Securing Non-Orthogonal Multiple Access Systems Against Simultaneous Eavesdropping Attacks Coming from Inside and Outside of the Network

Gustavo Anjos, Daniel Castanheira, Adão Silva, Atílio Gameiro
Instituto de Telecomunicações and DETI, University of Aveiro, Aveiro, Portugal

***Abstract*— The secrecy challenge of protecting a power domain non-orthogonal multiple access (NOMA) system is associated with the intrinsic superposition structure of the transmitted information. Because of this superposition operation, the interference generated by the other user's information must be first decoded by the receiver in order to allow the intended information to be acquired. Therefore, a robust secrecy solution for this type of channel access techniques must consider not only the existence of attacks coming from undetectable passive eavesdroppers located outside of the network, but also attacks carried out by eavesdroppers registered as legitimate users inside the system. In this work, a cooperative jamming technique is combined with a secure channel training solution in order to protect a two user power domain NOMA system against eavesdropping attacks coming simultaneously from inside and outside of the network. The proposed secrecy solution is evaluated numerically and the evaluation demonstrates that weak secrecy is achieved against the inside and outside eavesdroppers.**

Keywords— NOMA, inside attack, outside attack, cooperative jamming, square M-QAM, secure training, physical layer security.

I. INTRODUCTION

The integration of non-orthogonal multiple access techniques in the future 5G wireless standards [1], [2] is considered a mandatory step to increase the spectral efficiency of this new generation of networks. While in the orthogonal access different users are allocated to non-overlapped time-frequency resources, in the non-orthogonal solution the same resource is shared among multiple users, being the separation between them achieved exploiting different power or coding conditions. The high potential of this new type of access technology motivated the research community to start very recently addressing the secrecy issues associated with non-orthogonal multiple access techniques.

Taking into account the presence of a passive eavesdropper, optimal power allocation algorithms were developed in [3] with the target of maximizing the secrecy sum-rate of a power domain NOMA system. The secrecy performance of a non-orthogonal multiple access scheme was analyzed in [4] considering the order of decoding, the individual transmission rates and the power distribution as system parameters. Assuming multiple antennas at the transmitter, the exploitation of different antenna selection strategies was proposed in [5] with the aim of improving the secrecy level in this type of networks. While the authors of [3]-[5] focus the downlink direction, in [6] the secrecy vulnerabilities of a non-orthogonal access system were addressed from the uplink perspective assuming that multiple eavesdroppers cooperate during the attack. Through the use of a geometric framework, the evaluation of the secrecy outage probability of a multiuser power domain NOMA system was performed in [7] considering an eavesdropper exclusion zone around the base-station. In a second evaluation, the same authors studied the secrecy improvement obtained when artificial noise is generated at the transmitter side. The security constraints associated with the integration of non-orthogonal multiple access schemes with well-known relaying techniques was focused in [8]. In [9], a null-steering jamming technique was implemented using a self-cooperative and non-self-cooperative jamming solution. While in the self-cooperative version only the base-station generates artificial noise, in the non-self-cooperative solution the artificial noise is transmitted by idle NOMA users. The scenario in which different security clearances are assigned to multiple legitimate users was addressed in [10]. Considering a two-layered unicast system, an optimal artificial noise beamforming scheme was developed taking into account the specific secrecy constraints associated to each user. In order to implement the security solution developed in [10], channel knowledge of all users must be available at the base-station, even the one associated to the user with the lowest clearance level, i.e. the eavesdropper.

Following the literature trend, the works in [3]-[9] only consider that the system is attacked from the outside, where an external passive eavesdropper not registered in the network remains undetectable. Because of the intrinsic processing structure of non-orthogonal multiple access techniques, in which inter-user interference must be first decoded to allow the receiver to get the intended information, considering that the system can only be attacked from the outside is limitative from the perspective of achieving a robust secrecy solution. From a practical approach, designing a secrecy scheme that only takes into consideration the presence of external

passive eavesdroppers makes little sense if the system is not protected from inside, since in this context the attacker only needs to registered in the network as a legitimate user to access the information that he pretends to tap. In [10], the problem of securing the network from inside is addressed. However as the proposed solution requires channel knowledge of all users, even the ones with minimal clearance level, i.e. the eavesdropper, then the system is not prepared to handle with attacks carried by undetectable passive eavesdroppers located outside of the network. Contrarily to [3]-[10], the authors of [11] addressed the scenario in which the NOMA system is attacked from inside and outside. Nevertheless, the secrecy scheme proposed in [11] is supported on higher layer cryptographic protocols, and therefore does not provide a standalone physical security [12], [13] solution.

To address the secrecy limitation identified above, this work proposes the use of a cooperative jamming solution that when combined with a secure training process allows to protect a power domain non-orthogonal multiple access system against simultaneous inside and outside eavesdropping attacks. To the best of the author's knowledge, the development of standalone physical layer security solutions to protect power-domain NOMA systems against these two types of attacks is an open problem that remains untreated in the literature.

The remainder of the paper is organized as follows: Section II presents the system model and the secrecy metric used in this work. The secure communication solution proposed in this manuscript is formulated in section III. Section IV presents and discusses the results obtained in the evaluation of the developed technique. The main conclusions are outlined in V.

II. System Model and Secrecy Metric

This section defines in a comprehensive way the system scenario as well the security problem handled in this work. The non-orthogonal multiple access network considered throughout this work is depicted in the system model represented in Fig. 1. In the considered scenario, a two user power domain non-orthogonal multiple access system is applied by node "A" to exchange the information streams d_B and d_{E0} with the receiving nodes "B" and "E0", respectively. Moreover, this work

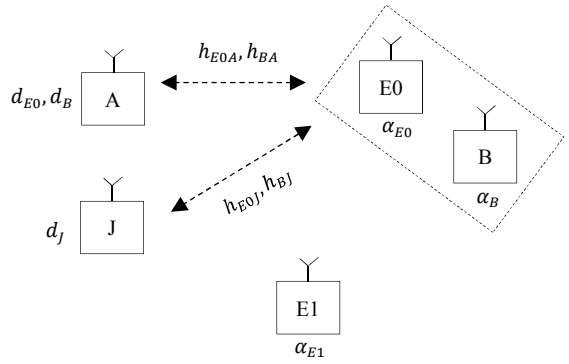

Fig. 1- System model

considers that the distance between node "A" and "E0" is lower than the distance between "A" and "B", therefore, as it is usually defined in the literature, "E0" is the strongest user with node "B" being the weakest user. In power domain non-orthogonal multiple access systems, the strongest user can only reach their intended information after decoding the interference generated by the weakest user, being this interference posteriorly canceled from the overall receiving signal using a successive interference cancellation (SIC) equalizer. Alternatively, a joint decoding of information and interference using a maximum likelihood (ML) equalizer can also be implemented. In this work, since "E0" will decode first the interference created by d_B before accessing the information sent to him, this node will be recognized by the network as a legitimate user that also has the capacity to eavesdrop d_B attacking the network from inside. Additionally, in order to model the occurrence of an outside attack, this work assumes also that a passive eavesdropper "E1" not registered in the network tries to tap the information d_B sent to node "B" in an undetectable way. Finally, to improve the secrecy level of the system, a jammer defined by node "J" cooperates with "A" generating a discrete jamming signal d_J.

As illustrated in Fig. 1, this work considers that all the nodes are equipped with a single antenna. The model previously described is general enough to encompass a scenario where silent Internet of Things (IoT) terminals are hacked through the network in order to get control of the respective physical layer resources for eavesdropping purposes. In such a scenario, "E1" could be regarded as a silent IoT terminal that at some point was hacked and started to work as an undetectable passive eavesdropper. Under such type of attack, all the higher layer security protocols applied at "E1" for access authentication and state monitoring would be broken, and the physical layer would become accessible to the hacker. The massive proliferation of low complexity IoT terminals expected for the upcoming years makes this type of attacks highly likely, particularly in scenarios where the access to the surrounding physical environment is well controlled.

The coefficient defined by h_{RT} with $R \in \{E0, B, E1\}$ and $T \in \{A, J\}$ represents small scale channel fading effects which are modeled by zero mean independent complex Gaussian random variables with variance σ_h^2. Additionally, the signals d_S, $S \in \{E0, B, J\}$ are also defined as independent random variables that follow a discrete uniform distribution. The path-loss attenuation between the transmitting nodes T and each one of the receiving nodes R is represented by the coefficients α_{E0}, α_B and α_{E1}, where it is assumed that $\alpha_B << \alpha_{E0}$. Furthermore, in this work "A" and "J" are at the same distance of each one of the other terminals, therefore, the same coefficient is applied to model the attenuation between this two terminals and each of the other receiving

nodes. The noise impairment at the receiving nodes R is represented by n_R and is modeled by zero mean complex Gaussian random variables with variance σ_n^2. Finally, ideal RF up- and down-conversion is assumed being all the baseband processing applied to an independent flat fading channel realization considering a time division duplex (TDD) context. The metric used in the evaluation of the proposed solution is formulated in Definition 1.

Definition 1: For d distributed uniformly across a set of M points, and y defined as the signal observed by the eavesdropper, weak secrecy can be formulated by

$$\lim_{M\to\infty}\left[\frac{I(d;y)}{\log_2(M)}\right]=0. \quad (1)$$

The ratio between the mutual information $I(d;y)$ and $\log_2(M)$ defined in (1) is used in the evaluation of the secrecy solution proposed in this work.

III. Secure Communication Scheme

The design of the secrecy solution proposed in this work will take into account not only the main communication phase but also the preliminary channel training process. Since in the proposed solution the design of the secure training scheme depends on the structure of the main communication phase, in this section the main communication phase will be introduced before the channel training method.

A. Communication Phase

The purpose of the main communication phase is to send d_{E0} and d_B to the intended receivers ensuring at the same time that "E0" is not able to acquire information regarding d_B, i.e. protect the system against the inside attack. In order to reach that goal, the signals transmitted by "A" and "J" are formulated as

$$x_A=\frac{1}{h_{E0A}}(p_L d_{E0}+p_H d_B), \quad (2)$$

$$x_J=\frac{1}{h_{E0J}}p_H d_J, \quad (3)$$

being p_L and p_H defined as known power allocation coefficients where the condition $p_L << p_H$ is verified. Taking into account (2) and (3), the signals observed by the receiving nodes are given by

$$\begin{aligned} y_{E0}&=\alpha_{E0}\left(h_{E0A}x_A+h_{E0J}x_J\right)+n_{E0}\\ &=\alpha_{E0}\left[p_L d_{E0}+p_H\left(d_B+d_J\right)\right]+n_{E0}, \end{aligned} \quad (4)$$

$$\begin{aligned} y_B&=\alpha_B\left(h_{BA}x_A+h_{BJ}x_J\right)+n_B\\ &=\alpha_B\left[\frac{h_{BA}}{h_{E0A}}\left(p_L d_{E0}+p_H d_B\right)+\frac{h_{BJ}}{h_{E0J}}p_H d_J\right]+n_B, \end{aligned} \quad (5)$$

$$\begin{aligned} y_{E1}&=\alpha_{E1}\left(h_{E1A}x_A+h_{E1J}x_J\right)+n_{E1}\\ &=\alpha_{E1}\left[\frac{h_{E1A}}{h_{E0A}}\left(p_L d_{E0}+p_H d_B\right)+\frac{h_{E1J}}{h_{E0J}}p_H d_J\right]+n_{E1}. \end{aligned} \quad (6)$$

In the case of the signal received at "E0" and assuming that the constants p_L and p_H are known, the term d_B+d_J is decoded in a first step considering $\alpha_{E0}p_L d_{E0}$ as low power noise. In a second step, $p_H\left(d_B+d_J\right)$ is cancelled from y_{E0} in order to allow "E0" to get their intended information d_{E0}. Alternatively, a joint ML decoding of d_{E0} and d_B+d_J can also be used to extract d_{E0} from (4). In terms of secrecy, the alignment of d_B with d_J in the same signal space forces the inside attacker "E0" to access the information related to d_B only through the observation of the integer addition d_B+d_J, which means that the level of protection against the inside attacker can be quantified computing the mutual information $I\left(d_B;d_B+d_J\right)$ between these two signals. As it was demonstrated in [14], the use of increasing order uniform square *M*-QAM signals independently generated for d_B and d_J allows to reach

$$\lim_{M\to\infty}\left[\frac{I\left(d_B;d_B+d_J\right)}{\log_2(M)}\right]=0, \quad (7)$$

which according to Definition 1 means that weak secrecy is achieved against the inside attacker "E0". Note that a discrete domain approach must be used to apply the SIC processing chain described above, hence, in this work uniform and equal order square *M*-QAM constellations are applied for d_{E0}, d_B and d_J. In the case of the signal observed by node "B", the assumption $\alpha_B p_L\approx 0$ is valid in the high SNR regime when the difference between p_H and p_L is significant. Therefore, the simplification

$$\hat{y}_B=\alpha_B p_H\left[\frac{h_{BA}}{h_{E0A}}d_B+\frac{h_{BJ}}{h_{E0J}}d_J\right]+n_B \quad (8)$$

can be applied for equation (5). When the difference between p_H and p_L is small, the recovery of d_B from (5) is achievable by making a joint ML decoding of d_{E0}, d_B and d_J. Taking into account the signal structure of (5) and (8), it is straightforward to conclude that in the high SNR regime d_B can be fully recovered when h_{BA}/h_{E0A} and h_{BJ}/h_{E0J} are available at node "B". As mentioned previously, the scenario considered in this work assumes

that node "B" is the only trustful receiver that is attacked by the eavesdroppers "E0" and "E1". In attacking occurrence, "E0" may connect to the network only to tap the information intended to "B", therefore, under such condition d_{E0} has no value to "B".

B. Training Phase

The design of the channel training process applied in this work is done respecting the following three main criterias: provide h_{E0A} and h_{E0J} to "A" and "J" respectively; ensure that h_{BA}/h_{E0A} and h_{BJ}/h_{E0J} are available at "B"; and minimize the amount of channel information leaked to the outside attacker "E1". In order to achieve the requirements mentioned above, in the proposed training solution the first two slots are applied for channel estimation, being the last two used for channel feedback. Moreover, in the remaining of this work it is assumed that the channel coherent interval is wide enough to perform channel training and transmission.

1) Channel Estimation

The objective of this point is to provide h_{BA}/h_{E0A} to node "A" and h_{BJ}/h_{E0J} to node "J", ensuring at the same time that terminal "E1" is not able to estimate their own channels for "A" and "J", i.e. in the proposed method these two terminals cannot send pilots. Assuming a perfect channel estimation process, in the first slot "E0" sends a pilot that provides h_{E0A} to "A" and h_{E0J} to node "J", while in the second slot the pilot is sent by "B" giving h_{BA} to "A" and h_{BJ} to "J".

2) Channel Feedback

In this step, the channels h_{BA}/h_{E0A} and h_{BJ}/h_{E0J} estimated in the first two slots of this training process are sent with some level of secrecy to node "B". To achieve that, in the third slot terminal "A" feedbacks h_{BA}/h_{E0A} to "B" sending $x_{F(A)}$, while in the fourth slot node "J" exchanges h_{BJ}/h_{E0J} with "B" through the transmission of signal $x_{F(J)}$. The transmitted signals mentioned before are formulated as

$$x_{F(A)} = p_H \frac{|h_{BA}|}{|h_{E0A}|^2} e^{j(\theta_{E0A}-2\theta_{BA})}, \quad (9)$$

$$x_{F(J)} = p_H \frac{|h_{BJ}|}{|h_{E0J}|^2} e^{j(\theta_{E0J}-2\theta_{BJ})}, \quad (10)$$

where $|h_{RT}|$ and θ_{RT} defines the magnitude and phase of the channel h_{RT}, respectively. In a noiseless channel scenario, the signals received at "B" during the third and fourth slots are defined as

$$\begin{aligned} y_{B,F(A)} &= \alpha_B x_{F(A)} h_{BA} \\ &= \alpha_B p_H \left(\frac{|h_{BA}|}{|h_{E0A}|} \right)^2 e^{j(\theta_{E0A}-\theta_{BA})}, \end{aligned} \quad (11)$$

$$\begin{aligned} y_{B,F(J)} &= \alpha_B x_{F(J)} h_{BJ} \\ &= \alpha_B p_H \left(\frac{|h_{BJ}|}{|h_{E0J}|} \right)^2 e^{j(\theta_{E0J}-\theta_{BJ})}. \end{aligned} \quad (12)$$

Considering that $\alpha_B p_H$ is a constant known at "B", the recovery of h_{BA}/h_{E0A} and h_{BJ}/h_{E0J} from (11) and (12) is done by performing the following operations at node "B"

$$\left(\frac{|y_{B,F(A)}|}{\alpha_B p_H} \right)^{1/2} e^{-j\theta_{B,F(A)}} = \frac{h_{BA}}{h_{E0A}}, \quad (13)$$

$$\left(\frac{|y_{B,F(J)}|}{\alpha_B p_H} \right)^{1/2} e^{-j\theta_{B,F(J)}} = \frac{h_{BJ}}{h_{E0J}}, \quad (14)$$

where $|y_{B,F(T)}|$ and $\theta_{B,F(T)}$ denote the magnitude and phase of $y_{B,F(T)}$, respectively. In the case of the outside attacker "E1", the signals observed by this node during the feedback phase are defined as

$$\begin{aligned} y_{E1,F(A)} &= \alpha_{E1} x_{F(A)} h_{E1A} \\ &= \alpha_{E1} p_H \frac{|h_{BA}| \times |h_{E1A}|}{|h_{E0A}|^2} e^{j(\theta_{E1A}+\theta_{E0A}-2\theta_{BA})} \\ &= |y_{E1,F(A)}| e^{j\theta_{E1,F(A)}} \end{aligned}, \quad (15)$$

$$\begin{aligned} y_{E1,F(J)} &= \alpha_{E1} x_{F(J)} h_{E1J} \\ &= \alpha_{E1} p_H \frac{|h_{BJ}| \times |h_{E1J}|}{|h_{E0J}|^2} e^{j(\theta_{E1J}+\theta_{E0J}-2\theta_{BJ})} \\ &= |y_{E1,F(J)}| e^{j\theta_{E1,F(J)}} \end{aligned}. \quad (16)$$

While for the inside attacker only the main communication phase impacts the secrecy, in the case of the outside attacker, both the main communication phase and the training phase must be considered in the secrecy assessment. Therefore, having already defined the signals observed by "E1" during the main communication and training phases, the quantification of the secrecy level obtained against the outside attacker can be done computing an upper bound on the mutual information $I(d_B; y_{E1}, y_{E1,F(A)})$. Since "E1" only pretends to tap the information associated to the source d_B, an upper bound on $I(d_B; y_{E1}, y_{E1,F(A)})$ can be derived assuming that the interference generated by d_{E0} and d_J in node "E1" is

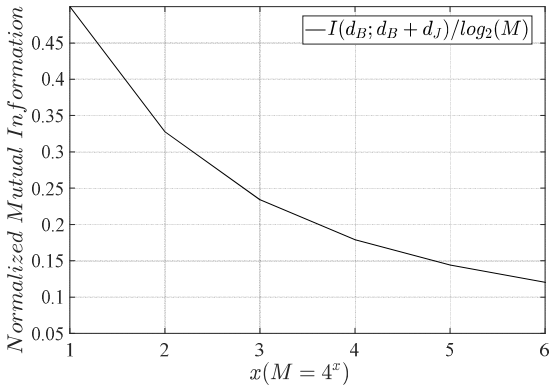

Fig. 2 – Secrecy level against the inside attacker "E0"

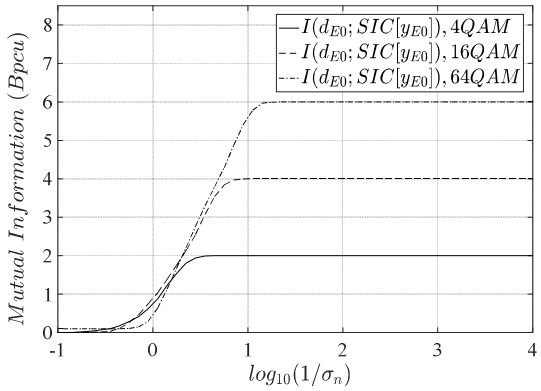

Fig. 3 – Mutual information between d_{E0} and the output of a SIC decoder applied to y_{E0}

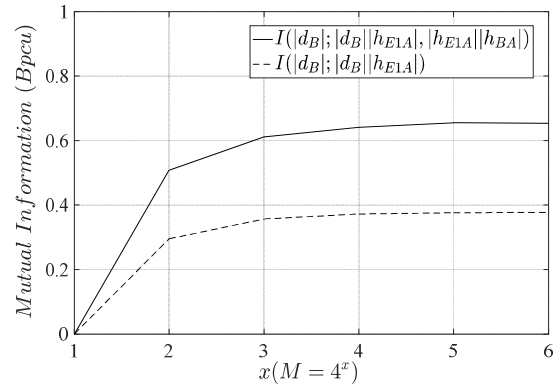

Fig. 4 – Non-normalized secrecy level against the outside attacker "E1"

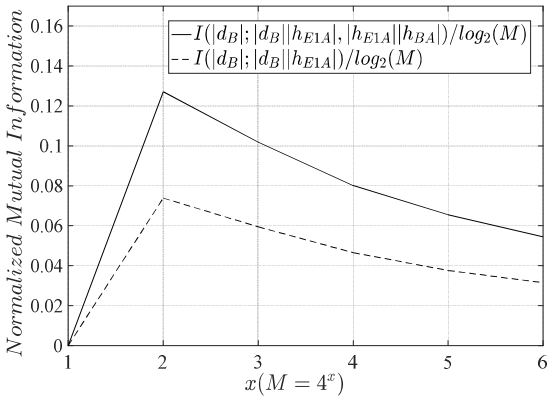

Fig. 5 – Secrecy level against the outside attacker "E1"

zero. Under the non-interference scenario, the signal observed at "E1" can be formulated as

$$\begin{aligned}\hat{y}_{E1} &= \alpha_{E1} p_H \frac{h_{E1A}}{h_{E0A}} d_B \\ &= \alpha_{E1} p_H \frac{|h_{E1A}| \times |d_B|}{|h_{E0A}|} e^{j(\theta_{E1A} - \theta_{E0A} + \theta_B)} \\ &= |\hat{y}_{E1}| e^{j\hat{\theta}_{E1}}\end{aligned}, \quad (17)$$

with $I\left(d_B; \hat{y}_{E1}, y_{E1,F(A)}\right)$ providing a valid upper bound for the amount of information leaked to "E1". Because the interference caused by d_J is not present in (17), the observation of $y_{E1,F(J)}$ doesn't add any useful information to recover d_B, and therefore can be ignored for the secrecy evaluation. Another important point that should be discussed is associated to the fact that the phases of $\hat{y}_{E1}$ and $y_{E1,F(A)}$, defined as $\hat{\theta}_{E1}$ and $\theta_{E1,F(A)}$ respectively, are mutually independent of d_B, which means that the information carried in the phase of d_B, i.e. θ_B, is fully protected from "E1". Hence, in the proposed solution "E1" can only get information associated to the magnitude of d_B through the observation of $|\hat{y}_{E1}|$ and $|y_{E1,F(A)}|$. Assuming that $|h_{E0A}|$ is known at "E1", and for $\alpha = \alpha_{E1} p_H$, an upper bound on the amount of information leaked to the outside attacker can be defined as

$$I\left(d_B; \hat{y}_{E1}, y_{E1,F(A)}\right) \le I\left(|d_B|; \alpha |d_B||h_{E1A}|, \alpha |h_{E1A}||h_{BA}|\right). \quad (18)$$

Through the comparison of the upper bound in (18) with $I\left(|d_B|; \alpha |d_B||h_{E1A}|\right)$, a quantitative reference regarding to the amount of information leaked by the proposed solution during the training phase can be evaluated. Therefore, a lower limit on the value of $I\left(|d_B|; \alpha |d_B||h_{E1A}|, \alpha |h_{E1A}||h_{BA}|\right)$ will be also assessed in this work computing $I\left(|d_B|; \alpha |d_B||h_{E1A}|\right)$.

Remark 1: The scaling of the proposed solution to the case where more than two users access the system was not analyzed in this work. Nevertheless, considering that such extension would be achievable by adding a dedicated

jammer for each user, an increase of the channel training complexity would be observed.

IV. RESULTS

The purpose of this section is to analyze the results associated to the evaluation of the secrecy solution developed in the scope of this work. The mutual information curves presented in the following points were obtained using kernel based density estimators considering a unitary scale parameter for the Rayleigh distributions that model the small-scale channel fading magnitudes defined by h_{RT} . Furthermore, the power conditions associated to the signals d_S are characterized by $\mathrm{E}\left[\left|d_S\right|^2\right]=1$, being $\alpha_{E0}p_L$ and $\alpha_B p_H$ unitary constants with $p_H = Kp_L$. With the parameters defined above, the system evaluated in the following points is fully characterized for a given value of K .

A. E0 – Inside Attacker

As mentioned before, the secrecy level obtained against the inside attacker can be quantified calculating $I\left(d_B; d_B + d_J\right)$, where d_B and d_J are square QAM signals of the same order M and with equal magnitude scaling. The analysis of Fig. 2 shows that when the constellations order M increases and for the noiseless regime, the percentage of information acquired by the inside attacker tends to zero. In the case of the information intended to node "E0", the curves in Fig. 3 were obtained computing the mutual information in bits per channel use (Bpcu) between d_{E0} and the output of a SIC decoder when the respective input is y_{E0} . The results presented in Fig. 3 shows that in the large SNR regime and considering $K=10$ for $M \in \{4,16,64\}$, the processing of y_{E0} using a SIC equalizer allows "E0" to get all the information associated to d_{E0} . Although the mutual information curves presented in Fig. 3 are limited to $M=64$, in the large SNR regime and for $K \to \infty$, the value of the mutual information $I\left(d_{E0}; SIC\left[y_{E0}\right]\right)$ scales up with the entropy of the source, which is defined as $\log_2\left(M\right)$.

B. E1 – Outside Attacker

As explained in section III, the level of secrecy at the outside attacker can be evaluated quantifying the amount of information leaked at "E1" computing the value of the mutual information $I\left(\left|d_B\right|; \alpha\left|d_B\right|\left|h_{E1A}\right|, \alpha\left|h_{E1A}\right|\left|h_{BA}\right|\right)$, being the calculation of $I\left(\left|d_B\right|; \alpha\left|d_B\right|\left|h_{E1A}\right|\right)$ used as a reference to assess the amount of information leaked by the proposed scheme during the channel training phase.

Starting by analyzing the results of the mutual information $I\left(\left|d_B\right|; \alpha\left|d_B\right|\left|h_{E1A}\right|, \alpha\left|h_{E1A}\right|\left|h_{BA}\right|\right)$ depicted in Fig. 4, a first observation shows that an upper bound on the amount of information leaked to the outside attacker "E1" saturates with the entropy of the source, remaining in this case always below than 0.8 bits for any value of M considered. Moreover, a quantitative reference for further improvements of the proposed solution is obtained evaluating $I\left(\left|d_B\right|; \alpha\left|d_B\right|\left|h_{E1A}\right|\right)$, which reveals that when full protection of $\left|h_{E1A}\right|$ is ensured, the secrecy level at "E1" can be reduced for values below than 0.4 bits. Note that because α is a constant has no impact on the mutual information bounds formulated in this work, therefore, it was ignored in the results presented in Fig. 4. While the results in Fig. 4 represent absolute mutual information values, the curves in Fig. 5 were normalized to the entropy of the source, i.e. $\log_2\left(M\right)$. As in the case of the inside attacker "E0", the curves in Fig. 5 show that increasing the order of d_B , the percentage of information acquired by the outside attacker "E1" tends to zero, which according to Definition 1 means that the proposed solution is approaching weak secrecy against "E1". Because α is a constant and has no impact in the secrecy bound computed for "E1", the increase of the value of p_H in equation (4), which is required to increase M and reach weak secrecy against the inside attacker "E0", can be done without affecting the secrecy level at "E1".

The level of secrecy obtained at "E1" results from the fact that with the proposed solution, full protection of the information carried in the phase of d_B is ensured, being the amount of information associated to the magnitude of d_B protected with the channel magnitude $\left|h_{E1A}\right|$, which in turn is secured from the outside attacker "E1" with $\left|h_{BA}\right|$.

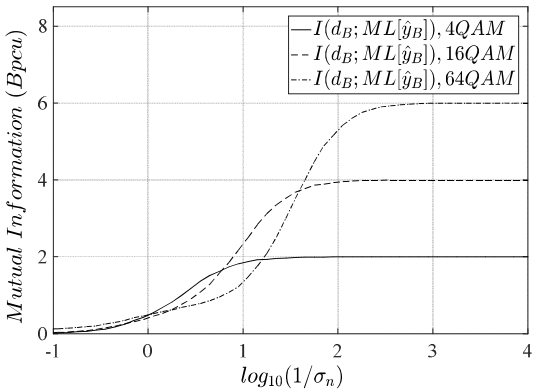

Fig. 6 – Mutual information between d_B and the output of an ML decoder applied to $\hat{y}_B$

C. B – Legitimate Receiver

As mentioned before, after the feedback of h_{BA}/h_{E0A} and h_{BJ}/h_{E0J} to "B", the recovery of d_B at this terminal is achieved equalizing $\hat{y}_B$ using a maximum likelihood

(ML) decoder. In this case, as can be concluded from the analysis of equation (8), in the large SNR regime the mutual information $I\left(d_B; ML[\hat{y}_B]\right)$ between d_B and the output of a ML equalizer with input $\hat{y}_B$ grows with the entropy of the source d_B for increasing M. This behavior can be confirmed in Fig. 6 for $M \in \{4,16,64\}$, where the mutual information results associated to this decoding operation show that in the high SNR regime all the information intended to the legitimate user "B" is obtained processing $\hat{y}_B$ with an ML decoder.

V. Conclusion

In order to improve the secrecy level of a power domain non-orthogonal multiple access system, a cooperative jamming solution was combined with a secure channel training scheme to protect the system against eavesdropping attacks coming from inside and outside of the network. The evaluation of the proposed scheme showed that when square *M*-QAM constellations are applied for data and jamming signals, weak secrecy against inside and outside eavesdropping attacks is obtained. In terms of future work, the extension of the proposed solution to the case in which node "B" is also an eavesdropper of the strong user "E0" emerges from the presented work as a new line of research to be followed. Additionally, the scaling of the developed scheme to the scenario where more than two users access the system is also an interesting research topic to be analyzed in the future.

Acknowledgement

This work was supported by project POCI-01-0145-FEDER-016753 SWING2 (PTDC/EEITEL/3684/2014), funded by Fundos Europeus Estruturais e de Investimento (FEEI) through Programa Operacional Competitividade e Internacionalização-COMPETE 2020 and by National Funds from FCT - Fundos Europeus Estruturais e de Investimento, and also by project UID/EEA/50008/2019 funded by FCT/MEC through national funds and when applicable co-funded by FEDER - PT2020 partnership agreement. G. Anjos is supported by Fundação para a Ciência e Tecnologia under the grant SFRH/BD/136787/2018.

References

[1] Linglong Dai, Bichai Wang, Zhiguo Ding, Zhaocheng Wang, Sheng Chen and Lajos Hanzo, "A Survey of Non-Orthogonal Multiple Access for 5G," *IEEE Commun. Surveys & Tutorials,* 2018.

[2] Yuanwei Liu, Zhijin Qin, Maged Elkashlan, Zhiguo Ding, Arumugam Nallanathan and Lajos Hanzo, "Nonorthogonal Multiple Access for 5G and Beyond," *Proceedings of IEEE,* vol. 105, no. 12, Dec. 2017.

[3] Yi Zhang, Hui-Ming Wang, Qian Yang and Zhiguo Ding, "Secrecy Sum Rate Maximization in Non-orthogonal Multiple Access," *IEEE Comm. Letters,* vol. 20, no. 5, pp. 930-933, May 2016.

[4] Biao He, An Liu, Nan Yang and Vincent K. N. Lau, "On the Design of Secure Non-Orthogonal Multiple Access Systems," *IEEE J. Sel. Areas Commun.,* vol. 35, no. 10, 2196-2206 , Oct. 2017.

[5] Hongjiang Lei, Jianming Zhang, Ki-Hong Park, Peng Xu, Imran Shafique Ansari, Gaofeng Pan, Basel Alomair and Mohamed-Slim Alouini, "On Secure NOMA Systems With Transmit Antenna Selection Schemes," *IEEE Access,* vol. 5, pp. 17450 - 17464, Aug. 2017.

[6] Kaiwei Jiang, Tao Jing, Yan Huo, Fan Zhang and Zhen Li, "SIC-Based Secrecy Performance in Uplink NOMA Multi-Eavesdropper Wiretap Channels," *IEEE Access,* vol. 6, pp. 19664 - 19680, Apr. 2018 .

[7] Yuanwei Liu, Zhijin Qin, Maged Elkashlan, Yue Gao and Lajos Hanzo, "Enhancing the Physical Layer Security of Non-Orthogonal Multiple Access in Large-Scale Networks," *IEEE Trans. Wireless Commun.,* vol. 16, no. 3, pp. 1656-1672, Mar. 2017.

[8] Jianchao Chen, Liang Yang and Mohamed-Slim Alouini, "Physical Layer Security for Cooperative NOMA Systems," *IEEE Trans. Veh. Technol.,* vol. 67, no. 5, pp. 4645-4649 , May 2018.

[9] Yamen Alsaba, Chee Yen Leow and Sharul Kamal Abdul Rahim, "Null-Steering Beamforming for Enhancing the Physical Layer Security of Non-Orthogonal Multiple Access System," *IEEE Acccess,* vol. 7, pp. 11397 - 11409, Jan. 2019.

[10] Wei Zhang, Jian Chen, Yonghong Kuo and Yuchen Zhou, "Artificial-Noise-Aided Optimal Beamforming in Layered Physical Layer Security," *IEEE Communications Letters,* vol. 3, no. 1, pp. 72 - 75, Jan. 2019.

[11] Datong Xu, Pinyi Ren and Hai Lin, "Combat Hybrid Eavesdropping in Power-Domain NOMA: Joint Design of Timing Channel and Symbol Transformation," *IEEE Trans. Veh. Technol.,* vol. 67, no. 6, pp. 4998 - 5012, Jun. 2018.

[12] Amitav Mukherjee, S. Ali A. Fakoorian, Jing Huang and A. Lee Swindlehurst, "Principles of Physical Layer Security in Multiuser Wireless Networks: A Survey," *IEEE Commun. Surveys & Tutorials,* vol. 16, no. 3, pp. 1550-1573, 2014.

[13] Yiliang Liu, Hsiao-Hwa Chen and Liangmin Wang, "Physical Layer Security for Next Generation Wireless Networks: Theories, Technologies, and Challenges," *IEEE Commun. Surveys & Tutorials,* vol. 19, no. 1, pp. 347-376, 2017.

[14] G. Anjos, D. Castanheira, A. Silva, A. Gameiro, M. Gomes and J. P. Vilela, "Exploiting the Reciprocal Channel for Discrete Jamming to Secure Wireless Communications Against Multiple-Antenna Eavesdropper," *IEEE Access,* vol. 6, pp. 33410-33420, July 2018.