Relay Selection for Optimized Cooperative Jamming Scheme

Asma Mabrouk
HANA Research Lab, ENSI,
Manouba University
Email: asma.mabrouk@ensi-uma.tn

Kamel Tourki
Mathematical and Algorithmic Sciences Lab,
France Research Center,
Huawei Technologies Co. Ltd.
Email: Kamel.tourki@huawei.com

Noureddine Hamdi
HANA Research Lab, ENSI,
Manouba University
Email: noureddine.hamdi@ept.rnu.tn

***Abstract*—In this paper, we study the problem of secure dual-hop transmission in the presence of an eavesdropper, where a secrecy-enhanced relay selection as well as a destination cooperation are presented to prevent the source information from being eavesdropped. Taking into account the total power budget, a power allocation scheme is investigated to optimize the destination contribution. We present the system performance in terms of secrecy capacity where we derive a closed form expression for its lower bound. Simulation results reveal that a higher power allocation to the jamming signal should be balanced by a closer placement of the relay to the source to get better system performance, and vice versa.**

I. Introduction

Wireless communication systems has became the most dynamic sector of the communication industry. However, the rapid expansion of heterogeneous wireless networks imposes significant technical security challenges. Conventionally, security issues has been primarily considered at upper-layers and are usually based on data encryption methods that provides computationally-secure protocols [1]. Nevertheless, the inherently shared and broadcast nature of the wireless medium leaves it vulnerable to security threats and makes eavesdropping extremely easy. Therefore, nodes within communication range can receive and eventually decode private transmission signals. Alternatively, physical layer security (PLS) has emerged as a promising candidate to complement and significantly strength the security of existing systems. However, to meet the aforementioned aim, relevant coding and precoding techniques that exploit the channel state information (CSI) should be designed. Unlike classic cryptography techniques, PLS could be a key-less security paradigm based on information-theoretic principles and does not rely on limited computational capacity of the eavesdropper.

To enhance the secrecy performance of wireless communications, systems with multiple antennas has been investigated [2], [3]. Using transmit antenna selection (TAS), the authors in [2] provided the closed form expression of the secrecy outage probability (SOP). Furthermore, the results in [3] have shown that the maximum secrecy outage diversity gain can be achieved using TAS, and generalized selection combining at the receiver. On the other side, motivated by the positive impact of cooperative communication on spectral efficiency [4], [5], transmission reliability [6] and communication range extension [7], relay cooperation has gained much interest in enhancing communication security. However, in relay networks, an eavesdropper may receive the same message several times due to redundant transmission. Therefore, it is essential to protect the information from being eavesdropped by unintended receivers.

The key idea of cooperative techniques is to boost the system's secrecy by improving the capacity of the main channel while reducing the capacity of the eavesdropper channel. To this end, several PLS approaches have been proposed following two main strategies referred to as cooperative relaying and cooperative jamming (CJ) [8], [9]. In cooperative relaying, the secrecy rate is improved by enhancing the signal-to-noise ratio (SNR) at the legitimate receiver where the relay acts as a helper to strengthen the main channel performance. In [8], using Amplify-and-Forward (AF) and Decode-and-Forward (DF) schemes, the authors investigated the PLS in the presence of an external eavesdropper. In [10], the authors analyze the secrecy performance of a cooperative DF and Randomize-and-Forward relaying network showing the effect of relay placement on the SOP. Moreover, relay selection (RS) has been used in [8] where an appropriate relay has been selected to assist the PLS taking into account the eavesdropper links. On the other hand, CJ is based on interfering the eavesdropper with artificial noise through nodes acting as friendly jammers to enhance the secrecy capacity. Conventionally, a friendly jammer could be an external node recruited to help the source [11]. Moreover, in CJ, the system performance heavily depends on the power devoted to the jamming signal. The jamming signal power should be high enough to disturb the received signal at the eavesdropper. However, allocating high power to the jamming signal can also degrade the signal quality at the legitimate receiver. Thus, several works have been proposed to master this limitation by optimizing the jamming power level. In [12], a destination-based jamming (DBJ) is proposed where the destination acts as a jammer to confuse the eavesdropper during the first phase. however, the authors in [13] considered cooperative scheme where the relay transmits both useful signal and jamming noise simultaneously, and a power allocation is adopted. This scenario has been improved where the source, the relay and

978-0-9928626-3-3/15/$31.00 ©2015 IEEE

the destination send the jamming signals [14].

In this paper, we investigate PLS using relay selection scheme where the DBJ is proposed under a total power constraint. The best second hop relay is selected and acts as a helper and does not make any malicious attack. The destination relies strongly on the second hop to receive the source's information. We investigate the power allocation scheme as well as the relay cluster placement enhancing the secrecy capacity. The results reveal that a higher power allocation to the jamming signal should be balanced by a closer placement of the selected relay to the source to get better system performance, and vice versa.

II. System model

A. System and transmission model

We consider a dual-hop secure communication system where a source (S) is communicating with a destination (D) through K relays $\{R_k\}_{k=1}^{K}$ in the presence of an eavesdropper (E). All nodes are equipped with single antenna and operate in half-duplex mode. The source has no direct link to the destination as well as to the eavesdropper[1]. The relays are assumed to be trusted and close to each other forming a cluster[2]. In our scheme, relays are used only to convey the source information toward the destination. We consider Rayleigh fading channels and we denote h_{ij} the channel coefficient between the nodes i and j, following $h_{ij} \sim CN\left(0, d_{ij}^{-\nu}\right)$, where d_{ij} is the distance between i and j, and ν is the path-loss exponent of wireless channels.

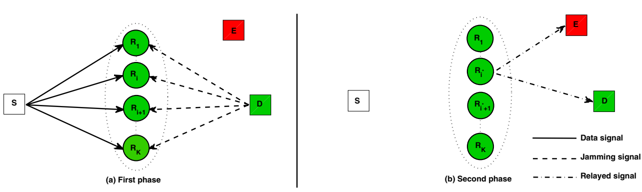

Fig. 1. System and transmission model.

During the first phase, the source transmits s, while the destination cooperates by transmitting a jamming signal z,where both s and z have unit power. The received signal at the k^{th} relay is given by

$$y_k = \sqrt{(1-\alpha)\frac{P}{2}} h_{sk} s + \sqrt{\alpha \frac{P}{2}} h_{kd} z + n_k, \quad (1)$$

where n_k is a complex additive white gaussian noise (AWGN) following $n_k \sim CN(0, \sigma_k^2)$, and α is the power allocation factor where $\alpha \in (0, 1]$. Considering a passive eavesdropper where its CSI is not available to the system, a conventional relay selection is adopted according to the following rule

$$i = \arg\max_{k} \left(\gamma_{kd}\right). \quad (2)$$

[1]We consider that E is close to D so that the information leakage occurs in the second phase only.

[2]Assuming a cluster-based relay system, channels from the relay nodes to S, D and E are independent and identically distributed (i.i.d).

During the second phase, the selected relay uses the AF protocol to convey the source information. Hence, the received signal at D is

$$y_d = G h_{id} y_i + n_d, \quad (3)$$

where n_d is the additive noise at D and G is the amplification factor at the selected relay, given by

$$G = \sqrt{\frac{\frac{P}{2}}{|h_{si}|^2 (1-\alpha)\frac{P}{2} + |h_{id}|^2 \alpha \frac{P}{2} + \sigma^2}}. \quad (4)$$

As the jamming signal is provided by D, the later can perform a self-interference subtraction to get the data signal.

$$y_d = \sqrt{(1-\alpha)\frac{P}{2}} G h_{si} h_{id} s + G h_{id} n_i + n_d. \quad (5)$$

On the other hand, the received signal at E is given by

$$y_e = \sqrt{(1-\alpha)\frac{P}{2}} G h_{si} h_{ie} s + \sqrt{\alpha \frac{P}{2}} G h_{id} h_{ie} z + G h_{ie} n_i + n_e, \quad (6)$$

where $n_e \sim CN(0, \sigma_e^2)$. We assume, for simplicity, that $\sigma_k^2 = \sigma^2$ for $k \in \{s, d, i, e\}$.

It is worth noting that the total power budget is P where $\frac{P}{2}$ for each phase. Thus, the source, the destination and the selected relay are transmitting using $P_s = (1-\alpha)\frac{P}{2}$, $P_z = \alpha \frac{P}{2}$ and $P_i = \frac{P}{2}$, respectively. Accordingly, we define the instantaneous SNRs of the source-relay, relay-destination and relay-eavesdropper links, as $\delta_s = (1-\alpha)|h_{sr}|^2 \frac{P}{2\sigma^2} = (1-\alpha)\gamma_s$, $\delta_d = \alpha |h_{rd}|^2 \frac{P}{2\sigma^2} = \alpha \gamma_d$, and $\delta_e = |h_{re}|^2 \frac{P}{2\sigma^2}$, respectively. The denote $\rho = \frac{P}{2\sigma^2}$.

B. Received SNRs

Referring to (4) and (5), the received SNR at D is given by

$$\Gamma_d = \frac{(1-\alpha)\gamma_s \gamma_d}{(1-\alpha)\gamma_s + (1+\alpha)\gamma_d + 1}, \quad (7)$$

where $\gamma_s = |h_{si}|^2 \rho$ and $\gamma_d = |h_{id}|^2 \rho$. On the other hand, the received SNR at the eavesdropper, Γ_e, is given by

$$\Gamma_e = \frac{(1-\alpha)\gamma_s \gamma_e}{(1-\alpha)\gamma_s + \alpha \gamma_d (\gamma_e + 1) + \gamma_e + 1}, \quad (8)$$

where $\gamma_e = |h_{ie}|^2 \rho$.

III. Performance analysis

In this section, we investigate the ergodic secrecy capacity (ESC) of the DBJ scheme, which is given by

$$C_s = E\left\{\left[\frac{1}{2}\log_2\left(\frac{1+\Gamma_d}{1+\Gamma_e}\right)\right]^+\right\}, \quad (9)$$

where $E[.]$ is the expectation operator. Since the closed form expression of the ESC is intractable, we derive its lower bound referred to as C_{LB}, and given by

$$\begin{aligned} C_{LB} &= \left[E\left\{\frac{1}{2}\log_2\left(\frac{1+\Gamma_d}{1+\Gamma_e}\right)\right\}\right]^+ \\ &= \left[\frac{1}{2\ln 2}\left(E\{\ln(1+\Gamma_d)\} - E\{\ln(1+\Gamma_e)\}\right)\right]^+ \end{aligned} \quad (10)$$

Hereafter, we denote $X = a\gamma_s$ and $Y = b\gamma_d$, where $a = 1-\alpha$ and $b = 1+\alpha$. Thus, we have

$$\begin{aligned} E\left\{\ln\left(1+\Gamma_d\right)\right\} &= E\left\{\ln\left(1+\frac{1}{b}\frac{XY}{X+Y+1}\right)\right\} \\ &\geq \ln\left(1+\frac{1}{b}e^{E\{\ln(XY)\}-E\{\ln(X+Y+1)\}}\right). \end{aligned} \tag{11}$$

Hence, the first term of C_{LB} is lower bounded by $\ln\left(1+\frac{1}{b}e^{I_1+I_2}\right)$ where I_1 and I_2 are given by:

$$I_1 = E\{\ln(XY)\} = \int_0^\infty \int_0^\infty \ln(xy) f_X(x) f_Y(y) \quad dxdy, \tag{12}$$

and

$$I_2 = E\{\ln(X+Y+1)\} = \int_0^\infty \ln(1+z) f_Z(z) \quad dz, \tag{13}$$

respectively, where $Z = X+Y$ whose probability density functions (pdfs) are given by $f_X(x)$ and $f_Y(y)$, respectively. Using [15, Eq.(4.331.1)], I_1 is given by

$$I_1 = \left(-\varepsilon - \ln\left(\frac{1}{a\overline{\gamma}_s}\right)\right) + \sum_{i=1}^{K}\binom{K}{i}(-1)^i\left(\varepsilon + \ln\left(\frac{i}{b\overline{\gamma}_d}\right)\right), \tag{14}$$

where ε is the Euler constant [15, Eq.(8.367.1)]. On the other hand, to calculate I_2, we should start by deriving $f_Z(.)$, given by:

$$\begin{cases} \sum_{i=1}^{K}\binom{K}{i}(-1)^{i-1}\frac{iz}{a\overline{\gamma}_s b\overline{\gamma}_d}e^{-\frac{z}{a\overline{\gamma}_s}} & , ia\overline{\gamma}_s = b\overline{\gamma}_d \\ \sum_{i=1}^{K}\binom{K}{i}(-1)^{i-1}\frac{i}{ia\overline{\gamma}_s - b\overline{\gamma}_d}e^{-\frac{z}{a\overline{\gamma}_s}}\times & \\ \qquad \left(1-e^{-\frac{ia\overline{\gamma}_s - b\overline{\gamma}_d}{a\overline{\gamma}_s b\overline{\gamma}_d}z}\right) & , ia\overline{\gamma}_s \neq b\overline{\gamma}_d \end{cases} \tag{15}$$

Then, using (15) and [15, Eq.(4.337.5)], I_2 can be simplified as given by (16) (as shown by Appendix.A).

On the other hand, and using the cumulative distribution function (cdf) of Γ_e, $F_{\Gamma_e}(.)$, the second term of ESC is given by

$$E\{\ln(1+\Gamma_e)\} = \int_0^\infty \frac{1}{1+x} \quad (1 - F_{\Gamma_e}(x))\, dx, \tag{17}$$

which is given by (18) (as shown by Appendix.B), where $\mu = \frac{\overline{\gamma}_e + a\overline{\gamma}_s}{a\overline{\gamma}_s\overline{\gamma}_e}$ and $\nu = \frac{i(\overline{\gamma}_e + a\overline{\gamma}_s)}{\alpha\overline{\gamma}_d\overline{\gamma}_e}$.

Finally, by substituting the results in (14), (16) and (18) into (10), the lower bound of ESC can be obtained.

IV. Performance Results

In this section, simulations results are presented to confirm the benefits of the joint DBJ/RS proposed scheme. Considering a linear topology where the distances are normalized by the S-D distance, d_{sd}, the relay cluster is located at a distance d_{sr} from S equal to $1-d_{rd}$. Furthermore, we consider that the distance between the selected relay and E, d_{re}, is equal to 1. For any i and j nodes, $E[|h_{ij}|^2] = d_{ij}^{-\nu}$ where ν is the path-loss exponent, set to 4.

We examine the effect of the network parameters such as K, d_{sr} and α, on the C_s expression. In Fig. 2, C_{LB} expression is presented as function of ρ where K varies. Considering the selected relay at the mid-distance between S and D ($d_{sr} = 0.5$), the simulations have been carried out using a jamming power level set to 0.5. We can note that using DBJ, the system performs better as the number of relays increases. Moreover, the results confirm the accuracy of the analysis for the derived bound C_{LB}. Thereafter, only theoretical curves will be presented.

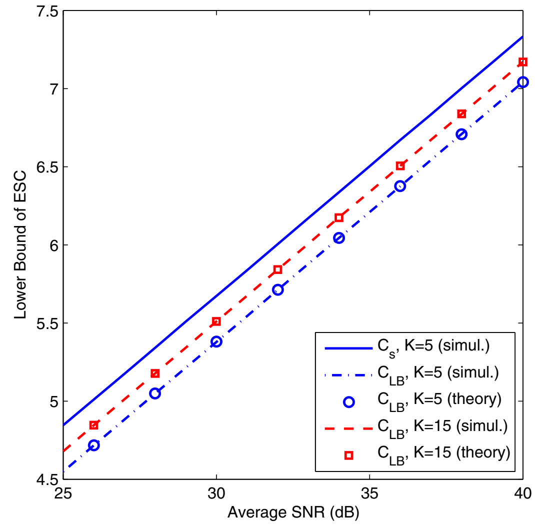

Fig. 2. The ESC as a function of ρ in Rayleigh fading channels using different values of K.

In Fig. 3, C_{LB} expression is presented as a function of d_{sr}. By varying the jamming power level, it has been shown that an optimum relay position can enhance significantly the secrecy capacity of the system. For a higher value of α, it follows that C_{LB} increases for a closer relay position to the source. The figure also pointed out that a better ESC performance is achieved when the relay at the middle between S and D when α has a moderate value. It is worth noting that K does not affect the optimal relay position. This is due to the clustered relays assumption.

In Fig. 4, we plot the ESC curves with respect to α where $d_{sr} = 0.5$. It can be seen that the optimal fraction of power allocated to the jamming signal, α^*, is influenced by ρ and the number of relays K. Indeed, for a given ρ, α^* decreases as K increases. This is due to the fact that, increasing K, implies a better selected relay-destination channel.

Results are expected since the performance of cooperative communications is, in general, limited by the weaker link. Specifically, when the relay-cluster is set closely to the source the second hop shows a poor channel quality improved by the proposed selection scheme, resulting in a remarkable performance enhancement. Here, most of the available power would be allocated for the jamming signal since the source has

$$I_2 = \begin{cases} \sum_{i=1}^{K} \binom{K}{i}(-1)^{i-1}\left(1+\left(\frac{1}{a\overline{\gamma}_s}-1\right)e^{\frac{1}{a\overline{\gamma}_s}}Ei\left(-\frac{1}{a\overline{\gamma}_s}\right)\right) & ,ia\overline{\gamma}_s = b\overline{\gamma}_d \\ \sum_{i=1}^{K} \binom{K}{i}(-1)^{i-1}\frac{i}{ia\overline{\gamma}_s - b\overline{\gamma}_d}\left(\frac{b\overline{\gamma}_d}{i}e^{\frac{i}{b\overline{\gamma}_d}}Ei\left(-\frac{i}{b\overline{\gamma}_d}\right) - a\overline{\gamma}_s e^{\frac{1}{a\overline{\gamma}_s}}Ei\left(-\frac{1}{a\overline{\gamma}_s}\right)\right) & ,ia\overline{\gamma}_s \neq b\overline{\gamma}_d \end{cases} \tag{16}$$

$$E\{\ln(1+\Gamma_e)\} = \begin{cases} \sum_{i=1}^{K} \binom{K}{i}(-1)^{i-1}\frac{ia\overline{\gamma}_s}{ia\overline{\gamma}_s - \alpha\overline{\gamma}_d} \quad (e^{\mu}Ei(-\mu) - e^{\nu}Ei(-\nu)) & , \quad ia\overline{\gamma}_s \neq \alpha\overline{\gamma}_d \\ \sum_{i=1}^{K} \binom{K}{i}(-1)^{i-1}(1+\mu e^{\mu}Ei(-\mu)) & , \quad ia\overline{\gamma}_s = \alpha\overline{\gamma}_d \end{cases} \tag{18}$$

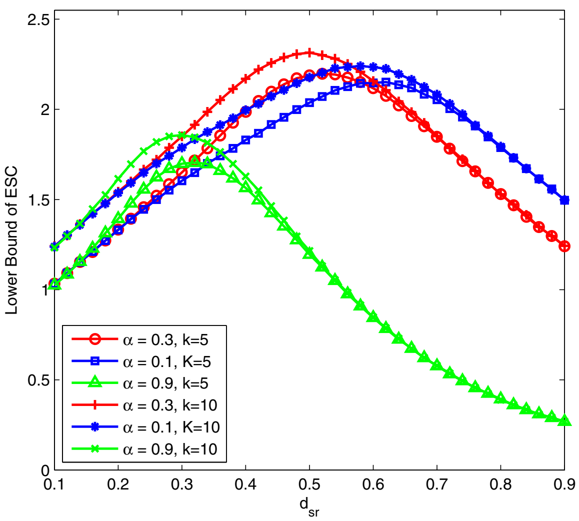

Fig. 3. The lower bound of ESC versus d_{sr} using different jamming power factors when $K = 5, 10$ and $\rho = 10$ dB.

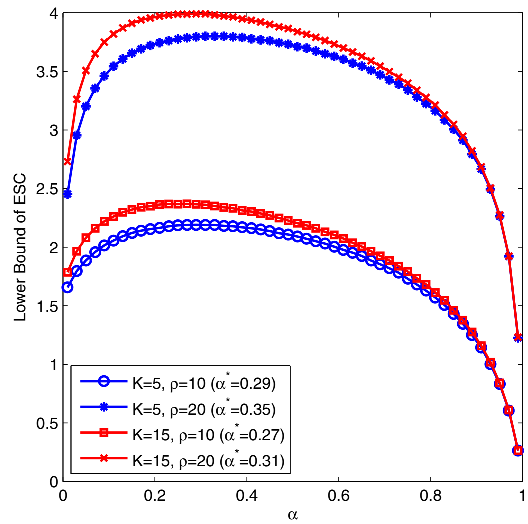

Fig. 4. Ergodic secrecy performance as function of the jamming power level for different values of ρ and K, when $d_{sr} = 0.5$.

strong channel with the relay to transmit its information in the first phase. However, when the relay-cluster is placed closer to the destination the first hop becomes the bottleneck of the communication performance and so the source use more power to send its data. The aforementioned observations address the key design issue on how to find an optimal relay position to guarantee the performance gains provided by RS. At last, with the destination-based jamming (DBJ) scheme under fixed transmission power assumption, the power allocation scheme provides efficient balance power handling along with secrecy performance improvement.

V. Conclusion

In this work, we investigated the problem of secure dual-hop transmission in the presence of an eavesdropper, where a secrecy-enhanced relay selection as well as a destination co-operation are presented to prevent the source information from being eavesdropped. An optimal power allocation between jamming and data signals has been proposed. We derived a closed-form expression for the lower bound of the secrecy capacity. Simulation results revealed that, the secrecy rate improves when increasing the number of relays. Furthermore, the transmit power should be adapted according to the selected relay placement to get better secrecy rate.

Appendix

A. Derivation of Eq.16

Based on the pdf expression in (15), the integral I_2 is given by

$$I_2 = \int_0^{\infty} \ln(1+z) f_Z(z) dz. \tag{19}$$

If $ia\overline{\gamma}_s = b\overline{\gamma}_d$, then using [15, Eq.(4.337.5)], I_2 is given by

$$\begin{aligned} I_2 &= \sum_{i=1}^{K} \binom{K}{i}(-1)^{i-1}\frac{i}{a\overline{\gamma_s}b\overline{\gamma_d}}\int_0^{\infty} z\ln(1+z)e^{-\frac{z}{a\overline{\gamma_s}}} \quad dz \\ &= \sum_{i=1}^{K} \binom{K}{i}(-1)^{i-1}\left(1-\left(\frac{1}{a\overline{\gamma}_s}-1\right)e^{\frac{1}{a\overline{\gamma}_s}}Ei\left(\frac{1}{a\overline{\gamma}_s}\right)\right), \end{aligned} \tag{20}$$

where Ei is the exponential integral function defined in [15, Eq.(8.21)]. However, when $ia\overline{\gamma}_s \neq b\overline{\gamma}_d$, and using [15, Eq.(4.337.2)], I_2 is given by

$$\begin{aligned} I_2 = &\sum_{i=1}^{K} \binom{K}{i}(-1)^{i-1}\frac{i}{ai\overline{\gamma_s} - b\overline{\gamma_d}}\times \\ &\left(\int_0^{\infty} \ln(1+z)e^{-\frac{z}{a\overline{\gamma_s}}} \quad dz - \int_0^{\infty} \ln(1+z)e^{-\frac{i}{b\overline{\gamma_d}}z} \quad dz\right) \end{aligned}$$

$$= \sum_{i=1}^{K} \binom{K}{i} (-1)^{i-1} \frac{i}{ia\overline{\gamma}_s - b\overline{\gamma}_d} \times \left(-a\overline{\gamma}_s e^{\frac{1}{a\overline{\gamma}_s}} Ei\left(-\frac{1}{a\overline{\gamma}_s}\right) + \frac{b\overline{\gamma}_d}{i} e^{\frac{i}{b\overline{\gamma}_d}} Ei\left(-\frac{i}{b\overline{\gamma}_d}\right) \right). \quad (21)$$

B. Derivation of Eq.18

We start by deriving the CDF expression of the received SNR at E, Γ_e^L, given by

$$F_{\Gamma_e^L}(z) = 1 - P\left[\min\{(1-\alpha)\gamma_s, \gamma_e(1+\alpha\gamma_d)\} \geq z(1+\alpha\gamma_d)\right] \quad (22)$$

$$= 1 - \int_0^{\infty} \left(1 - F_{\gamma_s} \frac{z(1+\alpha x)}{(1-\alpha)}\right) f_{\gamma_d}(x) \quad dx \times (1 - F_{\gamma_e}(z)) \quad (23)$$

$$= 1 - \left(I \times e^{-\frac{z}{\overline{\gamma}_e}}\right), \quad (24)$$

where I is given by:

$$I = \int_0^{\infty} e^{-\frac{z(1+\alpha x)}{\overline{\gamma}_s(1-\alpha)}} f_{\gamma_d}(x) \quad dx \quad (25)$$

$$= \sum_{i=1}^{K} \binom{K}{i} (-1)^{i-1} \frac{ia\overline{\gamma}_s}{\alpha\overline{\gamma}_d z + ia\overline{\gamma}_s} e^{-\frac{z}{\overline{\gamma}_s(1-\alpha)}}. \quad (26)$$

Therefore, based on $F_{\Gamma_e^L}(.)$, (18) can be derived by solving the following integration

$$E\{\ln(1+\Gamma_e)\} = \int_0^{\infty} \frac{1}{1+x} (1 - F_{\Gamma_e}(x)) \quad dx \quad (27)$$

$$= \sum_{i=1}^{K} \binom{K}{i} (-1)^{i-1} \times \int_0^{\infty} \frac{ia\overline{\gamma}_s}{(1+x)(\alpha\overline{\gamma}_d z + ia\overline{\gamma}_s)} e^{-\left(\frac{1}{a\overline{\gamma}_s} + \frac{1}{\overline{\gamma}_e}\right)z} \quad dx. \quad (28)$$

Two cases are considered, $\alpha\overline{\gamma}_d z = ia\overline{\gamma}_s$ and $\alpha\overline{\gamma}_d z \neq ia\overline{\gamma}_s$. Using [15, Eq.(3.353.3)] the result in (18) is obtained.

References

[1] Y.-S. Shiu, S. Y. Chang, H.-C. Wu, S.-H. Huang, and H.-H. Chen, "Physical layer security in wireless networks: a tutorial," *IEEE Wireless Communications*, vol. 18, no. 2, pp. 66–74, April 2011.

[2] H. Alves, R. Souza, M. Debbah, and M. Bennis, "Performance of transmit antenna selection physical layer security schemes," *IEEE Signal Processing Letters*, vol. 19, no. 6, pp. 372–375, June 2012.

[3] N. Yang, P. L. Yeoh, M. Elkashlan, R. Schober, and J. Yuan, "MIMO wiretap channels: Secure transmission using transmit antenna selection and receive generalized selection combining," *IEEE Communications Letters*, vol. 17, no. 9, pp. 1754–1757, September 2013.

[4] K. Tourki, M.-S. Alouini, and M. O. Hasna, "Wireless transmission with cooperation on demand for slow and fast fading environments," in *Proc. of IEEE International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC)*, Cannes, Sep. 2008.

[5] K. Tourki, H.-C. Yang, and M.-S. Alouini, "Error-rate performance analysis of incremental decode-and-forward opportunistic relaying," *IEEE Transactions on Communications*, vol. 59, no. 6, pp. 1519–1524, Jun. 2011.

[6] K. Tourki, D. Gesbert, and L. Deneire, "Cooperative diversity using per-user power control in the mutiuser MAC channel," in *IEEE International Symposium on Information Theory*, Nice, France, Jun. 2007.

[7] K. Tourki and L. Deneire, ""End-To-End Performance Analysis of Two-Hop Asynchronous Cooperative Diversity"," in *49th annual IEEE Global Telecommunications Conference*, San Francisco, California, USA, Nov. 2006.

[8] Y. Zou, X. Wang, and W. Shen, "Optimal relay selection for physical-layer security in cooperative wireless networks," *IEEE Journal on Selected Areas in Communications*, vol. 31, no. 10, pp. 2099–2111, October 2013.

[9] L. Fan, X. Lei, T. Duong, M. Elkashlan, and G. Karagiannidis, "Secure multiuser communications in multiple amplify-and-forward relay networks," *IEEE Transactions on Communications*, vol. 62, no. 9, pp. 3299–3310, Sept 2014.

[10] J. Mo, M. Tao, and Y. Liu, "Relay placement for physical layer security: A secure connection perspective," *Communications Letters, IEEE*, vol. 16, no. 6, pp. 878–881, June 2012.

[11] Z. Han, N. Marina, M. Debbah, and A. Hjørungnes, "Physical layer security game: interaction between source, eavesdropper, and friendly jammer," *EURASIP Journal on Wireless Communications and Networking*, vol. 2009, p. 11, 2009.

[12] K.-H. Park, T. Wang, and M.-S. Alouini, "On the jamming power allocation for secure amplify-and-forward relaying via cooperative jamming," *IEEE Journal on Selected Areas in Communications*, vol. 31, no. 9, pp. 1741–1750, September 2013.

[13] D. Fang, N. Yang, M. Elkashlan, P. L. Yeoh, and J. Yuan, "Cooperative jamming protocols in two hop amplify-and-forward wiretap channels," in *2013 IEEE International Conference on Communications (ICC)*, June 2013, pp. 2188–2192.

[14] Y. Liu, J. Li, and A. Petropulu, "Destination assisted cooperative jamming for wireless physical-layer security," *IEEE Transactions on Information Forensics and Security*, vol. 8, no. 4, pp. 682–694, April 2013.

[15] A. Jeffrey and D. Zwillinger, *Table of integrals, series, and products*. Academic Press, 2007.