Impact of Outdated CSI on the Secrecy Performance of Multiple Untrusted Relay Networks with Direct Link and Destination-Based Jamming

I. W. Gomes da Silva, M. Komono Tojeiro, E. E. Benitez Olivo, and D. P. Moya Osorio

Abstract— **This paper investigates the impact of outdated channel estimates on the secrecy performance of multiple untrusted relay networks, where the direct link is used as an additional path of information and a destination-based jamming method is employed. In the proposed setup, the destination is considered to be equipped with two antennas in order to operate in full-duplex mode, thus allowing the reception of information from the source, while sending a jamming signal to prevent the untrusted relays from eavesdropping information. The system performance is evaluated in terms of the secrecy outage probability via Monte Carlo simulations.**

Keywords— **Cooperative jamming, full duplex, outdated channel state information, physical layer security, untrusted relays.**

I. Introduction

Physical Layer Security (PLS) techniques have emerged as a promising solution to strengthen the security of the huge amount of sensitive information that is expected to be transmitted through the next generation of wireless networks (5G) [1]. In PLS techniques, the random nature of the wireless channel is intelligently exploited, so that channel imperfections, such as interference and fading, can be used to provide additional confidentiality to wireless communications, besides conventional key-based cryptographic techniques. The feasibility of PLS was theoretically proved by Wyner [2] in 1975, establishing that a source and its intended destination can secretly exchange messages at a non-zero rate (the so-called secrecy rate), if the eavesdropper channel is a degraded version of the legitimate channel. However, appalling channel conditions of the legitimate channel can hamper the effectiveness of PLS techniques. To counteract this problem, cooperative relaying techniques can be employed in order to boost the transmission reliability between source and destination. In this context, the combination of both PLS and cooperative relaying has attracted special interest as a means to provide secure and reliable communications [3].

An interesting way to explore user cooperation to enhance the secrecy rate in wireless networks with security constraints consists in degrading the eavesdropper channel by introducing controlled interference, which is referred as cooperative jamming (CJ) [4]–[9]. For instance, in [4], an opportunistic selection of two relay nodes was proposed for a multirelay cooperative network, whereby the first relay is intended to assist the communication between the source and destination, while the second relay is in charge of sending a jamming signal to interfere an eavesdropper. In [5], a CJ technique was investigated by considering a multiple-antenna relay acting as a jammer. In [6] and [7], scenarios with multiple relay nodes transmitting jamming signals to enhance the security of the communication link were analyzed.

Nevertheless, using cooperative relaying may not always contribute to enhance the network secrecy. In certain types of networks, such as heterogeneous networks, where the nodes have different levels of clearance, the relay node may try to extract useful information from the legitimate communication between source and relay to use it for its own benefit. In light of this, recently, many works have addressed scenarios considering untrusted relay nodes [9]–[13]. In particular, in [9], a source-based jamming technique was evaluated in combination with power allocation to improve the security in a network with one untrusted relay and the presence of direct link between source and destination. In [10], the achievable secrecy diversity order was studied for a cooperative network with a multiple-antenna source and multiple untrusted relays. In [11], the secrecy capacity and the secrecy outage probability (SOP) of a two-hop amplify-and-forward (AF) relaying network was evaluated in the presence of multiple untrusted relays and without the presence of direct link. Also, in [12] a cooperative network with a multiple-antenna source, a multiple-antenna destination, multiple untrusted relays, and external eavesdroppers was considered, where both source and destination transmit jamming signals in different phases of the communication process. In [13], a destination-based jamming for cooperative networks with multiple untrusted relays is evaluated considering the presence of the direct link.

However, a common assumption in all the aforementioned works is that perfect channel state information (CSI) is available, which is hardly obtained in practice due to the time-varying nature of the wireless channel. In this respect, the impact of outdated CSI over conventional relaying schemes has been widely treated in the literature [14]–[16]. Moreover, some works have studied the impact of outdated CSI over

I. W. Gomes da Silva, M. Komono Tojeiro, and D. P. Moya Osorio are with the Departament of Electrical Engineering, Center of Exact Sciences and Technology, Federal University of São Carlos, São Carlos-SP, Brazil, E-mails: mateuskomono@gmail.com, isbllwgomes@gmail.com, dianamoya@ufscar.br.

E. E. Benitez Olivo is with São Paulo State University (UNESP), Campus of São João da Boa Vista, São João da Boa Vista-SP, Brazil, E-mail: edgar.olivo@unesp.br.

This work was partially supported by the São Paulo Research Foundation (FAPESP), Procs. Nº 2017/17136-3 and Nº 2017/20990-6, and by the Brazilian National Council for Scientific and Technological Development (CNPq), Procs. Nº 428649/2016-5 and Nº 421850/2018-3.

the secrecy performance of cooperative networks [17], [18]. In [17], a joint relay and jammer selection with decode-and-forward relays under the effect of feedback delay is investigated. In [18], the secrecy performance of an untrusted AF relaying network is investigated under the assumption of outdated CSI, where a Source-based jamming method is employed and direct link is considered to be available.

On the other hand, except for the works in [9], [13] and [18], a common limitation for the above mentioned studies is that the direct link is neglected. In this paper, we aim to partially fill this gap by investigating the secrecy performance of a multiple untrusted AF relaying network, where the direct link is exploited as an additional path of information. Opposite to [13] a perfect knowledge of the CSI is not available and different from [9] and [18], we consider a destination-based jamming technique. To make this possible, a destination with full-duplex (FD) communication capability is considered in order to enable the reception of the information coming from the source, concurrently with the transmission of a jamming signal to interfere the untrusted relays. The secrecy performance is evaluated in terms of SOP through Monte Carlo simulations.

II. System Model

Fig. 1 illustrates a cooperative AF relaying network consisting of one source S, one destination D, and N untrusted AF relays R_n, with $n \in \{1, ..., N\}$. We further assume that the destination is equipped with two antennas, one for transmission and another for reception, in order to operate in FD mode. The other nodes are considered to be single-antenna devices. In this network, the direct link between S and D is assumed to be available and can be exploited as an additional path to transmit information, and one out of the N relays, R_{n^*}, is selected to assist the communication between S and D. Moreover, a time-division multiple access (TDMA) is adopted. The communication process is divided into two phases. In the first phase, S broadcasts the information signal, while D and the untrusted relays are listening. Simultaneously, D sends a jamming signal to cause interference at the relays. In the second phase, R_{n^*} retransmits an amplified version of its received signal to D. At the reception, D is assumed to be able to completely cancel the jamming signal, as it has previous knowledge of the transmitted artificial noise. Finally, D combines the signals received from S, via direct link in the first phase, and from R_{n^*}, in the second phase, employing a maximal-ratio combining (MRC) technique.

Additionally, all links are considered to undergo Rayleigh block fading and additive white Gaussian noise (AWGN) with mean power N_0. Therefore, the corresponding channel coefficients for the links S→R_n, R_n→D, S→D, and D→R_n are denoted, respectively, by h_i, with $i \in \{X_n, Y_n, Z, J_n\}$, and can be modeled as independent circularly-symmetric complex Gaussian variables, i.e., $h_i \sim \mathcal{CN}(0, d_i^{-\alpha})$, where d_i is the distance between the corresponding nodes and α is the path loss exponent. Therefore, $|h_{X_n}|^2$, $|h_{Y_n}|^2$, $|h_Z|^2$ and $|h_{J_n}|^2$ are the corresponding channel gains. Thus, the respective signal-to-noise ratios (SNRs) are given as $X_n{=}P_\mathrm{S}|h_{X_n}|^2/N_0$, $Y_n{=}P_\mathrm{R}|h_{Y_n}|^2/N_0$, $Z{=}P_\mathrm{S}|h_Z|^2/N_0$ and $J_n{=}P_\mathrm{D}|h_{J_n}|^2/N_0$, where P_S, P_R and P_D are the transmission powers at S, R_n and D, respectively. Moreover, it is assumed that an imperfect cancellation of the self-interference generated by the FD mode operation at D is performed, thus the residual self-interference (RSI) is modeled as a Rayleigh fading channel [19], with channel coefficient $h_U \sim \mathcal{CN}(0, \sigma^2)$, so that the corresponding received SNR is given as $U{=}P_\mathrm{D}|h_U|^2/N_0$.

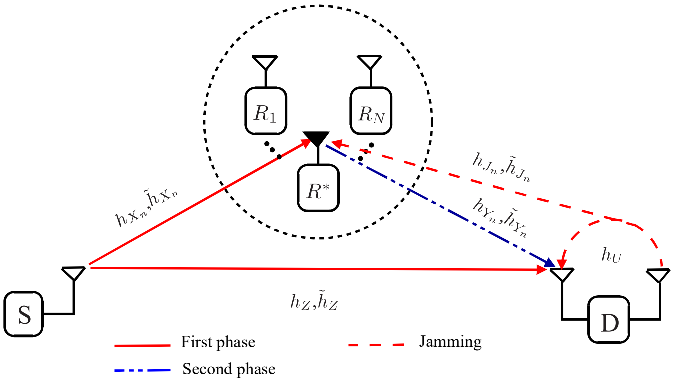
R_1
R_N
R^*
h_{X_n},$\tilde{h}_{X_n}$
h_{J_n},$\tilde{h}_{J_n}$
h_{Y_n},$\tilde{h}_{Y_n}$
h_U
h_Z,$\tilde{h}_Z$
S
D
First phase
Second phase
Jamming

Fig. 1. System model.

Under the above considerations, during the first phase, the received signals at R_n and D at time t are respectively given by

$$y_{\mathrm{R}_n}(t) = \sqrt{P_\mathrm{S}} h_{X_n} s_\mathrm{I}(t) + \sqrt{P_\mathrm{D}} h_{J_n} s_\mathrm{J}(t) + n_\mathrm{R}, \quad (1)$$

$$y_{\mathrm{D}_1}(t) = \sqrt{P_\mathrm{S}} h_Z s_\mathrm{I}(t) + \sqrt{P_\mathrm{D}} h_U s_\mathrm{J}(t) + n_\mathrm{D}, \quad (2)$$

where $s_\mathrm{I}(t)$ is the information signal transmitted from S, $s_\mathrm{J}(t)$ is the jamming signal transmitted from D, n_R and n_D are the noise components at R and D, respectively. Furthermore, according to the AF protocol, the received signal at D, during the second phase, is given by $y_{\mathrm{D}_2}(t) = \beta y_{\mathrm{R}_n}$, where β is the amplification factor. Also, it is assumed that the mean power of the signals $s_\mathrm{I}(t)$ and $s_\mathrm{J}(t)$ is normalized to unity, i.e., $E\{s_\mathrm{I}^2(t)\}{=}E\{s_\mathrm{J}^2(t)\}{=}1$, where $E\{\cdot\}$ is the expectation operator. In addition, the average noise power at R and D is considered to be equal to N_0. Then, by considering that D can effectively cancel the jamming signal, $y_{\mathrm{D}_2}(t)$ can be expressed as

$$y_{\mathrm{D}_2}(t) = \sqrt{P_\mathrm{R}} \sqrt{P_\mathrm{S}} \beta h_{Y_n} h_{X_n} s_\mathrm{I}(t) + \sqrt{P_\mathrm{R}} \beta h_{Y_n} n_\mathrm{R} + n_\mathrm{D}, \quad (3)$$

where the amplification factor β is given by

$$\beta = \sqrt{\frac{1}{P_\mathrm{S}|h_{X_n}|^2 + P_\mathrm{D}|h_{J_n}|^2 + N_0}}. \quad (4)$$

Therefore, the signal-to-interference-plus-noise ratios (SINRs) at D, during the first and second phases, can be expressed, respectively, as

$$\Gamma_{\mathrm{D}_1} = \frac{P_{\mathrm{S}}|h_Z|^2}{P_{\mathrm{D}}|h_U|^2 + N_0} = \frac{Z}{U+1} \tag{5}$$

$$\begin{aligned}\Gamma_{\mathrm{D}_2} =& \frac{P_{\mathrm{R}}|h_{Y_n}|^2\beta^2 P_{\mathrm{S}}|h_{X_n}|^2}{N_0(P_{\mathrm{R}}|h_{Y_n}|^2\beta^2+1)}\\ \overset{(a)}{=}& \frac{\left(\frac{P_{\mathrm{R}}|h_{Y_n}|^2}{N_0}\right)\left(\frac{P_{\mathrm{S}}|h_{X_n}|^2}{N_0}\right)}{\frac{P_{\mathrm{R}}|h_{Y_n}|^2}{N_0} + \frac{P_{\mathrm{S}}|h_{X_n}|^2}{N_0} + \frac{P_{\mathrm{D}}|h_{J_n}|^2}{N_0} + 1}\\ =& \frac{X_n Y_n}{X_n + Y_n + J_n + 1}.\end{aligned} \tag{6}$$

where the step (a) is obtained after replacing β given as in (4) and performing some mathematical manipulations.

Besides, due to the mobility of the nodes in this system, it is considered that the channels vary with the time. Therefore, we will denote the channels at the relay selection moment as $\tilde{h}_i$, with $i \in \{X_n, Y_n, Z, J_n\}$, which are outdated versions of the respective channels h_i at the transmission moment. Therefore, from the Jakes' model [20], the channel coefficient h_i and its outdated version $\tilde{h}_i$ are autocorrelated samples of the same complex-valued Gaussian fading process. That is, h_i and $\tilde{h}_i$ follow a bivariate Gaussian distribution with zero mean and correlation coefficient given by

$$\rho_i = J_0(2\pi f_{d,i} T_D). \tag{7}$$

where $f_{d,i}$ is the maximum Doppler frequency, T_D is the time delay between the relay selection and transmission moments, and $J_0(\cdot)$ is the zero-order Bessel function of the first kind. Therefore, the outdated channel coefficients can be expressed as [16]

$$\tilde{h}_i = \rho_i h_i + \left(\sqrt{1-\rho_i^2}\right) w_i \tag{8}$$

where w_i is a circularly-symmetric complex Gaussian random variable with the same variance of h_i. Thus, $\tilde{X}_n = P_{\mathrm{S}}|\tilde{h}_{X_n}|^2/N_0$, $\tilde{Y}_n = P_{\mathrm{R}}|\tilde{h}_{Y_n}|^2/N_0$, $\tilde{Z} = P_{\mathrm{S}}|\tilde{h}_Z|^2/N_0$, and $\tilde{J}_n = P_{\mathrm{D}}|\tilde{h}_{J_n}|^2/N_0$ are the outdated versions of the SNRs X_n, Y_n, Z, and J_n.

III. Secrecy Outage Probability

A. Preliminaries

The maximum secrecy rate (i.e., the secrecy capacity), at the transmission moment, can be calculated as the difference between the capacity of the legitimate channel $C_{L_{n^*}}$ and the capacity of the eavesdropping channel C_E, as follows [21]

$$\begin{aligned}C_{S_{n^*}} =& [C_{L_{n^*}} - C_E]^+\\ C_{S_{n^*}} =& \frac{1}{2}\log_2\left(\frac{1+\Gamma_{L_{n^*}}}{1+\Gamma_E}\right),\end{aligned} \tag{9}$$

where $[m]^+ \triangleq \max\{0, m\}$ and n^* refers to the index of the selected relay, R_{n^*}, according to the criterion presented in the next section. In addition, after performing a MRC technique, the instantaneous received end-to-end SINR at D is given by

$$\tilde{\Gamma}_{L_{n^*}} = \frac{X_{n^*} Y_{n^*}}{X_{n^*} + Y_{n^*} + J_{n^*} + 1} + \frac{Z}{U+1}. \tag{10}$$

Herein, we consider that the RSI channel is not time varying, as there is no relative movement of the collocated transmit and receive antennas at D, so that the RSI channel is not subject to outdated CSI. Also, in this system, any relay node is considered a potential eavesdropper, thus being untrustworthy. Then, the eavesdropped information is determined by the relay with the best channel conditions on the link S→ R_n [22], that is

$$\Gamma_E = \max_n \left\{\frac{X_n}{J_n+1}\right\}. \tag{11}$$

Therefore, the secrecy outage probability is defined as the probability of the attainable secrecy capacity C_S^* being below a target secrecy rate $\mathcal{R}$, that is

$$\mathrm{SOP} = \Pr\{C_{S_{n^*}} < \mathcal{R}\}, \tag{12}$$

where $\Pr\{\cdot\}$ denotes probability.

B. Relay Selection Criterion

At the relay selection moment, the relay is chosen according to the following criterion

$$n^* = \arg\max_n \{\tilde{C}_S\} \tag{13}$$

$$= \arg\max_n \left\{\frac{1 + \frac{\tilde{X}_n\tilde{Y}_n}{\tilde{X}_n + \tilde{Y}_n + \tilde{J}_n + 1} + \frac{\tilde{Z}}{U+1}}{1 + \max_n\left\{\frac{\tilde{X}_n}{\tilde{J}_n+1}\right\}}\right\} \tag{14}$$

IV. Numerical Results and Discussion

In this section, the secrecy performance of the considered system is evaluated via Monte Carlo simulations, by illustrating some sample cases. For this purpose, it is considered a two-dimensional network topology with normalized distances, where S and D are located at the coordinates (0; 0) and (1; 0), respectively. The relays are clustered and co-located at the coordinates (0.5; 0). Additionally, it is assumed that the pathloss exponent α is set to 4. Also, the target secrecy rate is set to $\mathcal{R} = 1$ bps/Hz, and the transmission powers at nodes S, D and R_n are considered to be equal, that is, $P_S = P_R = P_D = \frac{1}{3}$

Fig. 2 illustrates the secrecy outage probability versus the transmitted system SNR $\bar{\gamma_P}$, for different number of relays. Simulations were performed by considering different values of the correlation factor ρ=$0.1, 0.5$ and 0.99, as well as the case with perfect CSI presented in [13]. As expected, the case $N = 1$ does not present impact regarding the value of ρ as no relay selection process is performed. For the other values of N, it is observed that the higher the value of ρ, the better the secrecy performance. Therefore, depending on the level of severity of outdated CSI, the secrecy in the communication can be significantly deteriorated. On the other hand, for a same value of ρ, increasing the number of relays entails a certain loss in the secrecy performance; however, this loss is not significant, specially for values of ρ close to 1. It is noticed that the case $\rho = 0.99$ and the one displayed in [13] are very alike even with the relay selection criterion being

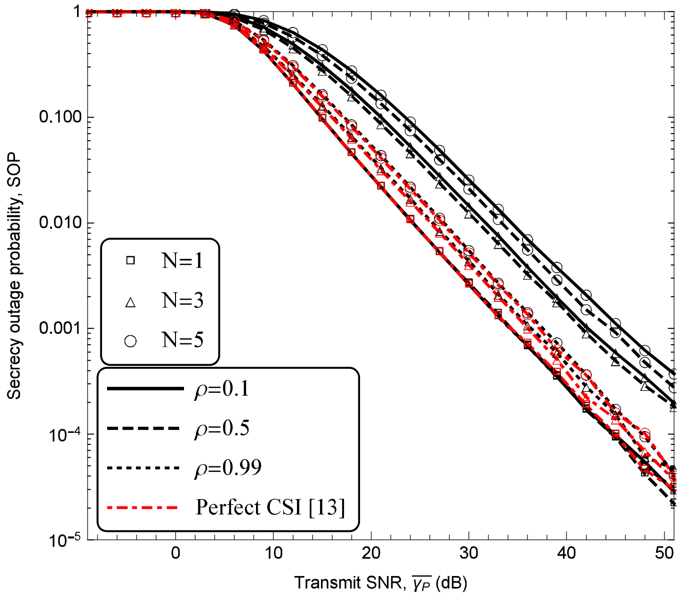

Fig. 2. Secrecy outage probability vs. $\bar{\gamma_P}$, for $N = 1, 3, 5$ and 7, with $\rho = 0.1, 0.5$ and 0.99, and $E\{|h_U|^2\} = -40$ dB.

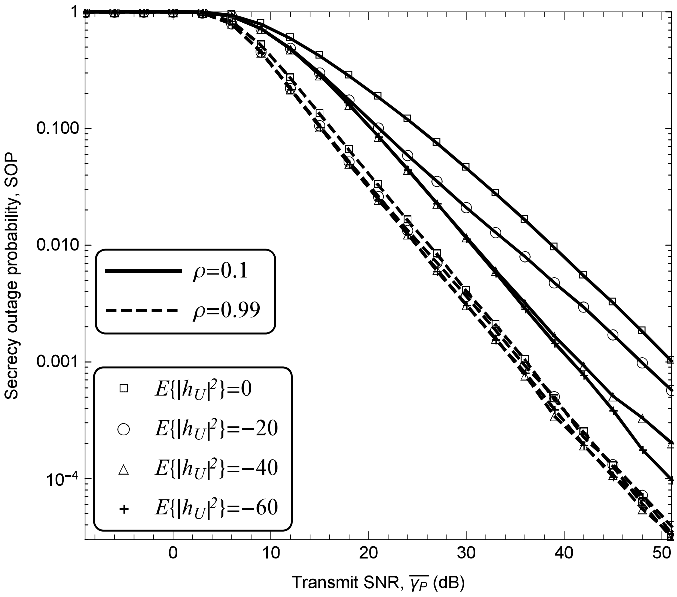

Fig. 4. Secrecy outage probability vs. $\bar{\gamma_P}$, for $N = 3$, $\rho = 0.1$ and 0.99, and varying the levels of RSI.

different, it shows that simpler relay selection schemes can be used to reduce power consumption without deteriorating the performance of the system.

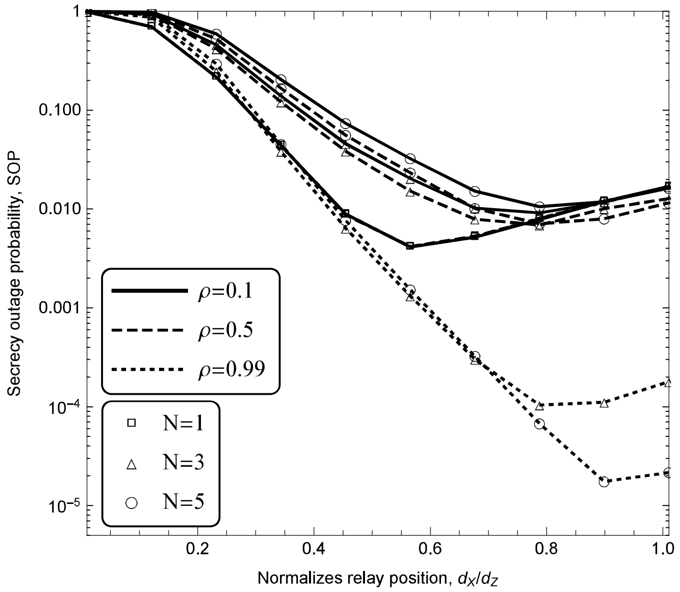

Fig. 3. Secrecy outage probability vs. relative position of the relay, for $N = 1, 3, 5$ and 7, with $\rho = 0.1, 0.5$, and 0.99, $E\{|h_U|^2\} = -40$ dB and $\bar{\gamma_P} = 30$ dB.

In order to complement the previous observations, Fig. 3 shows the secrecy outage probability versus the normalized relay position, d_{X_n}/d_Z, for ρ=$0.1, 0.5$ and 0.99, and different values of the number of relays. Notice that the positions closer to S present the worst performance, regardless of the value of ρ and the number of relays. This is due to the fact that, at those positions, the first-hop relaying link experiments good conditions, while the second-hop and jamming links are weak. Therefore, the signal arriving at R is strong, so that the probability of information eavesdropping is high, as the C_E considerably increases. On the other hand, for positions close to D, the outdated CSI severely impacts the secrecy performance of the system. In this region, for lower values of ρ, the performance does not present difference regarding the number of relays. However, for values of ρ close to 1, a significant difference in performance is appreciated as the number of relays increases. In that case, as the relay approaches D, the secrecy performance improves as N increases. This behavior is due to the fact that, from midway between S and D to the positions closer to D, both the legitimate and eavesdropper links deteriorate, still the deterioration of the eavesdropper link occurs at a higher rate. Therefore, the secrecy performance improves until a certain point very close to D, where there is a slight loss in secrecy performance. Additionally, depending on the values of ρ and N, the best relay positions are closer to D.

Fig. 4 illustrates the secrecy outage probability versus the system transmitted SNR $\bar{\gamma_P}$, for different levels of RSI. Two scenarios are evaluated, the first one considers a severe outdated CSI scenario, with $\rho = 0.1$, and the second one considers an almost perfect correlation, with $\rho = 0.99$. It can be observed that, for the first scenario, increasing the level of RSI induces a significant loss on the secrecy performance. However, for the second scenario, the RSI level does not significantly interfere on the secrecy performance.

Finally, in Fig. 5 is shown the secrecy outage probability versus the system transmitted SNR $\bar{\gamma_P}$ for different mobility scenarios, considering that (a) nodes are moving very slowly (ρ_{X_n}=ρ_{Y_n}=ρ_Z= 0.99); (b) all nodes are moving fastly (ρ_{X_n}=ρ_{Y_n}=ρ_Z= 0.1); (c) R$_n$ moves (ρ_Z= 0.99, ρ_{X_n}=ρ_{Y_n}= 0.1); (d) S moves (ρ_{Y_n}= 0.99, ρ_{X_n}=ρ_Z= 0.1); (e) D moves (ρ_{X_n}= 0.99, ρ_Z=ρ_{Y_n}= 0.1) and (f) all the scenarios it is considered that the correlation coefficient of self-interference, ρ_U, equals to 0.99. As expected, the best performance is

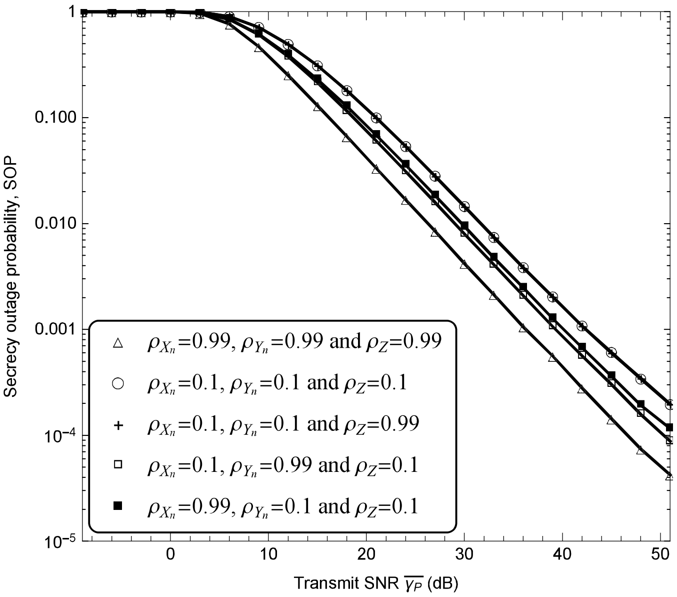

Fig. 5. Secrecy outage probability vs. $\overline{\gamma_P}$, for $N = 3$ and RSI$= -40$ dB, where ρ_{X_n} is the correlation coefficient of the first hop, ρ_{Y_n} of the second hop and jamming signal and ρ_Z of the direct link.

presented when the nodes are moving slowly. On the other hand, the worst-case scenario is presented when all nodes present high mobility. Note that when there is only mobility in the relays, the secrecy performance is similar to that of the case of mobility of all nodes. In addition, when S moves, the secrecy performance is better than when D is moving. In addition, the movement of R$_n$ is the most harmful case for the system secrecy performance.

V. Conclusion

In this paper, the secrecy performance of a multiple untrusted AF relay network is evaluated by considering outdated CSI and destination-based jamming via Monte Carlo simulations. It was observed that a severe level of outdated CSI results in a considerable loss of the system secrecy performance, while increasing the number of relays caused a slight deterioration on this performance. Moreover, different positions of the relay node caused a different impact on the secrecy performance. It was also observed that the level of RSI impacts the secrecy performance for the cases of severe outdated CSI. Finally, it was verified that the scenario in which only the relay is subject to high mobility is as detrimental as the scenario presenting high mobility in all the nodes in terms of the secrecy performance. Future reserches includes an extension of the system model, i.e. the analysis of a large scale network with multiple relays that can be trusted or untrusted where stochastic geometric tools can be apply. Beyond that, a power optimization problem that minimizes the SOP is also considered.

Referências

[1] N. Yang, L. Wang, G. Geraci, M. Elkashlan, J. Yuan, and M. D. Renzo, "Safeguarding 5g wireless communication networks using physical layer security," *IEEE Communications Magazine*, vol. 53, no. 4, pp. 20–27, April 2015.

[2] A. D. Wyner, "The wire-tap channel," *The Bell System Technical Journal*, vol. 54, no. 8, pp. 1355–1387, October 1975.

[3] L. Lai and H. E. Gamal, "The relay-eavesdropper channel: Cooperation for secrecy," *IEEE Transactions on Information Theory*, vol. 54, no. 9, pp. 4005–4019, Sept. 2008.

[4] I. Krikidis, J. S. Thompson, and S. Mclaughlin, "Relay selection for secure cooperative networks with jamming," *IEEE Transactions on Wireless Communications*, vol. 8, no. 10, pp. 5003–5011, October 2009.

[5] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor, "Cooperative jamming for wireless physical layer security," in *2009 IEEE/SP 15th Workshop on Statistical Signal Processing*, Aug 2009, pp. 417–420.

[6] K. Cumanan, G. C. Alexandropoulos, Z. Ding, and G. K. Karagiannidis, "Secure communications with cooperative jamming: Optimal power allocation and secrecy outage analysis," *IEEE Transactions on Vehicular Technology*, vol. 66, no. 8, pp. 7495–7505, Aug 2017.

[7] S. Luo, J. Li, and A. Petropulu, "Outage constrained secrecy rate maximization using cooperative jamming," in *2012 IEEE Statistical Signal Processing Workshop (SSP)*, Aug 2012, pp. 389–392.

[8] H. Song, Y. Gao, G. Zang, Q. Zhou, and F. Yao, "Security-concern relaying scheme for amplify-and-forward network with untrusted relay nodes," in *2016 5th International Conference on Computer Science and Network Technology (ICCSNT)*, Dec 2016, pp. 476–481.

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

[10] M. Chraiti, A. Ghrayeb, C. Assi, and M. O. Hasna, "On the achievable secrecy diversity of cooperative networks with untrusted relays," *IEEE Transactions on Communications*, vol. 66, no. 1, pp. 39–53, Jan 2018.

[11] A. Kuhestani, A. Mohammadi, and M. Masoudi, "Joint optimal power allocation and relay selection to establish secure transmission in uplink transmission of untrusted relays network," *IET Networks*, vol. 5, no. 2, pp. 30–36, March 2016.

[12] C. D. T. Thai, J. Lee, and T. Q. S. Quek, "Leaking rate region to eavesdroppers and untrusted relays," in *2016 IEEE Global Communications Conference (GLOBECOM)*, Dec 2016, pp. 1–6.

[13] D. P. Moya Osorio, E. E. Benitez Olivo, and H. Alves, "Secrecy performance for multiple untrusted relay networks using destination-based jamming with direct link," in *2018 IEEE 29th Annual International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC)*, Sep. 2018, pp. 1–5.

[14] D. S. Michalopoulos, H. A. Suraweera, G. K. Karagiannidis, and R. Schober, "Amplify-and-forward relay selection with outdated channel estimates," *IEEE Transactions on Communications*, vol. 60, no. 5, pp. 1278–1290, May 2012.

[15] D. P. M. Osorio, E. E. B. Olivo, D. B. da Costa, and J. C. S. S. Filho, "Impact of outdated channel estimates on a distributed link-selection scheme for af relaying networks," *IEEE Wireless Communications Letters*, vol. 4, no. 2, pp. 185–188, April 2015.

[16] J. L. Vicario, A. Bel, J. A. Lopez-salcedo, and G. Seco, "Opportunistic relay selection with outdated csi: outage probability and diversity analysis," *IEEE Transactions on Wireless Communications*, vol. 8, no. 6, pp. 2872–2876, June 2009.

[17] N. E. Wu and H. J. Li, "Effect of feedback delay on secure cooperative networks with joint relay and jammer selection," *IEEE Wireless Communications Letters*, vol. 2, no. 4, pp. 415–418, August 2013.

[18] A. Mabrouk, K. Tourki, and N. Hamdi, "Secure cooperative untrusted-relay network with outdated csi," in *2016 International Wireless Communications and Mobile Computing Conference (IWCMC)*, Sept 2016, pp. 90–95.

[19] M. Duarte, C. Dick, and A. Sabharwal, "Experiment-driven characterization of full-duplex wireless systems," *IEEE Transactions on Wireless Communications*, vol. 11, no. 12, pp. 4296–4307, Dec. 2012.

[20] W. C. Jakes, *Mobile Radio Propagation*. IEEE, 1974. [Online]. Available: https://ieeexplore.ieee.org/document/5263369

[21] J. Barros and M. R. D. Rodrigues, "Secrecy capacity of wireless channels," in *2006 IEEE International Symposium on Information Theory*, July 2006, pp. 356–360.

[22] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor, "Improving wireless physical layer security via cooperating relays," *IEEE Transactions on Signal Processing*, vol. 58, no. 3, pp. 1875–1888, March 2010.