Secrecy Performance for Multiple Untrusted Relay Networks Using Destination-Based Jamming with Direct Link

D. P. Moya Osorio
Department of Electrical Engineering
Federal University of São Carlos
Email: dianamoya@ufscar.br

E. E. Benitez Olivo
São Paulo State University (UNESP)
Campus of São João da Boa Vista
Email: edgar.olivo@unesp.br

H. Alves
Centre for Wireless Communications
University of Oulu
Email: hirley.alves@oulu.fi

***Abstract*—We propose a destination-based jamming scheme for cooperative networks with multiple untrusted amplify-and-forward relays, in which the destination operates in full-duplex mode so as to enable simultaneous reception of the information coming directly from the source and the transmission of jamming signals to the untrusted relay. An approximate analytical expression for the secrecy outage probability, under the effect of residual self-interference at the destination, is presented. The developed analysis is verified through Monte Carlo simulations.**

I. Introduction

Traditionally, complex and centralized upper-layer techniques, such as data-encryption and cryptographic-key approaches, have been used in order to provide information security in wireless networks. On the other hand, information-theoretic security or the so-called physical-layer security (PLS), the basis of which was introduced in [1], has increasingly attracted special interest of researchers over the few past years, as this new paradigm proves more propitious to next-generation high-density wireless networks.

Most related schemes addressing physical layer security in cooperative relaying networks consider that the relay node enlisted to cooperate in the communication process between a source-destination pair is reliable, and that any compromise of the communication security can only come from an outside eavesdropper. However, in many scenarios (such as, public, financial-institution or government-intelligence networks), where the nodes have different levels of security clearance, the relay node could have a lower level of access to information when compared to the legitimate source-destination pair, so that it represents a potential eavesdropper, thus being regarded as untrusted [2].

In order to counteract this problem, some works have directed their efforts to investigate cooperative jamming (CJ) techniques so as to enhance the communication security in wireless networks [3]–[7]. For example, in [3], the theoretical limits and practical designs of jamming approaches for cooperative-users based jamming, multi-antenna based jamming, and wireless energy-harvesting-based jamming techniques are investigated. In [4], the ergodic secrecy capacity for a two-hop amplify-and-forward (AF) cooperative system with multiple untrusted relays were analyzed. In that work, a destination-based jamming (DJ) technique was employed, while the direct link between the source and destination was assumed to be nonexistent. Interestingly, the system performance was shown to worsen as the number of relays increases. In [5], the secrecy outage probability (SOP) and the ergodic secrecy rate were evaluated for a two-hop relaying network consisting of a source and a destination both provided with multiple antennas, which are assisted by an untrusted AF relay. Therein a DJ strategy was used, but the direct link was disregarded. In [6], the secrecy outage probability and the ergodic secrecy capacity were studied for a cooperative network composed of a source, a destination, and a untrusted AF relay. In that work, a source-based jamming (SJ) scheme was employed, whereby the source transmits a jamming signal to confound the untrusted relay, in addition to the information signal through direct link. In [7], the achievable secrecy rates were investigated for a cooperative network consisting of a source, a destination, an untrusted AF relay, and a cooperative jammer, which is assumed to transmit a noise signal that is known at the destination. Therein two network setups were considered, in which the direct link is available and not. The results showed that secrecy rates improve when the direct link is employed in the communication process.

In this work, we contribute to the study of CJ techniques to enhance secrecy in cooperative networks with multiple untrusted AF relays. Differently from previous studies, we consider a DJ strategy, while exploiting the direct-link transmission between the legitimate source-destination pair. To do so, the destination is considered to operate in full duplex mode in order to simultaneously receive useful information from the source and transmit a jamming signal to the selected untrustworthy relay. We analyze the secrecy outage probability for the network under consideration.

Throughout this paper, $f_X(\cdot)$ and $F_X(\cdot)$ denote the probability density function (PDF) and cumulative distribution function (CDF) of a random variable X, respectively, $E[\cdot]$ is the expectation operator, and $\Pr[\cdot]$ stands for probability.

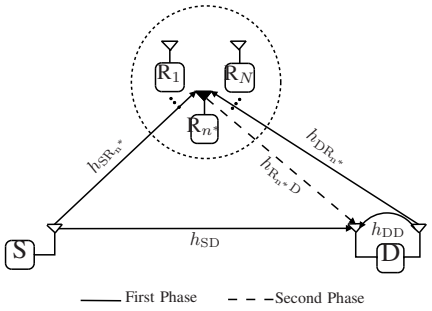

Fig. 1. System model.

II. System Model

The system model depicted in Fig. 1 illustrates a cooperative relaying network consisting of a single-antenna source S, N single-antenna AF untrusted relays R_n, with $n \in \{1, ..., N\}$, which may eavesdrop the information signal sending by S, and one destination D equipped with two antennas, one for reception and one for transmission, so as to enable FD mode operation. Because of this, D is subject to self-interference. In this system, one out of the N relays is selected to participate of the communication process, and the direct link is considered to be non-negligible, so that it can be exploited as a means to harvest additional transmission reliability. The communication process is performed in two phases, as detailed below:

- *First phase:* in this phase, S broadcasts an information signal $s_I(t)$, which is listened by the relays and the destination. Meanwhile, D sends an artificial jamming signal $s_J(t)$ to hinder the relays from eavesdropping the information sent by S.
- *Second phase:* in this phase, the selected relay R_{n^*} amplifies the signal received from S, which was interfered by the jamming signal sent by D, and forwards it to the destination. However, since D knows the jamming signal transmitted in the previous phase, this artificial information can be subtracted from the received signal.

All links in this network are considered to undergo independent Rayleigh block fading, as well as additive white Gaussian noise (AWGN) with mean power N_0. Therefore, the channel coefficients for the links S→D, S→R_n, R_n→D and D→R_n, denoted by h_{SD}, h_{SR_n}, $h_{\mathrm{R}_n\mathrm{D}}$, and h_{DR_n}, respectively, are independent complex circularly-symmetric Gaussian random variables with variance $\Omega_{\mathrm{MN}} = E\{|h_{\mathrm{MN}}|^2\}$, that is $\mathcal{CN}(0, \Omega_{\mathrm{MN}})$, with $\mathrm{M} \in \{\mathrm{S}, \mathrm{R}_n\}$ and $\mathrm{N} \in \{\mathrm{R}_n, \mathrm{D}\}$. Accordingly, the channel gains $g_{\mathrm{MN}} = |h_{\mathrm{MN}}|^2$ are exponentially distributed with mean value Ω_{MN}. These channel coefficients are supposed to remain constant during a data-block transmission, but vary independently through consecutive blocks. Furthermore, because of imperfect self-interference cancellation, a residual self-interference (RSI) remains at the FD destination, which is modeled as a Rayleigh fading channel, with channel coefficient $h_{\mathrm{DD}} \sim \mathcal{CN}(0, \Omega_{\mathrm{DD}})$, where $\Omega_{\mathrm{DD}} = E\{|h_{\mathrm{DD}}|^2\}$. Thus, the received signal-to-noise ratios (SNRs) at the direct link, nth first-hop relaying link, nth second-hop relaying link, jamming link, and RSI link are, respectively, given by $Z = g_{\mathrm{SD}} P_{\mathrm{S}}/N_0$, $X_n = g_{\mathrm{SR}_n} P_{\mathrm{S}}/N_0$, $Y_n = g_{\mathrm{R}_n\mathrm{D}} P_{\mathrm{R}}/N_0$, $J_n = g_{\mathrm{DR}_n} P_{\mathrm{D}}/N_0$, and $U = g_{\mathrm{DD}} P_{\mathrm{D}}/N_0$, where P_{S}, P_{R}, and P_{D} are the transmit powers at the source, nth relay and destination. In addition, the total transmit power is assumed to be limited to a value of P, for the whole transmission process. Thus, a power allocation factor η between S and D is used during the first phase. Accordingly, by denoting the total transmit system SNR as $\gamma_P = P/N_0$, the transmit SNRs at S, D, and R_n can be respectively written as $\gamma_{P_{\mathrm{S}}} = P_{\mathrm{S}}/N_0 = \eta\gamma_P/2$, $\gamma_{P_{\mathrm{D}}} = P_{\mathrm{D}}/N_0 = (1-\eta)\gamma_P/2$, and $\gamma_{P_{\mathrm{R}}} = P_{\mathrm{R}}/N_0 = \gamma_P/2$.

Under the above assumptions, the received signals at R_n and D during the first phase, by considering the nth relaying link are, respectively, given as

$$y_{\mathrm{R}_n}(t) = \sqrt{P_{\mathrm{S}}} h_{\mathrm{SR}_n} s_I(t) + \sqrt{P_{\mathrm{D}}} h_{\mathrm{DR}_n} s_J(t) + n_{\mathrm{R}_n}(t), \tag{1}$$

$$y_{\mathrm{D}}^1(t) = \sqrt{P_{\mathrm{S}}} h_{\mathrm{SD}} s_I(t) + \sqrt{P_{\mathrm{D}}} h_{\mathrm{DD}} s_J(t) + n_{\mathrm{D}}(t), \tag{2}$$

where the mean power of the signals $s_I(t)$ and $s_J(t)$ are normalized to unity, that is $E\{|s_I(t)|^2\} = E\{|s_J(t)|^2\} = 1$, and $n_{\mathrm{R}_n}(t)$ and $n_{\mathrm{D}}(t)$ are the AWGN components at R_n and D, respectively.

On the other hand, the received signal at D during the second phase is given by

$$y_{\mathrm{D}}^2(t) = \sqrt{P_{\mathrm{R}}} h_{\mathrm{R}_n\mathrm{D}} \mathcal{G} y_{\mathrm{R}_n}(t) + n_{\mathrm{D}}(t), \tag{3}$$

where $\mathcal{G}$ is the amplification factor, given as

$$\mathcal{G} = \frac{1}{\sqrt{P_{\mathrm{S}} g_{\mathrm{SR}_n} + P_{\mathrm{D}} g_{\mathrm{R}_n\mathrm{D}} + N_0}}. \tag{4}$$

Hence, by substituting (1) into (3) and considering that the jamming signal can be effectively removed at D, the received signal at D during the second phase can be rewritten as

$$y_{\mathrm{D}}^2(t) = \sqrt{P_{\mathrm{R}}} h_{\mathrm{R}_n\mathrm{D}} \mathcal{G} \sqrt{P_{\mathrm{S}}} h_{\mathrm{SR}_n} s_I(t) + \sqrt{P_{\mathrm{R}}} h_{\mathrm{R}_n\mathrm{D}} \mathcal{G} n_{\mathrm{R}_n}(t) + n_{\mathrm{D}}(t). \tag{5}$$

Thus, from (1) and (2), the instantaneous signal-to-interference-plus-noise ratios (SINRs) received at R_n and D during the first phase can be respectively expressed as

$$\Gamma_{\mathrm{R}_n} = \frac{P_{\mathrm{S}} g_{\mathrm{SR}_n}}{P_{\mathrm{D}} g_{\mathrm{R}_n\mathrm{D}} + N_0} = \frac{X_n}{J_n + 1}, \tag{6}$$

$$\Gamma_{\mathrm{D}}^1 = \frac{P_{\mathrm{S}} g_{\mathrm{SD}}}{P_{\mathrm{D}} g_{\mathrm{DD}} + N_0} = \frac{Z}{U + 1}, \tag{7}$$

whereas, from (5), the end-to-end instantaneous received SNR at D, via the nth relaying link, can be given as

$$\Gamma^2_{\mathrm{D},n} = \frac{P_{\mathrm{S}} g_{\mathrm{SR}_n} P_{\mathrm{R}} g_{\mathrm{R}_n\mathrm{D}}}{P_{\mathrm{S}} g_{\mathrm{SR}_n} N_0 + P_{\mathrm{R}} g_{\mathrm{R}_n\mathrm{D}} N_0 + P_{\mathrm{D}} g_{\mathrm{R}_n\mathrm{D}} N_0 + N_0} = \frac{X_n Y_n}{X_n + Y_n + J_n + 1}. \quad (8)$$

Herein, we consider that the relay enlisted to participate in the communication process between S and D is that which maximizes the SNR of the nth legitimate link, $\Gamma_{L_n} \triangleq \Gamma^1_{\mathrm{D}} + \Gamma^2_{\mathrm{D},n}$, given by the maximal-ratio combining (MRC) between the signals coming from the nth relaying link and the direct link, that is

$$n^* = \max_n \{\Gamma_{Ln}\} = \max_n \{\Gamma^1_{\mathrm{D}} + \Gamma^2_{\mathrm{D},n}\}. \quad (9)$$

For notation simplicity, from now on, we use Ω_X, Ω_Y, Ω_Z, Ω_J, and Ω_U to denote Ω_{SR_n}, Ω_{R_nD}, Ω_{SD}, Ω_{DR_n}, and Ω_{DD}, respectively.

III. Secrecy Outage Probability Analysis

By definition, the secrecy capacity is obtained as the difference between the capacity of the legitimate link, $C_{L_{n^*}}$, and that of the eavesdropping link, C_E, that is[1] [8]

$$C_S = [C_{L_{n^*}} - C_E]^+ = \frac{1}{2}\log_2\left(\frac{1+\Gamma_{L_{n^*}}}{1+\Gamma_E}\right), \quad (10)$$

where $[a]^+ \triangleq \max\{0, a\}$, and n^* is obtained as in (9). In the proposed system model, any relay represents a potential eavesdropper and there is no cooperation among the relays, so that the information rate being leaked is determined by the relay with the best received SINR at the first phase, similarly as considered in [9]. Therefore, the SNR Γ_E is given as

$$\Gamma_{\mathrm{E}} = \max_n \left\{\frac{X_n}{J_n + 1}\right\}, \quad (11)$$

Then, we can define the SOP as the probability of the achievable secrecy capacity being less than a target secrecy rate $\mathcal{R}_S$ [10], that is

$$\mathrm{SOP} = \Pr\left(C_S < \mathcal{R}_S\right) = \Pr\left(\frac{1+\Gamma_{L_{n^*}}}{1+\Gamma_E} < 2^{2\mathcal{R}_S} \triangleq \tau\right). \quad (12)$$

Thus, the SOP can be derived as in the following proposition.

Proposition 1. *An approximate expression for the secrecy outage probability of a multiple untrusted relay network using DJ with direct link is given by*

$$\mathrm{SOP} \approx \int_0^\infty \left[F_{\Gamma_{L_n}}(\tau\gamma_E)\right]^N f_{\Gamma_E}(\gamma_E)\, d\gamma_E, \quad (13)$$

[1]Note from (10) that, even though the destination operates in FD mode to concurrently receive information from S and transmit the jamming signal to R_n, the underlaying cooperative protocol operates in half-duplex mode; therefore, the pre-log factor 1/2 is used.

where $f_{\Gamma_E}(\cdot)$ and a lower bound for $F_{\Gamma_{L_n}}(\cdot)$ can be obtained in closed form as in Lemmas 1 and 2, respectively, which are presented later on.

Proof. From (12), by considering the relay selection criterion in (9) and applying the Total Probability Theorem [11], the SOP can be determined as

$$\begin{aligned}\mathrm{SOP} &= \sum_{n=1}^N \Pr\left(\frac{1+\Gamma_{L_n}}{1+\Gamma_E} < \tau | n = n^*\right)\Pr(n = n^*) \\ &\overset{(a)}{\approx} \sum_{n=1}^N \Pr(\Gamma_{L_n} < \tau\Gamma_E | n = n^*) \\ &\quad \times \Pr\left(\Gamma_{L_n} > \max_{\substack{i=1,\ldots,N \\ i\neq n}} \{\Gamma_{L_i}\}\right) \\ &\approx N\int_0^\infty \int_0^{\tau\gamma_E} \left[F_{\Gamma_{L_n}}(\gamma_{L_n})\right]^{N-1} f_{\Gamma_{L_n}}(\gamma_{L_n}) \\ &\quad \times f_{\Gamma_E}(\gamma_E)\, d\gamma_{L_n} d\gamma_E \\ &\approx \int_0^\infty F_{\Gamma_{L_n}}(\tau\gamma_E)^N f_{\Gamma_E}(\gamma_E)\, d\gamma_E, \end{aligned} \quad (14)$$

where step (a) follows from a high-SINR regime assumption. □

Now, $f_{\Gamma_E}(\cdot)$ and a lower-bound for $F_{\Gamma_{L_n}}(\cdot)$ can be obtained as in the following lemmas.

Lemma 1. *The PDF of Γ_E is given by*

$$f_{\Gamma_E}(\gamma_E) = N\left(\frac{\phi\eta(1-\eta)\Omega_J\Omega_X}{\theta^2} + \frac{2\phi}{\gamma_P\theta}\right)\left(1 - \frac{\phi\eta\Omega_X}{\theta}\right)^{N-1}, \quad (15)$$

where $\phi \triangleq e^{-\frac{2\gamma_E}{\gamma_P\eta\Omega_X}}$ and $\theta \triangleq \gamma_E(1-\eta)\Omega_J + \eta\Omega_X$.

Proof. To derive the PDF of Γ_E, we first obtain the corresponding CDF as follows

$$\begin{aligned} F_{\Gamma_E}(\gamma_E) &= \Pr(\Gamma_E < \gamma_E) \\ &= \prod_{i=1}^N \Pr\left(\frac{X_i}{J_i+1} < \gamma_E\right) \\ &= \prod_{i=1}^N \int_0^\infty \Pr(X_i < \gamma_E(j_i+1)) f_{J_i}(j_i)\, dj_i \\ &= \prod_{i=1}^N \int_0^\infty F_{X_i}(\gamma_E(j_i+1)) f_{J_i}(j_i)\, dj_i \\ &= \left(1 - \frac{\phi\Omega_X}{\theta}\right)^N. \end{aligned} \quad (16)$$

Then, by finding the derivative of the above expression, $f_{\Gamma_E}(\cdot)$ can be obtained as in (15). □

Lemma 2. *A lower bound expression for the CDF of Γ_{Ln} is given by* (17)*, shown at the top of the next page. In that expression, $\mu \triangleq \gamma_P(1-\eta)\eta\Omega_U\Omega_X\Omega_Y\Omega_Z$ and $\nu \triangleq \Omega_X\Omega_Y - \eta\Omega_X\Omega_Z - \Omega_Y\Omega_Z$.*

$$F_{\Gamma_{L_n}}(\gamma_{L_n}) = \frac{\eta\Omega_Z}{\mu}\left[\left(1-e^{-\frac{2\gamma_L(\eta\Omega_X+\Omega_Y)}{\gamma_P\eta\Omega_X\Omega_Y}}\right)\frac{\mu}{\eta\Omega_Z}+2e^{\frac{2\Omega_Z[\eta\Omega_X\Omega_Y-(\eta\Omega_X+\Omega_Y)(\gamma_L(1-\eta)\Omega_U+\eta\Omega_Z)]}{\mu}}(\eta\Omega_X+\Omega_Y)\Omega_Z\right.$$
$$\left.\times\left(\mathrm{Ei}\left(-\frac{2\nu}{\gamma_P\Omega_U\Omega_X\Omega_Y(1-\eta)}\right)-\mathrm{Ei}\left(-\frac{2(\gamma_L(1-\eta)\Omega_U+\eta\Omega_Z)\nu}{\mu}\right)\right)\right]. \quad (17)$$

Proof. By considering the well-known result that $XY/(X+Y+1) < \min\{X,Y\}$, where X and Y are SNRs, and that $XY/(X+Y+1) \approx \min\{X,Y\}$, for the high-SNR regime, an upper bound for $F_{\Gamma_{L_n}}(\cdot)$ can be obtained from the following relationship $\frac{X_nY_n}{X_n+Y_n+J_n+1} < \frac{X_nY_n}{X_n+Y_n+1} < \min\{X_n,Y_n\}$, yielding

$$\Gamma_{L_n} < \min\{X_n,Y_n\} + \frac{Z}{U+1} \triangleq \Gamma_{L_n}^{\mathrm{UB}} \quad (18)$$

Therefore, a lower-bound for the CDF of Γ_L can be attained as follows

$$\begin{aligned} F_{\Gamma_{L_n}}^{\mathrm{LB}}(\gamma_{L_n}) &= \Pr\left(\Gamma_{L_n}^{\mathrm{UB}} < \gamma_L\right) \\ &= \Pr\left(\min\{X_n,Y_n\} < \gamma_{L_n} - \Psi\right) \\ &= \int_0^{\gamma_{L_n}} \left[F_X(\gamma_{L_n}-\psi) + F_Y(\gamma_{L_n}-\psi)\right. \\ &\quad \left. - F_X(\gamma_{L_n}-\psi)F_Y(\gamma_{L_n}-\psi)\right] \\ &\quad \times f_\Psi(\psi)\,d\psi, \end{aligned} \quad (19)$$

where $\Psi \triangleq \frac{Z}{U+1}$, the CDF of which can be attained similarly as in Lemma 1, with $N=1$ and Ω_X and Ω_J being substituted by Ω_Z and Ω_U, respectively. Then, the corresponding PDF, $f_\Psi(\cdot)$, can be obtained by taking the derivative of the referred CDF. Finally, after performing the corresponding integrations and simplifications of expressions of exponentials functions, $F_{\Gamma_{L_n}}(\cdot)$ is obtained as in (17). □

IV. Numerical Results and Discussions

In this section, the derived analytical expression is validated by Monte Carlo simulations, through some illustrative cases. For this purpose, it is considered a two-dimensional network topology, where S and D are located at the coordinates $(0,0)$ and $(1,0)$ (assuming normalization), respectively, while the relays are clustered together and collocated midway between S and D. Moreover, without loss of generality, it is assumed that the average channel gain for all links is determined by the distance between the respective pair of nodes, i.e., $\Omega_A = d_{\mathrm{MN}}^{-\alpha}$, with $A \in \{X,Y,Z\}$, $\mathrm{M} \in \{\mathrm{S},\mathrm{R}_n\}$, and $\mathrm{N} \in \{\mathrm{R}_n,\mathrm{D}\}$, where d_{MN} is the distance between the corresponding nodes, and α is the path loss exponent. For the evaluated cases, we consider $\alpha = 4$ (urban environment) and $\mathcal{R} = 1$ bps/Hz.

Fig. 2 shows the secrecy outage probability of the proposed system versus the transmit system SNR for different values of $N = 2,4,6$. Notice that our proposed approximation is effectively validated by the simulation results. Moreover, a performance loss is observed, as the number of untrusted relays increases, as expected; however, this performance loss is not significant.

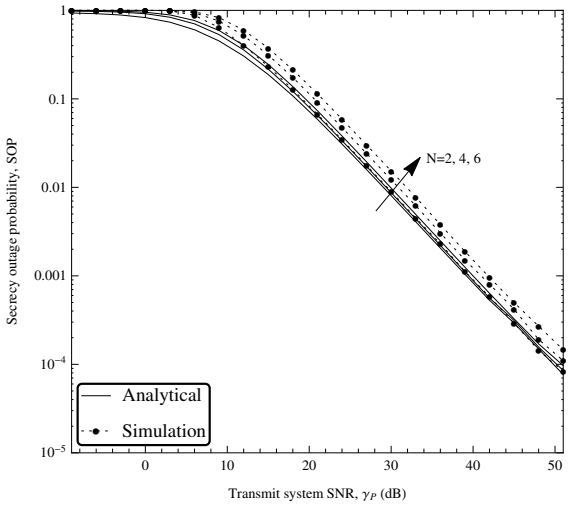

Fig. 2. Secrecy outage probability versus Total Transmit SNR for different values of $N = 2,4,6$, $\Omega_U = -40$ dB, and $\eta = 0.8$.

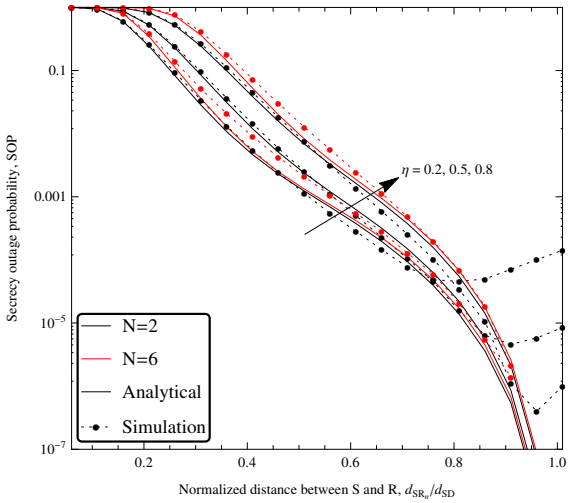

Fig. 3. Secrecy outage probability versus Normalized distance between S and R for different values of η, $\Omega_U = -40$ dB, and $\gamma_P = 30$ dB.

Fig. 3 illustrates the secrecy outage probability versus the normalized distance between S and R, for different values of the allocation factor η. It can be noticed that the secrecy performance improves as the selected relay approaches D, as can be seen for the case $N = 6$. However, for lower values of N (for instance, $N = 2$)

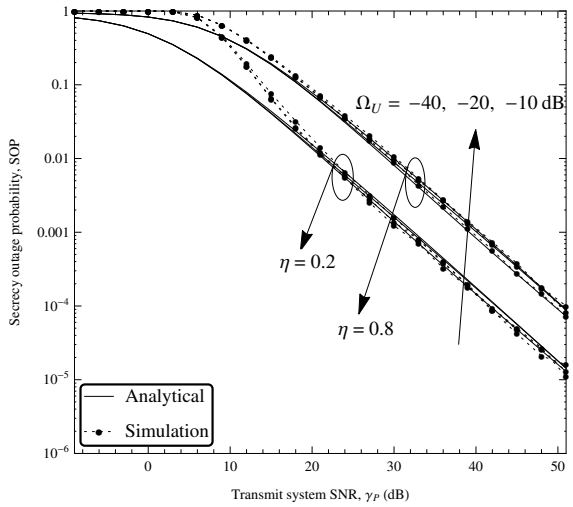

Fig. 4. Secrecy outage probability versus Total Transmit SNR for different values of Ω_U and $d_{SR_n}/d_{SD} = 0.5$ dB.

and relay positions closer to D, the simulation curves deviate from the analytical approximation, indicating a degradation in the secrecy performance at this region, for which the proposed approximation is not accurate. This behavior can be explained by noting that, as R approaches D, the eavesdropping capacity decreases due to the first-hop relaying link weakens, while the jamming link strengthens. Hence, in the region closer to D, the eavesdropping link is very weak, thus the secrecy capacity is governed by the state of the legitimate link, which, after the midpoint from S to D, starts losing performance, thus causing a slightly rise of the curve at those positions. Moreover, regarding the effect of the power allocation between S and D, it is observed that, for higher values of N (for instance, $N = 6$), lower values of η attain better performance, thus allocating more power to D is the best strategy. Nonetheless, an opposite effect is observed for $N = 2$ at positions closest to D, where the best strategy is to allocate more power to S.

Fig. 4 shows the effect of the RSI over the secrecy performance of the system, thus the secrecy outage probability is plotted versus the transmit system SNR for different values of Ω_U. From the figure, we can observe that, as the average channel gain of the RSI link increases, a slight loss in the secrecy performance is obtained. This behavior holds for different values of η, thus an increment of the transmit power at D does not result in a significant secrecy performance loss due to the effect of RSI.

V. Conclusions

In this paper, the secrecy performance of a destination-based jamming scheme was investigated for a cooperative network with multiple untrusted AF relays, in which the destination was considered to operate in FD mode, so as to enable simultaneous reception of the information coming directly from the source and the transmission of jamming signals to the untrusted relays. An accurate approximate expression for the SOP of the proposed system was derived. Besides, the probability distributions for the SINRs of the eavesdropping and legitimate links were obtained as byproducts. Our results showed that, as the number of relays increases, the secrecy performance slightly diminishes. Also, for higher values of N, the performance presents an improvement, as R approaches D and more power is allocated to D. However, for lower values of N and relay positions close to D, the proposed approximation loses accuracy, and simulations showed that the system presents a loss in performance, and allocating more power to S is the best strategy. Finally, results exhibit that the level of RSI do not significantly affects the secrecy performances, even for different levels of transmit power at D.

Acknowledgment

The authors would like to thank the Brazilian National Council for Scientific and Technological Development (CNPq), Project N° 428649/2016-5, and the Academy of Finland, Project SAFE Grant N° 303532.

References

[1] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, Oct. 1975.

[2] X. He and A. Yener, "Cooperation with an untrusted relay: A secrecy perspective," *IEEE Trans. Inf. Theory*, vol. 56, no. 8, pp. 3807–3827, Aug. 2010.

[3] K. Cumanan et al, "Physical Layer Security Jamming: Theoretical Limits and Practical Designs in Wireless Networks," *IEEE Access*, vol. 5, pp. 3603–3611, Dec. 2016.

[4] L. Sun, T. Zhang, Y. Li, and H. Niu, "Performance study of two-hop amplify-and-forward systems with untrustworthy relay nodes," *IEEE Trans. Veh. Technol.*, vol. 61, no. 8, pp. 3801–3807, Oct. 2012.

[5] A. Kuhestani and A. Mohammadi, "Destination-based cooperative jamming in untrusted amplify-and-forward relay networks: Resource allocation and performance study," *IET Commun.*, vol. 10, no. 1, pp. 17–23, Feb. 2016.

[6] L. Lv, J. Chen, L. Yang, and Y. Kuo, "Improving physical layer security in untrusted relay networks: Cooperative jamming and power allocation," *IET Commun.*, vol. 11, no. 3, pp. 393–399, Feb. 2017.

[7] B. Ali, N. Zamir, M. Fasih, U. Butt, and S. X. Ng, "Physical layer security: Friendly jamming in an untrusted relay scenario," in *Proc. 24th European Signal Process. Conf.* (EUSIPCO), Budapest, Hungary, 2016, pp. 958–962.

[8] J. Barros and M. R. D. Rodrigues, "Secrecy capacity of wireless channels," in *Proc. IEEE Int. Symp. Inf. Theory*, Jul. 2006, pp. 356–360.

[9] L. Dong, Z. Han, A. P. Petropulu and H. V. Poor, "Improving Wireless Physical Layer Security via Cooperating Relays," in *IEEE Trans. Signal Process.*, vol. 58, no. 3, pp. 1875–1888, Mar. 2010.

[10] M. Bloch, J. Barros, M. R. D. Rodrigues and S. W. McLaughlin, "Wireless Information-Theoretic Security," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2515–2534, Jun. 2008.

[11] A. Papoulis, *Probability, Random Variables, and Stochastic Processes*, 4th ed. New York, NY, USA: McGraw-Hill, 2002.

[12] D. P. Moya Osorio, E. E. Benitez Olivo, D. B. da Costa, and J. C. S. Santos Filho, "Distributed link selection in multirelay multiuser networks," *Transactions on Emerging Telecommunications Technologies*, vol. 27, no. 7, pp. 939–951, Dec. 2016.