\gamma}_{\rm sr}}\left(\frac{\zeta}{\bar{\gamma}_{\rm rd}}\right)^k e^{-\left(\frac{\zeta}{\bar{\gamma}_{\rm rd}}+\frac{x}{\bar{\gamma}_{\rm sr}}\right)}dx\\&=1-\frac{1}{\bar{\gamma}_{\rm sr}\Gamma(N_{\rm d})}\int_0^{\infty}e^{-\frac{x}{\bar{\gamma}_{\rm sr}}}\Gamma\left(N_{\rm d},\frac{\zeta}{\bar{\gamma}_{\rm rd}}\right)dx\end{aligned} \tag{17}$$

where $\zeta=2x(2^{-2R_x}+2^{-2R}-1)^{-2}$ and $\Gamma(\bullet,\bullet)$ denotes the complementary incomplete Gamma function. We used these facts that we first get the conditional probability of a random variable and then we took an average of that random variable, also the fact that $\gamma_{\rm rd}$ is a chi-square random variable with $2Nd$ degrees of freedom and its CDF is deterministic [12], also the fact that $\gamma_{\rm sr}$ has the exponential pdf. Hence, for large N_d, a single numerical integration was presented to evaluate the SOP. For very large scale antenna arrays ($v\to0$), we can write

$$P_{out} = P_r\{\frac{1}{2}\log_2(1+\gamma_{sr}) < R\} = F_{\gamma_{sr}}\left(2^{2R}-1\right) \quad (18)$$

where the CDF of γ_{sr} is $F_{\gamma_{sr}}(x)$=1-exp(-$x/\bar{\gamma}_{sr}$).

6- Numerical results

In this section, we present some numerical results to verify the ESR and SOP of the proposed secure transmission scheme by Monte-Carlo simulations. We consider OPA and equal power allocation (EPA) (λ=0.5) as well as the case without DBCJ (λ=1). We set $\mu_{sr}=\mu_{rd}$=5. Moreover, we consider N_d=64 for VLSA and N_d=16 for LSA.

Fig. 1 shows the ESR for VLSA. It shows that:

- The curve obtained from (12) is in precise agreement with Monte-Carlo simulation at high SNR regime.

- Our large system analysis in (15) well approximates the ESR at all SNRs.

- For a specific ESR, the OPA is more power efficient than the other power allocation strategies. For example, for 3 *bits/s/Hz*, the OPA saves the power about 3.5 *dB*.

- Without using the DBCJ method, the secure transmission rate is always zero.

We have also provided Fig. 2 to show the accuracy of the evaluated expressions for a smaller number of antenna arrays.

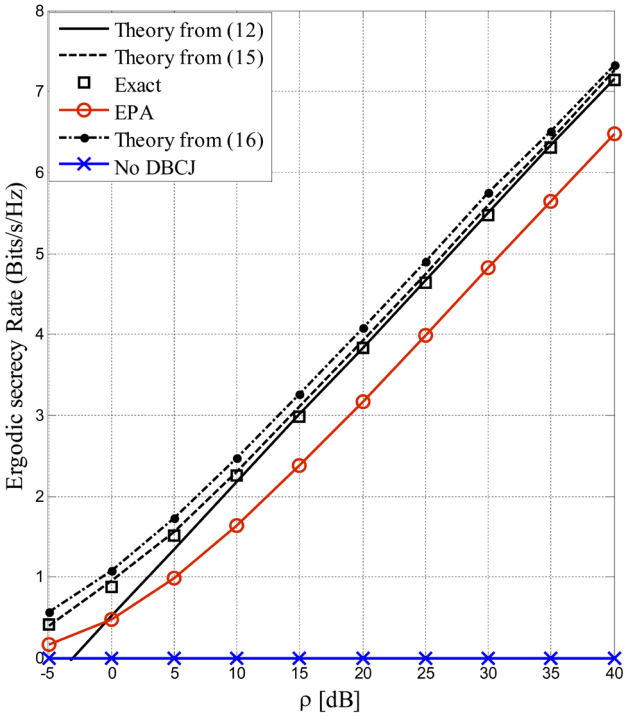

Fig. 1. The ESR versus transmit SNR for VLSA N_d=64. The power of channel gains are set to $\mu_{sr}=\mu_{rd}$=5.

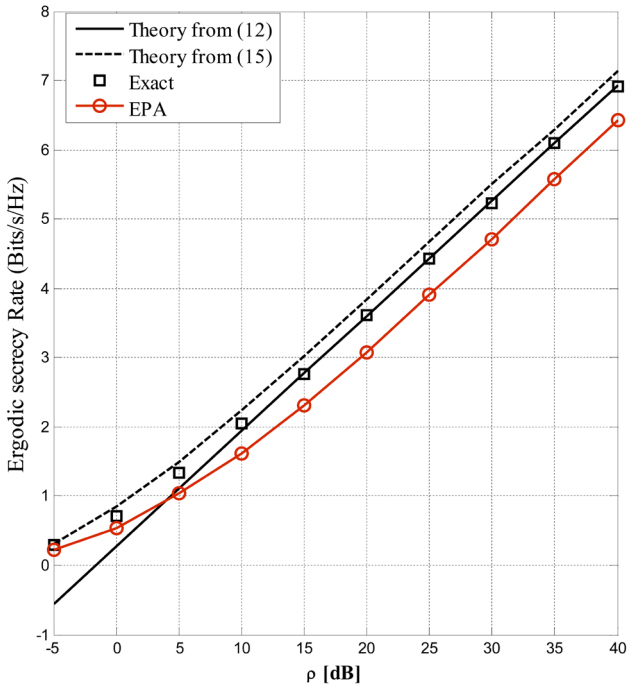

Fig. 2. The ESR versus transmit SNR for VLSA N_d=16. The power of channel gains are set to $\mu_{sr}=\mu_{rd}$=5.

Fig. 3 displays the SOP of the secrecy rate for three power allocation methods. We consider the outage threshold of the secrecy rate as R=1 [*bpcu*]. As can be seen in this figure:

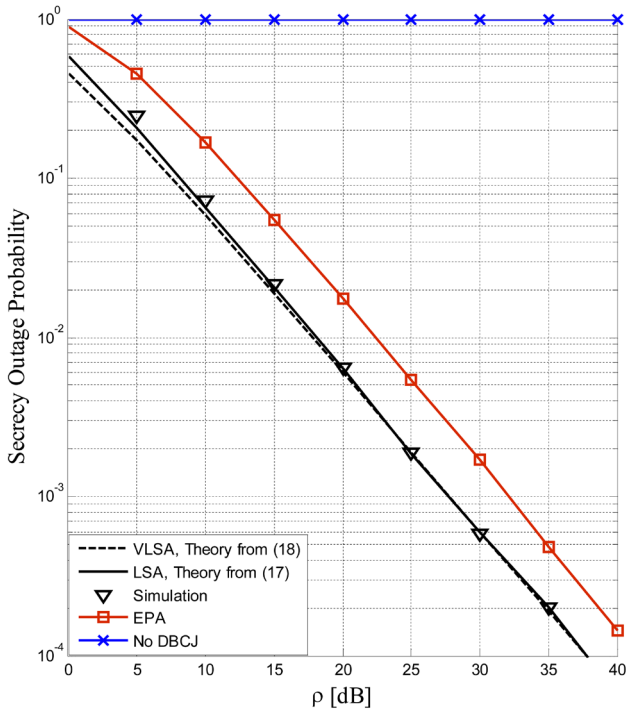

Fig. 3. The SOP versus transmit SNR and the role of different power allocation strategies on the performance of the proposed system. 16 antennas are used for large-scale antenna analysis. The target rate and the average of the channel gains are set to R=1 [*bpcu*] and $\mu_{sr}=\mu_{rd}$=5.

- For large N_d=16, the achieved expressions (17) and (18) are in precise agreement with Monte-Carlo simulations for ρ>20 *dB* or equivalently P_{out}<0.002.

- The OPA offers better SOP than the EPA. For example, at the target SOP P_{out}=0.01, this gap is about 5 *dB*, which presents the efficiency of the proposed OPA.

- As mentioned before, without using the DBCJ method, the system is always in an outage.

Finally, we prepare Fig. 4 to show that $\varphi(\lambda)$ is a quasiconcave function [13] of λ at high γ_{rd}=50. As cen be seen, by increasing v, λ^* decreases, i.e., most of the power is dedicated to the source. Furthermore, by decreasing v, λ^* increases. This means that most of the power is dedicated to the destination.

7- Conclusion

We investigated secure communication in a two-hop wireless relaying network with an untrusted relay. To prevent the relay from intercepting the source message, the DBCJ was proposed. The optimal power allocation (OPA) technique is considered for the system. Based on the OPA, we evaluated the ESR and SOP for the case that the destination is equipped with multiple antenna arrays while the other nodes are equipped with a single antenna. The closed-form expressions were presented for the case. Numerical results showed that the achieved expressions are in proper agreement with Montecarlo simulations. Moreover, the proposed OPA significantly improves the power efficiency in comparison with EPA technique.

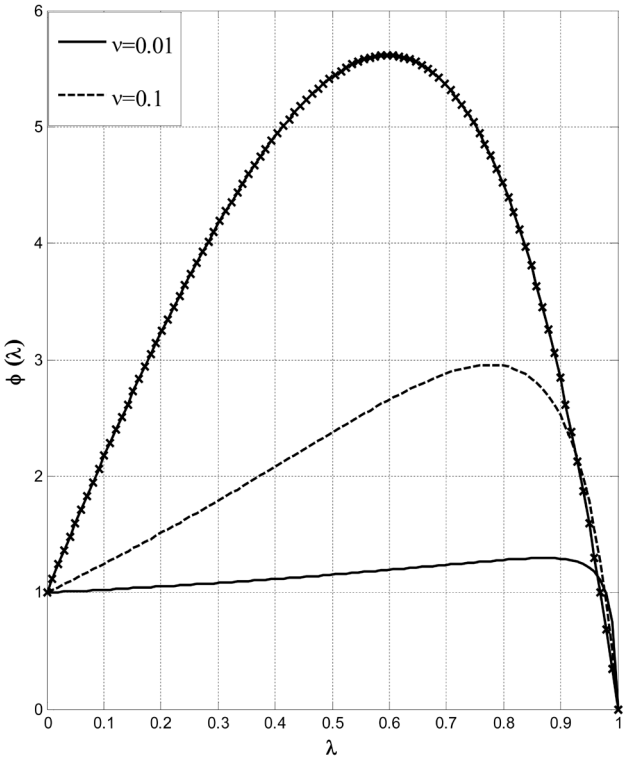

Fig. 4. $\phi(\lambda)$ versus the power allocation factor λ at high γ_{rd}= 50

8- References

[1] Laneman, J. N.; Tse, D. N. C. and Wornell, G. W.; "Cooperative Diversity in Wireless Networks: Efficient Protocols and Outage Behavior," *IEEE Trans. Inf. Theory*, Vol. 50, No. 12, pp. 3062–3080, 2004.

[2] Bloch, M.; Barros, J.; Rodriques, M. R. D. and McLaughlin, S. W.; "Wireless Information-Theoretic Security," *IEEE Trans. Inf. Theory*, Vol. 54, No. 6, pp. 2515–2534, 2008.

[3] Wyner, A. D.; "The Wire-Tap Channel," *Bell Syst. Tech. J.*, Vol. 54, No. 8, pp. 1355–1387, 1975.

[4] Huang, J.; Mukherjee, A. and Swindlehurst, A. L.; "Secure Communication via an Untrusted Non-Regenerative Relay in Fading Channels," *IEEE Trans. Signal Process.*, Vol. 61, No. 10, pp. 2536–2550, 2013.

[5] He, X. and Yener, A.; "Two-Hop Secure Communication Using an Untrusted Relay: A Case for Cooperative Jamming," *in Proc. IEEE Globecom*, New Orleans, LA, p. 15, 2008.

[6] He, X. and Yener, A.; "Two-Hop Secure Communication Using an Untrusted Relay," *EURASIP J. Wireless Commun. Netw.*, p. 13, 2009.

[7] Huang, J.; Mukherjee, A. and Swindlehurst, A. L.; "Outage Performance for Amplify and Forward Channels with an Unauthenticated Relay," *in Proc. IEEE Int. Commun. Conf.*, pp. 893–897, 2012.

[8] Sun, L.; Zhang, T.; Li, Y. and Niu, H.; "Performance Study of Two-Hop Amplify and Forward Systems with Untrustworthy Relay Nodes," *IEEE Trans. Veh. Technol.*, Vol. 61, No. 8, pp. 3801–3807, 2012.

[9] Wang, J.; Elkashlan, M.; Huang, J.; Tran, N. H. and Duong, T. Q.; "Secure Transmission with Optimal Power Allocation in Untrusted Relay Networks," *IEEE Wireless Commun. Lett.*, Vol. 3, No. 3, pp. 289–292, 2014.

[10] Geraci, G.; Couillet, R.; Yuan, J.; Debbah, M. and Collings, I. B.; "Large System Analysis of

Linear Precoding in MISO Broadcast Channels with Confidential Messages," *IEEE J. Sel. Areas Commun.*, Vol. 31, No. 9, pp. 1660–1671, 2013.

[11] Anghel, P. A. and Kaveh, M.; "Exact Symbol Error Probability of a Cooperative Network in a Rayleigh-Fading Environment," *IEEE Trans. Wireless Commun.*, Vol. 3, No. 5, pp. 1416–1421, 2004.

[12] Papoulis, A.; "Probability, Random Variables, and Stochastic Processes," *McGraw-Hill*, New York, 1984.

[13] Boyd, S. and Vandenberghe. L.; "Convex Optimization," *Cambridge University Press*, 2004.

[14] Gradshteyn, I. S. and Ryzhik, I. M.; "Table of Integrals, Series and Products," *Academic*, New York, 7th Edition, 2007.