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 pre-coding 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 noise simultaneously, and a power allocation is adopted.
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 send the jamming signals [14].

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

\[
y_d = G h_{id} y_i + n_d,
\]

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

\[
G = \sqrt{\frac{P}{\left| h_{si} \right|^2 (1 - \alpha) \frac{P}{2} + \left| h_{id} \right|^2 \alpha \frac{P}{2} + \sigma^2}}.
\]

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

\[
y_{de} = \sqrt{(1 - \alpha) \frac{P}{2} G h_{si} h_{id} s + G h_{id} n_i + n_d}.
\]

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

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

where \( n_e \sim \mathcal{CN}(0, \sigma_e^2) \). We assume, for simplicity, that \( \sigma_k^2 = \sigma_e^2 \) 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 \( P_s = (1 - \alpha) \frac{P}{2} \), \( P_d = \alpha \frac{P}{2} \) and \( P_t = \frac{P}{2} \), respectively. Accordingly, we define the instantaneous SNRs of the source-relay, relay-destination and relay-eavesdropper links, as \( \delta_s = (1 - \alpha) |h_{sr}|^2 \frac{P}{2} \), \( \delta_d = \alpha |h_{rd}|^2 \frac{P}{2} = \alpha \gamma_d \), and \( \delta_e = |h_{re}|^2 \frac{P}{2} \), respectively.

The denote \( \rho = \frac{P}{2\sigma_e} \).

B. Received SNRs

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

\[
\Gamma_d = \frac{(1 - \alpha) \gamma_d \gamma_d}{(1 - \alpha) \gamma_s + (1 + \alpha) \gamma_d + 1},
\]

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

\[
\Gamma_e = \frac{(1 - \alpha) \gamma_s \gamma_e + \alpha \gamma_e (\gamma_e + 1) + \gamma_e + 1}{\gamma_e},
\]

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

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

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

\[
C_{LB} = \left[ \frac{1}{2} \log_2 \left( \frac{1 + \Gamma_d}{1 + \Gamma_e} \right) \right]^+ = \left[ \frac{1}{2} \ln \left( E \{\ln (1 + \Gamma_d)\} - E \{\ln (1 + \Gamma_e)\} \right) \right]^+.
\]
Hereafter, we denote $X = a\gamma_s$ and $Y = b\gamma_d$, where $a = 1 - \alpha$ and $b = 1 + \alpha$. Thus, we have

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

(11)

Hence, the first term of $C_{LB}$ is lower bounded by $\ln (1 + 1/e^{i_1 + i_2})$ where $I_1$ and $I_2$ are given by:

$$I_1 = E(\ln(\Gamma_d)) = \int_0^\infty \int_0^\infty \ln(xy) f_X(x)f_Y(y) \, dxdy,$$

(12)

and

$$I_2 = E(\ln(\Gamma_d + 1)) = \int_0^\infty \ln(1 + z) f_Z(z) \, dz,$$

(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

$$I_1 = \left( -\varepsilon - \ln \left( \frac{1}{\alpha \sigma_y} \right) \right) + \sum_{i=1}^K \left( \frac{K}{i} \right) (-1)^i \left( \varepsilon + \ln \left( \frac{i}{\alpha \sigma_d} \right) \right),$$

(14)

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

$$\sum_{i=1}^K \left( \frac{K}{i} \right) (-1)^i \int \frac{\alpha \sigma_y}{\gamma_s} e^{-\frac{\gamma_s}{\alpha \sigma_y}} \cdot \left( 1 - e^{-\frac{\gamma_s}{\alpha \sigma_d \gamma_2 \gamma_3}} \right) \, d\gamma_s = b\gamma_d$$

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 $\Gamma_e, F_{\Gamma_e}(\cdot)$, the second term of ESC is given by

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

(17)

which is given by (18) (as shown by Appendix.B), where $\mu = \frac{\gamma_s + \sigma_d}{\sigma_d \gamma_1}$ and $\nu = \frac{\gamma_s + \sigma_d}{\sigma_d \gamma_1 \gamma_2} h$.

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, $d_{sr}$, the relay cluster is located at a distance $d_{sr}$ from S equal to 1. 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 $\nu$ is the path-loss exponent, set to 4.

We examine the effect of the network parameters such as $K, d_{sr}$ and $\alpha$, on the $C_s$ expression. In Fig. 2, $C_{LB}$ expression is presented as function of $\rho$ 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.

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 $\alpha$, 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 $\alpha$ 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 $\alpha$ where $d_{sr} = 0.5$. It can be seen that the optimal fraction of power allocated to the jamming signal, $\alpha^*$, is influenced by $\rho$ and the number of relays $K$. Indeed, for a given $\rho$, $\alpha^*$ 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
$$I_2 = \begin{cases} \sum_{i=1}^{K} \binom{K}{i} (-1)^{i-1} \left( 1 + \left( \frac{1}{\sigma_s^2} - 1 \right) e^{\frac{1}{\sigma_s^2}} Ei \left( -\frac{1}{\sigma_s^2} \right) \right) \\ \sum_{i=1}^{K} \binom{K}{i} (-1)^{i-1} \frac{i}{a \sigma_s^2 - b \sigma_d^2} \left( b \sigma_d^2 e^{\frac{1}{\sigma_d^2}} Ei \left( -\frac{i}{\sigma_d^2} \right) - a \sigma_d^2 e^{\frac{1}{\sigma_d^2}} Ei \left( -\frac{1}{\sigma_d^2} \right) \right) \end{cases}$$

$$E \{ \ln(1 + \Gamma_c) \} = \begin{cases} \sum_{i=1}^{K} \binom{K}{i} (-1)^{i-1} \frac{\alpha \sigma_s^2}{\alpha \sigma_s^2 - \alpha \sigma_d^2} (e^\alpha Ei(-\mu) - e^\nu Ei(-\nu)) , & \alpha \sigma_s^2 \neq \alpha \sigma_d^2 \\ \sum_{i=1}^{K} \binom{K}{i} (-1)^{i-1} (1 + \mu e^\nu Ei(-\mu)) , & \alpha \sigma_s^2 = \alpha \sigma_d^2 \end{cases}$$

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 $\rho$ and $K$, when $d_{sr} = 0.5$.

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 cooperation 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

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

If $\alpha \sigma_s^2 = \alpha \sigma_d^2$, then using [15, Eq.(4.337.5)], $I_2$ is given by

$$I_2 = \sum_{i=1}^{K} \binom{K}{i} (-1)^{i-1} \frac{i}{a \sigma_s^2 - b \sigma_d^2} \int_0^\infty z \ln(1 + z) e^{-\frac{z}{a \sigma_s^2}} \ dz$$

$$= \sum_{i=1}^{K} \binom{K}{i} (-1)^{i-1} \left( 1 - \left( \frac{1}{a \sigma_s^2} - 1 \right) e^{\frac{1}{a \sigma_s^2}} Ei \left( \frac{1}{a \sigma_s^2} \right) \right), \quad (20)$$

where $Ei$ is the exponential integral function defined in [15, Eq.(8.21)]. However, when $\alpha \sigma_s^2 \neq \alpha \sigma_d^2$, and using [15, Eq.(4.337.2)], $I_2$ is given by

$$I_2 = \sum_{i=1}^{K} \binom{K}{i} (-1)^{i-1} \frac{i}{a \sigma_s^2 - b \sigma_d^2} \times$$

$$\left( \int_0^\infty \ln(1 + z) e^{\frac{z}{a \sigma_s^2}} \ dz - \int_0^\infty \ln(1 + z) e^{\frac{z}{a \sigma_d^2}} \ dz \right)$$
\[ E \{ \ln(1 + \Gamma_e) \} = \int_0^\infty \frac{1}{1 + x} (1 - F_{\gamma_e}(x)) \, dx \]

\[ = \sum_{i=1}^K \binom{K}{i} (-1)^{i-1} \frac{ia\gamma_s}{ia\gamma_s + b\gamma_d} \times \]

\[ \left( -a\gamma_s e^{\gamma_d} E_1 \left( -\frac{1}{a\gamma_s} \right) + \frac{b\gamma_d}{i} e^{\gamma_d} E_1 \left( -\frac{i}{b\gamma_d} \right) \right) . \]

(21)

**B. Derivation of Eq. 18**

We start by deriving the CDF expression of the received SNR at \( \Gamma_e \), given by

\[ F_{\Gamma_e}(z) = 1 - P \{ \min \{ (1 - \alpha)\gamma_s, \gamma_e(1 + \alpha\gamma_d) \} \geq z \} \]

(22)

\[ = 1 - \int_0^\infty \left( 1 - F_{\gamma_e} \left( \frac{z(1 + \alpha x)}{1 - \alpha} \right) \right) f_{\gamma_d}(x) \, dx \times (1 - F_{\gamma_e}(z)) \]

(23)

\[ = 1 - \left( I \times e^{-\frac{z}{\gamma_d}} \right) , \]

(24)

where \( I \) is given by:

\[ I = \int_0^\infty e^{-\frac{z(1 + x)}{\alpha \gamma_d}} f_{\gamma_d}(x) \, dx \]

(25)

\[ = \sum_{i=1}^K \binom{K}{i} (-1)^{i-1} \frac{ia\gamma_s}{ia\gamma_s + b\gamma_d} e^{-\frac{z}{\gamma_d} \frac{1 + x}{1 - \alpha}} . \]

(26)

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

\[ E \{ (1 + \Gamma_e) \} = \int_0^\infty \frac{1}{1 + x} (1 - F_{\gamma_e}(x)) \, dx \]

(27)

\[ = \sum_{i=1}^K \binom{K}{i} (-1)^{i-1} \times \]

\[ \int_0^\infty \frac{ia\gamma_s}{(1 + x)(ia\gamma_s + b\gamma_d)} e^{-\frac{z}{\gamma_d} \frac{1 + x}{1 - \alpha}} \, dx . \]

(28)

Two cases are considered, \( \alpha \gamma_s \gamma_d = 0 \) and \( \alpha \gamma_s \gamma_d \neq 0 \). Using [15, Eq.(3.353.3)] the result in (18) is obtained.

**References**


