XXXVII SIMPÓSIO BRASILEIRO DE TELECOMUNICAÇÕES E PROCESSAMENTO DE SINAIS - SBrT2019, 29/09/2019–02/10/2019, PETRÓPOLIS, RJ

Robustness of the Tomlinson-Harashima Precoder in Physical-layer Security to Attacks with Non-linear CMA

Pedro Ivo da Cruz, Ricardo Suyama and Murilo Bellezoni Loiola

***Abstract*— Physical-layer security techniques have proven to be a good alternative to the computational high-cost traditional security mechanisms for wireless communications. In this work, the secrecy level provided by a Tomlinson-Harashima precoder is evaluated in a scenario in which the eavesdropper is allowed to perform extra signal processing at the received signal, aiming to recover the confidential information. The results indicate that even with the extra effort using unsupervised channel equalization methods, the eavesdropper is not able to totally recover the information.**

***Keywords*— Physical-layer Security, Precoding, Blind equalization.**

I. Introduction

Recently, Physical-layer Security (PLS) has drawn a lot of attention due to its low computational power and energy requirements, which makes it feasible to applications such as Internet of Things [1]. The PLS explores random channel characteristics, such as fading, to secure the information to be transmitted in wireless communications systems [2].

Several PLS techniques have been studied for Mutliple Input Multiple Output (MIMO) and MIMO Orthogonal Frequency Division Multiplexing (MIMO-OFDM) systems [3]–[6]. However, single carrier and single antenna (SC-SA) systems are being employed, for instance, in IoT applications, where the limited space makes it difficult to employ more than one antenna per device. Nevertheless, little attention has been given to PLS in SC-SA systems, and very few techniques have been studied and developed specifically for them. For instance, the work in [7] proposes a technique to employ artificial noise for SC-SA systems. Also, the work in [8] considers a type of precoding that only pre-distorts the phase of the signal to be transmitted. The work in [9] investigates the use of linear precoders for securing SC-SA systems under frequency selective fading channels.

The precoding technique pre-distorts the confidential information at the transmitter in such a way that, after undergoing into fading of the authentic channel, the distortion will be removed. As the signal received at the eavesdropper goes under a different fading, the eavesdropper will still receive a distorted message. However, by using a linear precoder at the transmitter, the eavesdropper might employ a blind equalizer, such as the constant modulus algorithm (CMA), the multiple modulus algorithm [10] or the Shalvi-Weinstein algorithm [11] to remove the distortion and retrieve the confidential information [9]. These algorithms use linear structures to blindly equalize the received signal and, thus, are also able to mitigate the combined effects of a linear precoder and the eavesdropper channel.

To prevent that, other structures, such as a non-linear precoder – as the Tomlinson-Harashima precoder (THP) [12], [13] – may be employed. In this case, standard blind equalization methods are unable to recover the original message, but it would be important to analyze if it would be possible to employ a modified unsupervised method (possibly encompassing a nonlinear structure) to circumvent this security scheme.

Some works in the literature have shown that non-linear blind equalizers might be used at the receiver side to help improve the performance of the system with THP at the transmitter. The work in [14] shows that bounding the kurtosis of the signal at the THP output, not only helps to remove distortions originated from channel variations and channel estimation errors in the transmitter, but also helps the convergence of the blind equalizer. This would be a drawback for the THP when used for PLS purposes since it suggests that an eavesdropper may recover the confidential information by employing a blind equalizer with a non-linear structure.

Thus, the objective of this work is to investigate this possible vulnerability of THP-based PLS scheme in SA systems. In this study, it is considered that an unsupervised channel equalization algorithm, the non-linear CMA (NLCMA), is used to try recovering the information at the eavesdropper even with the confidential message being precoded by the THP.

The rest of the paper is organized as follows: the signal and eavesdropping model is presented at section II, together with the description of the THP; in section III the NLCMA is described; simulations and the results obtained are shown and discussed in section IV; finally, conclusions are highlighted in section V.

II. System Modeling

In the model considered in this work, summarized in Fig. 1, Alice sends a confidential message $m(n)$ to Bob, which consists of quadrature phase-shift keying (QPSK) modulated symbols. In order to accomplish that, the message is precoded by the

Pedro Ivo da Cruz, Ricardo Suyama and Murilo Bellezoni Loiola are with the Engineering, Modeling and Applied Social Sciences Center, Federal University of ABC, Santo André, SP, Brazil, E-mails: pedro.cruz@ufabc.edu.br, ricardo.suyama@ufabc.edu.br, murilo.loiola@ufabc.edu.br. This study was financed in part by the Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - Brasil (CAPES) - Finance Code 001, FAPESP (2013/25977-7) and the National Council for Scientific and Technological Development – CNPq.

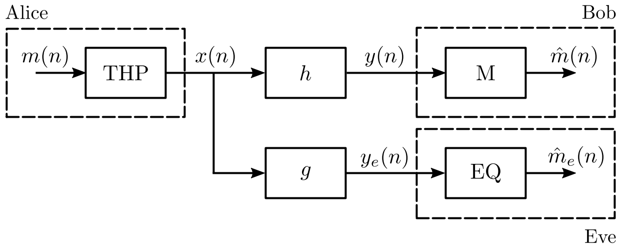

Fig. 1. Block diagram of the signal model used in this work.

THP as

$$x(n) = \frac{1}{h_0} \mathrm{M}\left\{ m(n) - \sum_{l=1}^{L-1} h_l x(n-l) \right\}, \tag{1}$$

where h_l for $l = 0, \cdots, L-1$ are the L taps of the authentic channel. The modulo operation $\mathrm{M}\{\cdot\}$ is given by

$$\mathrm{M}\{\alpha\} = \alpha - 2A \left\lfloor \frac{\alpha + A + jA}{2A} \right\rfloor, \tag{2}$$

where $A = \sqrt{N_M}$, $N_M = 4$ is the QPSK modulation order, α is the input of the modulo operation, j is the imaginary number and $\lfloor\cdot\rfloor$ denotes the round floor operation, i.e., it rounds its argument to the nearest integer less than or equal to that argument.

By letting $\mathbf{x}(n) = [x(n),\ x(n-1),\ \cdots,\ x(n-L+1)]^{\mathrm{T}}$ and $v(n) \sim \mathcal{CN}(0, \sigma^2)$ complex Gaussian noise with zero mean and power σ^2, the signal received by Bob can be written as

$$y(n) = \mathbf{x}^{\mathrm{T}}(n)\mathbf{h} + v(n). \tag{3}$$

The vector $\mathbf{h} = [h_0,\ h_1,\ \cdots,\ h_{L-1}]^{\mathrm{T}}$ is the channel vector containing the L taps of the authentic channel between Alice and Bob.

To recover the information, the signal received by Bob goes through the same non-linear operation used at the precoder. In other words, the estimate of the confidential message is given by $\hat{m}(n) = \mathrm{M}\{y(n)\}$.

Similarly, defining $\mathbf{g} = [g_0,\ g_1,\ \cdots,\ g_{L-1}]^{\mathrm{T}}$ as the channel vector of the channel between Alice and Eve, the signal received by Eve is given by

$$y_e(n) = \mathbf{x}^{\mathrm{T}}(n)\mathbf{g} + v_e(n), \tag{4}$$

where $v_e(n) \sim \mathcal{CN}(0, \sigma_e^2)$. The estimate of the confidential message at Eve is the output of the equalizer EQ, given by $\hat{m}_e(n)$.

III. Non-linear CMA

If Eve wants to recover the message sent by Alice, it should obtain a signal as close as possible to the one received by Bob. One way to accomplish that would be to remove the effects of the channel $\mathbf{g}$ from its received signal, $y_e(n)$, and pass the resulting signal through a filter with the weights given by the authentic channel, $\mathbf{h}$.

In order to obtain a filter that performs such tasks and considering that it is possible to obtain the inverse of the channel (there is a sufficient number of coefficients to approximate the channel inverse) one should obtain the result of the convolution of the Wiener solution for the eavesdropper channel inversion, $\mathbf{g}_o$, and the authentic channel $\mathbf{h}$, which leads to the optimal weights

$$\mathbf{w}_o = \mathbf{H}\mathbf{g}_o, \tag{5}$$

where

$$\mathbf{g}_o = \mathbf{d}\mathbf{G}^{\mathrm{H}} \left(\mathbf{G}\mathbf{G}^{\mathrm{H}} + \sigma^2 \mathbf{I} \right)^{-1}. \tag{6}$$

In both (5) and (6), $\mathbf{H}$ and $\mathbf{G}$ are convolution matrices generated from $\mathbf{h}$ and $\mathbf{g}$, respectively. The vector $\mathbf{d}$ in (6) is a delay vector, filled with zeros and with 1 in the position of the desired delay. Filtering the signal received at Eve with a filter with taps obtained through (5), the expected output is the same signal received at Bob.

It is important to highlight at this point that Alice does not send any reference signal, so Eve has neither the knowledge of its channel $\mathbf{g}$, nor the authentic channel $\mathbf{h}$, and, thus, Eve is not able to compute (5) explicitly. In order to obtain a solution to this problem, Eve might employ blind equalization algorithms, such as the CMA. However, the traditional CMA is expected not to work when the transmitter employs the THP due to the presence of the non-linear operation $\mathrm{M}\{\cdot\}$ in it.

The traditional CMA is an unsupervised (blind) iterative algorithm aimed to obtain the filter weights $\mathbf{w} = [w_0,\ w_1,\ \cdots,\ w_{K-1}]^{\mathrm{T}}$ that best approximates the absolute value of the filter output to an specific parameter γ [10]. This parameter is computed using statistics of the transmitted signal, requiring no knowledge about the signal itself, which is necessary for supervised algorithms. The block diagram of the signal flow in an equalizer using the CMA is shown in Fig 2.

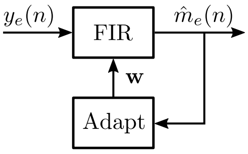

Fig. 2. Block diagram of the CMA equalizer.

The non-linear CMA (NLCMA) that takes the modulo operation of the THP into consideration tries to approximate the magnitude of the modulo operation output to the value of the γ parameter as given by

$$\min_{\mathbf{w}} \mathrm{E}\left\{ \gamma - |\,\mathrm{M}\{\mathbf{u}(n)\mathbf{w}\}\,|^2 \right\}, \tag{7}$$

where $\mathbf{u}(n) = [y_e(n),\ y_e(n-1),\ \cdots,\ \ y_e(n-K+1)]$. Differently from the idea in [14], this structure aims to revert the effects of the eavesdropper channel $\mathbf{g}$ and emulate the fading effects of the authentic channel $\mathbf{h}$ on the signal received at the eavesdropper. To achieve this, the NLCMA uses the signal at the output of the modulo operation, as shown in Fig. 3, to compute the adaptation for the filter taps. For a QPSK modulation, the γ parameter can be set to $\gamma = 1$, since the modulus of the QPSK symbols is 1. The weight adaptation algorithm is summarized in the Algorithm 1, where μ is the adaptation step and $e^*(n)$ corresponds to the conjugate of the value $e(n)$.

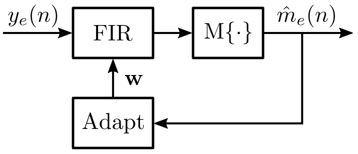

Fig. 3. Block diagram of the NLCMA equalizer.

Algorithm 1 NLCMA for THP.

```
Initialization
w: Random
$\mu$ between 0 e 1
for $n \geq 0$ do
    $\hat{m}_e(n) = \mathrm{M}\{\mathbf{u}(n)\mathbf{w}\}$
    $e(n) = \gamma - |\hat{m}_e(n)|^2$
    $\mathbf{w} = \mathbf{w} + \mu\mathbf{u}^{\mathrm{T}}(n)m_e(n)e^*(n)$
end for
```

IV. Simulations and Results

To evaluate the NLCMA, simulations were carried out with an authentic channel $\mathbf{h} = [1,\ 0.6]^{\mathrm{T}}/1.6$ and an eavesdropper channel with only one tap generated randomly, $g_0 \sim \mathcal{N}(0, 1)$. The equalizer, therefore, was set to have only two taps. This number of taps for the channels and equalizer is chosen in order to plot the surface error since a higher number of taps would not allow it to be visualized in three dimensions. The surface error is generated by evaluating the error $e(n) = \gamma|\hat{m}_e(n)|^2$ for different values of $\mathbf{w}$. The results shown in Figs. 4 and 5, were obtained with $\mathbf{g} = [0.6937]^{\mathrm{T}}$. For this case, the Wiener channel inversion given by (6) results in a one-tap filter, which convoluted with the two-tap authentic channel, results in $\mathbf{w}_o$ with two taps. Therefore, the NLCMA considered has also two taps.

The error surface for a two-tap filter is shown in Fig. 4, where it is possible to see two prominent minima: one in $\mathbf{w} = [0.9,\ 0.5395]^{\mathrm{T}}$ and other in $\mathbf{w} = [-0.9,\ -0.5395]^{\mathrm{T}}$. These minima are close to the Wiener solution $\mathbf{w}_o = [0.8991,\ 0.5395]^{\mathrm{T}}$, obtained through (5), and are also capable of recovering the confidential message at Eve. This happens because, in these simulations, it is possible to invert the eavesdropper channel with only one tap, and the optimal solution is the result of the convolution with the authentic channel. The bit error rate (BER) obtained for these weights achieved by the NLCMA is 0, i.e., the Eve was able to recover the information.

However, as it is possible to see in Fig. 5, other local minima are observed, as expected from the CMA cost function. This figure shows the contours of the NLCMA error function and helps to visualize less prominent minima that would not be observed in Fig. 4 due to the amplitude variation of the cost function. One minimum is observed around $\mathbf{w} = [0.6,\ 0]^{\mathrm{T}}$ and other in $\mathbf{w} = [-0.6,\ 0]^{\mathrm{T}}$. This would, therefore, compromise the performance of the NLCMA.

Fig. 6 shows the surface error for the NLCMA cost function in a 10 dB SNR environment. The prominent minima is around $\mathbf{w} = [0.7950,\ 0.437]^{\mathrm{T}}$ and $\mathbf{w} = [-0.7950,\ -0.437]^{\mathrm{T}}$, and the NLCMA converged to $\mathbf{w} = [0.7513,\ 0.4462]^{\mathrm{T}}$ by initiating close to the former. The BER obtained for this filter weights is 1.2×10^{-3}.

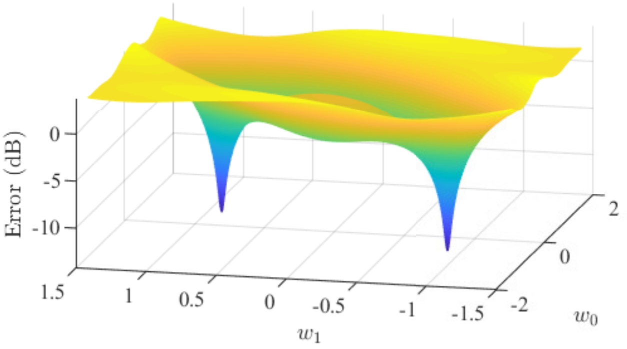

Fig. 4. Error surface for the NLCMA for $\mathbf{h} = [1,\ 0.6]^{\mathrm{T}}/1.6$ and $\mathbf{g} = [0.6937]^{\mathrm{T}}$ and 30 dB SNR.

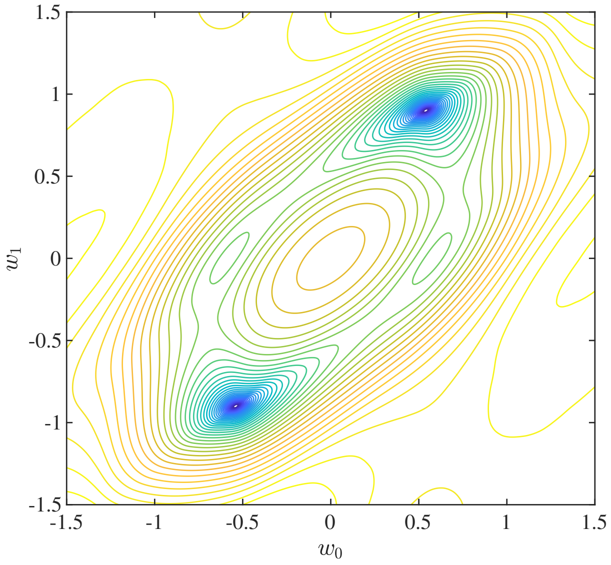

Fig. 5. Contour lines for the NLCMA error for $\mathbf{h} = [1,\ 0.6]^{\mathrm{T}}/1.6$ and $\mathbf{g} = [0.6937]^{\mathrm{T}}$ and 30 dB SNR.

Although the BER obtained is very low, the contour lines shown in Fig. 7 also show some local minima at the same position seen in Fig. 5, which will also degrade the convergence performance of the NLCMA depending on the initialization.

To evaluate the impact of the initialization, 2×10^3 trials, each of them considering the transmission of 10^5 symbols, were carried out to obtain the number of trials the NLCMA would converge to a solution close to the Wiener solution. To determine how close the solution $\mathbf{w}$ is to the optimal solution $\mathbf{w}_o$, it was considered the mean squared error (MSE) between both, given by

$$\mathrm{MSE}(\mathbf{w}) = \frac{1}{K}\sum_{k=0}^{K-1} ||w_k| - |w_{o,k}||^2, \tag{8}$$

where $w_{o,k}$ is the k-th element of $\mathbf{w}_o$. If the MSE is below a certain threshold ϕ, then the algorithm is considered to have satisfactorily achieved the optimal solution. The initial taps of $\mathbf{w}$ in each trial are determined by a complex random Gaussian process with zero mean and unit variance, and the taps are

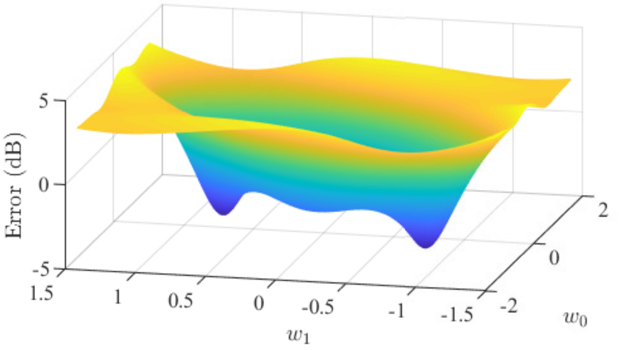

Fig. 6. Error surface for the NLCMA for $\mathbf{h} = [1,\ 0.6]^{\mathrm{T}}/1.6$, $\mathbf{g} = [0.6937]^{\mathrm{T}}$ and 10 dB SNR.

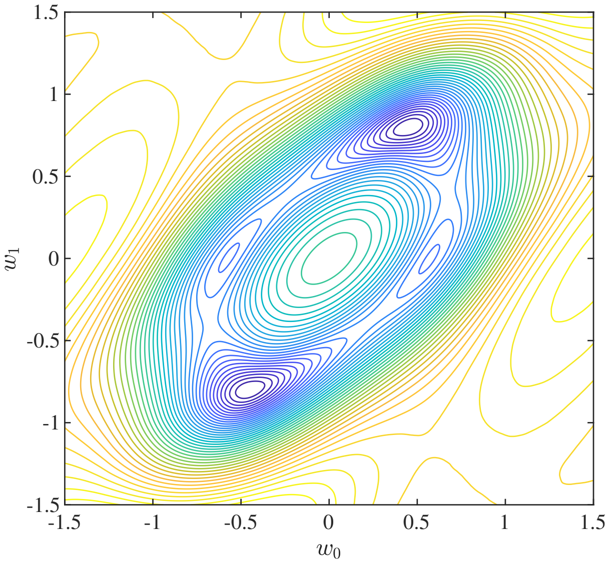

Fig. 7. Contour lines for the NLCMA error for $\mathbf{h} = [1,\ 0.6]^{\mathrm{T}}/1.6$, $\mathbf{g} = [0.6937]^{\mathrm{T}}$ and 10 dB SNR.

independent to each other. In other words, $w_l \sim \mathcal{CN}(0,1)$. Both authentic and eavesdropper channels are randomly generated in each trials considering a Gaussian distribution, $h_l \sim \mathcal{N}(0,\sigma_l^2)$ and $g_l \sim \mathcal{N}(0,\sigma_l^2)$.

The Tables I and II show the results obtained considering different values of ϕ for SNR of 10 dB and 30 dB, respectively. Other SNR values were also evaluated and have shown similar behaviour. As can be seen in both tables, by reducing the adaptation step, the number of trials that passes the test reduces. This is because the filters tap might have converged to one of the local minima and, if μ is large enough, it is possible that the algorithm can lead the taps out of the local minimum and to one of the global minima. This, however, is not possible if μ is too small, which results in the weight taps remaining inside the local minima. The increase of the ϕ value results in a larger rate in which the algorithm achieved a satisfactory MSE since the required value is larger.

The BER was also evaluated and it is shown in Fig. 8 for different values of SNR and μ. It is possible to observe that the step size and the SNR does not impact significantly on the BER performance, whose values do not show a good performance

TABLE I

RATE OF TRIALS THAT CONVERGED TO OPTIMAL SOLUTION IN A 10 dB SNR ENVIRONMENT.

ϕ	$\mu = 0.00100$	$\mu = 0.00010$	$\mu = 0.00001$
0.01	5.65 %	6.00 %	5.85 %
0.05	10.70 %	11.00 %	12.45 %
0.10	14.90 %	15.10 %	17.10 %

TABLE II

RATE OF TRIALS THAT CONVERGED TO OPTIMAL SOLUTION IN A 30 dB SNR ENVIRONMENT.

ϕ	$\mu = 0.00100$	$\mu = 0.00010$	$\mu = 0.00001$
0.01	5.70 %	4.95 %	5.15 %
0.05	10.60 %	9.60 %	10.15 %
0.10	14.60 %	13.10 %	13.75 %

in terms of detection since they range between 0.25 and 0.42. Nevertheless, it is possible to see that the BER decreases as the SNR increases for all values of μ. Although it looks like a large variation, it is, however, very small in terms of BER. It is also interesting to notice that, a higher value of μ results in a smaller BER, which is observed for SNR values above 10 dB. This reinforces the fact that when μ is small, the filter taps were led inside one of the local minima and remained there. When the value of μ is higher, it is possible for the filter taps to overcome the local minimum and to converge to one of the global minima.

Previous simulations were carried out considering channel taps with real values. A more realistic wireless channel model [15] considers its taps as circularly symmetric complex normal random variables with zero mean and variance σ_l^2. This implies in a Rayleigh distribution for the channel magnitude, thus this is called Rayleigh model, and a uniform distribution between 0 and 2π for the channel phase. To assure the same behaviour presented previously is also present for complex taps, simulations were carried out considering both authentic and eavesdropper channels with two taps randomly generated in each trial, with $h_l \sim \mathcal{CN}(0,\sigma_l^2)$ and $g_l \sim \mathcal{CN}(0,\sigma_l^2)$. The variance σ_l^2 is given by the power profile of the channel, defined as

$$\sigma_l^2 = \exp\left\{-\frac{l}{2}\right\}. \tag{9}$$

The results in Tables III and IV show that the number of trials

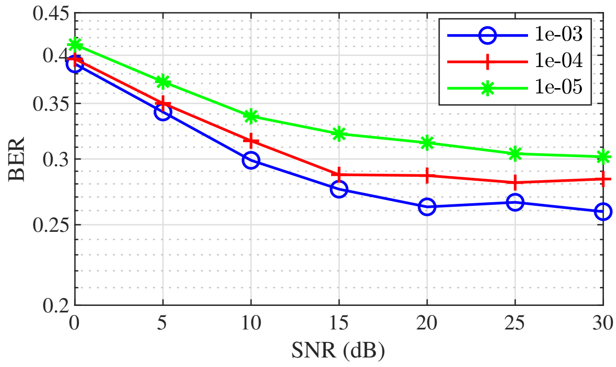

Fig. 8. BER for different SNR values and different adaptation steps μ.

that passes the tests reduced significantly by considering the Rayleigh channel model. This reveals that there is no significant variation in the rate the NLCMA converged to an MSE value below the threshold. For instance, considering $\mu = 0.01$, the rate that the filter converged to an MSE bellow $\phi = 0.01$ is 5.65% for the channel with real taps in a SNR of 10 dB. For Rayleigh Channel, this increased to 6.15%, a difference of 0.5%. It is possible to observe, however, that there is a slight decrease in this rate when the SNR increases, which also happens for the channel with real taps. This happens since the noise is also present in the filter output and, thus, higher noise levels might help the NLCMA to leave local minima and converge to one of the global minima. Therefore, the rate of convergence is slightly higher for lower SNR values.

TABLE III

RATE OF TRIALS THAT CONVERGED TO OPTIMAL SOLUTION FOR RAYLEIGH FADING CHANNELS IN A 10 dB SNR ENVIRONMENT.

ϕ	$\mu = 0.00100$	$\mu = 0.00010$	$\mu = 0.00001$
0.01	6.15 %	6.45 %	6.00 %
0.05	14.25 %	12.35 %	12.20 %
0.10	19.75 %	16.80 %	17.75 %

TABLE IV

RATE OF TRIALS THAT CONVERGED TO OPTIMAL SOLUTION FOR RAYLEIGH FADING CHANNELS IN A 30 dB SNR ENVIRONMENT.

ϕ	$\mu = 0.00100$	$\mu = 0.00010$	$\mu = 0.00001$
0.01	5.90 %	5.25 %	5.20 %
0.05	11.80 %	12.50 %	11.00 %
0.10	15.70 %	16.15 %	16.30 %

The BER values obtained in these simulations are shown in Fig. 9. It is possible to observe again that there is no significant variation in the BER values, which suggests, again, that the performance is degraded less by the SNR values and the adaptation step, than by the initialization. Nonetheless, the behaviour is similar to the one presented in Fig. 8. This further reinforces that, in a practical environment, the THP is still robust against blind equalization in the eavesdropper.

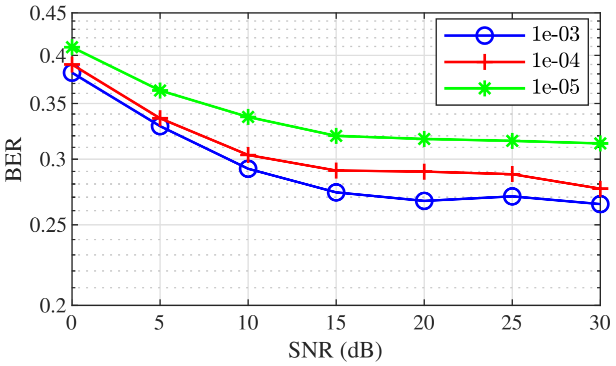

Fig. 9. BER for different SNR values and different adaptation steps μ in a Rayleigh fading channel.

It is important to highlight that the simulations were conducted considering a two-tap authentic channel and a two-tap eavesdropper channel. This number of taps benefits the NLCMA. Would this channels have more taps, as they usually have in an indoor environment [15] for instance, the number of taps necessary for the NLCMA to recover the information increases, since the inversion of the eavesdropper channel by a finite impulse response filter would require a much higher number of taps for it to approximate the channel inverse. This higher complexity level at the receiver is not always possible, which helps the precoder security against the NLCMA.

V. CONCLUSIONS

This work has investigated the use of a non-linear blind equalizer, here named as NLCMA, to overcome the security of the THP at an eavesdropper.

First, tests were conducted through numerical simulations considering real, predefined channels. Although the system can recover part of the information, this is not always possible, and the initialization of the NLCMA algorithm has a significant influence on its performance.

It was also conducted tests considering a more practical channel model. The results have shown that, in this scenario, the THP still provides reliable security against the NLCMA.

REFERENCES

[1] S. Al-Sarawi, M. Anbar, K. Alieyan, and M. Alzubaidi, "Internet of things (IoT) communication protocols: Review," in *2017 8th International Conference on Information Technology (ICIT)*, May 2017, pp. 685–690.

[2] Y. Wu, A. Khisti, C. Xiao, G. Caire, K.-K. Wong, and X. Gao, "A survey of physical layer security techniques for 5g wireless networks and challenges ahead," *IEEE J. Sel. Areas Commun.*, vol. 36, no. 4, pp. 679–695, 2018.

[3] G. Geraci, A. Y. Al-Nahari, J. Yuan, and I. B. Collings, "Linear precoding for broadcast channels with confidential messages under transmit-side channel correlation," *IEEE Commun. Lett.*, vol. 17, no. 6, pp. 1164–1167, Jun. 2013.

[4] S. Ji, W.-q. Wang, H. Chen, and S. Zhang, "On physical-layer security of FDA communications over rayleigh fading channels," *IEEE Trans. on Cogn. Commun. Netw.*, vol. PP, no. c, pp. 1–1, 2019.

[5] S. Atapattu, N. Ross, Y. Jing, and M. Premaratne, "Source-based jamming for physical-layer security on untrusted full-duplex relay," *IEEE Commun. Lett.*, vol. PP, no. c, pp. 1–1, 2019.

[6] Y. Liu and L. Dai, "Improving secrecy via extension to regularized channel inversion precoding," *IEEE Commun. Lett.*, vol. 22, no. 5, pp. 1030–1033, May 2018.

[7] B. He, Y. She, and V. K. N. Lau, "Artificial noise injection for securing single-antenna systems," *IEEE Trans. Veh. Technol.*, vol. 66, no. 10, pp. 9577–9581, Oct. 2017.

[8] H. Koorapaty, A. Hassan, and S. Chennakeshu, "Secure information transmission for mobile radio," *IEEE Commun. Lett.*, vol. 4, Feb. 2000.

[9] P. I. da Cruz, R. Suyama, and M. B. Loiola, "Wireless physical-layer security using precoding and an active eavesdropper," in *XXXV Simpósio Brasileiro de Telecomunicações e Processamento de Sinais*, 2017, pp. 999–1003.

[10] A. Sayed and K. (Firm), *Fundamentals of Adaptive Filtering*, ser. Wiley - IEEE. Wiley, 2003.

[11] O. Shalvi and E. Weinstein, "Super-exponential methods for blind deconvolution," *IEEE Trans. Inf. Theory*, vol. 39, no. 2, pp. 504–519, March 1993.

[12] M. Tomlinson, "New automatic equaliser employing modulo arithmetic," *Electronics Letters*, vol. 7, no. 5-6, p. 138, 1971.

[13] H. Harashima and H. Miyakawa, "Matched-transmission technique for channels with intersymbol interference," *IEEE Trans. Commun.*, vol. 20, no. 4, pp. 774–780, Aug. 1972.

[14] R. Adnan and M. G. Lee, "Blind equalization bounds for Tomlinson-Harashima precoded systems," in *2006 IEEE International Conference on Communications*, vol. 7, Jun. 2006, pp. 3310–3316.

[15] M. C. Jeruchim, P. Balaban, and K. S. Shanmugan, Eds., *Simulation of Communication Systems: Modeling, Methodology and Techniques*, 2nd ed. Norwell, MA, USA: Kluwer Academic Publishers, 2000.